



**Cisco** *live!*

July 10-14, 2016 • Las Vegas, NV

Your Time Is Now



# Advanced Troubleshooting of Wireless LANs

Tim Smith, Wireless TAC Technical Lead

BRKEWN-3011



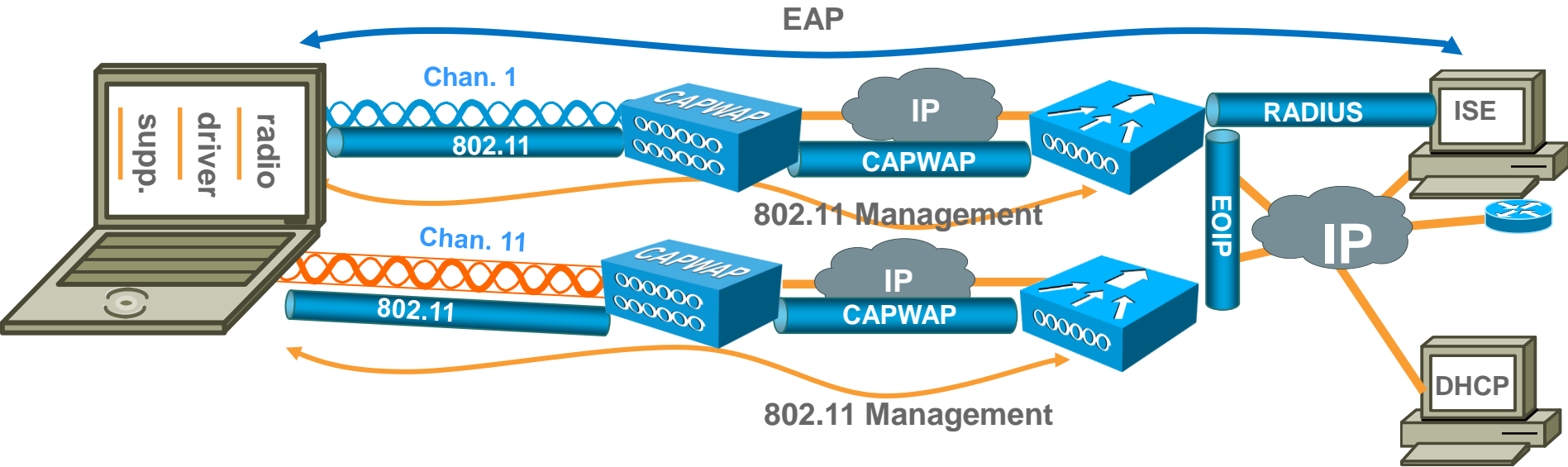
# Agenda

- Where do we start?
- Understand the Client State
- Client Troubleshooting
- AP Join Troubleshooting
- The AP Show Controller
- Mobility
- Tools of the Trade
- Key Takeaways to Remember
- Questions?

# Where do we start?

# Where do we start?

Client can't connect....

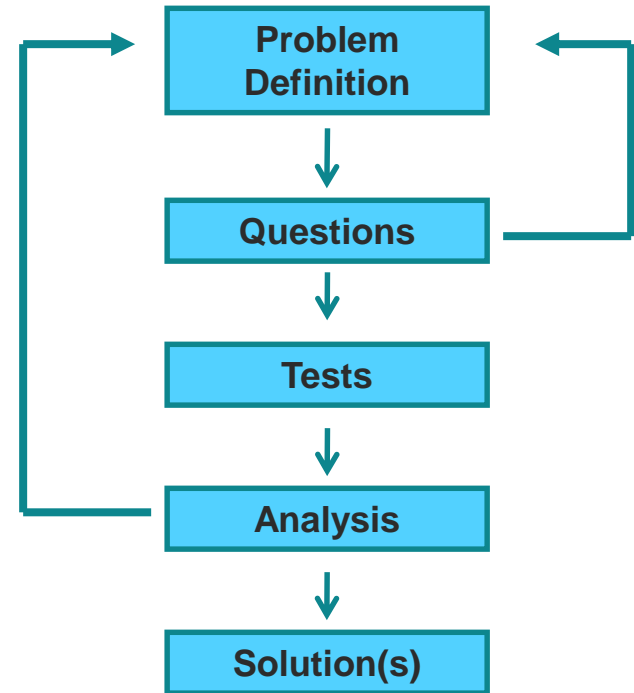




# Where do we Start – What is Troubleshooting?

## Troubleshooting 101

- Clearly define the problem
- Understand any possible triggers
- Know the expected behavior
- Reproducibility
- **Do not jump to conclusions**



# Understanding the Client State

# What's a Client State?

- Lets us know where in the process the client is currently at.
- Key item to know for effective troubleshooting, needed to narrow your problem scope!
- The Controller keeps Client state for all connected clients.
- Some items handle on the AP only (Probes, Open Authentication), mainly done for efficiency.

**Application Slowness?**

**No IP Address?**

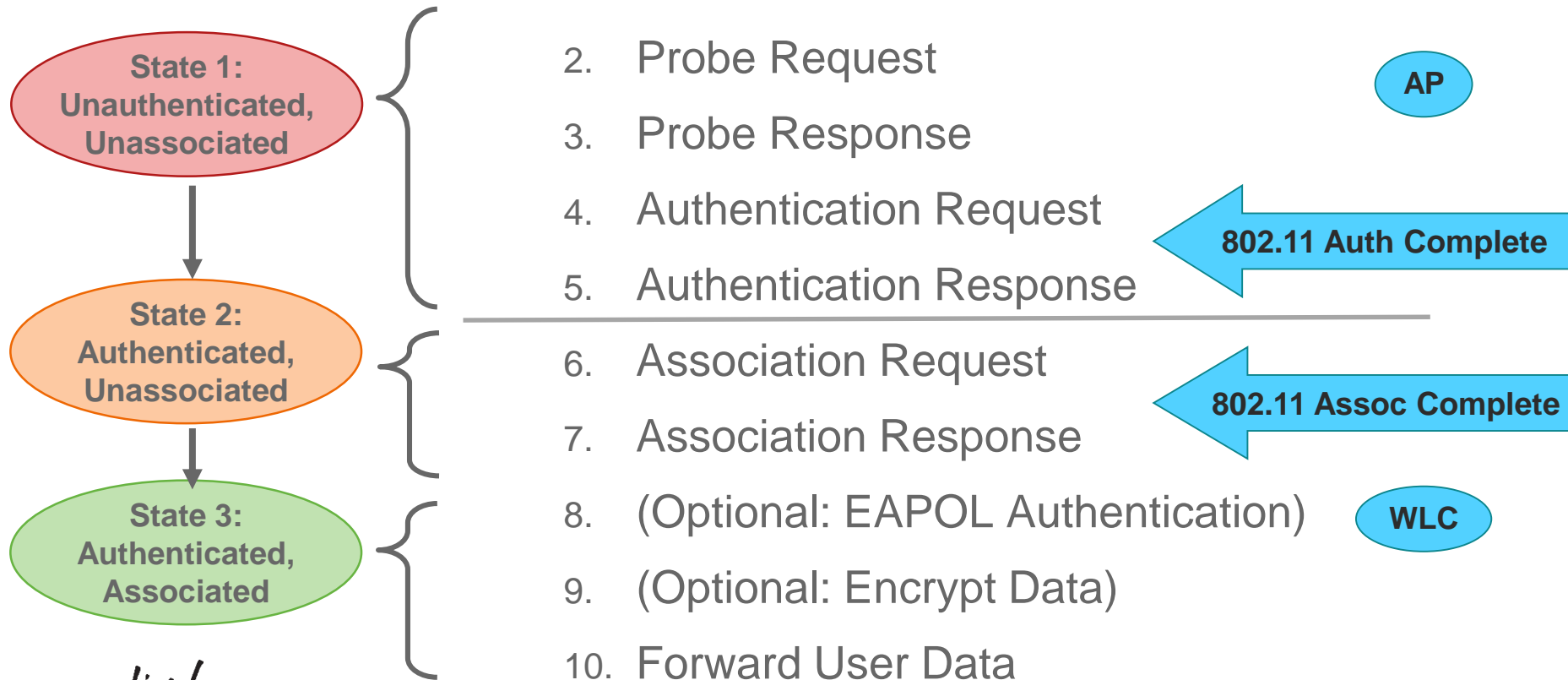
**Authentication Failed?**

**Can't See the SSID?**

**RF Health?**

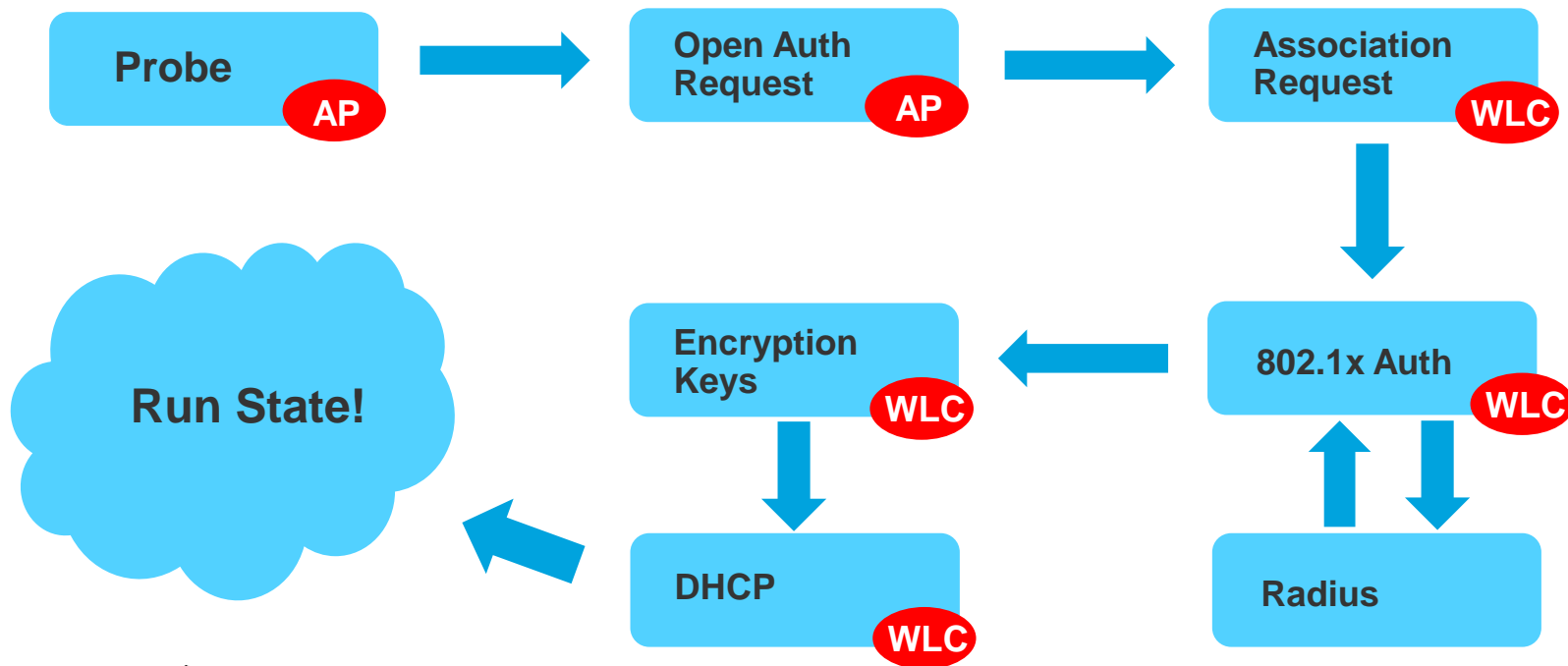


# The 802.11 Connection Process



# The 802.11 Connection Process

- All 802.11 Clients will follow roughly the same path from initial Probing (if needed) to the final RUN state



# Client State == Policy Manager State

Name	Description
8021X_REQD	802.1x (L2) Authentication Pending
DHCP_REQD	IP Learning State
WEBAUTH_REQD	Web (L3) Authentication Pending
RUN	Client Traffic Forwarding



The image shows the Cisco Monitor Clients interface. On the left is a navigation menu with 'Monitor' selected, containing links for Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, and Clients. The main area is titled 'Clients' and shows a 'Current Filter' section with a link for 'Client MAC Addr' and the value '00:16:ea:b2:04:36'.

## Client Properties

MAC Address 00:16:ea:b2:04:36  
IP Address 10.10.3.199

Policy Manager State RUN

(Cisco Controller) >show client detail 00:16:ea:b2:04:36  
Client MAC Address..... 00:16:ea:b2:04:36

.....  
Policy Manager State..... WEBAUTH\_REQD

00:16:ea:b2:04:36 10.10.1.103 DHCP\_REQD (7) Change state to **RUN (20)** last state RUN (20)



# Policy Enforcement Module

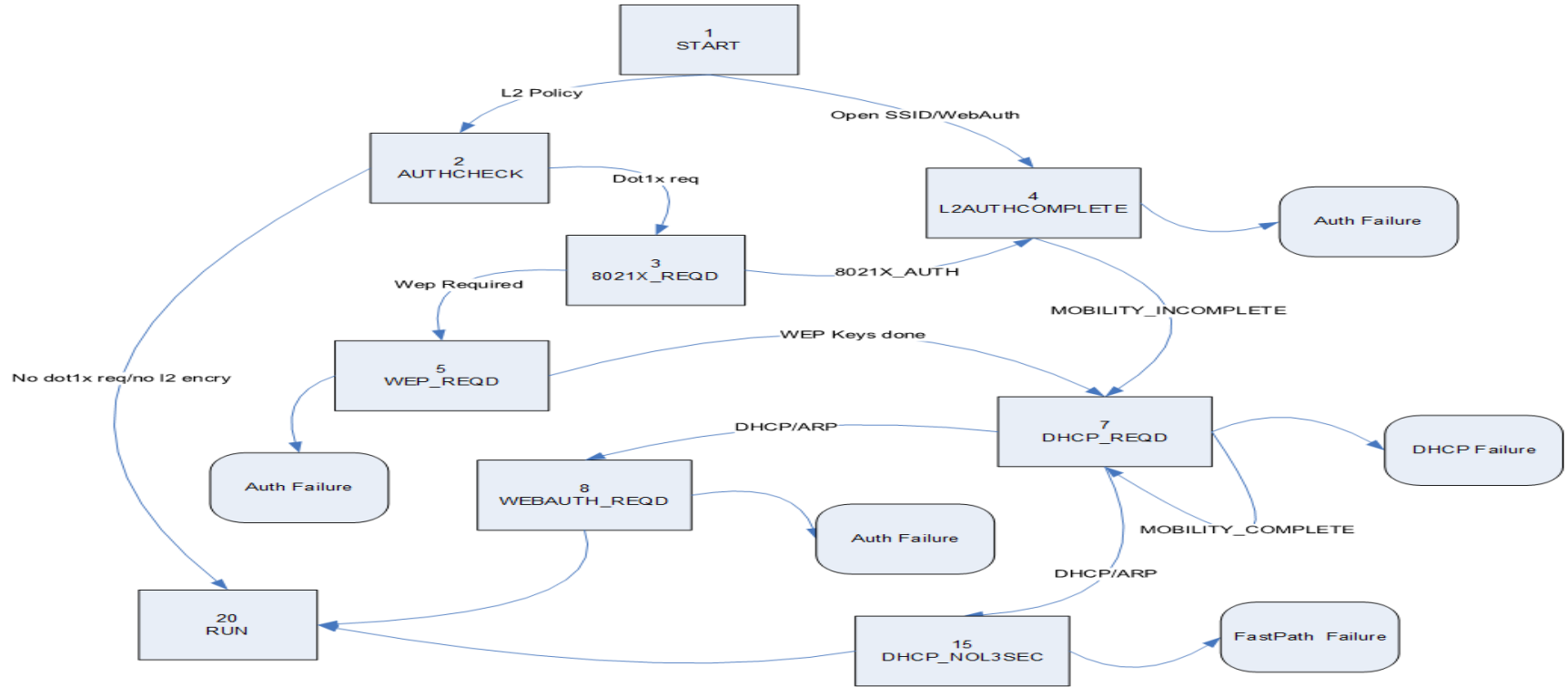


Based on the WLAN configuration, the client passes through a series of steps. PEM ensures this is done in order for it to comply with the required L2 and L3 security policies.

Here is a subset of the PEM states relevant for the analysis of a client debug:

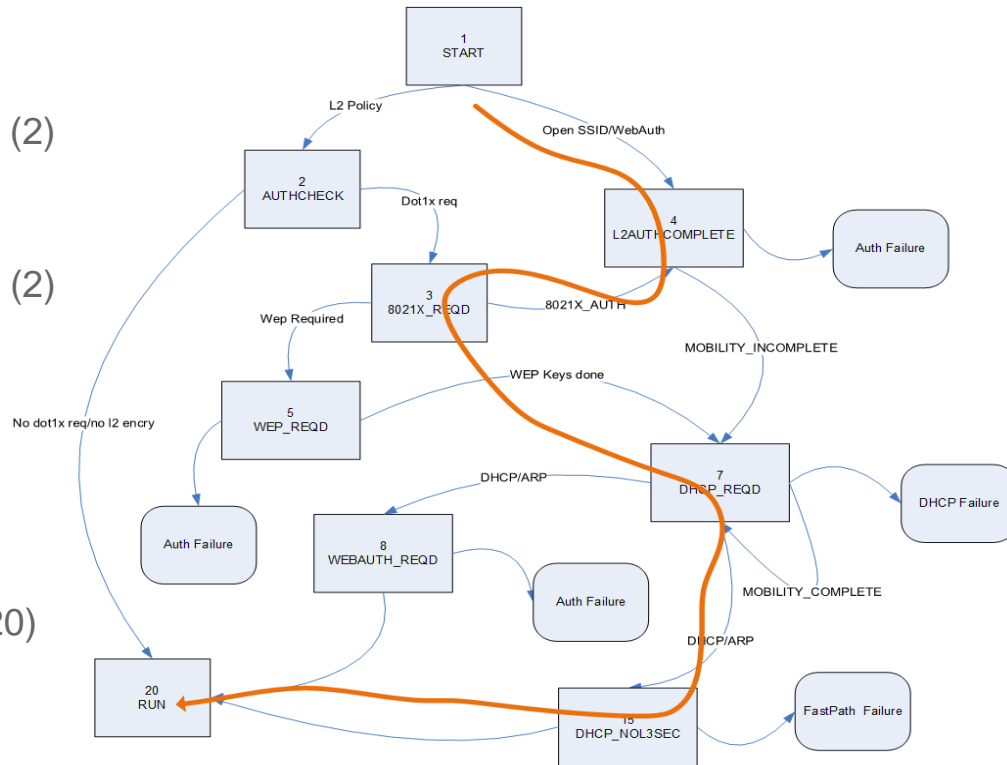
- **START**—Initial status for new client entry.
- **AUTHCHECK**—WLAN has an L2 authentication policy to enforce.
- **8021X\_REQD**—Client must complete 802.1x authentication.
- **L2AUTHCOMPLETE**—Client has successfully finished the L2 policy. The process can now proceed to L3 policies (address learning, Web auth, etc). Controller sends here 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 needs to learn the L3 address from client, which is done either by ARP request, DHCP request or renew, or by information learned from other controller 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)
- **RUN**—Client has successfully completed the required L2 and L3 policies and can now transmit traffic to the network.

# The Client State Flow Chart



# Navigating the Client State – An Example

- START (0) Change state to AUTHCHECK (2) last state START (0)
- AUTHCHECK (2) Change state to 8021X\_REQD (3) last state AUTHCHECK (2)
- 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3)
- DHCP\_REQD (7) last state L2AUTHCOMPLETE (4)
- DHCP\_REQD (7) Change state to RUN (20) last state DHCP\_REQD (7)





# Client Troubleshooting

# Always the First Step - Determine What's Failing

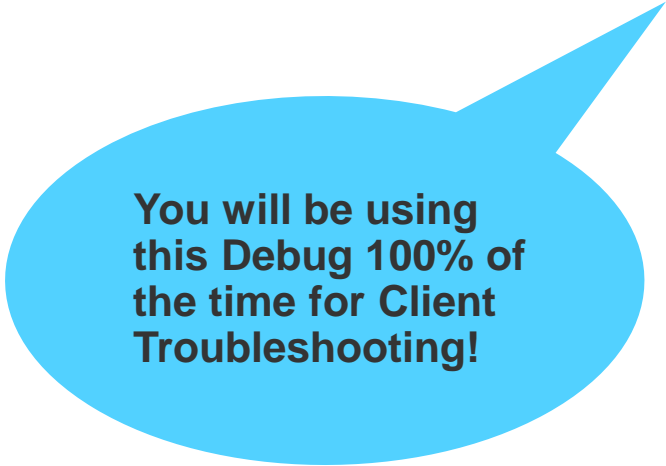
1. Get the facts on what's happening
  - Many conditions can lead to the same outcome
2. Get as much Client Details as possible
  - Type of OS, Wireless card, Driver version
3. Try to determine location of Client
  - Needed to narrow down AP location, AP load, RF Conditions, Time of Day issue is occurring
4. Check Client State on the Controller to pinpoint possible cause of failure.

# The Client Debug – Its your Friend!

A multi-debug macro that covers over all the main client states

(Cisco Controller) > **debug client 00:16:EA:B2:04:36**

- Up to 10 MAC addresses can be used



**You will be using  
this Debug 100% of  
the time for Client  
Troubleshooting!**

(Cisco Controller) > show debug

**MAC address ..... 00:16:EA:B2:04:36**

Debug Flags Enabled:

**dhcp packet enabled.**

**dot11 mobile enabled.**

**dot11 state enabled.**

**dot1x events enabled.**

**dot1x states enabled.**

**pem events enabled.**

**pem state enabled.**



# Client Debugs - Examples on WLC

`debug client <MAC Address>`

`debug aaa events/errors enable`

**Used for Radius  
Authentications**

`debug dot1x all enable`

`debug web-auth redirect enable mac <client mac address>`

**Used for Web  
Authentication**

`debug mdns all enable`

**Used for Apple Bonjour**

# Client Debugs - Examples on the AP

`debug dot11 <do0/do1> monitor addr <client mac address>`

**Used to filter  
your MAC Addr**

`debug dot11 <d0/d1> trace print client mgmt keys rxev txev rcv xmt`

`debug dot11 wpa-cckm-km-dot1x`

`debug dot11 events`

**Used to track  
IEEE dot11 states**

`debug capwap client mgmt`

**Used to track client  
dot11 states to WLC**

**Low Level  
Radio Driver  
Debug, use  
to view  
what's  
received  
and  
transmitted**

# Got a Client, but no Debug logs...

- Hey, I have a client trying to connect, but nothing is showing up!
- After 7.0: Client probing activity is aggregated, will not show up in the logs
- Deb client will not show anything for “just probing” client

>debug dot11 probe event enable

>\*apfProbeThread: Jan 03 07:59:30.738: Received aggregated probe, dataLen = 127

\*apfProbeThread: Jan 03 07:59:30.738: 00:1a:70:35:84:d6 probing client, ver=1, slot=0, wlan=0, snr=23, tx\_pwr=0, chan=11, reg\_class=0, ts\_diff=346ms, seq\_num=12303, ant\_cnt=2, rssi[0]=214, rssi[1]=205

- Typical reasons:
  - Misconfigured SSID/security settings
  - IE on response not handled properly by client

**Be careful, can generate a lot of output!**



# Client not Seeing the SSID?

- Is the WLAN enabled to Broadcast the SSID?
- Check to see if the WLAN is enable, if using AP Groups, make sure the WLAN is added to the AP Group for the Client location

Ap Groups > Edit 'timsmith'

General WLANs RF Profile AP 802.11u Location Ports/Module

WLAN ID	WLAN SSID(2/6)	Interface/Interface Group(G)	SNMP NAC State
2	CCKM	management	Disabled
3	Bonjour	management	Disabled
4	80211w-WLC	management	Disabled

WLANs > Edit 'wlc2504-timsmith-wlan1'

General Security QoS Policy-Mapping Advanced

Profile Name wlc2504-timsmith-wlan1

Type WLAN

SSID wlc2504-timsmith-wlan1

Status ☒ Enabled

Security Policies [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) vlan-250

Multicast vlan feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS ID none

# Client Flow

The Route Toward the RUN State:



# Client Debug: Association Example

\*apfMsConnTask\_4: Dec 16 11:30:42.058: 00:1c:58:8e:a5:84 Association received from mobile on BSSID 00:3a:9a:a8:ac:d2..

Applying Local Bridging Interface Policy for station 00:1c:58:8e:a5:84 - vlan 50, interface id 14, interface 'vlan50'  
processSsidIE statusCode is 0 and status is 0

processSsidIE ssid\_done\_flag is 0 finish\_flag is 0

STA - rates (8): 130 132 139 12 18 150 24 36 0 0 0 0 0 0 0

suppRates statusCode is 0 and gotSuppRatesElement is 1

STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0

extSuppRates statusCode is 0 and gotExtSuppRatesElement is 0.0.0.0 START (0) Change state to AUTHCHECK (2)  
last state START (0)

0.0.0.0 AUTHCHECK (2) Change state to 8021X\_REQD (3) last state AUTHCHECK (2)

\*apfMsConnTask\_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 apfPemAddUser2 (apf\_policy.c:333) Changing state for mobile 00:1c:58:8e:a5:84 on AP 00:3a:9a:a8:ac:d0 from Idle to Associate

\*apfMsConnTask\_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 Sending Assoc Response to station on BSSID 00:3a:9a:a8:ac:d2 (status 0) ApVapId 3 Slot 0

Status 0 == Good

# Client Debug: Roaming Example

\*apfMsConnTask\_1: Dec 16 14:42:18.472: 00:1e:be:25:d6:ec **Reassociation received from mobile on BSSID f8:4f:57:a1:d8:a2**

..

\*apfMsConnTask\_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec Applying Local Bridging Interface Policy for station 00:1e:be:25:d6:ec - vlan 50, interface id 14, interface 'vlan50'

processSsidIE statusCode is 0 and status is 0

processSsidIE ssid\_done\_flag is 0 finish\_flag is 0

STA - rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0

suppRates statusCode is 0 and gotSuppRatesElement is 1

STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0

extSuppRates statusCode is 0 and gotExtSuppRatesElement is 1

\*apfMsConnTask\_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec 192.168.50.100 RUN (20) **Deleted mobile LWAPP rule on AP [04:da:d2:28:94:c0]**

\*apfMsConnTask\_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec **Updated location for station old AP 04:da:d2:28:94:c0-0, new AP f8:4f:57:a1:d8:a0-0**



**Re-association  
was Received**



# Client Association Failure – What to Check

- Check to see if you have some type of MAC Filter enabled
- Check to see if the Client has been Black Listed
  - Too many Association failures
  - Too many 802.1x authentication failures
- Do you have Fast SSID Change enabled?
  - If not, then there is a hold down timer for the client when switching WLAN's
- Has the Client been added to the Manual Exclusion list?

# Client Debug: Association Failed Example

\*apfMsConnTask\_0: Oct 11 15:11:33.604: **cc:52:af:fc:89:26 Association received from mobile on AP 00:17:0e:aa:46:30**  
0.0.0.0 START (0) Changing ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf\_policy.c:1626)  
STA - rates (7): 22 24 36 48 72 96 108 0 0 0 0 0 0 0  
Processing RSN IE type 48, length 20 for mobile cc:52:af:fc:89:26  
Received RSN IE with 0 PMKIDs from mobile cc:52:af:fc:89:26

\*apfMsConnTask\_0: Oct 11 15:11:33.604: cc:52:af:fc:89:26 apfProcessAssocReq (apf\_80211.c:5118) Changing state for  
mobile cc:52:af:fc:89:26 on AP 00:17:0e:aa:46:30 from Authenticated to AAA Pending

\*apfMsConnTask\_0: Oct 11 15:11:33.604: **cc:52:af:fc:89:26 Scheduling deletion of Mobile Station:** (callerId: 20) in 10  
seconds

\*radiusTransportThread: Oct 11 15:11:33.610: **cc:52:af:fc:89:26 Access-Reject received from RADIUS server**  
10.100.76.10 for mobile cc:52:af:fc:89:26 receiveId = 0


\*radiusTransportThread: Oct 11 15:11:33.611: **cc:52:af:fc:89:26 Returning AAA Error 'Authentication Failed' (-4) for**  
mobile

\*apfReceiveTask: Oct 11 15:11:33.611: cc:52:af:fc:89:26 Sending Assoc Response to station on BSSID  
00:17:0e:aa:46:30 (**status 1**) ApVapId 4 Slot 0

**Status 1 == Bad**

# Client Debug: Association Failed due to Blacklisted

\*apfMsConnTask\_0: Dec 16 15:29:40.487: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion  
00:40:96:b5:db:d7 \*apfMsConnTask\_0: Dec 16 15:29:41.494: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion  
\*apfMsConnTask\_0: Dec 16 15:29:42.499: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion  
\*apfMsConnTask\_0: Dec 16 15:29:43.505: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion



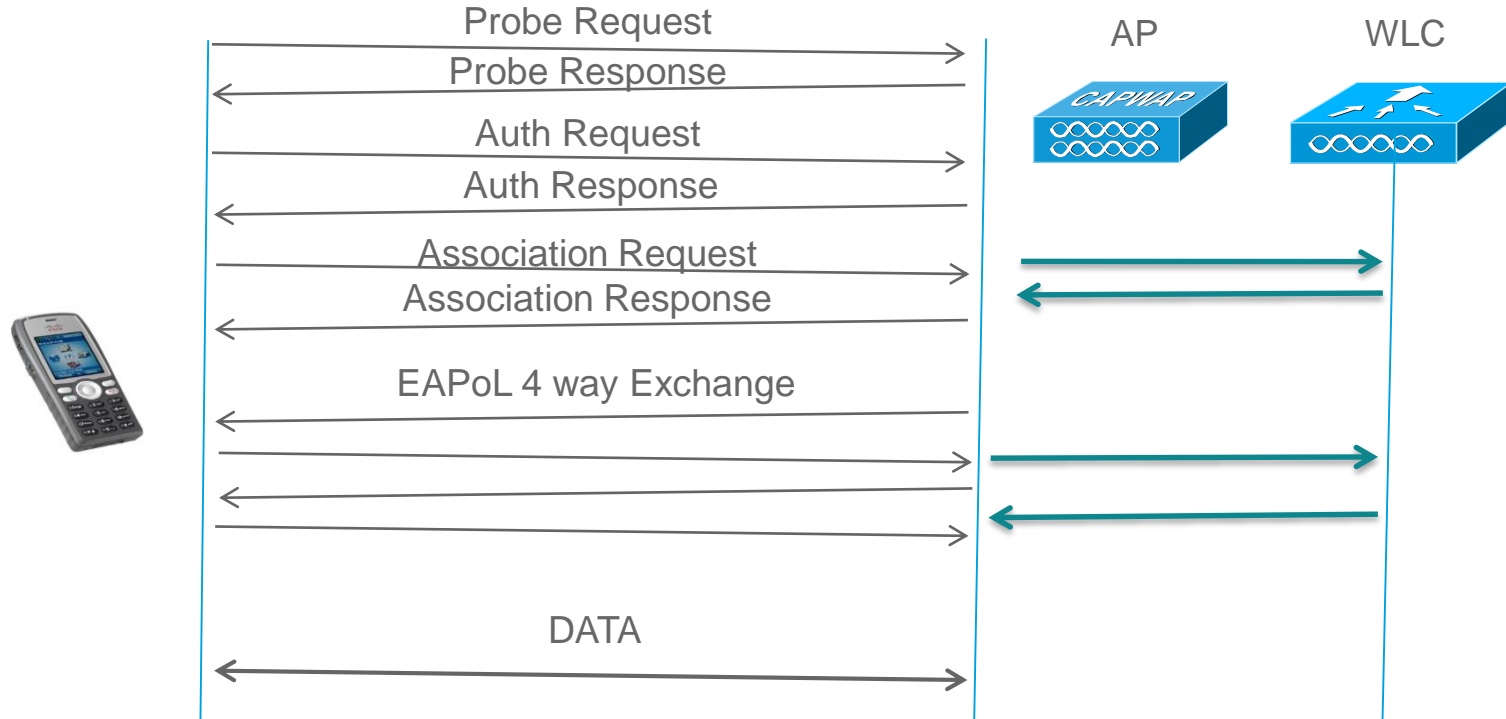
**We are Ignoring  
your Requests,  
you've been  
excluded!**

# Client Flow

## The Route Toward the RUN State:



# PSK authentication





# Client Debug: PSK – Successful Example

\*apfMsConnTask\_1: Dec 16 15:30:14.920: 00:40:96:b5:db:d7 **Association received from mobile** on BSSID f8:4f:57:a1:d8:aa

\*apfMsConnTask\_1: Dec 16 15:30:14.921: 00:40:96:b5:db:d7 **Sending Assoc Response to station** on BSSID f8:4f:57:a1:d8:aa (status 0)

\*spamApTask3: Dec 16 15:30:14.923: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 Initiating RSN PSK to mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 **dot1x - moving mobile 00:40:96:b5:db:d7 into Force Auth state**

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 **Starting key exchange to mobile 00:40:96:b5:db:d7, data packets will be dropped**

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 **Sending EAPOL-Key Message** to mobile 00:40:96:b5:db:d7 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 **Received EAPOL-Key from mobile 00:40:96:b5:db:d7**

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Received EAPOL-key in PTK\_START state (**message 2**) from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 **Sending EAPOL-Key Message to mobile 00:40:96:b5:db:d7** state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.01

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 **Received EAPOL-Key** from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Received EAPOL-key in PTKINITNEGOTIATING state (**message 4**) from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 0.0.0.0 8021X\_REQD (3) Change state to **L2AUTHCOMPLETE (4)** last state 8021X\_REQD (3)

**PSK Key passed, Layer 2  
Auth done**

# Client Debug: PSK – Wrong secret Example

\*apfMsConnTask\_1: Dec 16 15:25:28.923: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa

\*apfMsConnTask\_1: Dec 16 15:25:28.925: 00:40:96:b5:db:d7 **Sending Assoc Response** to station on BSSID f8:4f:57:a1:d8:aa (status 0) ApVapId 6 Slot 1

\*spamApTask3: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 **Starting key exchange to mobile** 00:40:96:b5:db:d7, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7

config clid\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Ignoring invalid EAPOL version (1) in EAPOL-key message

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-key in PTK\_START state (message 2) from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 **Received EAPOL-key M2 with invalid MIC from mobile**

\*osapiBsnTimer: Dec 16 15:25:30.019: 00:40:96:b5:db:d7 **802.1x 'timeoutEvt' Timer expired** for station 00:40:96:b5:db:d7 and for message = M2

\*dot1xMsgTask: Dec 16 15:25:32.019: 00:40:96:b5:db:d7 **Retransmit failure for EAPOL-Key M1 to mobile** 00:40:96:b5:db:d7, retransmit count 3, mscb deauth count 2

\*dot1xMsgTask: Dec 16 15:25:32.020: 00:40:96:b5:db:d7 **Sent Deauthenticate to mobile** on BSSID f8:4f:57:a1:d8:a0 slot 1(caller 1x\_ptsm.c:570)

\*dot1xMsgTask: Dec 16 15:25:32.020: 00:40:96:b5:db:d7 **Scheduling deletion of Mobile Station:** (callerId: 57) in 10 seconds

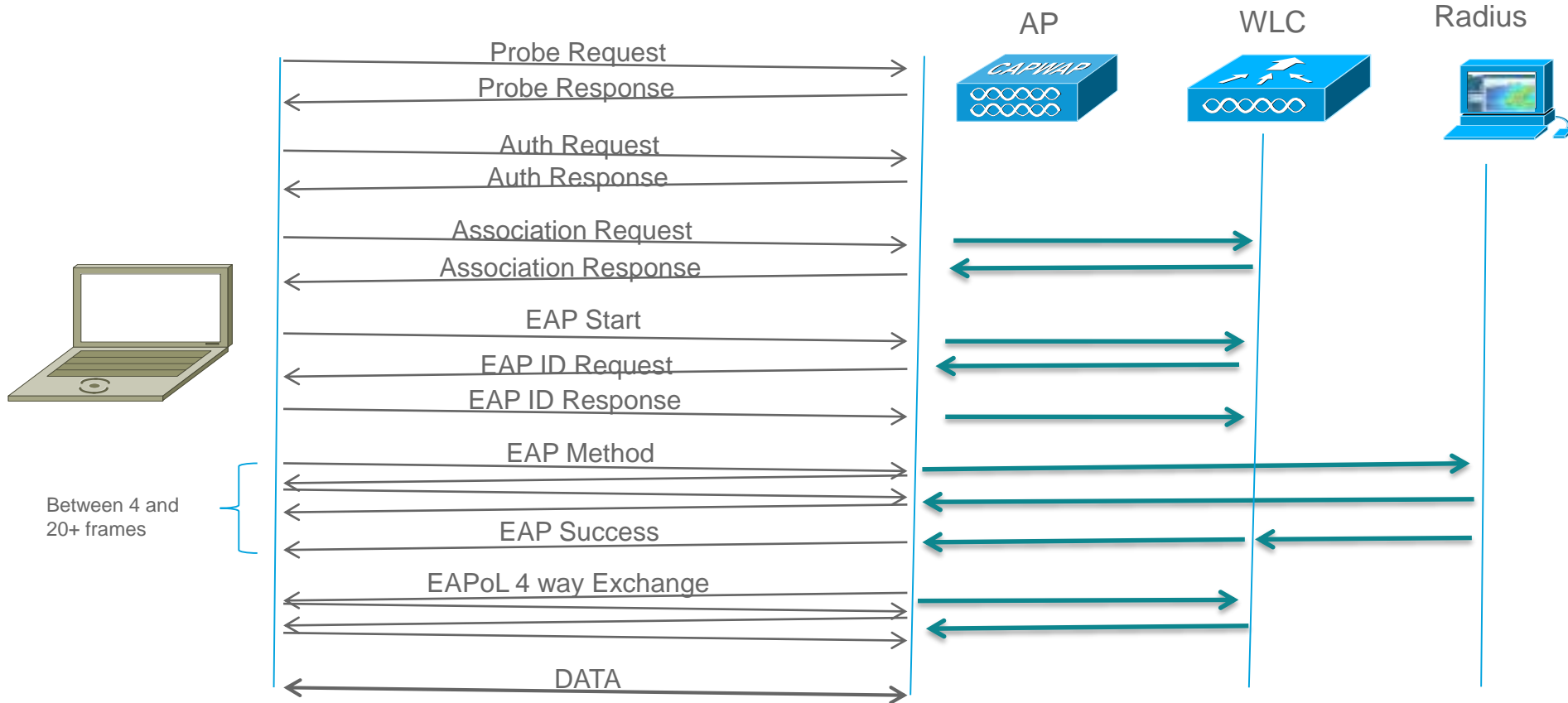
**PSK Key is wrong on Client so we Fail EAPOL-Key M2**

# Client Debug: PSK – Wrong secret - excluded

\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd Blacklisting (if enabled) mobile 68:7f:74:75:f1:cd  
\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd apfBlacklistMobileStationEntry2 (apf\_ms.c:5850) Changing state for mobile 68:7f:74:75:f1:cd on AP 04:da:d2:4f:f0:50 from **Associated to Exclusion-list (1)**  
  
\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd **Scheduling deletion of Mobile Station: (callerId: 44) in 10 seconds**  
\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd 0.0.0.0 8021X\_REQD (3) Change state to START (0) last state 8021X\_REQD (3)  
  
\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd 0.0.0.0 START (0) **Reached FAILURE:** from line 5274  
\*dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd **Scheduling deletion of Mobile Station: (callerId: 9) in 10 seconds**

If Client Exclusion is enabled, and we Fail PSK, the client will get moved to the exclusion list for 60 (default)

# 802.1X Authentication



# Client Debug: 802.1x - Successful

\*apfMsConnTask\_0: Dec 16 15:36:07.557: 00:40:96:b5:db:d7 **Sending Assoc Response** to station on BSSID 04:da:d2:28:94:ce (status 0) ApVapId 2 Slot 1

Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.559: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.560: 00:40:96:b5:db:d7 **Sending EAP-Request/Identity** to mobile 00:40:96:b5:db:d7 (EAP Id 1)

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.566: 00:40:96:b5:db:d7 **Received EAPOL START** from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.566: 00:40:96:b5:db:d7 **Sending EAP-Request/Identity to mobile** 00:40:96:b5:db:d7 (EAP Id 2)

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 **Received Identity Response** (count=2) from mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 EAP State update from Connecting to Authenticating for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Authenticating state

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 **Entering Backend Auth Response state for mobile** 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 **Processing Access-Challenge for mobile** 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Entering Backend Auth Req state (id=220) for mobile 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 WARNING: updated EAP-Identifier 2 ==> 220 for STA 00:40:96:b5:db:d7

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 **Sending EAP Request from AAA** to mobile 00:40:96:b5:db:d7 (EAP Id 220)



# Client Debug: 802.1x – Successful (continued..)

\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.575: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.575: 00:40:96:b5:db:d7 **Received EAP Response from mobile** 00:40:96:b5:db:d7 (EAP Id 220, EAP Type 3)  
..  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.718: 00:40:96:b5:db:d7 **Entering Backend Auth Response state** for mobile 00:40:96:b5:db:d7  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 **Processing Access-Accept** for mobile 00:40:96:b5:db:d7  
  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 **Username entry (cisco) created in mscb** for mobile, length = 253  
  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 **Setting re-auth timeout to 1800 seconds, got from WLAN config.**  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Station 00:40:96:b5:db:d7 setting dot1x reauth timeout = 1800  
  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 **Creating a PKC PMKID Cache entry for station** 00:40:96:b5:db:d7 (RSN 2)  
\*Dot1x\_NW\_MsgTask\_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 **Sending EAP-Success to mobile** 00:40:96:b5:db:d7 (EAP Id 228)

**Radius has Passed the  
Client Authentication  
Request**

# Layer 2 Authentication (as seen on AP)

## AP Radio Debugs

```
*Jan 15 02:50:07.804: A6504097 r 1 3 - B008 2800 2FB698 6F9E11 6F9E11 CFC0 auth | 6
*Jan 15 02:50:07.807: A6504BC0 t 1 69/67 14- B008 13A 6F9E11 2FB698 6F9E11 65C0 auth | 6
*Jan 15 02:50:07.809: A6505313 r 1 69/67 19- 0000 13A 6F9E11 2FB698 6F9E11 65D0 assreq | 139
*Jan 15 02:50:07.827: A6509A92 t 1 2 - 1008 000 2FB698 6F9E11 6F9E11 CFE0 assrsp | 151
*Jan 15 02:50:07.829: A650A056 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0290 q7 l87
EAPOL3 EAP id 93 req ident 0 "networkid=peapradius,nasid=SURBG-5508,portid=0"
*Jan 15 02:50:07.879: A6516524 r 1 68/67 19- 8801 13A 6F9E11 2FB698 6F9E11 0010 q7 l22
EAP id 93 resp ident "surbg"
```

Rest of the EAP Transaction

```
*Jan 15 02:50:08.247: A6570622 t 1 0 - 8802 000 2FB698 6F9E11 6F9E11 0330 q7 l54
EAPOL3 EAP id 93 success
```

**AP debugs are much more cryptic, but you will need to look for EAP Success key words in the flow**

# 802.1x Client Connection - Example

## Client Connection -> client info + debug client

```
(5500-1) > show client detail 00:1a:70:35:84:d6
```

```
Client MAC Address..... 00:1a:70:35:84:d6
```

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

```
AP MAC Address..... 84:78:ac:8c:7e:c0
```

```
AP Name..... a1-ap3600-sw2-11
```

```
AP radio slot Id..... 0
```

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

```
BSSID..... 84:78:ac:8c:7e:c0
```

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

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

# Debug Client: 802.1x Client Connection Failure

## Output taken from a Debug client and Debug AAA events

\*apfMsConnTask\_2: Jan 10 07:56:55.936: 00:1a:70:35:84:d6 **Association received from mobile on BSSID 84:78:ac:8c:7e:c0**

\*apfMsConnTask\_2: Jan 10 07:56:55.936: 00:1a:70:35:84:d6 Received RSN IE with 0 PMKIDs from mobile 00:1a:70:35:84:d6

\*apfMsConnTask\_2: Jan 10 07:56:55.937: 00:1a:70:35:84:d6 **Sending Assoc Response to station on BSSID 84:78:ac:8c:7e:c0 (status 0)** ApVapId 1 Slot 0

\*Dot1x\_NW\_MsgTask\_6: Jan 10 07:56:55.939: 00:1a:70:35:84:d6 Sending EAP-Request/Identity to mobile 00:1a:70:35:84:d6 (EAP Id 1)

\*Dot1x\_NW\_MsgTask\_6: Jan 10 07:56:59.233: 00:1a:70:35:84:d6 Received EAPOL START from mobile 00:1a:70:35:84:d6

\*Dot1x\_NW\_MsgTask\_6: Jan 10 07:56:59.233: 00:1a:70:35:84:d6 Sending EAP-Request/Identity to mobile 00:1a:70:35:84:d6 (EAP Id 2)

\*Dot1x\_NW\_MsgTask\_6: Jan 10 07:57:10.979: 00:1a:70:35:84:d6 **Received Identity Response (count=2) from mobile 00:1a:70:35:84:d6**

# Client Debug: 802.1x Client Connection Failure

```
*aaaQueueReader: Jan 10 07:57:10.980: RADIUS Msg Queue: actual count 0, count 0 (OK), ordering OK (caller radius_db.c:676)
```

```
*aaaQueueReader: Jan 10 07:57:10.980: RADIUS Msg Queue: actual count 1, count 1 (OK), ordering OK (caller radius_db.c:659)
```

```
*radiusTransportThread: Jan 10 07:57:11.004: ****Enter processIncomingMessages: response code=11
```

```
..
```

```
*radiusTransportThread: Jan 10 07:57:11.018: ****Enter processIncomingMessages: response code=3
```

```
*radiusTransportThread: Jan 10 07:57:11.018: ****Enter processRadiusResponse: response code=3
```

```
*radiusTransportThread: Jan 10 07:57:11.019: 00:1a:70:35:84:d6 Returning AAA Error 'Authentication Failed' (-4) for mobile 00:1a:70:35:84:d6
```

**Look for  
keywords like  
Success or Fail**



# 802.1x Client Connection Failure

Lets look in the ACS Logs...

```
01/10/2014,08:48:11,Authen failed,john,Default Group,00-1a-70-35-84-  
d6,(Default),ACS user unknown,,,1,192.168.15.51,,,17,LEAP,,talwar1,
```

```
01/10/2014,08:48:24,Authen failed,john,Default Group,00-1a-70-35-84-  
d6,(Default),ACS user unknown,,,1,192.168.15.51,,,17,LEAP,,talwar1,
```

```
01/10/2014,08:48:32,Authen failed,john,Default Group,00-1a-70-35-84-  
d6,(Default),ACS user unknown,,,1,192.168.15.51,,,17,LEAP,,talwar1,
```

# 802.1x Failure – What to Check

- Enable Client debugs to see if the Radius Server is rejecting the Client
- Check the Monitor->Stats->Radius Servers to make sure your Radius Server is responding!
- Are we passing 802.1x but failing on WPA Keying? The Client Debugs will help us there!!
- Check to see if the Client has been Black Listed
- For very large scale 802.1x deployment, check your controller message queues to make sure you are not exceeding the MAX number of outstanding Radius requests (show radius queue summary)

# Client Flow

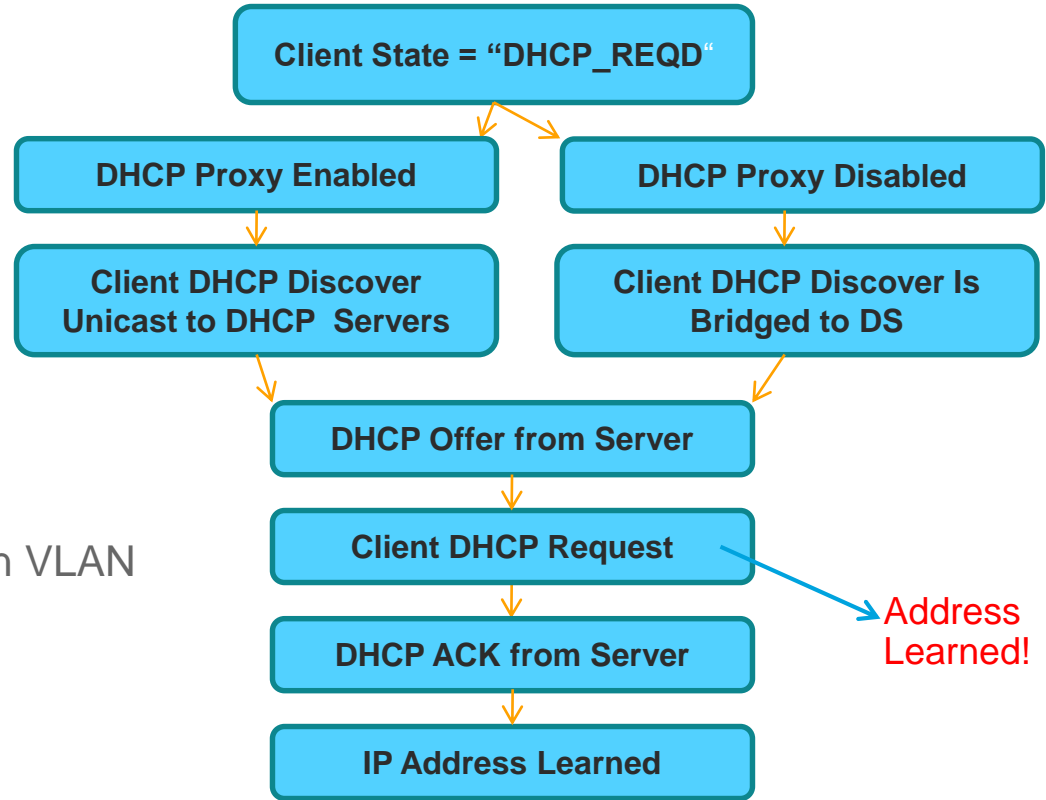
The Route Toward the RUN State:



# Client DHCP

Client is in DHCP\_REQD state

- **Proxy Enabled:**  
DHCP Relay/Proxy  
Between WLC and Server  
Required for Internal DHCP
- **Proxy Disabled:**  
Between Client and Server  
DHCP is forwarded as a broadcast on VLAN  
IP helper or other means required



# Client Debug: Client DHCP

\*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP\_REQD (7) **State Update from Mobility-Incomplete to Mobility-Complete**, mobility role=Local, **client state=APF\_MS\_STATE\_ASSOCIATED**

\*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 **DHCP\_REQD** (7) pemAdvanceState2 5752, Adding TMP rule

\*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP\_REQD (7) Adding Fast Path rule

type = Airespace AP - **Learn IP address**

on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0

IPv4 ACL ID = 255, IPv

**We are now in IP Learn State**

\*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP\_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 **Local Bridging Vlan = 50**, Local Bridging intf id = 12

\*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP\_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)

\*pemReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 **Added NPU entry of type 9, dtlFlags 0x0**

**We are Bridging the  
DHCP Request on Vlan 50**

# Client DHCP – Process Start

DHCP received op BOOTREQUEST (1) (len 308,vlan 5, port 1, encap 0xec03)  
DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:ff:ff

DHCP **selected relay 1** - 192.168.50.1 (local address 192.168.50.15, gateway 192.168.50.1, VLAN 50, port 1)

DHCP transmitting **DHCP DISCOVER (1)**

DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

DHCP **xid: 0xa504e3** (10814691), secs: 0, flags: 0

DHCP **chaddr: 68:7f:74:75:f1:cd**

DHCP **ciaddr: 0.0.0.0**, yiaddr: 0.0.0.0

DHCP siaddr: 0.0.0.0, **giaddr: 192.168.50.15**

DHCP sending REQUEST to 192.168.50.1 (len 350, port 1, vlan 50)



**DHCP Proxy  
is Enable!**



# Client DHCP – Offer

DHCP received op BOOTREPLY (2) (len 308,vlan 50, port 1, encap 0xec00)  
DHCP setting server from **OFFER** (server 192.168.0.21, yiaddr 192.168.50.101)  
DHCP **sending REPLY to STA** (len 418, port 1, vlan 5)  
DHCP transmitting DHCP OFFER (2)  
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0  
DHCP **xid: 0xa504e3** (10814691), secs: 0, flags: 0  
DHCP **chaddr: 68:7f:74:75:f1:cd**  
DHCP ciaddr: 0.0.0.0, **yiaddr: 192.168.50.101**  
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0  
DHCP **server id: 1.1.1.1 rcvd server id: 192.168.0.21**  
DHCP received op BOOTREQUEST (1) (len 335,vlan 5, port 1, encap 0xec03)  
DHCP (encap type 0xec03) mstype 0xff:ff:ff:ff:ff:ff

**Notice how both the  
Virtual IP address and  
Actual DHCP Server seen!**

# DHCP – Request - ACK

```
DHCP selected relay 1 - 192.168.0.21 (local address 192.168.50.15, gateway 192.168.50.1, VLAN 50, port 1)
DHCP transmitting DHCP REQUEST (3)
DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP   xid: 0xa504e3 (10814691), secs: 0, flags: 0
DHCP   chaddr: 68:7f:74:75:f1:cd
DHCP   ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP   siaddr: 0.0.0.0, giaddr: 192.168.50.15
DHCP   requested ip: 192.168.50.101
DHCP   server id: 192.168.0.21 rcvd server id: 1.1.1.1
DHCP sending REQUEST to 192.168.50.1 (len 374, port 1, vlan 50)
```

```
DHCP received op BOOTREPLY (2) (len 312,vlan 50, port 1, encap 0xec00)
192.168.50.101 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)
```

```
192.168.50.101 WEBAUTH_REQD (8) pemAdvanceState2 6662, Adding TMP rule
```

```
192.168.50.101 WEBAUTH_REQD (8) Replacing Fast Path rule
```

```
type = Airespace AP Client - ACL passthru
```

```
on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0
```

```
IPv4 A
```

```
Plumbing web-auth redirect rule due to user logout
```

```
Assigning Address 192.168.50.101 to mobile
```



**We have a Client  
IP Address**

# DHCP – Rejected

DHCP transmitting DHCP REQUEST (3)

DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

DHCP xid: 0xf3a2fca6 (4087544998), secs: 3, flags: 0

DHCP chaddr: d0:b3:3f:33:1c:88

DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

DHCP siaddr: 0.0.0.0, giaddr: 10.87.193.2

DHCP requested ip: 10.65.8.177

DHCP sending REQUEST to 10.87.193.1 (len 374, port 1, vlan 703)

DHCP selecting relay 2 - control block settings:

dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,

dhcpGateway: 0.0.0.0, dhcpRelay: 10.87.193.2 VLAN: 703

DHCP selected relay 2 - NONE

Client  
Requested IP  
Address

DHCP received op BOOTREPLY (2) (len 308, vlan 703, port 1, encap 0xec00)

DHCP sending REPLY to STA (len 402, port 1, vlan 701)

DHCP transmitting DHCP NAK (6)

DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 1

DHCP xid: 0xf3a2fca6 (4087544998), secs: 0, flags: 8000

DHCP chaddr: d0:b3:3f:33:1c:88

DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0

DHCP server id: 1.1.1.1 rcvd server id: 10.65.8.1

DHCP Server  
Rejecting the  
Clients Request

# Learning IP without DHCP

**\*Orphan Packet from 10.99.76.147 on mobile**

**\*0.0.0.0 DHCP\_REQD (7) Successfully plumbed mobile rule (ACL ID 255)**

**\*Installing Orphan Pkt IP address 10.99.76.147 for station**

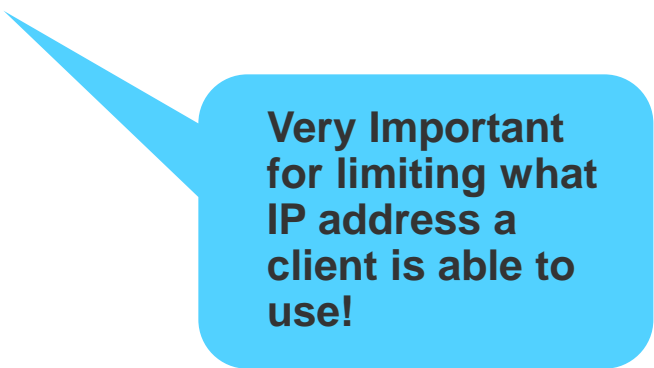
**\*10.99.76.147 DHCP\_REQD (7) Change state to RUN (20) last state RUN**

- Multiple mechanisms to learn Client IP address:
  - Mobility Announcement
  - ARP/GARP from client
  - Traffic from/to client
  - DHCP
- Non-DHCP: Seen with mobile devices that attempt to send data before validating DHCP
- Up to client to realize their address is not valid for the subnet
- DHCP Required enabled on WLAN mitigates this client behavior

**Without DHCP  
Required  
Checked, we  
honor what IP  
address the  
client uses!**

# DHCP Required - Caveats

- Modifies Address learning
  - Limits Address learning to only DHCP and Mobility messages
- **Good for security**
- It can cause problems if client is deleted
  - On new association client must do DHCP renew
  - Client may hold until DHCP half-lease time



**Very Important  
for limiting what  
IP address a  
client is able to  
use!**

# DHCP - Takeaways

- Verify if you are using DHCP proxy, the DHCP server addresses setup on the WLC interfaces only matter if DHCP proxy is enabled
- If DHCP proxy is disabled, make sure you have some type of IP helper on the layer 3 interface for that WLAN's interface, it will be needed if there is no DHCP server on that interface
- Check to see if you have run out of IP addresses, many times DHCP leases are long enough that leases are not released quick enough to handle the amount of users joining the WLAN
- Be careful of using secondary IP addressing on your layer 3 gateway for the controller as a way to increase the number of IP addresses available (its not really supported)

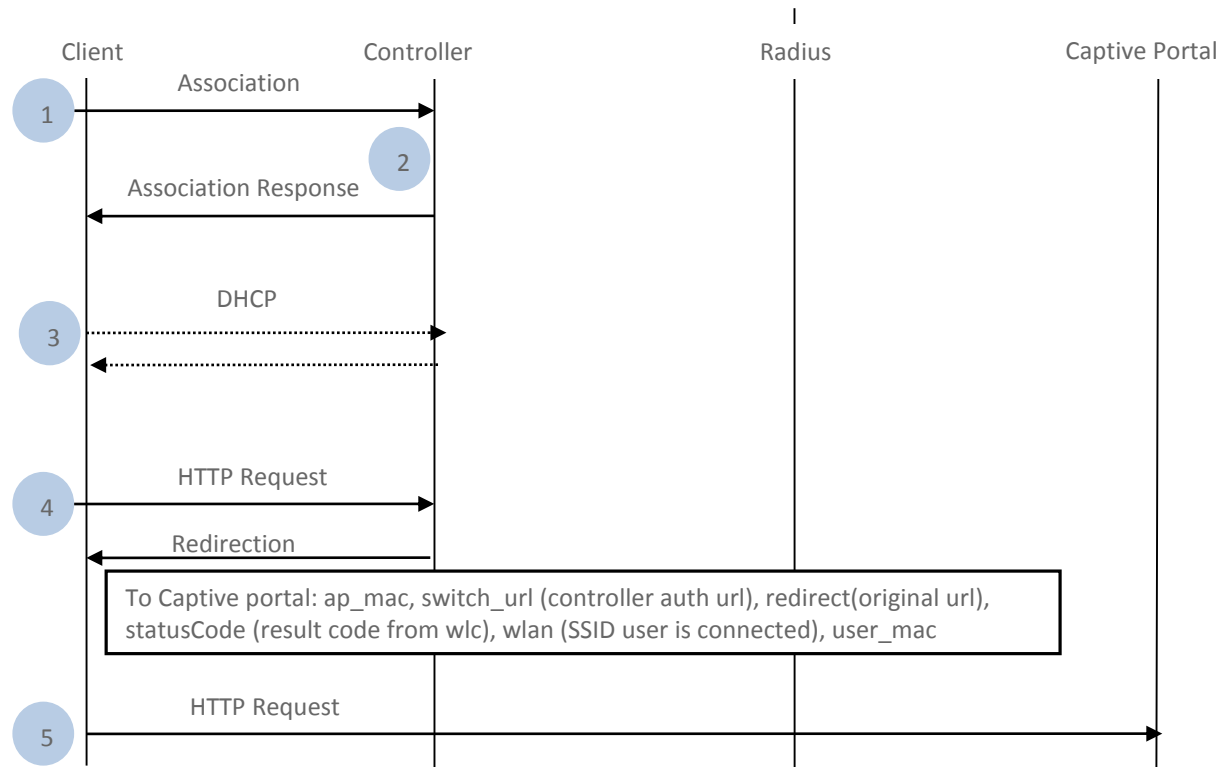
# Client Flow

The Route Toward the RUN State:

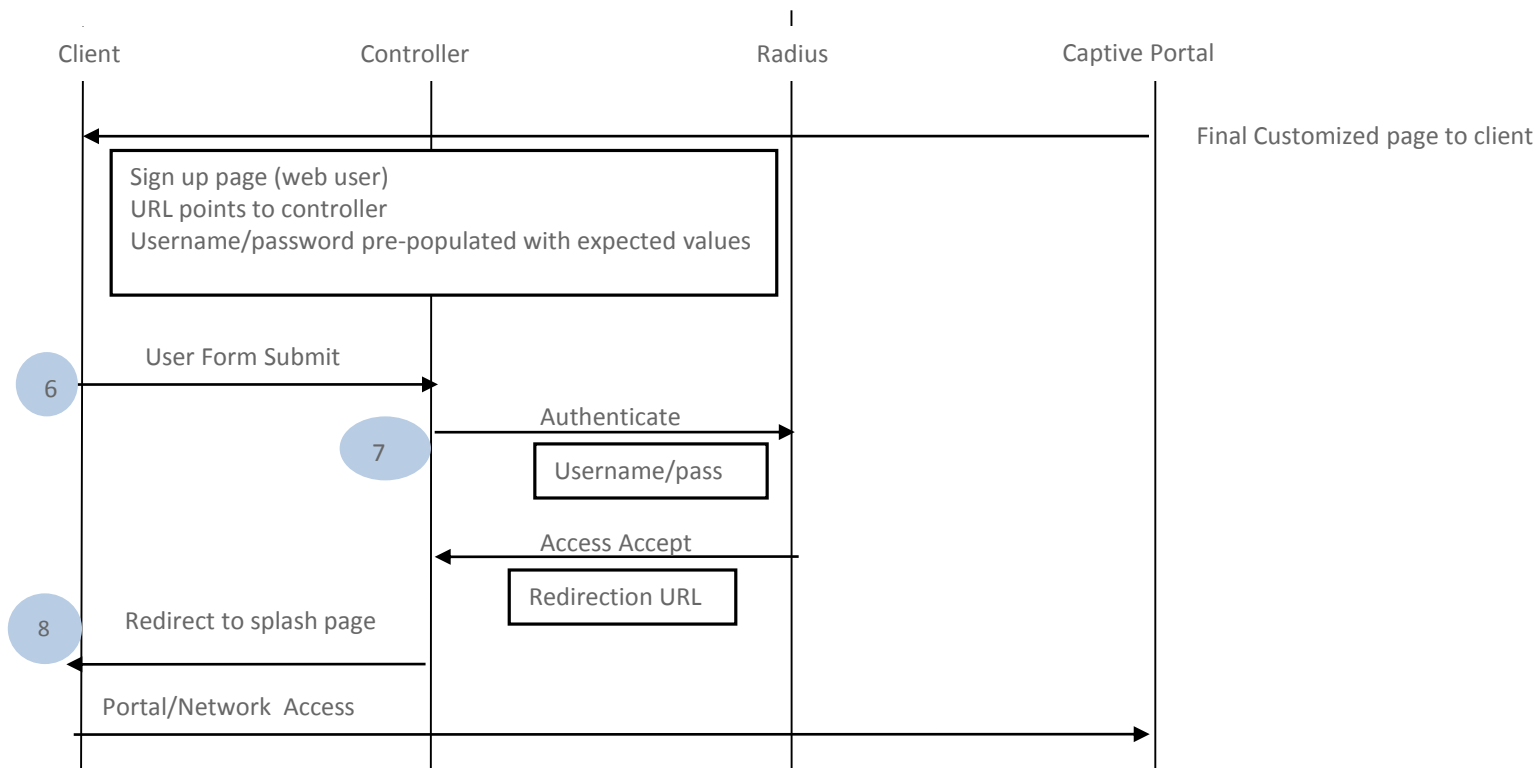




# Webauth- Walkthrough



# Webauth- Walkthrough



# Debug Web-auth: Webauth Redirect Example

```
*pemReceiveTask: Jan 02 10:45:30.824: 68:7f:74:75:f1:cd 192.168.50.101 Added NPU entry of type 2, dtlFlags 0x0
captive-bypass detection disabled, Not checking for wispr in HTTP GET, client mac=68:7f:74:75:f1:cd
Preparing redirect URL according to configured Web-Auth type
Checking custom-web config for WLAN ID:2
unable to get the hostName for virtual IP, using virtual IP =1.1.1.1
Global status is enabled, checking on web-auth type
Web-auth type Internal, no further redirection needed. Presenting default login page to user
http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-
control" content="no-cache"><META http-equiv="Pragma" content="
http_response_msg_body2 is "></HEAD></HTML>
parser host is 192.168.0.45
- parser path is /
added redirect=, URL is now https://1.1.1.1/login.html?
str1 is now https://1.1.1.1/login.html?redirect=192.168.0.45/
clen string is Content-Length: 302
Message to be sent is
  HTTP/1.1 200 OK
Location: https://1.1.1.1/login.html?redirect=192.168.0.45/
Content-Type: text/html
Content-Length: 302
<HTML><HEAD><TITLE>
send data length=428
```

**We are doing Internal Webauth, originally Browsing to Web Site at 192.168.0.45**

# Webauth Success

\*emWeb: Jan 02 10:46:42.904:

ewaURLHook: Entering:url=/login.html, virtIp = 1.1.1.1, ssl\_connection=1, secureweb=1

\*ewmwebWebauth1: Jan 02 10:46:42.905: 68:7f:74:75:f1:cd Username entry (cisco) created for mobile, length = 5

\*ewmwebWebauth1: Jan 02 10:46:42.905: 68:7f:74:75:f1:cd Username entry (cisco) created in mscb for mobile, length = 5

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 **WEBAUTH\_REQD (8) Change state to WEBAUTH\_NOL3SEC (14) last state WEBAUTH\_REQD (8)**

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd apfMsRunStateInc

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd **192.168.50.101 WEBAUTH\_NOL3SEC (14) Change state to RUN (20) last state WEBAUTH\_NOL3SEC (14)**

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd **Session Timeout is 1800 - starting session timer for the mobile**

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 **RUN (20)** Reached PLUMBFASPATH: from line 6550

\*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 **RUN (20)** Replacing Fast Path rule

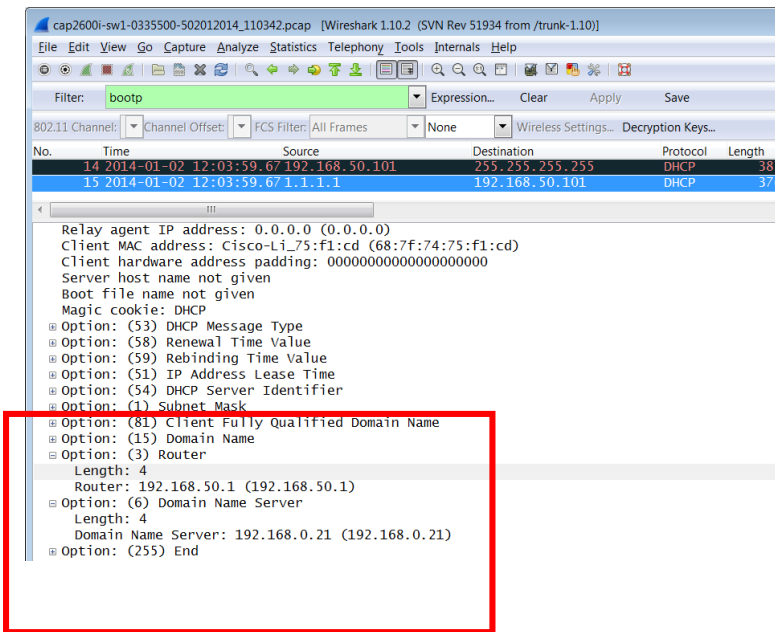


**Success! We are  
in the RUN state**

# Webauth Typical problems

- No DNS resolution
- No default GW
- Client doing request on different port
  - No HTTPS, or using 8000, etc.

**Always verify we have proper DNS addressing being returned by DHCP**



No.	Time	Source	Destination	Protocol	Length
14	2014-01-02 12:03:59.67	192.168.50.101	255.255.255.255	DHCP	387
15	2014-01-02 12:03:59.67	1.1.1.1	192.168.50.101	DHCP	376

Relay agent IP address: 0.0.0.0 (0.0.0.0)  
Client MAC address: Cisco-Li\_75:f1:cd (68:7f:74:75:f1:cd)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Option: (53) DHCP Message Type  
Option: (58) Renewal Time Value  
Option: (59) Rebinding Time Value  
Option: (51) IP Address Lease Time  
Option: (54) DHCP Server Identifier  
Option: (1) Subnet Mask  
Option: (81) Client Fully Qualified Domain Name  
Option: (15) Domain Name  
Option: (3) Router  
Length: 4  
Router: 192.168.50.1 (192.168.50.1)  
Option: (6) Domain Name Server  
Length: 4  
Domain Name Server: 192.168.0.21 (192.168.0.21)  
Option: (255) End

# Webauth Typical problems

## No Pre-Auth ACL for External Webauth

- Server IP must be allowed on the Pre-Auth ACL... otherwise, we will get in a loop!

```
*webauthRedirect: Jan 02 12:27:08.254: 68:7f:74:75:f1:cd- Web-auth type External, using
URL:http://192.168.0.21/login.htm
..
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser host is 192.168.0.21
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser path is /
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- added redirect=, URL is now
http://192.168.0.21/login.htm?switch_url=https://1.1.1.1/login.html&ap_mac=04:da:d2:4f:f0:50&client_mac=68:7f:
74:75:f1:cd&wlan=webauth&
```

NEXT:

```
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- parser host is 192.168.0.21
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser path is /
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- added redirect=, URL is now
...
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- str1 is now
http://192.168.0.21/login.htm?switch_url=https://1.1.1.1/login.html&ap_mac=04:da:d2:4f:f0:50&client_mac=68:7f:
74:75:f1:cd&wlan=webauth&redirect=192.168.0.21/
```

# Webauth Typical problems

## Untrusted Cert

- Specially important when using ISE or any other external web server
- Depending on client type/version:
  - External server not displayed
  - Authentication form not posted -> WLC sends internal page
  - **Nothing is sent -> “client hangs”**

## Session Timeout too low

- Users may need to re-authenticate often

## HTTP Request too large for WLC

- WLC has a max size per HTTP request of 2k
- Typically caused by website using very large cookies – CSCuy81133

**Careful, Websites using large Cookies happens more often than one would think!**

# Webauth - Takeaway

- If using external webauth
  - Certificate trust is critical (both WLC and external server). If suspected test with https disabled
  - Pre-auth ACL
- DHCP/ARP/DNS must work before you can do anything
- Additional debug needed
  - **debug web-auth redirect enable mac <mac addr>**
- Client side capture/logs may be needed
  - Fiddler software running on client machine
  - Wireshark

**This Point is so very Important, a good 60% of Web-Auth TAC Case are due to DNS not working**



# Client Flow

## The Route Toward the RUN State:



# RUN state - We can now pass data!

- RUN means: client has completed all required policy states
- “NPU entry of Type 1” is the goal

```
*dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Reached PLUMBFASPATH: from line
6076Nov 5 *dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Adding Fast Path rule
*dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Fast Path rule (contd...) 802.1P = 5,
DSCP = 0, TokenID = 15206 Local Bridging Vlan = 101, Local Bridging intf id = 18
*dot1xMsgTask: Nov 05 14:35:11.841: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Successfully plumbed mobile rule
(IPv4 ACL ID 255, IPv6 ACL ID 255)Nov 5 14:35:13 btwlc01 BTWLC01 *bcmReceiveTask:
Nov 05 14:35:11.842: 2c:54:2d:ea:e7:aa 10.253.42.45 Added NPU entry of type 1, dtlFlags 0x0
```

**Once we have a NPU state  
of 1, we are in the RUN  
state and can pass traffic**

# RUN state - Typical Problems

- Random Disconnections – Radio Reset

- There are normal radio resets: Channel changes, etc

```
emWeb: Jan 03 08:56:14.809: 00:1a:70:35:84:d6 Cleaning up state for STA 00:1a:70:35:84:d6 due to event for AP 04:da:d2:4f:f0:50(0)
```

```
*apfReceiveTask: Jan 03 08:56:14.810: 00:1a:70:35:84:d6 Scheduling deletion of Mobile Station: (callerId: 45) in 10 seconds
```

- Watch out for anomalous reset counts in short uptime



**Show Controller  
used to view the  
Radio Level Data**

```
>show controller dot11 0 | begin Reset
```

```
Last radio reset code: 62
```

```
Radio resets - total:113 retries:0 failed:0
```

```
Reset Stats: Start Cnt: 94, Recovery: Cnt 0, Last Ret: 0, Fails: 0, Recvry Status: Stalled  
NO, In Prog NO
```

```
Code/Count: 37/00010 84D7 51/00021 F25E 52/00012 F25E 54/00002 84D6
```

```
Code/Count: 62/00067 F25F 67/00001 0
```

# RUN state - Typical Problems

## Environmental trigger

- Typical high channel utilization

Run on AP or  
View Data on GUI

```
ap2600-sw1-0-31# show controller dot11 0 | begin QBS
```

```
QBSS Load: 0xFE Tx 0 Rx 0 AP 0
```

```
*Nov 21 10:59:06.244: %DOT11-3-NO_BEACONING: Error on Dot11Radio0 - Not Beacons for too long - Current 2887074 Last 2887074*Nov 21 10:59:06.274: %LINK-5-CHANGED: Interface
```

```
Dot11Radio0, changed state to reset
```

```
*Nov 21 10:59:07.693: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down
```

```
*Nov 21 10:59:08.485: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to up
```

```
*Nov 21 10:59:09.485: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
```

# An Easier Way to Check on RF Load Status!

## ACCESS POINT VIEW

### GENERAL



AP Name  
**CAP3602-1-timsmith**

Location  
**default location**

---

MAC Address 60:73:5c:41:f7:ec

IP Address 192.168.158.106

CDP / LLDP rtp12-timsmith-sw,  
GigabitEthernet0/21

Model / Domain AIR-CAP3602I-A-K9 / 802.11bg:-A  
802.11a:-A

Serial Number FTX1637GJLJ

Groups AP Group: timsmith, Flex Group: Not  
a member

Mode / Sub-mode FlexConnect / Not Configured

Max Capabilities 802.11n 2.4GHz, 802.11ac 5GHz  
Spatial Streams : 3(2.4GHz),  
3(5.0GHz)  
Max. Data Rate : 217Mbps(2.4GHz),  
450Mbps(5.0GHz)

### PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	6	100
Configured Rate	Min: 1 Mbps, Max: 217 Mbps	Min: 6 Mbps, Max: 217 Mbps
Usage Traffic	913 KB	79 GB
Throughput	0	12 KB
Transmit Power	11 dBm	2 dBm
Noise	Not Available	-91

Channel Utilization	0%	3%
Interference	0%	3%
Traffic	0%	0%

Air Quality	-	99
Admin Status	Disable	Enable

Logout | Refresh

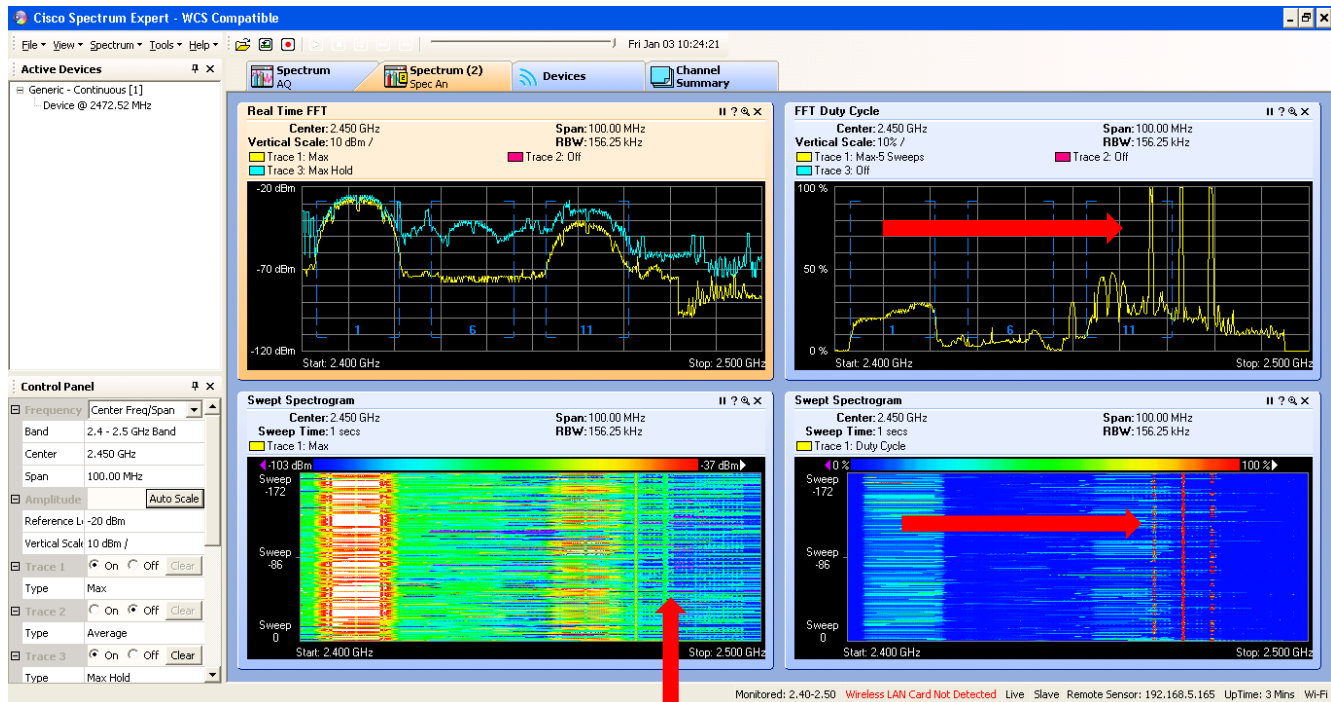
Home

Click the  
"HOME"  
button for  
new  
monitoring  
options!

# RUN state - Typical Problems

## Poor Performance

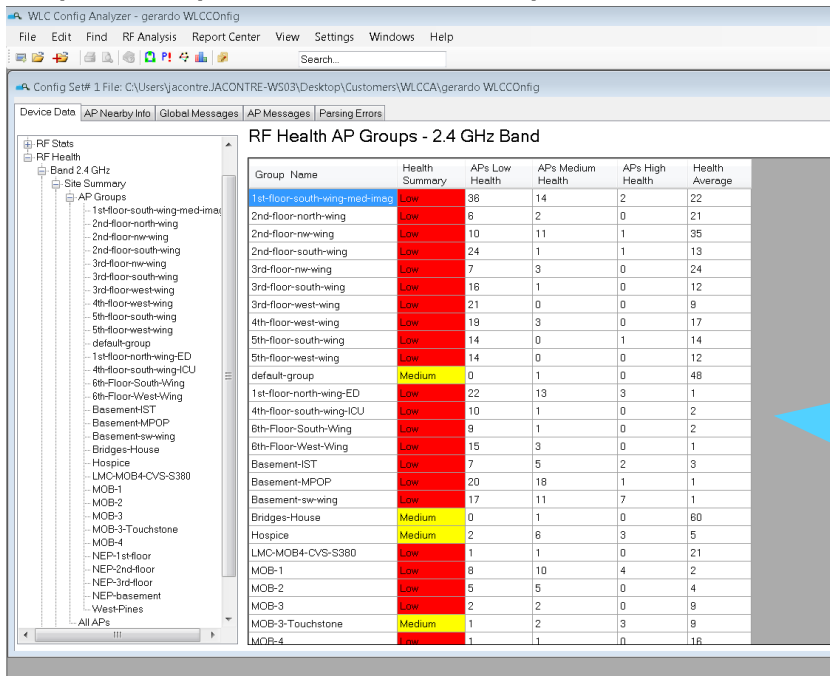
- RF issues
- Client side bugs



# RUN state - RF Analysis the Automated Way!

## WLCCA

- New tool for quick RF analysis
- RF Health - > simplified quick view on RF, per Band, AP, AP Group, Flex Group



WLCCA Config Analyzer - gerardo WLCCAConfig

File Edit Find RF Analysis Report Center View Settings Windows Help

Search...

Config Set# 1 File: C:\Users\jacontre\JACONTE-WS03\Desktop\Customers\WLCCA\gerardo WLCCAConfig

Device Data AP Neerby Info Global Messages AP Messages Parsing Errors

RF Stats

RF Health

Site Summary

Band 2.4 GHz

AP Groups

1st-floor-south-wing-med-imag

2nd-floor-north-wing

2nd-floor-nw-wing

2nd-floor-south-wing

3rd-floor-nw-wing

3rd-floor-south-wing

3rd-floor-west-wing

4th-floor-west-wing

5th-floor-south-wing

5th-floor-west-wing

default-group

1st-floor-north-wing-ED

4th-floor-south-wing-ICU

6th-floor-south-wing

6th-floor-west-wing

Basement-IST

Basement-MPOP

Basement-sw-wing

Bridges-House

Hospice

LMC-MOB4-CVS-S380

MOB-1

MOB-2

MOB-3

MOB-3-Touchstone

MOB-4

NEP-1st-floor

NEP-2nd-floor

NEP-3rd-floor

NEP-basement

West-Pines

All APs

RF Health AP Groups - 2.4 GHz Band

Group Name	Health Summary	APs Low Health	APs Medium Health	APs High Health	Health Average
1st-floor-south-wing-med-imag	Low	38	14	2	22
2nd-floor-north-wing	Low	6	2	0	21
2nd-floor-nw-wing	Low	10	11	1	35
2nd-floor-south-wing	Low	24	1	1	13
3rd-floor-nw-wing	Low	7	3	0	24
3rd-floor-south-wing	Low	16	1	0	12
3rd-floor-west-wing	Low	21	0	0	9
4th-floor-west-wing	Low	19	3	0	17
5th-floor-south-wing	Low	14	0	1	14
5th-floor-west-wing	Low	14	0	0	12
default-group	Medium	0	1	0	48
1st-floor-north-wing-ED	Low	22	13	3	1
4th-floor-south-wing-ICU	Low	10	1	0	2
6th-floor-south-wing	Low	9	1	0	2
6th-floor-west-wing	Low	15	3	0	1
Basement-IST	Low	7	5	2	3
Basement-MPOP	Low	20	18	1	1
Basement-sw-wing	Low	17	11	7	1
Bridges-House	Medium	0	1	0	60
Hospice	Medium	2	6	3	5
LMC-MOB4-CVS-S380	Low	1	1	0	21
MOB-1	Low	8	10	4	2
MOB-2	Low	5	5	0	4
MOB-3	Low	2	2	0	9
MOB-3-Touchstone	Medium	1	2	3	9
MOB-4	Low	1	1	0	16

**RF Health uses various stats gathered for each AP and presented in the “show run-config” that you upload into the tool**

# RUN state - WLCCA Overall RF View

WLC Config Analyzer - gerardo WLCCONfig

File Edit Find RF Analysis Report Center View Settings Windows Help

Search...

Config Set# 1 File: C:\Users\jacontre.JACONTRE-WS03\Desktop\Customers\WLCCA\gerardo WLCCONfig

Device Data AP Nearby Info Global Messages AP Messages Parsing Errors

## RF Stats AP Groups - 2.4 GHz Band

Group Name	Total Clients	Clients High SNR	Clients Low SNR	Total APs	APs with High Cochannel Interf.	APs with High Noise	APs with High Utilization	APs with Auto Channel	APs with Manual Channel	APs with Auto Power	APs with Manual Power
1st-floor-north-wing-ED	54	32	22	38	108	0	26	38	0	38	0
1st-floor-south-wing-med-imag	61	27	34	52	206	0	41	52	0	52	0
2nd-floor-north-wing	11	6	5	8	24	0	8	8	0	8	0
2nd-floor-nw-wing	15	10	5	22	33	0	16	22	0	22	0
2nd-floor-south-wing	60	23	37	26	99	0	25	26	0	26	0
3rd-floor-nw-wing	10	0	10	10	17	0	9	10	0	10	0
3rd-floor-south-wing	37	12	25	17	59	0	17	17	0	17	0
3rd-floor-west-wing	30	14	16	21	83	0	20	21	0	21	0
4th-floor-south-wing-ICU	22	15	7	11	28	0	10	11	0	11	0
4th-floor-west-wing	22	13	9	22	61	0	21	22	0	22	0
5th-floor-south-wing	19	9	10	15	45	0	14	15	0	15	0
5th-floor-west-wing	22	12	10	14	47	0	14	14	0	14	0
6th-floor-south-wing	18	5	13	10	14	0	9	10	0	10	0
6th-floor-west-wing	18	8	10	18	39	0	17	18	0	18	0
Basement-HST	7	5	2	14	34	0	6	14	0	14	0
Basement-MPOP	26	17	9	39	121	0	24	39	0	39	0
Basement-sw-wing	18	6	12	35	106	0	18	35	0	35	0
Bridges-House	5	3	2	1	0	0	0	1	0	1	0
Hospice	23	12	11	11	5	0	1	11	0	11	0
LMC-MOB4-CVS-S380	0	0	0	2	1	0	1	2	0	2	0
MOB-1	60	27	33	22	11	0	10	22	0	22	0
MOB-2	39	21	18	10	10	0	8	10	0	10	0
MOB-3	24	4	20	4	0	0	1	4	0	4	0
MOB-3-Touchstone	10	1	9	6	3	0	1	6	0	6	0
MOB-4	11	3	8	2	1	0	1	2	0	2	0
NEP-1st-floor	46	11	35	30	28	0	7	30	0	30	0



# Client Got Deauthenticated - What Happened?

- Idle Timeout

Occurs after no traffic received from Client at AP

Default Duration is 300 seconds

**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)

- Session Timeout

Occurs at scheduled duration (default 1800 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**

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)

# Client Got Deauthenticated - What Happened?

- WLAN Change

- Modifying a WLAN in anyway Disables and Re-enables WLAN

**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)

- Manual Deauthentication

- From GUI: Remove Client
- From CLI: config client deauthenticate <mac address>

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)

# Client Got Deauthenticated - What Happened?

- Authentication Timeout

Auth or Key Exchange max-retransmissions reached

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

**Sent Deauthenticate to mobile** on BSSID 00:26:cb:94:44:c0 slot 0(caller 1x\_ptsm.c:534)

- AP Radio Reset (Power/Channel)

AP disasassociates clients but WLC does not delete entry

**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)

# Debug Client: Deauthenticated Client Example

## Failed Broadcast key rotation

```
*dot1xMsgTask: Oct 22 15:32:49.863: 24:77:03:c2:8a:20 Key exchange done, data packets from mobile  
24:77:03:c2:8a:20 should be forwarded shortly
```

```
*dot1xMsgTask: Oct 22 15:32:49.863: 24:77:03:c2:8a:20 Sending EAPOL-Key Message to mobile  
24:77:03:c2:8a:20
```

```
*osapiBsnTimer: Oct 22 15:32:51.056: 24:77:03:c2:8a:20 802.1x 'timeoutEvt' Timer expired for station  
24:77:03:c2:8a:20 and for message = M5*dot1xMsgTask: Oct 22 15:32:51.056: 24:77:03:c2:8a:20  
Retransmit 1 of EAPOL-Key M5 (length 131) for mobile 24:77:03:c2:8a:20*osapiBsnTimer: Oct 22
```

```
..  
*dot1xMsgTask: Oct 22 15:32:53.056: 24:77:03:c2:8a:20 Retransmit failure for EAPOL-Key M5 to mobile  
24:77:03:c2:8a:20, retransmit count 3, mscb deauth count 0
```

```
*dot1xMsgTask: Oct 22 15:32:53.056: 24:77:03:c2:8a:20 Sent Deauthenticate to mobile on BSSID  
20:3a:07:e4:c8:f0 slot 0(caller 1x_ptsm.c:570)
```

# GUI for Client Troubleshooting

# WLC - Real-Time Client Troubleshooting Tools

## Packet Capture Tool (Delivered in 8.2)

CLIENT TEST

PING TEST   **PACKET CAPTURE**   EVENT LOG

Capture Point

APname: C2700-AP3   Time (min):

Capture Filters

IP Protocol

☐ ARP   ☐ Broadcast   ☒ Control  
☐ Data   ☐ Dot1x   ☐ Multicast  
☐ IP   ☐ IAPP   ☐ UDP  
☐ TCP   ☒ Management

FTP Details

IPAddress: 192.168.11.10   FTPPath: /

Username: cisco   Password: \*\*\*\*\*

Capture States

ClientStatus

**Start**   **Stop**

## Connection Test Tool (New for 8.3)

CLIENT TEST

CONNECTIVITY   PING TEST   **CONNECTION**

**Start**   **Stop**

802.11 Association	●
Security Policy RSN-PSK	●
Network Membership	●
IP Addressing	●
IPv4 Additional Options	●

## Event Log Tool (New for 8.3)

CLIENT TEST

PING TEST   PACKET CAPTURE   **EVENT LOG**

**Start**   **Stop**   **Save To Disk**

Time	Module	Sever...	MsgType	MsgSub...	VarArg
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-R...
Mon Sep...	CIAAA	ERROR	AAA_ER...	DHCP_R...	None
Mon Sep...	Dot1x	ERROR	ACCESS...	MESSAG...	None
Mon Sep...	Misce	ERROR	MISC_R...		00:00:00...
Mon Sep...	Dot1x	ERROR	EAP_ID...	MESSAG...	None
Mon Sep...	PEM	ERROR	PEM_EV...	DOT_802...	None

# Where do I find these tools?




Click on the “HOME” button on the Controller GUI



## CLIENT VIEW

### GENERAL



User Name  
**Unknown**   
Host Name  
**Unknown**

MAC Address: 38:71:de:4e:43:8b  
Uptime: Associated since 1 Minute 45 Seconds  
SSID: Bonjour  
AP Name:  CAP702-1-timsmith (Ch 132)  
Nearest APs:  CAP3502-BetaUnit-timsmith(-40 dBm)  
 APcc16.7ee1.06cc(-32 dBm)  
 OEAP1810-1-timsmith(-44 dBm)  
Device Type: Performance  
Signal Strength: -36 dBm Signal Quality: 62 dB Connection Speed: 54 Mbps Channel Width: 40 MHz  
Capabilities: 802.11a (5GHz) Spatial Stream: 1  
Cisco Compatible: Not Supported  
Connection Score: 100%

# Packet Capture Tool

## Packet Capture Tool

## Overview

CLIENT TEST

PING TEST   **PACKET CAPTURE**   EVENT LOG

**Capture Point**

APName:    Time (min):

**Capture Filters**

IP Protocol

<input type="checkbox"/> ARP	<input type="checkbox"/> Broadcast	<input checked="" type="checkbox"/> Control
<input type="checkbox"/> Data	<input type="checkbox"/> Dot1x	<input type="checkbox"/> Multicast
<input type="checkbox"/> IP	<input type="checkbox"/> IAPP	<input type="checkbox"/> UDP
<input type="checkbox"/> TCP	<input checked="" type="checkbox"/> Management	

**FTP Details**

IPAddress:    FTPPath:

Username:    Password:

**Capture States**

ClientStatus

- 802.11 packet capture tool for administrators and TAC
  - Previously only available in the CLI (config ap packet dump)
  - Enabled per client (1 session max)
  - Capture times 1 – 60 minutes (default 10 minutes)
  - 802.11 and Protocol based capture filters
- Packet captures are streamed to a FTP server in .pcap format for offline analysis
  - Capture files are automatically named using <AP-NAME><WLC-NAME>-<DATE>\_<TIME>
- WLC 8.2 Code Needed



# Packet Capture Tool

## Packet Capture Tool

CLIENT TEST

PING TEST   PACKET CAPTURE   EVENT LOG

**Capture Point**

APname:    Time (min):

**Capture Filters**

IP Protocol

<input type="checkbox"/> ARP	<input type="checkbox"/> Broadcast	<input checked="" type="checkbox"/> Control
<input type="checkbox"/> Data	<input type="checkbox"/> Dot1x	<input type="checkbox"/> Multicast
<input type="checkbox"/> IP	<input type="checkbox"/> IAPP	<input type="checkbox"/> UDP
<input type="checkbox"/> TCP	<input checked="" type="checkbox"/> Management	

**FTP Details**

IPAddress:    FTPPath:

Username:    Password:

**Capture States**

ClientStatus

## Considerations

- Client must be in the session table to initiate the packet capture using the WebUI
- 1 packet capture session per WLC
- Only captures packets between the selected client and the AP it is currently associated
- Only packets that reach the radio driver are captured
- No support for inter-controller or intra-controller roaming scenarios

# Connection Test Tool

New for 8.3

## Connection Test Tool

## Overview

- A helpdesk level tool for quick and easy client connection troubleshooting
  - 802.11 Phases
  - IP Addressing
  - Network Membership
- Traffic light indicators to visually determine where a problem resides
- Simple messaging that clearly communicates what the problem is
- Enabled per client
  - Once initiated will run for up to 3 minutes allowing the end-user time to disconnect and re-connect the client to the network

### CLIENT TEST

CONNECTIVITY

PING TEST

CONNECTION

Start

Stop

802.11 Association



Security Policy RSN-PSK



Network Membership



IP Addressing



IPv4 Additional Options



# Event Log Tool

## Event Log Tool

## Overview

- Event log debugging tool for administrators and TAC
  - Full debug view of the Connection Test tool
  - Enabled per client (20 sessions max)
  - Provides a debug view of the 802.11 connection phases, EAP, RADIUS, 4-way handshake and DHCP exchange
- Option to export captured events to Excel for offline analysis

New for 8.3

Access-Reject  
received from  
RADIUS Server  
192.168.10.6,  
receiveId = 9

CLIENT TEST

PING TEST    PACKET CAPTURE    EVENT LOG

Start Stop Save To Disk

Time...	Module	Sever...	MsgType	MsgSub...	VarArg
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-R...
Mon Sep...	CIAAA	ERROR	AAA_ER...	DHCP_R...	None
Mon Sep...	Dot1x	ERROR	ACCESS...	MESSAG...	None
Mon Sep...	Misce	ERROR	MISC_R...		00:00:00:...
Mon Sep...	Dot1x	ERROR	EAP_ID_...	MESSAG...	None
Mon Sep...	PEM	ERROR	PEM_EV...	DOT_802...	None

# Event Log Tool

## Event Log Tool

## Offline Analysis - Microsoft Excel

### CLIENT TEST

PING TEST

PACKET CAPTURE

EVENT LOG

Start Stop Save To Disk

Time...	Module	Sever...	MsgType	MsgSub...	VarArg
Mon Sep...	Dot1x	INFO	EAP_ID...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-R...
Mon Sep...	CIAAA	ERROR	AAA_ER...	DHCP_R...	None
Mon Sep...	Dot1x	ERROR	ACCESS...	MESSAG...	None
Mon Sep...	Misce	ERROR	MISC_R...	00:00:00...	
Mon Sep...	Dot1x	ERROR	EAP_ID...	MESSAG...	None
Mon Sep...	PEM	ERROR	PEM_EV...	DOT_802...	None

TimeStamp	Module	Sever...	MsgType	MsgSub...	VarArg
29 Mon Sep 21 08:01:54 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 6
30 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	ACCESS_CHALLENGE	MESSAGE_RECEIVED	None
31 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_REQ	ASSOC_REQ_RECEIVED	None
32 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
33 Mon Sep 21 08:01:54 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 6
34 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	ACCESS_CHALLENGE	MESSAGE_RECEIVED	None
35 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_REQ	ASSOC_REQ_RECEIVED	None
36 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
37 Mon Sep 21 08:01:54 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 6
38 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	ACCESS_CHALLENGE	MESSAGE_RECEIVED	None
39 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_REQ	ASSOC_REQ_RECEIVED	None
40 Mon Sep 21 08:01:54 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
41 Mon Sep 21 08:01:54 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 6
42 Mon Sep 21 08:01:54 EDT 2015	CIAAA	ERROR	AAA_ERROR	DHCP_RETRY_COUNT_EXCEEDED	None
43 Mon Sep 21 08:01:54 EDT 2015	Dot1x	ERROR	ACCESS_REJECT	MESSAGE_RECEIVED	None
44 Mon Sep 21 08:01:54 EDT 2015	Misce	ERROR	MISC_RADIUM_EVENTS		00:00:00:00:00:00, 1, 192.168.10.6/30, 1, AAA_AUTH_FAILURE
45 Mon Sep 21 08:01:54 EDT 2015	Dot1x	ERROR	EAP_ID_RES	MESSAGE_SENT_FROM_RADIUS_SERVER_TO_CLIENT	None
46 Mon Sep 21 08:01:59 EDT 2015	Dot1x	INFO	EAP_ID_RES	RECEIVED_INTERFACE_CHANGE	None
47 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
48 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	ASSOC_REQ	INVALID_RSN_IE	None
49 Mon Sep 21 08:02:04 EDT 2015	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STATIC_DYNAMIC_WEP	None
50 Mon Sep 21 08:02:04 EDT 2015	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_AUTH_NOT_REQ_OR_STATIC_DYNAMIC_WEP_SUPP	None
51 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	ASSOC_REQ	CLIENT_MOVED_TO_ASSOCIATED_STATE	None
52 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	RECEIVED_INTERFACE_CHANGE	None
53 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAPOL_START	MESSAGE_RECEIVED	None
54 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	RECEIVED_INTERFACE_CHANGE	None
55 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
56 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
57 Mon Sep 21 08:02:04 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 9
58 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	ACCESS_CHALLENGE	MESSAGE_RECEIVED	None
59 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_REQ	ASSOC_REQ_RECEIVED	None
60 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
61 Mon Sep 21 08:02:04 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 9
62 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	ACCESS_CHALLENGE	MESSAGE_RECEIVED	None
63 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_REQ	ASSOC_REQ_RECEIVED	None
64 Mon Sep 21 08:02:04 EDT 2015	Dot1x	INFO	EAP_ID_RES	MESSAGE_RECEIVED	None
65 Mon Sep 21 08:02:04 EDT 2015	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREATION_FAILED	Access-Challenge received from RADIUS server 192.168.10.6, received = 9

# Event Log Tool

## Event Log Tool

CLIENT TEST

PING TEST

PACKET CAPTURE

EVENT LOG

Start Stop Save To Disk

Time...	Module	Sever...	MsgType	MsgSub...	VarArg
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-C...
Mon Sep...	Dot1x	INFO	ACCESS...	MESSAG...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	ASSOC_...	None
Mon Sep...	Dot1x	INFO	EAP_ID_...	MESSAG...	None
Mon Sep...	CIAAA	INFO	AAA_AUTH	AAA_ME...	Access-R...
Mon Sep...	CIAAA	ERROR	AAA_ER...	DHCP_R...	None
Mon Sep...	Dot1x	ERROR	ACCESS...	MESSAG...	None
Mon Sep...	Misce	ERROR	MISC_R...		00:00:00:...
Mon Sep...	Dot1x	ERROR	EAP_ID_...	MESSAG...	None
Mon Sep...	PEM	ERROR	PEM_EV...	DOT_802...	None

## Considerations

- Client must be in the session table to initiate the event log capture using the WebUI
- Up to 20 sessions per WLC
- 10 Minute timeout / session
- Works for roaming clients

# Decoding Client Debugs? We have Automation!

- Goto to the following URL:
  - <https://cway.cisco.com/tools/WirelessDebugAnalyzer/>
- Upload any wireless debug client output
- Choose appropriate client mac from list for analysis.

# Decoding Client Debugs? We have Automation!



[Tools Catalog](#) / Wireless Debug Analyzer

Cisco TAC Tool

Timothy Smith



## Wireless Debug Analyzer BETA

[Contributors](#)

Parses debug logs file for AireOS (WLC 5500/2500/8500/7500/WISM1-2/vWLC)

Makes it easier to troubleshoot issues with wireless client association, authentication, roaming or connectivity issues. [details](#) ^

Tool aims to provide logical analysis based on log sequence matching against existing issues.

Reading and interpreting some of these voluminous debug log outputs with multiple client mac-addresses can become cumbersome.

Input: "debug client <mac1> <mac2>..."

This tool also can parse through some portions of "debug aaa/webauth/mdns"



Upload wireless "debug client" output here

☒ [Group by client MAC](#)

Parse

# Decoding Client Debugs? We have Automation!

Select a client MAC Address and connection to see logs.

3c:a9:f4:01:21:84 ▾

Connection 1 of 2 ⏪ ⏩ ⏴ ⏵

☒ Show Time ☒ Show Task ☒ Show Translated ☐ Show Original ☐ Show Prior First Connection ☐ Show All

Time	Task	Translated
Oct 15 15:48:13.747	*apfMsConnTask_1	Client made new Association to AP/BSSID BSSID ec:c8:82:a4:5b:c4 AP VoiceAP_1042
Oct 15 15:48:13.748	*apfMsConnTask_1	The WLC/AP has found from client association request Information Element that claims PMKID Caching support
Oct 15 15:48:13.750	*apfMsConnTask_1	Client is entering the 802.1x or PSK Authentication state
Oct 15 15:48:13.750	*apfMsConnTask_1	Client has successfully cleared AP association phase
Oct 15 15:48:13.750	*apfMsConnTask_1	Client is entering PSK Dot1x or WEP authentication phase
Oct 15 15:48:13.750	*apfMsConnTask_1	WLC/AP is sending an Association Response to the client with status code status 0
Oct 15 15:48:13.755	*Dot1x_NW_MsgTask_4	4-Way PTK Handshake, Sending M1
Oct 15 15:48:14.036	*osapiBsnTimer	4-Way PTK Handshake, Client did not respond with M2
Oct 15 15:48:14.037	*dot1xMsgTask	4-Way PTK Handshake, Retransmitting M1 retry #1
Oct 15 15:48:14.436	*osapiBsnTimer	4-Way PTK Handshake, Client did not respond with M2
Oct 15 15:48:14.436	*dot1xMsgTask	4-Way PTK Handshake, Retransmitting M1 retry #2
Oct 15 15:48:14.836	*osapiBsnTimer	4-Way PTK Handshake, Client did not respond with M2
Oct 15 15:48:14.837	*dot1xMsgTask	Client has been deauthenticated



# Decoding Client Debugs? We have Automation!

Select a client MAC Address and connection to see logs.

e8:2a:ea:77:e1:8d ▾


Connection 1 of 1 |<< < > >>|

☒ Show Time ☒ Show Task ☒ Show Translated ☐ Show Original ☐ Show Prior First Connection ☐ Show All

Oct 15 15:48:16.099	*apfMsConnTask_1	Client made new Association to AP/BSSID BSSID ec:c8:82:a4:5b:c4 AP VoiceAP_1042
Oct 15 15:48:16.100	*apfMsConnTask_1	The WLC/AP has found from client association request Information Element that claims PMKID Caching support
Oct 15 15:48:16.100	*apfMsConnTask_1	Client is entering the 802.1x or PSK Authentication state
Oct 15 15:48:16.100	*apfMsConnTask_1	Client has successfully cleared AP association phase
Oct 15 15:48:16.100	*apfMsConnTask_1	Client is entering PSK Dot1x or WEP authentication phase
Oct 15 15:48:16.101	*apfMsConnTask_1	WLC/AP is sending an Association Response to the client with status code status 0
Oct 15 15:48:16.106	*Dot1x_NW_MsgTask_5	4-Way PTK Handshake, Sending M1
Oct 15 15:48:16.112	*Dot1x_NW_MsgTask_5	4-Way PTK Handshake, Received M2
Oct 15 15:48:16.112	*Dot1x_NW_MsgTask_5	4-Way PTK Handshake, Sending M3
Oct 15 15:48:16.114	*Dot1x_NW_MsgTask_5	4-Way PTK Handshake, Received M4
Oct 15 15:48:16.114	*Dot1x_NW_MsgTask_5	Client has completed PSK Dot1x or WEP authentication phase
Oct 15 15:48:16.117	*Dot1x_NW_MsgTask_5	Client has entered DHCP Required state
Oct 15 15:48:16.131	*DHCP Socket Task	Received DHCP Discover from client
Oct 15 15:48:16.131	*DHCP Socket Task	Sending DHCP Request to DHCP Server 192.168.120.1 through gateway 192.168.120.2 requesting 192.168.120.22 on VLAN 120
Oct 15 15:48:16.133	*DHCP Socket Task	Client has entered RUN state
Oct 15 15:48:16.134	*DHCP Socket Task	Received DHCP ACK, assigning IP Address 192.168.120.22
Oct 15 15:48:19.207	*DHCP Socket Task	Received DHCP Discover from client

# Client Troubleshooting - Takeaways

- Client can be removed for numerous reasons
  - ✓ WLAN change, AP change, configured interval
- Start with Client Debug to see if there is a reason for a client's deauthentication
- Further Troubleshooting
  - ✓ Client debug should give some indication of what kind of death is happening
  - ✓ Packet capture or client logs may be required to see the exact reason
  - ✓ Never forget Radio status and RF conditions



**RF is the Road  
that all things are  
Built on!**

# AP Join Troubleshooting

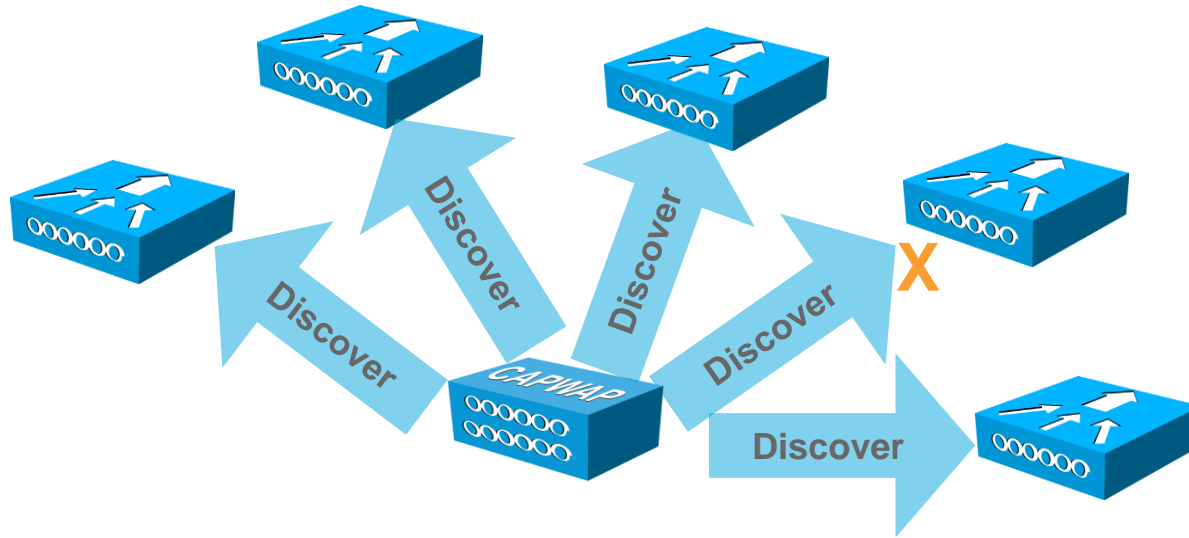
# AP Join Process

- WLC Discovery
- DTLS Setup
- WLC Join
- Image Download
- Configuration Check
- REG

More information:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html>

# L3 WLC Discovery



**AP tries to send discover messages to all the WLC addresses that its hunting process has turned up**

# AP Discover/Join

- AP Discovery Request sent to known and learned WLCs
- Broadcast
  - Reaches WLCs with MGMT Interface in local subnet of AP
  - Use “ip helper-address <ip>” with “ip forward-protocol udp 5246”
- Dynamic
  - DNS: cisco-capwap-controller
  - DHCP: Option 43
- Configured (nvram)
  - High Availability WLCs – Pri/Sec/Ter/Backup
  - Last WLC
  - All WLCs in same mobility group as last WLC
  - Manual from AP - “capwap ap controller ip address <ip>”

**Very Useful trick when you can't modify DNS or DHCP**

# AP Debug: AP Discover/Join – AP Side

```
*Jan  2 15:41:42.035: %CAPWAP-3-EVENTLOG: Starting Discovery. Initializing discovery latency in
discovery responses.
*Jan  2 15:41:42.035: %CAPWAP-3-EVENTLOG: CAPWAP State: Discovery.
*Jan  2 15:41:42.035: CAPWAP Control msg Sent to 192.168.70.10, Port 5246
*Jan  2 15:41:42.039:           Msg Type      : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control msg Sent to 192.168.5.55, Port 5246
*Jan  2 15:41:42.039:           Msg Type      : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control msg Sent to 255.255.255.255, Port 5246
*Jan  2 15:41:42.039:           Msg Type      : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control msg Recd from 192.168.5.54, Port 5246
*Jan  2 15:41:42.039:           HLEN 2,      Radio ID 0,      WBID 1
*Jan  2 15:41:42.039:           Msg Type      : CAPWAP_DISCOVERY_RESPONSE
*Jan  2 15:41:42.055: CAPWAP Control msg Recd from 192.168.5.55, Port 5246
*Jan  2 15:41:42.055:           HLEN 2,      Radio ID 0,      WBID 1
*Jan  2 15:41:42.055:           Msg Type      : CAPWAP_DISCOVERY_RESPONSE
```

# AP Debug: AP Discover/Join – AP Side

```
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Calling wtpGetAcToJoin from timer expiry.  
*Jan  2 15:41:52.039: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-5'(index 0).  
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Selected MWAR '5500-5' (index 2).  
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Ap mgr count=1  
*Jan  2 15:41:52.039: %CAPWAP-3-ERRORLOG: Go join a capwap controller  
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Adding Ipv4 AP manager 192.168.5.55 to least load  
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Choosing AP Mgr with index 0, IP = 192.168.5.55, load =  
3..  
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Synchronizing time with AC time.  
*Jan  2 15:41:52.000: %CAPWAP-3-EVENTLOG: Setting time to 15:41:52 UTC Jan 2 2014  
  
*Jan  2 15:41:52.467: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip:  
192.168.5.55 peer_port: 5246
```

**We need DTLS setup before  
we can send the Join!**



# AP Discover/Join – WLC Side Debug

```
*spamApTask7: Jan 02 15:35:57.295: 04:da:d2:4f:f0:50 Discovery Request from 192.168.5.156:7411
*spamApTask7: Jan 02 15:35:57.296: 04:da:d2:4f:f0:50 ApModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apType = 27 apModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apType: 0x1b bundleApImageVer: 7.6.100.0
*spamApTask7: Jan 02 15:35:57.296: version:7 release:6 maint:100 build:0
*spamApTask7: Jan 02 15:35:57.296: 04:da:d2:4f:f0:50 Discovery Response sent to 192.168.5.156 port
7411
*spamApTask7: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c DTLS keys for Control Plane are plumbed
successfully for AP 192.168.5.156. Index 7
*spamApTask6: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c DTLS Session established server
(192.168.5.55:5246), client (192.168.5.156:7411)
*spamApTask6: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c Starting wait join timer for AP:
192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.764: 04:da:d2:4f:f0:50 Join Request from 192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 Join resp: CAPWAP Maximum Msg element len = 83
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 Join Response sent to 192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 CAPWAP State: Join
```

# AP Join – Country Mismatch – AP Side Debug

```
*Jan  3 07:48:36.603: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-4'(index 0).
*Jan  3 07:48:36.603: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Jan  3 07:48:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.5.54
peer_port: 5246
*Jan  3 07:48:37.467: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip:
192.168.5.54 peer_port: 5246
*Jan  3 07:48:37.467: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.5.54
*Jan  3 07:48:37.467: %CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination.
*Jan  3 07:48:37.467: %CAPWAP-3-ERRORLOG: CAPWAP SM handler: Failed to process message type 10 state
5.
*Jan  3 07:48:37.467: %CAPWAP-3-ERRORLOG: Failed to handle capwap control message from controller
*Jan  3 07:48:37.467: %CAPWAP-3-ERRORLOG: Failed to process encrypted capwap packet from
192.168.5.54
```

**The AP Debugs  
really don't tell us  
Much!**

# AP Join – Country Mismatch – WLC Side Debug

\*spamApTask5: Jan 03 07:49:16.571: #CAPWAP-3-POST\_DECODE\_ERR: capwap\_ac\_sm.c:5660 Post decode processing failed for Config status from AP 04:da:d2:28:94:c0

\*spamApTask5: Jan 03 07:49:16.563: #LWAPP-3-RD\_ERR4: capwap\_ac\_sm.c:3085 **The system detects an invalid regulatory domain 802.11bg:-A 802.11a:-A for AP 04:da:d2:28:94:c0**

\*spamApTask5: Jan 03 07:49:16.563: #LOG-3-Q\_IND: spam\_lrad.c:10946 **Country code (ES ) not configured** for AP 04:da:d2:28:94:c0[...It occurred 2 times.!]

**But the Controller  
Debugs tell us the  
exact Issue!**

# Troubleshooting Lightweight AP Join Issues

Can the AP and the WLC communicate?

- Make sure the AP is getting an address from DHCP (check the DHCP server leases for the AP's MAC address)
- If the AP's address is statically set, ensure it is correctly configured
- Try pinging from AP to controller and vice versa
- If pings are successful, ensure the AP has **at least one method to discover** the WLC
- Console or telnet/ssh into the controller to run debugs
- If you do not have access to APs, use “**show cdp neighbors port <x/y> detail**” on connected switch to verify if the AP has an IP address

# Troubleshooting Lightweight AP Join Issues

Debugs to be enabled

## On the WLC:

- debug mac addr <AP Ethernet/Radio mac>
- debug capwap events enable
- debug capwap errors enable
- debug dtls all enable
- debug pm pki enable

## On the AP:

- debug dhcp detail
- debug capwap client detail

# AP Blackbox recorder

## AP keeps recordings at multiple levels

```
#dir
```

```
Directory of flash:/
```

33	drwx	2240	Oct 29 2014 11:53:23 +00:00	ap3g2-k9w8-mx.wnbu_bt.201410071110
2	-rwx	125850	Oct 13 2014 16:16:26 +00:00	<b>event.r0</b>
15	-rwx	64	Oct 29 2014 11:53:37 +00:00	sensord_CSPRNG0
16	-rwx	64	Oct 29 2014 11:53:37 +00:00	sensord_CSPRNG1
3	-rwx	965	Oct 8 2014 09:02:03 +00:00	lwapp_mm_mwar_hash.cfg
18	-rwx	56220	Oct 29 2014 11:53:46 +00:00	<b>event.log</b>
19	drwx	384	Oct 29 2014 11:56:45 +00:00	configs
4	-rwx	280	Oct 29 2014 11:56:40 +00:00	lwapp_officeextend.cfg
5	-rwx	75	Oct 29 2014 11:56:38 +00:00	capwap-saved-config
6	-rwx	126063	Oct 13 2014 16:16:45 +00:00	<b>event.r1</b>
7	-rwx	95008	Oct 29 2014 11:53:34 +00:00	lwapp_reap.cfg.bak
9	-rwx	50428	Oct 29 2014 12:01:57 +00:00	lwapp_non_apspecific_reap.cfg
8	-rwx	7192	Oct 29 2014 11:56:44 +00:00	private-multiple-fs
14	-rwx	95008	Oct 29 2014 11:56:52 +00:00	lwapp_reap.cfg
31	-rwx	60856	Oct 29 2014 11:52:32 +00:00	<b>event.capwap</b>
12	-rwx	359	Oct 29 2014 11:56:38 +00:00	env_vars

# AP Event log Example

```
Oct 29 11:52:22.723: %EVT-5-NTC_PROC: dot11_return_serving_channel:DFS Enable
Process: Dot11 driver
Oct 29 11:52:23.303: %CAPWAP-3-ERRORLOG: Retransmission count for packet exceeded max(CAPWAP_WTP_EVENT_REQUEST
., 4)
Oct 29 11:52:27.159: %EVT-5-NTC_PROC: dot11_set_rm_scan:DFS Disable
Process: Dot11 Offchannel PROCESS
Oct 29 11:52:27.563: %EVT-5-NTC_PROC: mh_driver_off_chnl_complete: to Channel 136 for d1
Process: Dot11 driver
Oct 29 11:52:27.563: %EVT-5-NTC_PROC: dot11_return_serving_channel: d1 Channel 40
Process: Dot11 driver
Oct 29 11:52:27.563: %EVT-5-NTC_PROC: dot11_return_serving_channel:DFS Enable
Process: Dot11 driver
Oct 29 11:52:32.415: %EVT-4-WRN: Write of flash:/event.capwap done
Oct 29 11:52:32.459: %LWAPP-3-CLIENTERRORLOG: Switching to Standalone mode
Oct 29 11:52:32.459: %CAPWAP-3-ERRORLOG: GOING BACK TO DISCOVER MODE
Oct 29 11:52:32.459: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.100.54:5246
Oct 29 11:52:32.527: %EVT-5-NTC: CAPWAP state change 5
Oct 29 11:52:42.531: %CAPWAP-3-ERRORLOG: Go join a capwap controller
Oct 29 11:48:18.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.252.56 peer_port: 5246
Oct 29 11:48:18.711: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.252.56 peer_port:
5246
Oct 29 11:48:18.711: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.252.56
```

**Reviewing the  
AP Event log  
can tell you  
much of what  
happened!**

# AP Join Troubleshooting - Takeaways

- Make sure your AP is getting an IP address (use CDP to verify)
- The AP out of the box will syslog to the broadcast address, you can use a syslog server on the same subnet to capture what the AP is doing
- Debugs are needed on the Controller to check where in the process the AP join is failing
- Make sure you have enabled the correct Country code for the AP's trying to Join
- Verify the Time and Date are correctly set on the Controller



# The AP Show Controller

# Show controller dX (X is the Radio Interface #)

```
# show controller dot11 0
```

```
!
```

```
interface Dot11Radio0
```

```
Radio EN 2.4GHz, Base Address 8478.ac99.53f0, BBlock version 0.00, Software version 4.18.2
```

```
Serial number: FOC16444LCU
```

```
Unused dynamic SDRAM memory: 0x0000C7C0 (49 KB)
```

```
Unused dynamic SDRAM memory: 0x000841E8 (528 KB)
```

```
Spectrum FW version: 1.15.2
```

```
Number of supported simultaneous BSSID on Dot11Radio0: 16
```

```
Carrier Set: Spain (ES) (-E)
```

```
Uniform Spreading Required: No
```

```
Configured Frequency: 2412 MHz Channel 1
```

```
Allowed Frequencies:
```

```
    2412( 1) 2417( 2) 2422( 3) 2427( 4) 2432( 5) 2437( 6) 2442( 7) 2447( 8)
2452( 9) 2457(10) 2462(11) 2467(12) 2472(13)
```

```
Listen Frequencies:
```

```
    2412( 1) 2417( 2) 2422( 3) 2427( 4) 2432( 5) 2437( 6) 2442( 7) 2447( 8)
2452( 9) 2457(10) 2462(11) 2467(12) 2472(13) 2484(14)
```

```
Beacon Flags: 0, Interface Flags 2020105, Interface Events 0, Mode 9; Beacons are enabled; Probes are enabled
```

0 – 802.11b/g/n

1 – 802.11a/n/ac

# Show controller dot11 X – What does it tell Us?

- Interface status

Beacon Flags: 0, Interface Flags 20105, Interface Events 0, Mode 9;  
Beacons are enabled; Probes are enabled

- Channel

Configured Frequency: 2412 MHz Channel 1

- QBSS

QBSS Load: 0x24

- TX Queues

Transmit queues: Limit 419 Current 20 In-Progress 20

# Show controller dot11 X – What does it tell Us?

- Driver blocks

Driver TX blocks: in use 0, high 0, at reset 0, fail 0 drop 0

- Authentications in progress

8021x auth in prog 0 allowed 0

- SSID client count

Vlan	BSSID	Clients	PSP	Pri	U/M	HT	Encr	Key0	Key1	Key2	Key3	SSIDs	MFP
0n	4450	0	0	0	0	0	0						
2	4451	1	0	0	3	3	0					imago	0
3	4452	2	0	0	3	3	0					setup-wifi	0
4	4453	3	5	1	3	3	0	204	128	x128		eduroam	0

- Radio Resets

Last radio reset code: 37

Radio resets - total:9 retries:0 failed:0

Reset Stats: Start Cnt: 6, Recovery: Cnt 0, Last Ret: 0, Fails: 0,

Recvry Status: Stalled NO, In Prog NO

Code/Count: 37/00006 1 62/00002 1 67/00001 0

# Show controller dot11 X – What does it tell Us?

- Queue status

```
----- Active ----- In-Progress ----- Counts -----
      Cnt  Quo  Bas  Max  Cl  Cnt  Quo  Bas      Sent  Discard  Fail      Retry  Multi
Uplink    0   64    0    0    0    0    5    0          0         0    0         0    0
Voice     0  512    0    0    0    0   60    0          0         0    0         0    0
Video     0 1024    0    0    0    0  200    0          0         0    0         0    0
Best      0 1024    0    0    0    0  200    0        6404         0    0         0    0
```

- Radio commands

```
Radio commands - total:126328 delayed:0 elapsed:0 timeouts:0 time high
00000000 low 00000000 usecs 00000000
```

# Show controller dot11 X – What does it tell Us?

## ■ Packets Stuck

### Packet Tx (in radio) Metrics

Max Stuck time:	Normal	MC	Off Channel
Stuck Cnt	Normal	MC	Off Channel
Paks > 30 Secs	0	0	0
Paks > 20 Secs	0	0	0
Paks > 15 Secs	0		
Paks > 10 Secs	0	0	0
Paks > 5 Secs	0		
Paks > 1 Secs	0	0	0

## ■ Beacon loss

### TXSM Beacon information:

Monitoring State: 1  
Flags: 00000000  
Beacons seen: 383143  
Time since: 0  
Max Time w/o beacons: 1747  
Beacon stopped count: 0  
Counts > 120 1  
Counts > 90 0  
Counts > 60 0  
Counts > 30 0  
Counts > 15 0  
Counts > 10 0

# Show controller dot11 X – What does it tell Us?

## ■ Stats

### RECEIVER

Host Rx K Bytes:	515595	/	1628
Unicasts Rx:	10	/	0
Unicasts to host:	10	/	0
Broadcasts Rx:	1511048	/	118
Beacons Rx:	1239980	/	96
Broadcasts to host:	1511048	/	118
Multicasts Rx:	0	/	0
Multicasts to host:	0	/	0
Mgmt Packets Rx:	271078	/	22
RTS received:	0	/	0
Duplicate frames:	0	/	0
CRC errors:	226797	/	0
WEP errors:	0	/	0
Buffer full:	0	/	0
Host buffer full:	0	/	0
Header CRC errors:	0	/	0
Invalid header:	0	/	0
Length invalid:	0	/	0
Incomplete fragments:	0	/	0
Rx Concats:	0	/	0
R2H Buffer full:	0	/	0

### TRANSMITTER

Host Tx K Bytes:	494	/	0
Unicasts Tx:	0	/	0
Unicasts by host:	0	/	0
Broadcasts Tx:	1	/	0
Beacons Tx:	1	/	0
Broadcasts by host:	0	/	0
Multicasts Tx:	6408	/	0
Multicasts by host:	6408	/	0
Mgmt Packets Tx:	0	/	0
RTS transmitted:	0	/	0
CTS not received:	0	/	0
Unicast Fragments Tx:	0	/	0
Retries:	0	/	0
Packets one retry:	0	/	0
Packets > 1 retry:	0	/	0
Protocol defers:	0	/	0
Energy detect defers:	0	/	0
Jammer detected:	0	/	0
Packets aged:	0	/	0
Tx Concats:	0	/	0

**We can tell  
the number  
of packets  
being sent  
or received  
and their  
type!**

# Client status as Seen by the AP

```
# show capwap client mn
```

```
CAPWAP mobile database
```

```
-----  
MAC                State                WLAN  Interface  
6073.5c7e.e002     CAPWAP_MN_ST_ADDED  1     Dot11Radio0
```

```
# show controller dot11 0 | b -Clients
```

```
---Clients 0  AID VLAN Status:S/I/B/A Age TxQ-R(A) Mode Enc Key  Rate  Mask Tx  Rx  
BVI  Split-ACL 6073.5c7e.e002  1  1 30 40004 000 0FA 297  0-0 (0) 33B0 200 0-10  
1EFFFF0000000000000000 0107 207 - - - - -  
6073.5c7e.e002      RxPkts KBytes  Dup Dec Mic Txc  TxPkts  KBytes  Retry RSSI SNR  
                      95      13      0  0  0  0      54      3      8    12  86
```



# Client status as Seen by the AP

## # show capwap reap association

```
Address      : 001d.4546.a204      Name      : NONE
IP Address   : 0.0.0.0              IPv6 Address : ::
Gateway Address : 0.0.0.0
Netmask Address : 0.0.0.0          Interface   : Dot11Radio 0
Bridge-group  : 0
reap_flags_1  : 0x0                ip_learn_type : 0x0          transient_static_ip : 0x0
Device       : WGB-client          Software Version : NONE
CCX Version   : NONE              Client MFP      : Off
```

```
State        : Assoc              Parent      : 6073.5c7e.e002
SSID         : wgb-roamer
WLAN         : 1
Hops to Infra : 0
Clients Associated: 0              Repeaters associated: 0
11w Status   : Off
REAP Data Switching: Local
```

```
Address      : 6073.5c7e.e002      Name      : wgb2600-sw2-4
IP Address   : 0.0.0.0              IPv6 Address : ::
Gateway Address : 0.0.0.0
Netmask Address : 0.0.0.0          Interface   : Dot11Radio 0
Bridge-group  : 4
reap_flags_1  : 0x0                ip_learn_type : 0x0          transient_static_ip : 0x0
Device       : WGB                Software Version : NONE
```

# Other AP info

- Show Interface

# **show interface dot11 0**

**Dot11Radio0 is up, line protocol is up**

Hardware is 802.11N 2.4GHz Radio, address is 6073.5c7e.e002 (bia 34a8.4e70.1b40)

MTU 1500 bytes, BW 54000 Kbit/sec, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

ARP type: ARPA, ARP Timeout 04:00:00

Last input never, output 00:00:00, output hang never

Last clearing of "show interface" counters never

**Input queue: 0/18174/103037/0 (size/max/drops/flushes); Total output drops: 79722**

Queueing strategy: fifo

Output queue: 0/30 (size/max)


5 minute input rate 2000 bits/sec, 7 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

# Mobility

# Mobility - Types

- Legacy – Flat
  - Old style
  - Discriminator is the mobility group name
- New – Hierarchical
  - For 7.5+ and Converged access
  - Supports large setups, multiple device roles

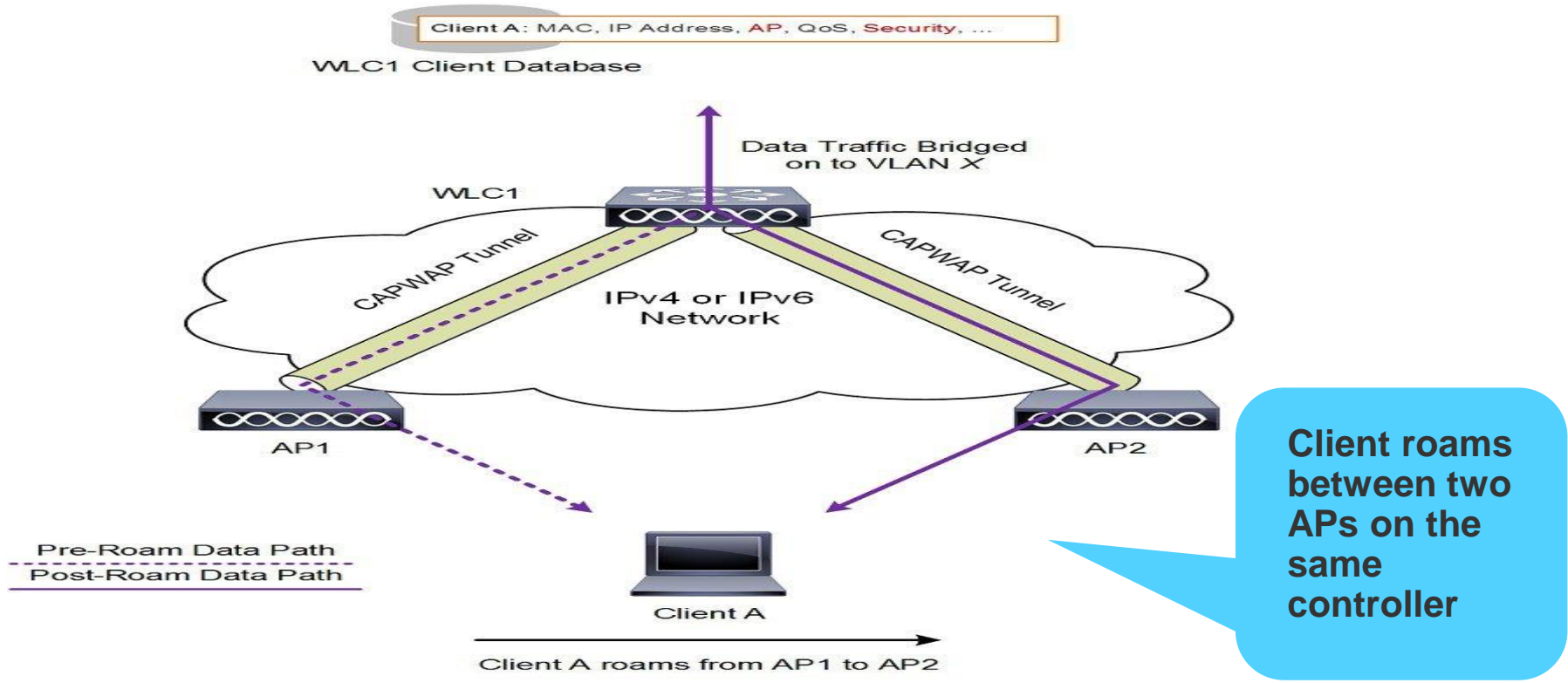


**Stay with Legacy  
unless you are  
needing to use  
Converged Access  
Setups**

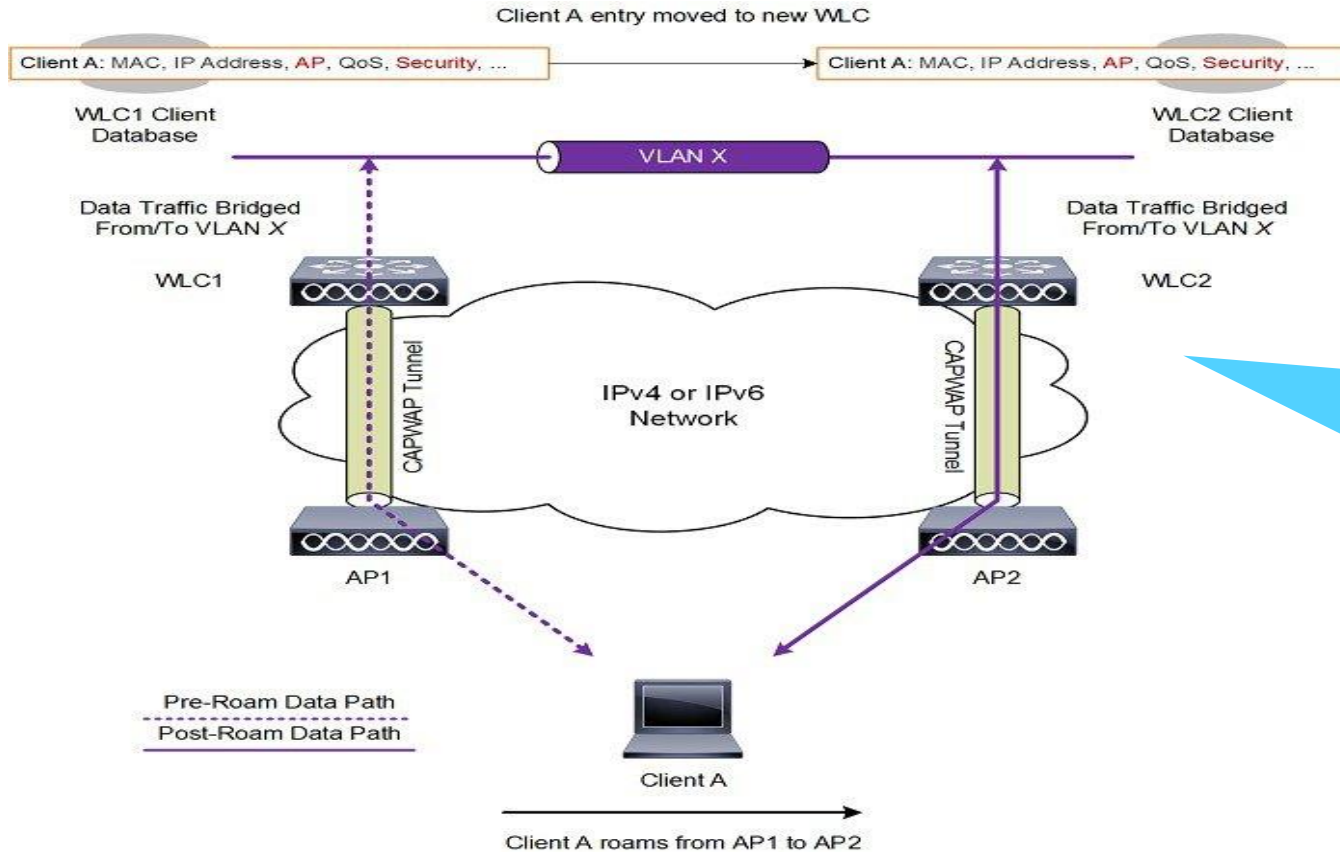
# Mobility - Messaging Flow

- When a client connects to a WLC for the first time, the following happens:
  - New WLC sends MOBILE\_ANNOUNCE to all controllers in the mobility group when client connects (note: if possible, configure multicast mobility to lower CPU load and handoff times)
  - Old WLC sends HANDOFF\_REQUEST, telling the new WLC **I have an entry for this client, here is the client status**
  - New WLC sends HANDOFF\_REPLY, telling the old WLC **OK**

# Mobility - Intra-Controller

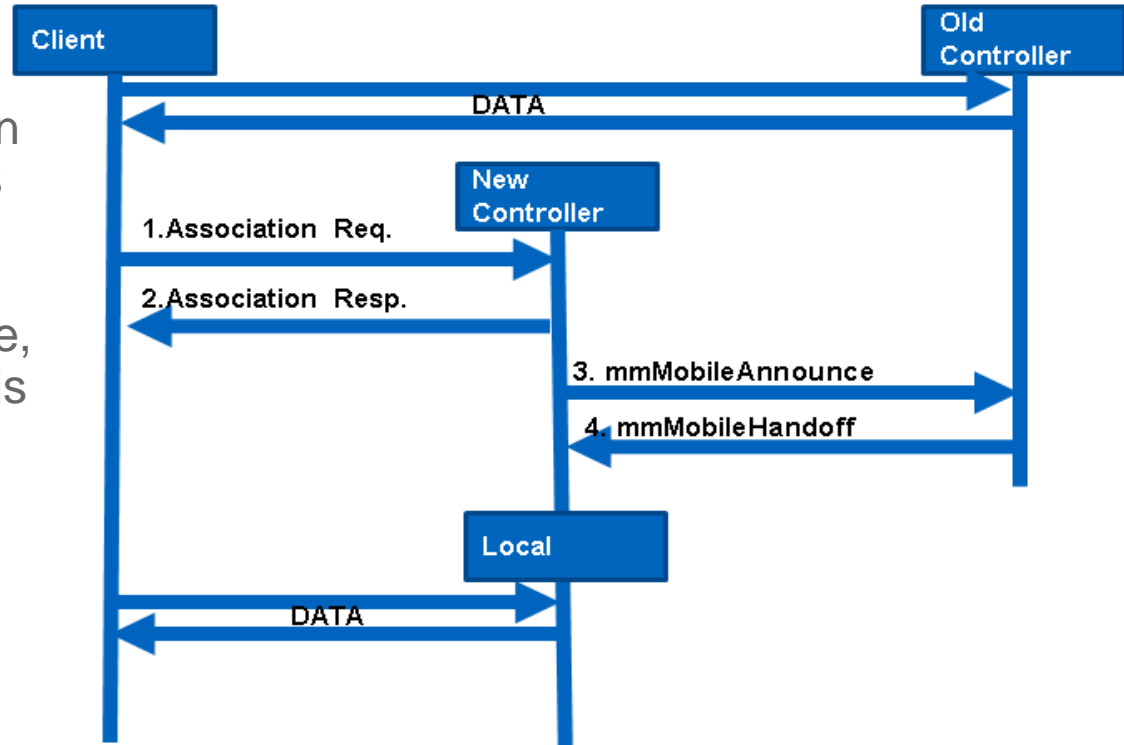


# Mobility - Inter-Controller (Layer 2)



# What's Layer 2 roaming

- Layer 2 roaming occurs when you move between WLCs and both WLCs have connectivity to the same client subnets. In this case, the client database entry is simply moved to the new WLC.





# Mobility - Layer 2 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

## MobileAnnounce

Mobility packet received from:  
10.10.1.5, port 16666  
type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 71 seq: 118 len 116 flags 0  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC: , IP: 0.0.0.0, instance: 0  
VLAN IP: 10.10.3.5, netmask: 255.255.255.0  
Switch IP: 10.10.1.5

Handoff as Local, Client IP: 10.10.3.235 Anchor IP: 0.0.0.0  
Anchor Mac : 00.00.00.00.00.00

## MobileHandoff

Mobility packet sent to:  
10.10.1.5, port 16666  
type: 5(MobileHandoff) subtype: 0 version: 1 xid: 71 seq: 99 len 546 flags 0  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC: , IP: 10.10.3.235, instance: 0  
VLAN IP: 10.10.3.4, netmask: 255.255.255.0

10.10.3.235 8021X\_REQD (3) State Update from Mobility-Complete to Mobility-Incomplete.....  
Mobile associated with another AP elsewhere, delete mobile  
10.10.3.235 8021X\_REQD (3) mobility role update request from Local to Handoff  
Peer = 0.0.0.0, Old Anchor = 10.10.1.4, New Anchor = 0.0.0.0  
Clearing Address 10.10.3.235 on mobile  
apfMmProcessDeleteMobile (apf mm.c:548) Expiring Mobile!

0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE  
Mobility query, PEM State: L2AUTHCOMPLETE

Mobility packet sent to:  
10.10.1.4, port 16666  
type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 71 seq: 118 len 116 flags 0  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC: , IP: 0.0.0.0, instance: 0  
VLAN IP: 10.10.3.5, netmask: 255.255.255.0  
.....  
0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state DHCP\_REQD (7)  
0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0  
.....

Mobility packet received from:  
10.10.1.4, port 16666  
type: 5(MobileHandoff) subtype: 0 version: 1 xid: 71 seq: 99 len 546 flags 0  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC: , IP: 10.10.3.235, instance: 0  
VLAN IP: 10.10.3.4, netmask: 255.255.255.0  
Switch IP: 10.10.1.4

Mobility handoff, NAC State Download ( Client's NAC OOB State : Access, Quarantine)  
Mobility handoff for client:  
Ip: 10.10.3.235  
Anchor IP: 0.0.0.0, Peer IP: 10.10.1.4

10.10.3.235 DHCP\_REQD (7) Change state to RUN (20) last state RUN (20)  
.....  
10.10.3.235 RUN (20) mobility role update request from Unassociated to Local  
= 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5  
10.10.3.235 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete,  
.....  
10.10.3.235 Added NPU entry of type 1, dtlFlags 0x0

## Mobility - Inter-Controller (Layer 3)

- Layer 3 roaming (a.k.a. **anchor/foreign**)

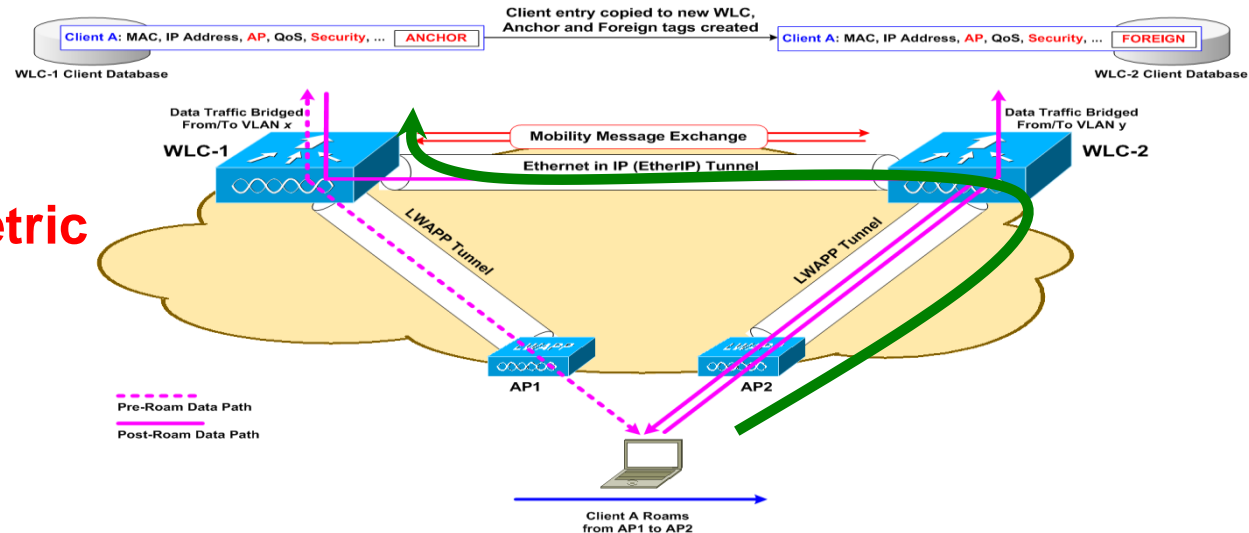
- Dual client ownership
- Foreign owns “L2”: 802.1x, encryption, AP
- Anchor owns “L3”: IP address, webauth

- Two main types

- Auto anchor
- Dynamic

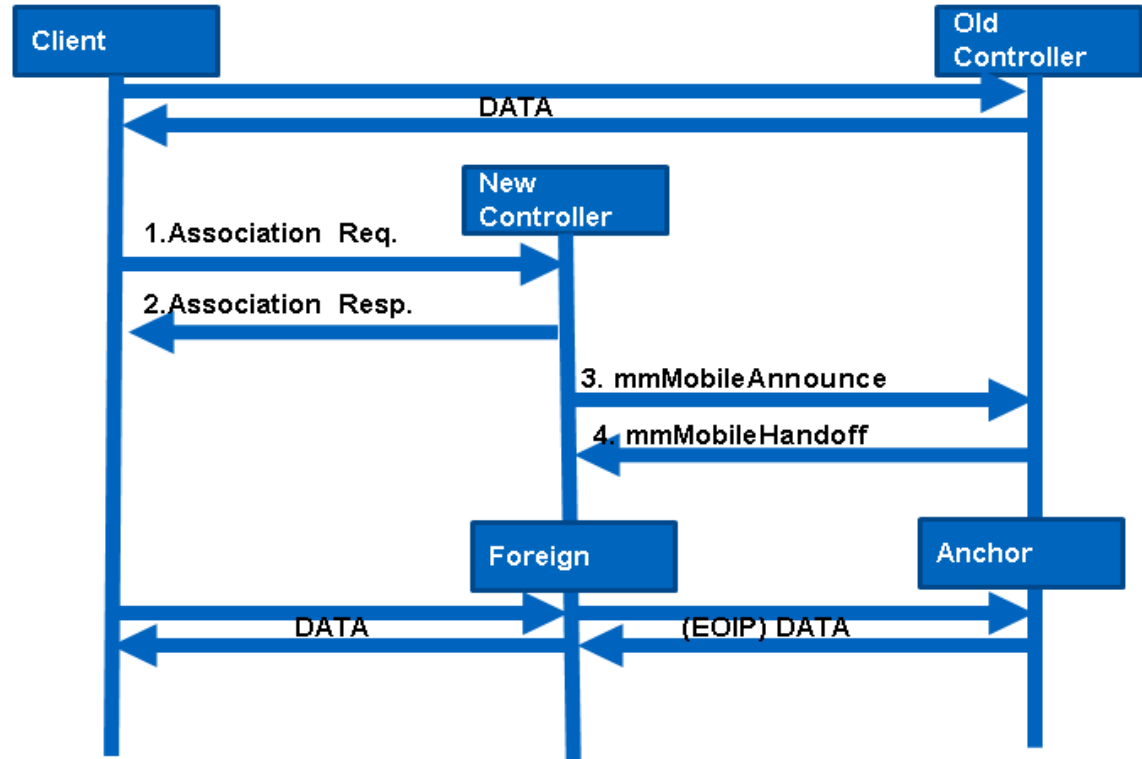
- We have a Symmetric traffic path

## Typically used for Guest Anchoring of Clients



# What's Layer 3 Roaming

- Layer 3 roams occur when the controllers do not have matching VLANs, so we have to tunnel the traffic back to the original controller, so the client session is not interrupted. This tunnel is an Ethernet-over-IP tunnel (EoIP), and in 7.3 and later WLC code it can be configured to be a CAPWAP tunnel (new mobility)



# Mobility - Layer 3 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

**MobileAnnounce**

Mobility packet received from:  
10.10.1.4, port 16666  
type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 177 seq: 180  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC:, IP: 0.0.0.0, instance: 0  
VLAN IP: 10.10.3.4, netmask: 255.255.255.0  
~~Switch IP: 10.10.1.5~~  
Handoff as Local, Client IP: 10.10.1.103 Anchor IP: 10.10.1.5  
Anchor Mac : f8.66.f2.fa.a8.40

Mobility packet sent to:  
10.10.1.4, port 16666  
type: 5(MobileHandoff) subtype: 0 version: 1 xid: 177 seq: 204 len 546  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC:, IP: 10.10.1.103, instance: 0  
VLAN IP: 10.10.1.5, netmask: 255.255.255.0

10.10.1.103 RUN (20) State Update from Mobility-Complete to Mobility-In-  
Updated location for station old AP 00:16:9c:4b:c4:c0, new AP 00:00:00:00:00:00  
10.10.1.103 RUN (20) mobility role update request from Local to Anchor  
Peer = 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5

0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE  
Mobility packet sent to:  
10.10.1.5, port 16666  
type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 177 seq: 180 len 116  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC:, IP: 0.0.0.0, instance: 0  
VLAN IP: 10.10.3.4, netmask: 255.255.255.0

Mobility packet received from:  
10.10.1.5, port 16666  
type: 5(MobileHandoff) subtype: 0 version: 1 xid: 177 seq: 204 len 546  
group id: b9ae3d89 9e4b49a5 ec945669 6ad03857  
mobile MAC:, IP: 10.10.1.103, instance: 0  
VLAN IP: 10.10.1.5, netmask: 255.255.255.0  
Switch IP: 10.10.1.5  
Mobility handoff, NAC State Payload [ Client's NAC OOB State : Access, Quarantined ]  
Mobility handoff for client:  
Ip: 10.10.1.103  
Anchor IP: 10.10.1.5, Peer IP: 10.10.1.5

0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state DHCP\_REQD (7)  
10.10.1.103 DHCP\_REQD (7) Change state to RUN (20) last state RUN (20)  
10.10.1.103 RUN (20) Reached PLUMBFASSTPATH: from line 5273  
10.10.1.103 RUN (20) Change state to RUN (20) last state RUN (20)  
Assigning Address 10.10.1.103 to mobile  
Handoff confirm: Pre Handoff PEM State: RUN  
10.10.1.103 RUN (20) mobility role update request from Unassociated to Foreign  
Peer = 10.10.1.5, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5

# Mobility Group vs. Mobility Domain

- Mobility Group - WLCs with the same group name

- L2/L3 Handoff
- Auto Anchoring
- **Fast Secure Roaming**

- APs get all of these as a Discover candidate

Local Mobility Group		group			
MAC Address	IP Address	Group Name	Multicast IP	Status	
f8:66:f2:fa:a8:40	10.10.1.5	group	0.0.0.0	Up	
88:43:e1:31:6e:80	10.10.1.4	group	0.0.0.0	Up	

- Mobility Domain - WLCs in the mobility list

- L2/L3 Handoff
- Auto Anchoring

Local Mobility Group		group			
MAC Address	IP Address	Group Name	Multicast IP	Status	
f8:66:f2:fa:a8:40	10.10.1.5	group	0.0.0.0	Up	
88:43:e1:31:6e:80	10.10.1.4	domain	0.0.0.0	Up	

# Mobility - Typical Problems

- Misconfiguration

- Wrong policy set (WLAN's between the two controller are too different)

```
*mmListen: Jan 03 12:03:36.613: 68:7f:74:75:f1:cd Adding mobile on Remote AP  
00:00:00:00:00:00(0)
```

```
*mmListen: Jan 03 12:03:36.613: 68:7f:74:75:f1:cd mmAnchorExportRcv:, Mobility role is Unassoc
```

```
*mmListen: Jan 03 12:03:36.614: 68:7f:74:75:f1:cd mmAnchorExportRcv Ssid=webauth Security  
Policy=0x2050
```

```
*mmListen: Jan 03 12:03:36.614: 68:7f:74:75:f1:cd mmAnchorExportRcv: WLAN webauth policy  
mismatch between controllers, WLAN webauth not found, or WLAN disabled. Ignore ExportAnchor  
mobility msg. Delete client.
```

- Wrong IP/MAC/Mobility name setup in the Controller Mobility Table

# Tools of Trade

# Troubleshooting Tools

- Wireless Sniffer
  - Examples: OmniPeek, Apple MAC running OSX 10.6 or above (10.11 Best)
  - Wireshark without special drivers will not capture raw frames....
- Wired Packet Capture
- Spectrum Analyzer
  - Spectrum Expert with Card or Clean-Air AP
- The “Debug client”
- AP Packet Capture
- Local HTTP Proxy
  - Example: Fiddler



# Troubleshooting Tools - When to use What?

- Wireless Sniffer
  - Interaction between client and AP at the 802.11 level
  - Interoperability issues
  - Roaming
  - Performance problems
  - Failed Authentication
- Wired Packet Capture
  - At AP, WLC, Server ports, for performance problems
  - CAPWAP issues
  - Flexconnect issues (ACL, local switch, webauth, etc)
  - Packet loss
  - Fragmentation

# Troubleshooting Tools - When to use What?

- AP Capture
  - Authentication
  - Webauth
  - Voice
- Spectrum Capture
  - Performance/High Packet Error Rate
  - Radar
- Local HTTPS Proxy
  - Webauth
- Combined (AP + WLC + Wireless)
  - Packet loss
  - AP Join

# Tips for Successful Wireless Packet Capture

- Type is important
  - 11ac/11n/etc
  - Multichannel for roaming
  - 1SS/2SS/3SS
- Location is important
  - Roaming issues -> Near Client
- Time is important
  - 1 second difference can be 20,000 frames later
- Roaming
  - One capture per channel
  - Use either Aps or USBs

# Key things to remember

# Key “Takeaways”

## Troubleshooting

- ✓ Proper problem description
- ✓ Divide and conquer: during a problem isolate on which client state is happening
- ✓ Know how to reproduce the problem
- ✓ Understanding is key: working vs non working scenarios
- ✓ Have the Data, Client Debug, Type of Client, Controller version, AP type, Flex vs Local

# Questions?

# Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a \$750 Amazon gift card.
- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on [CiscoLive.com/us](https://CiscoLive.com/us).



Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at [CiscoLive.com/Online](https://CiscoLive.com/Online)

# Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions



# Thank you



**Cisco** *live!*

July 10-14, 2016 • Las Vegas, NV

# Wireless Cisco Education Offerings

Course	Description	Cisco Certification
<ul style="list-style-type: none"> <li>Designing Cisco Wireless Enterprise Networks</li> <li>Deploying Cisco Wireless Enterprise Networks</li> <li>Troubleshooting Cisco Wireless Enterprise Networks</li> <li>Securing Cisco Wireless Enterprise Networks</li> </ul>	Professional level instructor led trainings to prepare candidates to conduct site surveys, implement, configure and support APs and controllers in converged Enterprise networks. Focused on 802.11 and related technologies to design, deploy, troubleshoot as well as secure Wireless infrastructure. Course also provide details around Cisco mobility services Engine, Prime Infrastructure and wireless security.	CCNP® Wireless Version 3.0 (Available March 22 <sup>nd</sup> , 2016)
Implementing Cisco Unified Wireless Network Essential	Prepares candidates to design, install, configure, monitor and conduct basic troubleshooting tasks of a Cisco WLAN in Enterprise installations.	CCNA® Wireless (Available Now)
Deploying Basic Cisco Wireless LANs (WDBWL)	Understanding of the Cisco Unified Wireless Networking for enterprise deployment scenarios. In this course, you will learn the basics of how to install, configure, operate, and maintain a wireless network, both as an add-on to an existing wireless LAN (WLAN) and as a new Cisco Unified Wireless Networking solution.	1.2
Deploying Advanced Cisco Wireless LANs (WDAWL)	The WDAWL advanced course is designed with the goal of providing learners with the knowledge and skills to successfully plan, install, configure, troubleshoot, monitor, and maintain advanced Cisco wireless LAN solutions such as QoS, “salt and pepper” mobility, high density deployments, and outdoor mesh deployments in an enterprise customer environment.	1.2
Deploying Cisco Connected Mobile Experiences (WCMX)	WCMX will prepare professionals to use the Cisco Unified Wireless Network to configure, administer, manage, troubleshoot, and optimize utilization of mobile content while gaining meaningful client analytics.	2.0

For more details, please visit: <http://learningnetwork.cisco.com>

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)