Cisco live!

6-9 March 2018 · Melbourne, Australia

Advanced Troubleshooting of Wireless LANs

Ishant Varshney - Team Lead – Wireless

CCIE-Wireless # 46457

BRKEWN-3011

Cisco live!

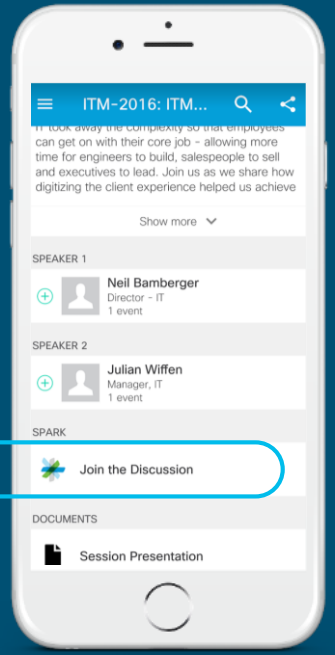
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

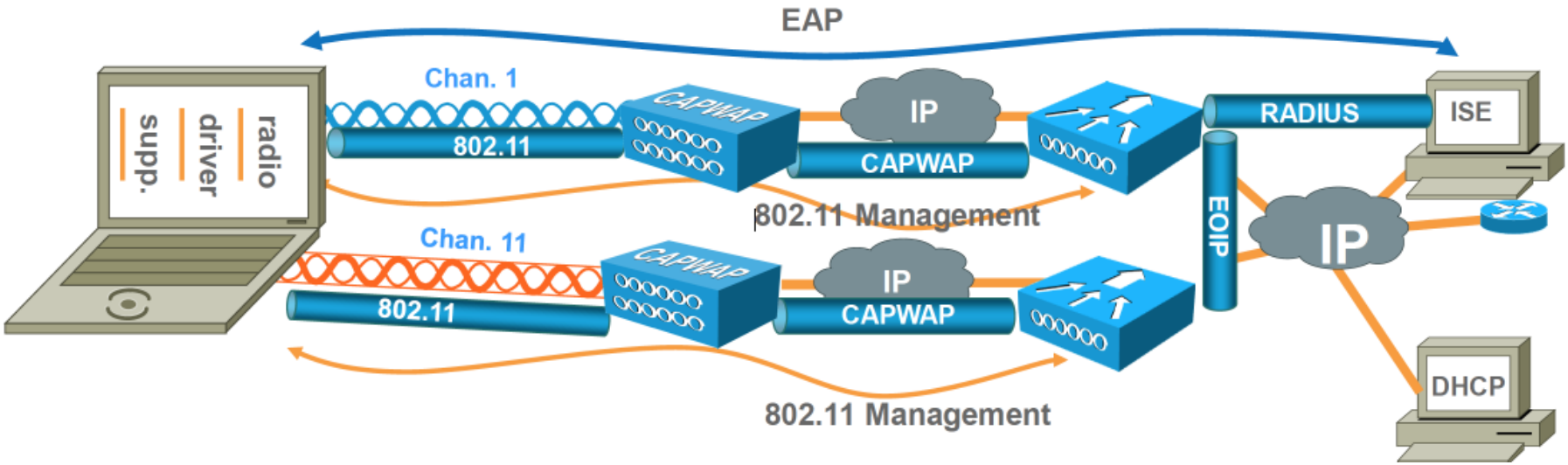
How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wireless – A complex world



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- How things work
- What to check when it breaks
- How to Fix it
- Q & A

Software and Support

Software and Support

Cisco Support Model - Expectations

- **What to expect from TAC**

  - ✓ Configuration assistance
  - ✓ Problem analysis / bug isolation
  - ✓ Workarounds or fixes
  - ✓ Action plan to resolve SR
  - ✓ Hardware replacement
  - ✓ Engage BU when appropriate

What not to expect from TAC

- ❖ Design and deployment
- ❖ Complete configuration
- ❖ Sales related information
- ❖ RF tuning
- ❖ Feature requests

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Software and Support

Opening a TAC Service Request

- What should I have ready?
  - Clear problem description
  - Always: **Show run-config**
  - If client involved, always: **debug client <mac address>**
  - Your analysis of any data provided
  - Set clear expectation of timeline and severity

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Software and Support

Opening a TAC Service Request

- Have at hand:
  - Show run-config
  - Clear problem description
  - Problem reproduction if known
- Client issues
  - Debug client <mac-address>
- Crash AP
  - Show tech (from the AP)
  - Crash file (transfer upload…)
- Crash WLC
  - Crash file and if possible , Core dump

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Question

- **How to get crash file out of standby box??**

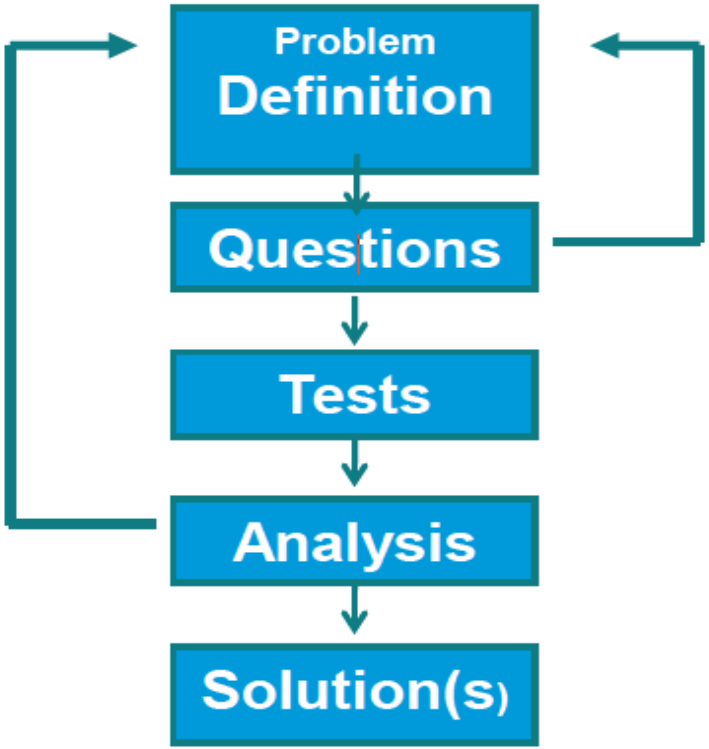
transfer upload peer-start

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Methodology

Troubleshooting Basics

- Troubleshooting 101
  - Clearly define the problem
  - Understand any possible triggers
  - Know the expected behaviour
  - Reproducibility
  - Do not jump to conclusions



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Basics

- Troubleshooting is an art with no right or wrong procedure, but best with a logical methodology.
- Step 1: Define the problem
  - Bad description: “Client slow to connect”
  - Good description: “Client associations are rejected with Status17 several times before they associate successfully.”
  - Reduce Scope!
  - Isolate multiple possible problems over same setup
- Refer: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107457-load-balancing-wlc.html

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Basics

- Step 2: Understand any possible triggers
  - If something previously worked but no longer works, there should be an identifiable trigger
  - Understanding any and all configuration or environmental changes could help pinpoint a trigger
  - Finding a pattern may help with root cause isolation
- Step 3: Know the expected behaviour
  - If you know the order of expected behaviour that is failing, defining where the behaviour breaks down (Problem Description) is better than defining the end result.
  - Example: “One way audio between Phone A and B, because Phone A does not get an ARP Response for Phone B”

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Basics

- Step 4: Reproducibility
  - Any problem that has a known procedure to reproduce (or frequently randomly occurs) should be easier to diagnose
  - Being able to easily validate or disprove a potential solution saves time by being able to quickly move on to the next theory
  - If the problem can be reproduced, it makes things much easier to work with development, test the fix and deliver with lower impact to the end customer
  - Tests will be conducted to isolate the root cause
- Step 5: Fix
  - Validate Root Cause Analysis
  - Develop Fix
  - Test for solution, intersection

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Useful Troubleshooting Tools

- Wireless Sniffer
  - Example: Linksys USB600N with Omnipeek
  - TAC can publish Omnipeek-Remote Assistant if you have compatible HW
  - Windows 7 with Netmon3.4 https://supportforums.cisco.com/docs/DOC-16398
  - Mac OS X 10.6+ https://supportforums.cisco.com/docs/DOC-19212
  - NOTE: Wireshark running on a PC is not able to capture a promiscuous Wireless trace
  - AP on Sniffer mode

- Wired Packet Capture
  - Example: Wireshark
    - Use for spanned switch ports of AP/WLC or client side data

- Spectrum Analyser
  - Spectrum Expert with Card or Clean-Air AP

- Debug client

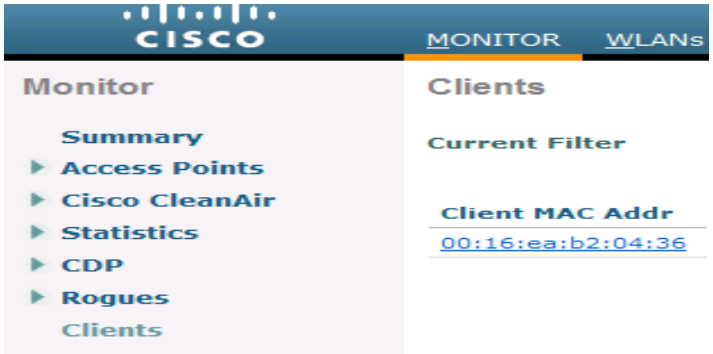
- AP Packet Capture

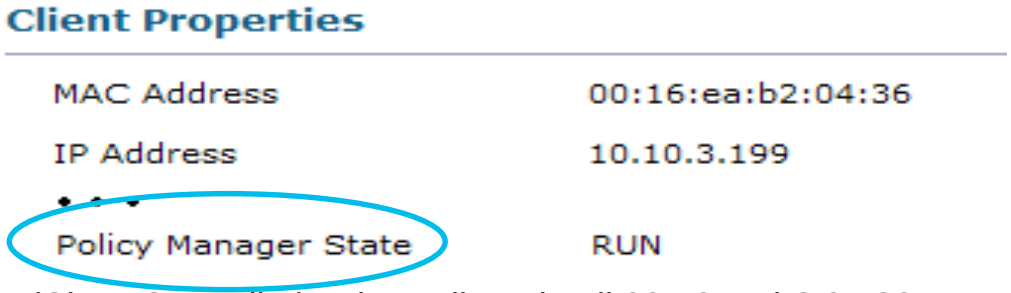
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Troubleshooting - Local

Understanding the Client 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



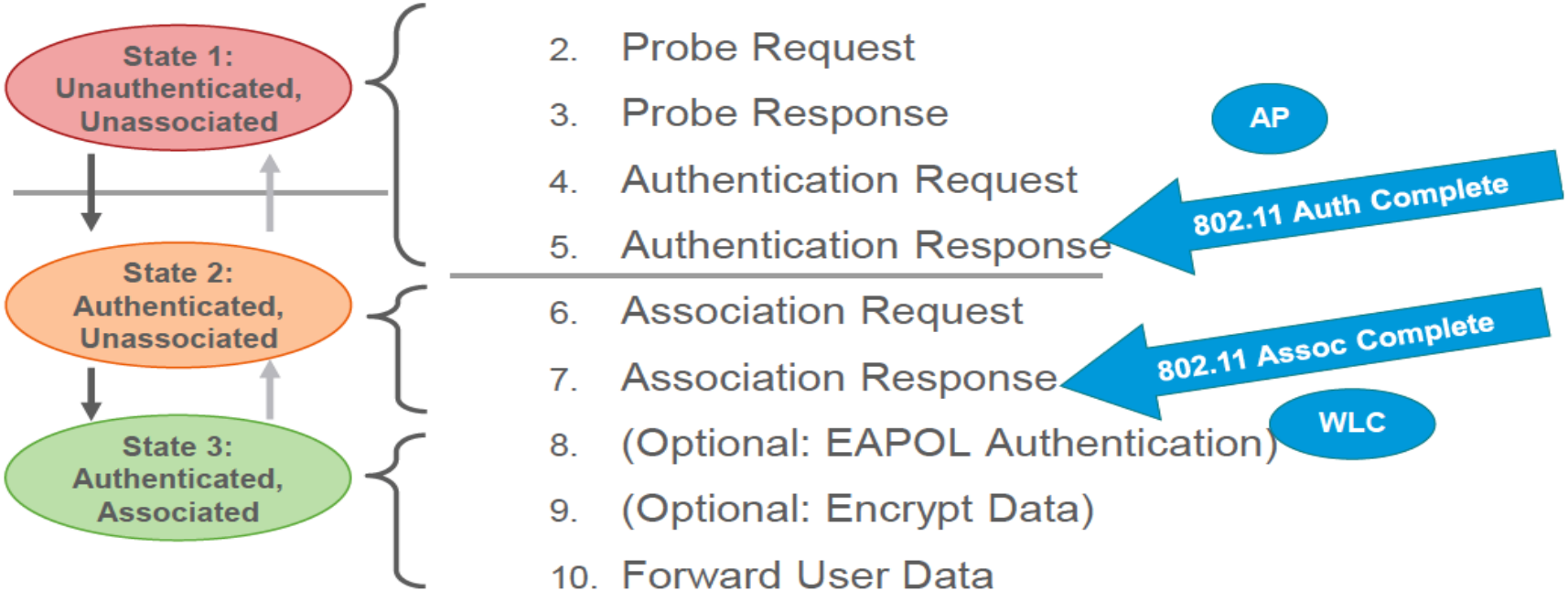


(Cisco Controller) >show client detail 00:16:ea:b2:04:36
Client MAC Address..... 00:16:ea:b2:04:36
....
Policy Manager State..... WEBAUTH_REQD

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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Steps to Building an 802.11 Connection



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Question

- **Is this always true ??**

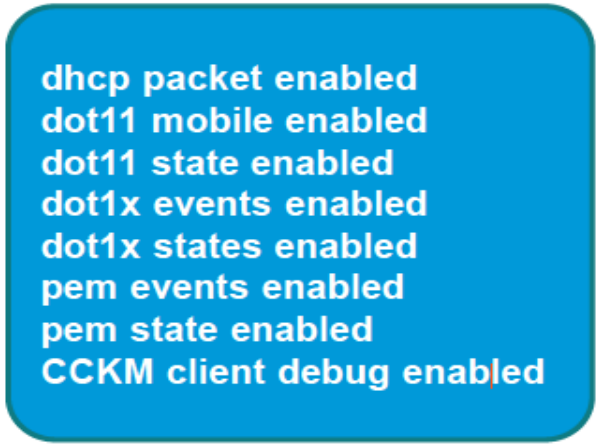
NO --- If AP is Flex Mode ..initial association is handled by AP

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Client Debug

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

- (Cisco Controller) >**debug client 00:16:EA:B2:04:36**
- (Cisco Controller) >show debug
- MAC address 00:16:ea:b2:04:36
- Up to 3 addresses in 7.2
- Up to 10 in 7.3 and higher



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs

On the WLC: **debug client <MAC Address>**

debug aaa events/errors enable

debug dot1x all enable

debug web-auth redirect enable mac <client mac address> (~Webauth)

debug mdns all enable (~Bonjour)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs

On IOS AP: **debug dot11 <do0/do1> monitor addr<client mac address>**

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

debug dot11 wpa-cckm-km-dot1x

debug dot11 events

debug capwap client mgmt

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State:

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Association

*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 -vlan50, interface id 14, interface 'vlan50'

processSsidIE statusCodeis 0 and status is 0

processSsidIE ssid_done_flagis 0 finish_flagis 0

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

suppRatesstatusCodeis 0 and gotSuppRatesElementis 1

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

extSuppRates status Code is 0 and gotExtSuppRates Element 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)

Rate – 128 by 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

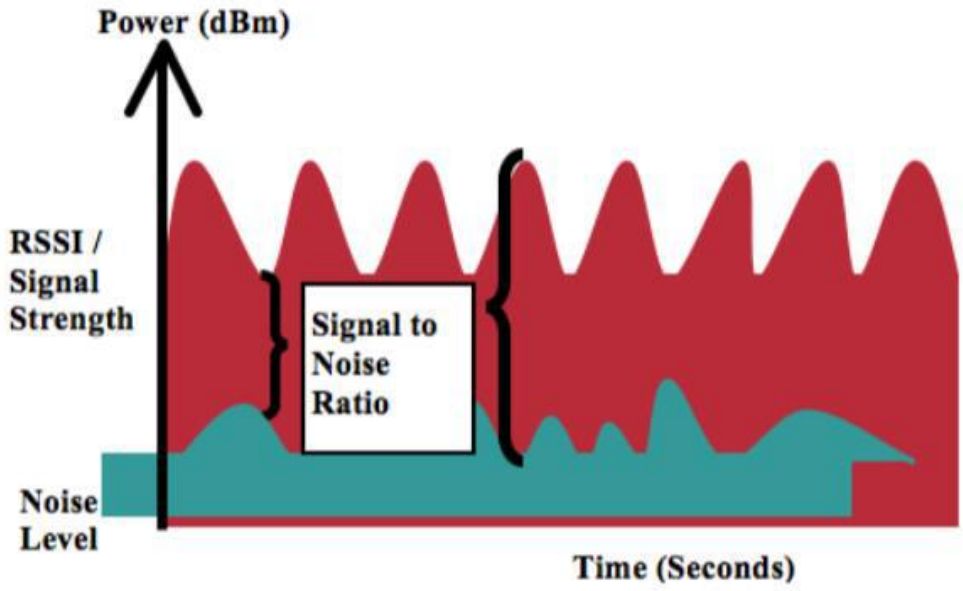
*apfMsConnTask_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 Sending Assoc Response to station on BSSID 00:3a:9a:a8:ac:d2 (status 0) ApVapId3 Slot 0

*apfMsConnTask_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 apfProcessAssocReq(apf_80211.c:7975) Changing state for mobile 00:1c:58:8e:a5:84 on AP 00:3a:9a:a8:ac:d0 from Associated to Associated

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Validating Signal Strength

- For Real-Time applications (Voice, Video) the recommendation is to have at least a **25 dB** Signal-to-noise ratio (SNR)
- Using a standard noise floor of -92 dBm, a 25 dB SNR gives us a Received Signal Strength Indicator (RSSI) of **-67 dBm**
- Many tools available to validate proper RSSI and SNR for desired coverage area



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

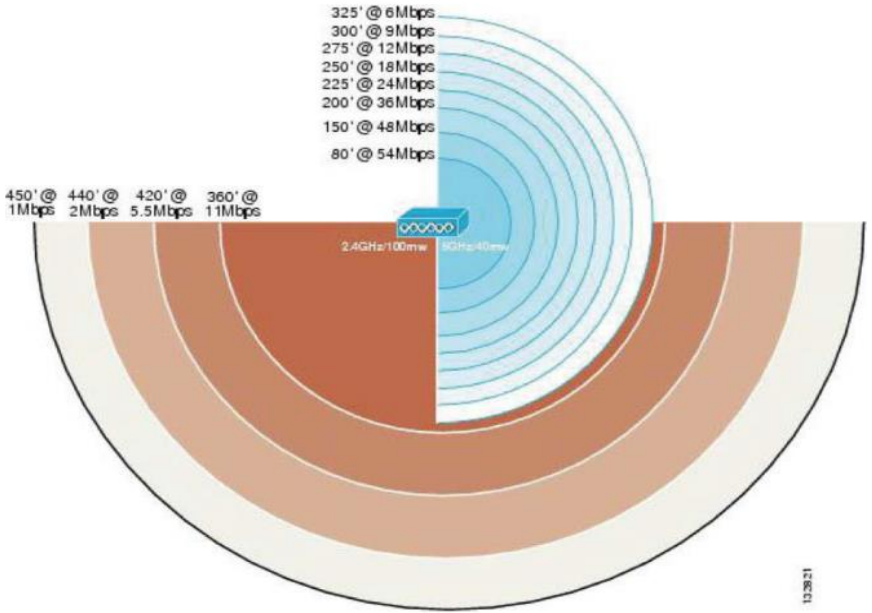
How Many SSIDs Do We Need?

- Every SSID will need to send a beacon frame every 100 ms, which can eat up a lot of channel utilisation.
- Limit the number of SSIDs whenever possible

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Rates

- Data rates have a direct relationship with effective cell size. Lower data rates reduce performance, so it is desired to disable 802.11b data rates, and often anything under 12 mbps
- Reducing the cell size will ensure that devices transmit more efficiently, increasing available throughput



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Association - Roaming

```
*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 -vlan50, interface id 14, interface
'vlan50'
processSsidIE statusCode is 0 and status is 0
processSsidIEv ssid_done_flagis 0 finish_flag is 0
STA -rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
suppRatesstatusCode 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 status Code 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Association – AAA Filter Failed

```
*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 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  -- A Timer is attached to each state.
*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 AssocResponse to station
on BSSID 00:17:0e:aa:46:30 (status 1) ApVapId4 Slot 0
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Association - 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Got a Client, But No 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: 39:c4:eb:dd:1b:00 aggregated probe IE elmId=221, elm_len=9, dataLen=127
*apfProbeThread: Jan 03 07:59:30.738: aggregated probe IE: TIMESTAMP
*apfProbeThread: Jan 03 07:59:30.738: 00:1a:70:35:84:d6 aggregated probe IE elmId=221, elm_len=27, dataLen=116
*apfProbeThread: Jan 03 07:59:30.738: 00:1a:70:35:84:d6 aggregated probe IE: AGGR PROBE
*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]=
```

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

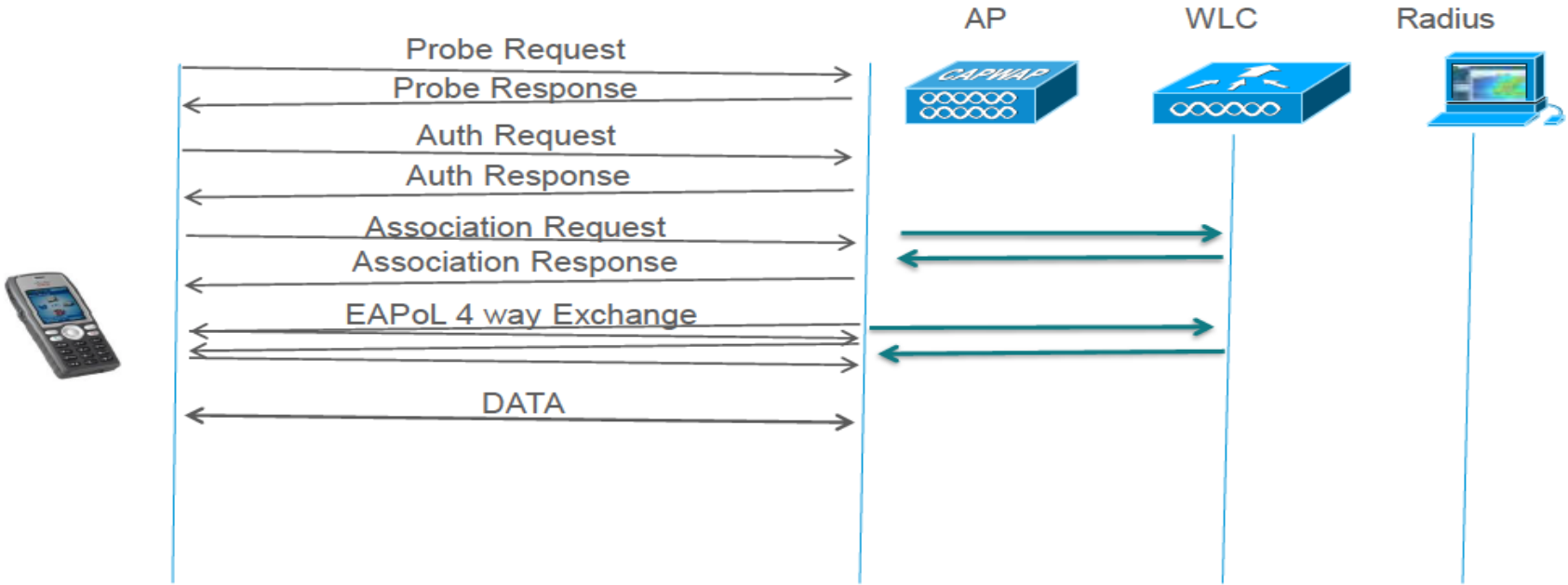
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State:

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSK Authentication



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSK - Successful

*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 Authstate
*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 00.00.00.00.00.00.00.00
*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 00.00.00.00.00.00.00.01
*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)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Flexconnect Debugs

REAP Mgmt: FR_SM: dot11_mgmt_smact_lwapp_fast_roam(): a088.b41f.cb24 :: INIT (FAST_ROAM, 0x0) -> PMKID_VALIDATED

REAP Mgmt: dot11_lwapp_fr_sm_before_4way_add_to_drv(): a088.b41f.cb24 : PMK Validated, before 4way handshake adding client to driver, reap_flags0x800

REAP Mgmt: dot11_lwapp_fr_sm_start_4way_hs():client a088.b41f.cb24 : Starting WPAv2 4way handshake

dot11_mgr_sm_send_wpav2_ptk_msg1: [1] Sent PTK msg1 to a088.b41f.cb24, no timer set

dot11_dot1x_verify_ptk_handshake: verifying PTK msg2 from a088.b41f.cb24

dot11_dot1x_build_ptk_handshake: building PTK msg3 for a088.b41f.cb24

dot11_mgr_disp_client_send_eapol: sending eapolto client a088.b41f.cb24 on BSSID a89d.2131.be2f

dot11_mgr_sm_send_wpav2_ptk_msg3: [1] Sent PTK msg3 to a088.b41f.cb24, no timer set

dot11_dot1x_verify_ptk_handshake: verifying PTK msg4from a088.b41f.cb24

REAP Mgmt: FR_SM: dot11_mgmt_lwapp_aaa_resp(): a088.b41f.cb24 :: 4WAY_HS_STARTED (AAA_SUCCESS_RSP, 0x0) -> AUTHENTICATED

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSK – Wrong Secret

***Dot1x_NW_MsgTask_7: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Starting key exchange to mobile00:40:96: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 cl;d*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 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 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 00:40:96:b5:db:d7 version 2**

***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 deauthcount 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**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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**

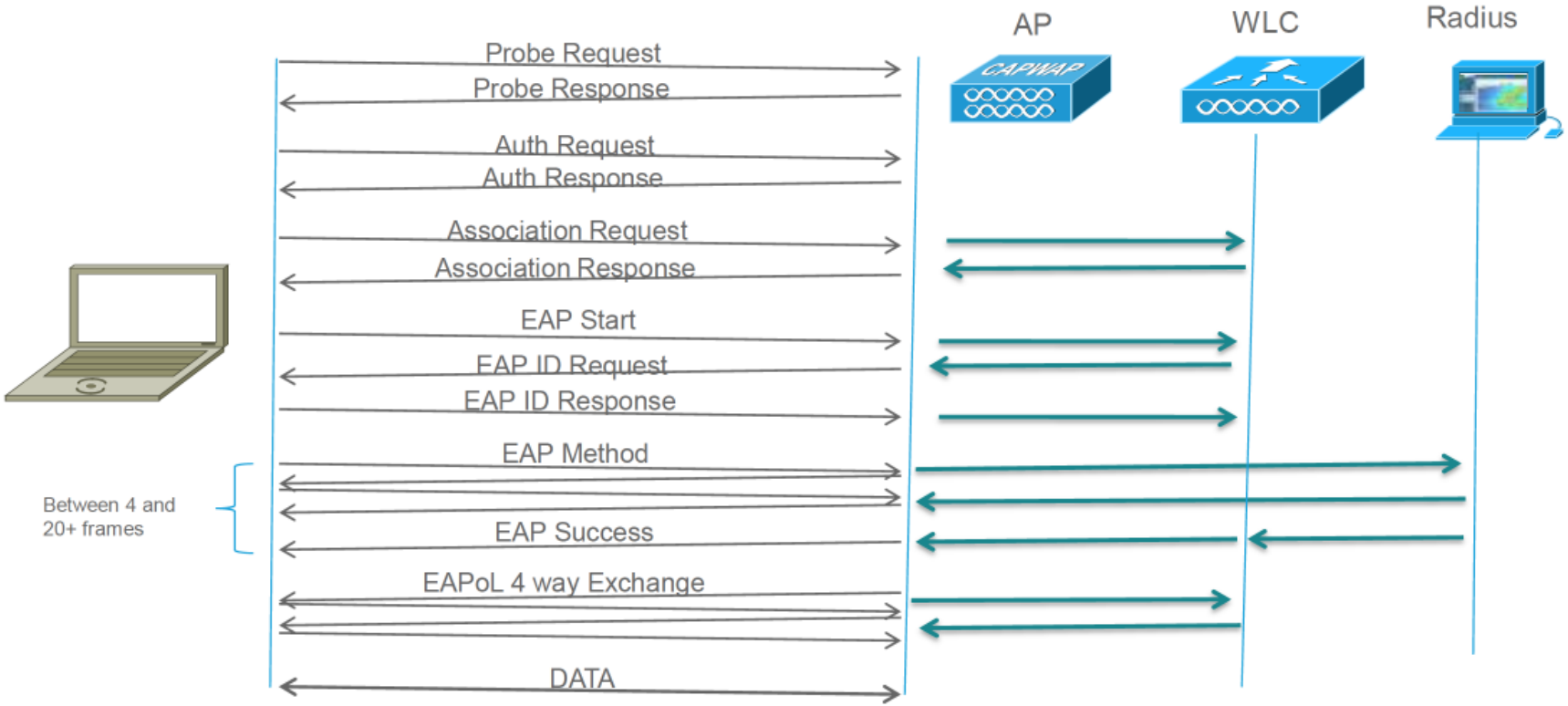
***dot1xMsgTask: Jan 02 11:19:56.190: 68:7f:74:75:f1:cd 0.0.0.0 8021X_REQD (3) Change state to START (0) last state 8021X_REQD (3)**

***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**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

802.1X Authentication



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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) ApVapId2 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 15:36:07.567: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.567: 00:40:96:b5:db:d7 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received Identity Response (count=2) from mobile 00:40:96:b5:db:d

*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 Reqstate (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)

*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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

802.1x -Successful

*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 AuthResponse 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 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 aclfrom 255 to 255

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 Flex aclfrom 65535 to 65535

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Username entry (cisco) already exists in name table, length = 253

*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-authtimeout 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 reauthtimeout = 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)

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 Freeing AAACB from Dot1xCB as AAA authis done for mobile 00:40:96:b5:db:d7

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Authentication

- AP Radio Debugs

*Jan 15 02:50:07.804: A6504097 r 1 3 -B008 2800 2FB698 6F9E11 6F9E11CFC0 auth l 6

*Jan 15 02:50:07.807: A6504BC0 t 1 69/67 14-B008 13A 6F9E11 2FB698 6F9E11 65C0 auth l 6

*Jan 15 02:50:07.809: A6505313 r 1 69/67 19-0000 13A 6F9E11 2FB698 6F9E11 65D0 assreq l 139

*Jan 15 02:50:07.827: A6509A92 t 1 2 -1008 000 2FB698 6F9E11 6F9E11CFE0 assrsp l 151

*Jan 15 02:50:07.829: A650A056 t 1 0 -8802 000 2FB698 6F9E11 6F9E110290 q7 l87

EAPOL3 EAP id 93 reqident 0 "networkid=peapradius,nasid=LIVE-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 respident “LIVE"

|

Rest of the EAP Transaction

|

*Jan 15 02:50:08.247: A6570622 t 1 0 Jan 15 02:50:08.247: A6570622 t 1 0 -8802 000 2FB698 6F9E11 6F9E110330 q7 l54

EAPOL3 EAP id 93 success

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

A SUPER HERO TIP

Few things we can do before involving server and client team

(Cisco Controller) > **test aaa radius username <user name> password <password> wlan-id <wlan-id> ap-group <apgroup-name> server-index <server-index>**

(Cisco Controller) >**test aaa show radius**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Failed Authentication Attempt

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server              Retry Status
-------------              ----- ------
10.20.227.52               1     Success
```

Authentication Response:

Result Code: **Authentication failed** ------>This indicates that the user authentication will fail.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Communication Failed Between WLC and Server

- (Cisco Controller) >test aaa show radius previous test command still not completed, try after some time

You need to wait for the WLC to finish it's retries before it displays the output. The time can vary based on the retry thresholds configured.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id.......................................... 1
  ApGroup Name..................................... default-group
  Server Index..................................... 3
Radius Test Response
Radius Server              Retry Status
-------------              ----- ------
10.20.227.72               6     No response received from server
Authentication Response:
  Result Code: No response received from server
  No AVPs in Response
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

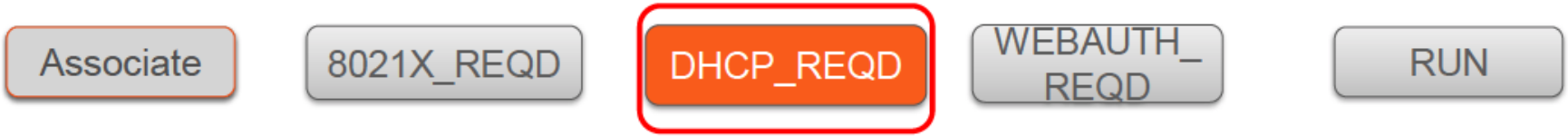
Radius Fallback

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
Radius Test Response
Radius Server              Retry Status
-------------              ----- ------
10.20.227.62               6     No response received from server
10.20.227.52               1     Success
Authentication Response:
  Result Code: Success
  Attributes                          Values
  ----------                          ------
  User-Name                           admin
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State:

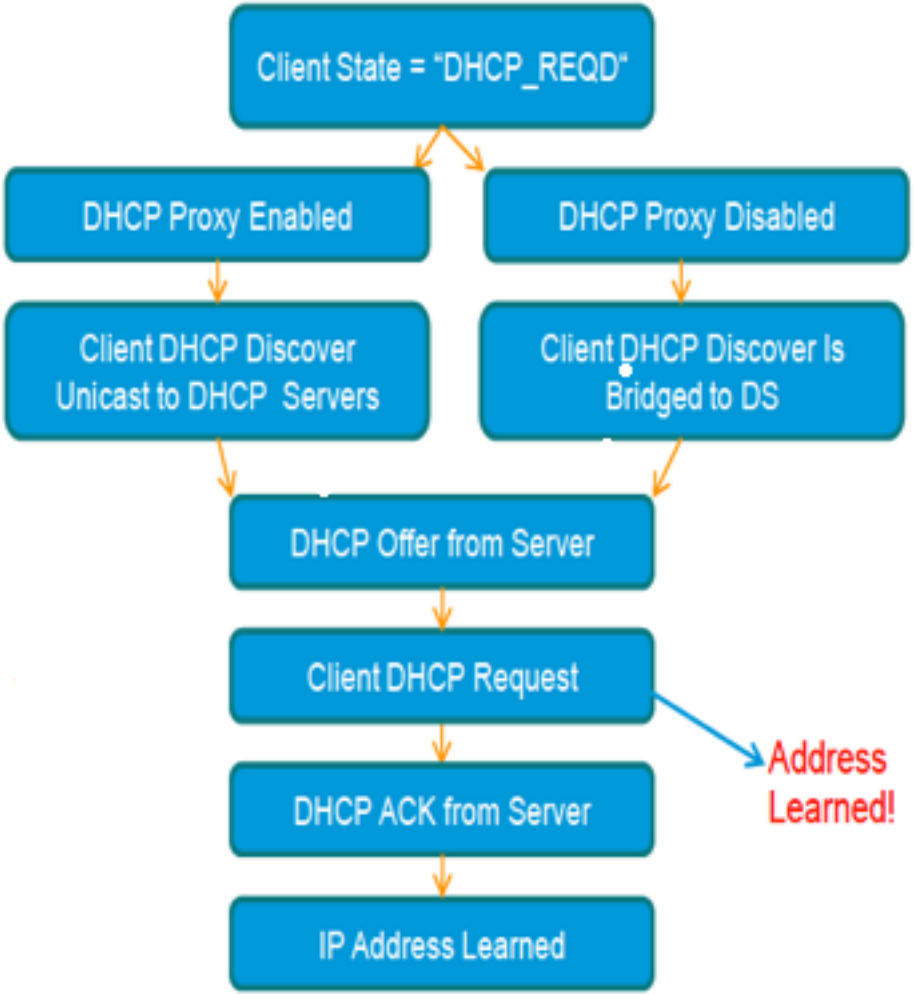


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 = AirespaceAP -Learn IP address
on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*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 intfid = 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, dtlFlags0x0
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client DHCP without Proxy

```
DHCP received op BOOTREQUEST (1) (len 308,vlan 258, port 13, encap 0xec03, xid 0xd1fbbbdf)
DHCP processing DHCP DISCOVER (1)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0xd1fbbbdf (3522935775), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP Opt82 bridge mode insertion enabled, inserts opt82 if opt82 is enabled vlan=279, datalen
DHCP successfully bridged packet to DS
DHCP received op BOOTREPLY (2) (len 319,vlan 279, port 13, encap 0xec00, xid 0xd1fbbbdf)
DHCP processing DHCP OFFER (2)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0xd1fbbbdf (3522935775), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.179.101
DHCP server id: 192.168.150.25 rcvd server id: 192.168.150.25
DHCP successfully bridged packet to STA
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client DHCP without Proxy

```
DHCP received op BOOTREQUEST (1) (len 333,vlan 258, port 13, encap 0xec03, xid 0xd1fbbbdf)
DHCP processing DHCP REQUEST (3)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0xd1fbbbdf (3522935775), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP requested ip: 192.168.179.101
DHCP server id: 192.168.150.25 rcvd server id: 192.168.150.25
DHCP Opt82 bridge mode insertion enabled, inserts opt82 if opt82 is enabled vlan=279, datalen =18, optlen=89
DHCP successfully bridged packet to DS

Assigning Address 192.168.179.101 to mobile

DHCP received op BOOTREPLY (2) (len 319,vlan 279, port 13, encap 0xec00, xid 0xd1fbbbdf)
DHCP processing DHCP ACK (5)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0xd1fbbbdf (3522935775), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.179.101
DHCP siaddr: 0.0.0.0, giaddr: 192.168.179.1
DHCP server id: 192.168.150.25 rcvd server id: 192.168.150.25
DHCP successfully bridged packet to STA
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client DHCP with Proxy - Discover

```
DHCP received op BOOTREQUEST (1) (len 308,vlan 258, port 13, encap 0xec03, xid 0x4f73543b)
DHCP (encap type 0xec03) mstype 0ff:ff:ff:ff:ff:ff
DHCP selecting relay 1 - control block settings: \dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0, dhcpGateway:
0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0
DHCP selected relay 1 - 192.168.150.25 (local address 192.168.179.91, gateway 192.168.179.1, VLAN 279, port
13)
DHCP transmitting DHCP DISCOVER (1)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP xid: 0x4f73543b (1332958267), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP siaddr: 0.0.0.0, giaddr: 192.168.179.91
DHCP sending REQUEST to 192.168.179.1 (len 350, port 13, vlan 279)
```

If Multiple DHCP Servers are listed on an Interface, we will sent to both, but only accept the first response

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client DHCP with Proxy - Offer

```
DHCP received op BOOTREPLY (2) (len 319,vlan 279, port 13, encap 0xec00, xid 0x4f73543b)

DHCP setting server from OFFER (server 192.168.150.25, yiaddr 192.168.179.101)

DHCP sending REPLY to STA (len 426, port 13, vlan 258)
DHCP transmitting DHCP OFFER (2)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0x4f73543b (1332958267), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.179.101
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP server id: 1.1.1.1 rcvd server id: 192.168.150.25
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client DHCP with Proxy – Request / ACK

```
DHCP selected relay 1 - 192.168.150.25 (local address 192.168.179.91, gateway 192.168.179.1, VLAN 279, port
13)

DHCP transmitting DHCP REQUEST (3)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP siaddr: 0.0.0.0, giaddr: 192.168.179.91
DHCP requested ip: 192.168.179.101
DHCP server id: 192.168.150.25 rcvd server id: 1.1.1.1
DHCP sending REQUEST to 192.168.179.1 (len 374, port 13, vlan 279)

Assigning Address 192.168.179.101 to mobile

DHCP sending REPLY to STA (len 426, port 13, vlan 258)
DHCP transmitting DHCP ACK (5)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0x4f73543b (1332958267), secs: 0, flags: 0
DHCP chaddr: 20:68:9d:dc:3b:d0
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.179.101
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP server id: 1.1.1.1 rcvd server id: 192.168.150.25
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 (len374, port 1, vlan703)
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
DHCP received op BOOTREPLY (2) (len308,vlan 703, port 1, encap0xec00)
DHCP sending REPLY to STA (len402, port 1, vlan701)
DHCP transmitting DHCP NAK (6)
DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 (20)
```

- Multiple mechanisms to learn Client IP address:
  - Mobility
  - 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 realise their address is not valid for the subnet
- DHCP Required enabled on WLAN mitigates this client behaviour

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Required -Caveats

```
DTL-1-ARP_POISON_DETECTED: STA [00:0b:7d:0e:33:33,0.0.0.0] ARP (op 1) received
with invalid SPA 192.168.1.152/TPA 192.168.0.206
```

- Modifies Address learning
  - Limits to only DHCP and mobility
- Good for security
- It can cause problems if client is deleted
  - On new association client must do DHCP renew

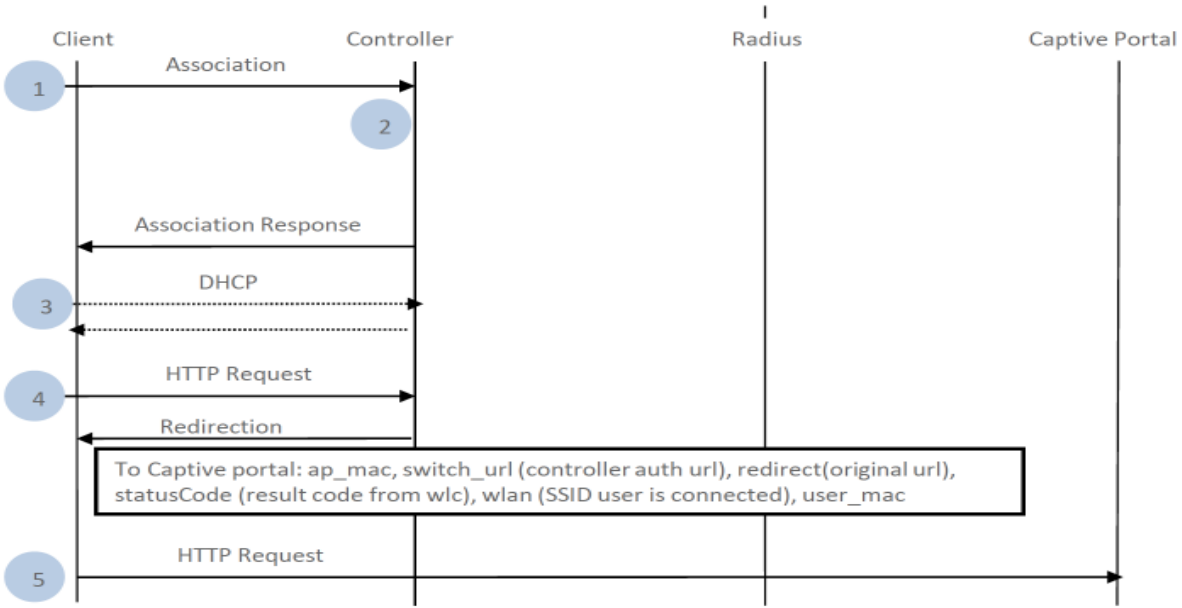
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State:

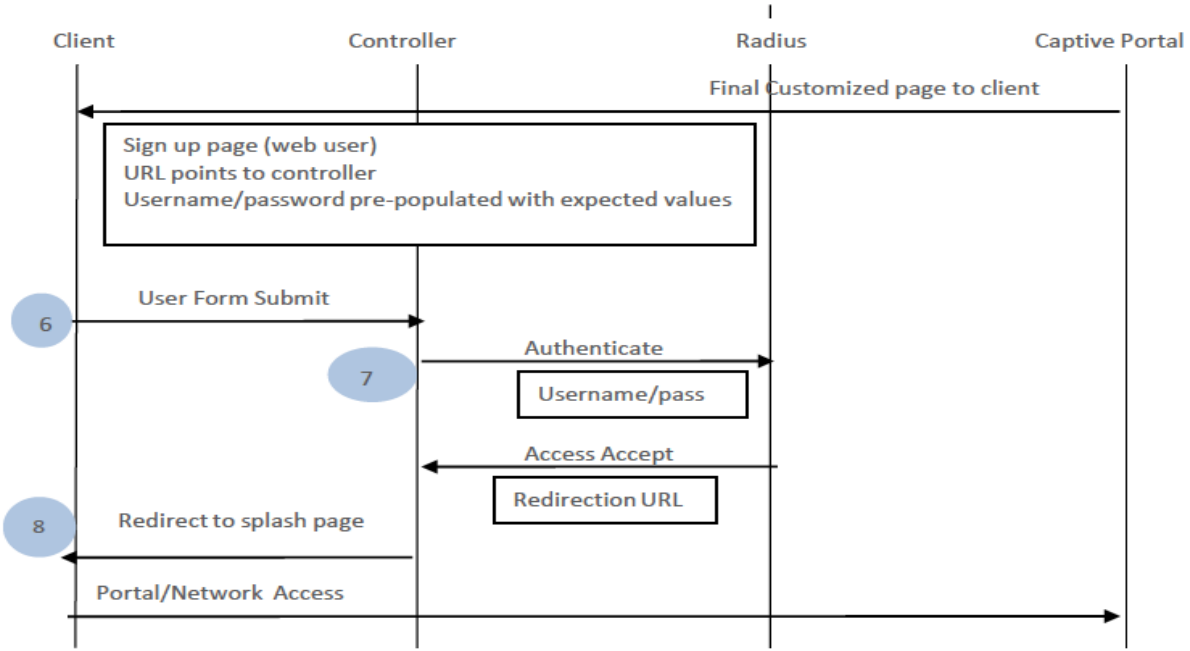
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth-Walkthrough



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth-Walkthrough



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Redirect

```
*pemReceiveTask: Jan 02 10:45:30.824: 68:7f:74:75:f1:cd 192.168.50.101 Added NPU entry of type 2, dtlFlags0x0
captive-bypass detection disabled, Not checking for wisprin HTTP GET, client mac=68:7f:74:75:f1:cd
Preparing redirect URL according to configured Web-Authtype
Checking custom-web configfor WLAN ID:2
unable to get the hostNamefor virtual IP, using virtual IP =1.1.1.1
Global status is enabled, checking on web-authtype
Web-authtype 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/
clenstring 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Redirect –IPv6

```
webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7-str1 is now
https://[::FFFF:1.1.1.1]/login.html?redirect=www.apple.com/library/test/success.html

*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7-clenstring is Content-Length: 337

*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7-Message to be sent is

HTTP/1.1 200 OK

Location: https://[::FFFF:1.1.1.1]/login.html?redirect=www.apple.com/library/test/success.html

Content-Type: text/html

Content-L

*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7-send data length=498
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Success

```
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 mscbfor 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 PLUMBFASTPATH: 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Typical Problems

- No DNS resolution
- No default GW
- HTTPS redirection enabled

- Client doing request on different port
  - No HTTPS, or using 8000, etc.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Typical Problems

No Preauth-ACL for External Webauth

- Server IP must be allowed on the preauthACL… otherwise, we get a loop!

```
*webauthRedirect: Jan 02 12:27:08.254: 68:7f:74:75:f1:cd-Web-authtype 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/
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 reauthenticate often

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webauth Take Away

- If using external webauth
  - Certificate trust is critical (both WLC and external server). If suspected test with https disabled
  - PreauthACL

- ARP/DNS must work before you can do anything
- Additional debug needed
  - debug web-authredirect enable mac <mac addr>
- Client side capture/logs may be needed

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Flow

The Route Toward the RUN State:

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status

- 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 PLUMBFASTPATH: 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 intfid = 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*pemReceiveTask:

Nov 05 14:35:11.842: 2c:54:2d:ea:e7:aa 10.253.42.45 Added NPU entry of type 1, dtlFlags0x0
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status -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

```
>sh cont d0 | b Reset
Last radio reset code: 62
Radio resets - total:113 retries:0 failed:0
Reset Stats: Start Cnt: 94, Recovery: Cnt0, Last Ret: 0, Fails: 0, RecvryStatus:
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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status -Typical Problems

Environmental trigger

- Typical high channel utilisation
- **QBSS Value based on a maximum of 0xFF (255). Convert value from hex and divide by 255 to see as a percentage**
  - 0xFE = 254, divide by 255 = 99.6% Channel Utilisation

ap2600-sw1-0-31#sh cont d0 | b QBSS

```
QBSS Load: 0xFE Tx0 Rx 0 AP 0
```

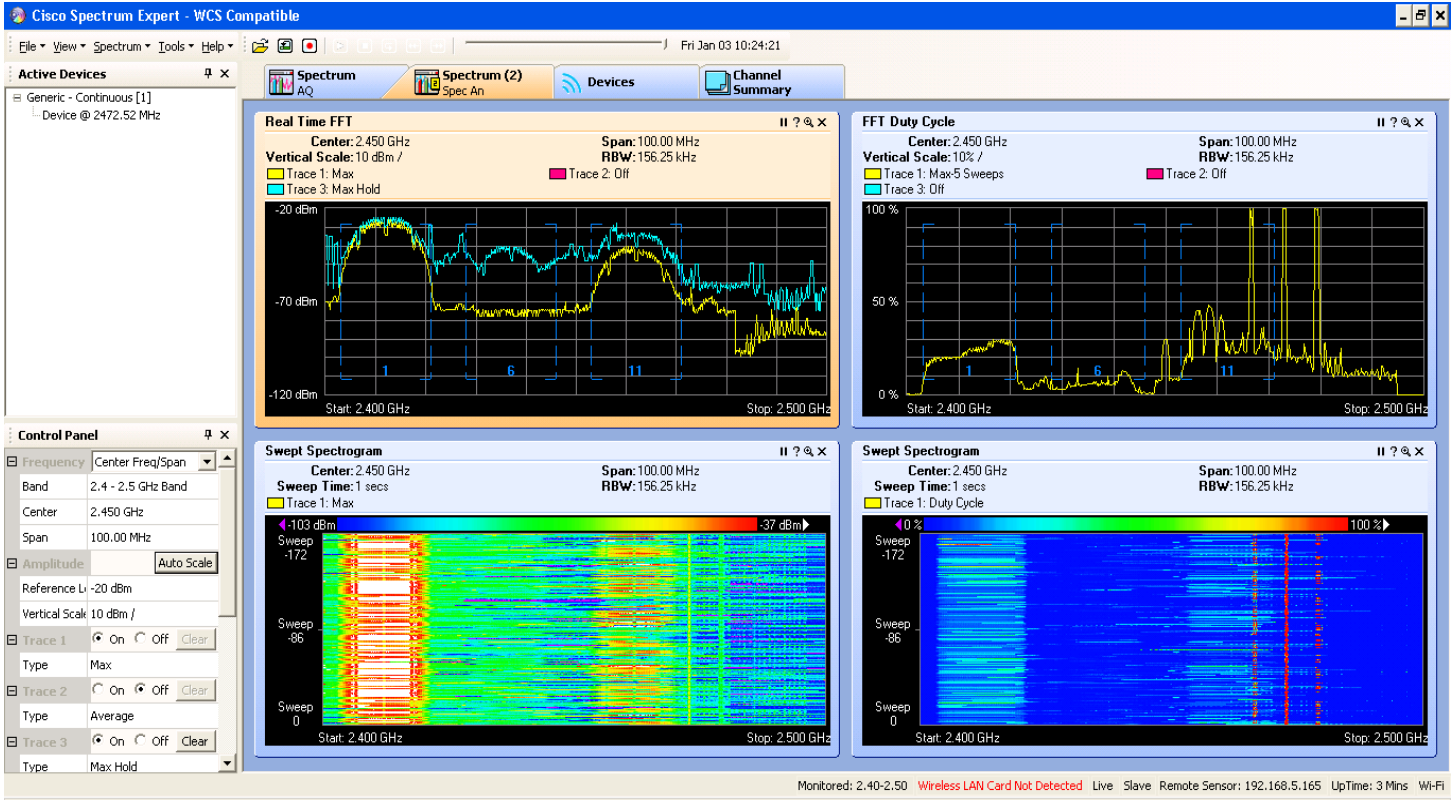
```
*Nov 21 10:59:06.244: %DOT11-3-NO_BEACONING: Error on Dot11Radio0 -Not Beaconing for
too long -Current 2887074 Last 2887074*Nov 21 10:59:06.274: %LINK-5-CHANGED: Interface
Dot11Radio0, changed state to reset
*Nov 21 10:59:07.693: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status -Typical Problems

Poor Performance

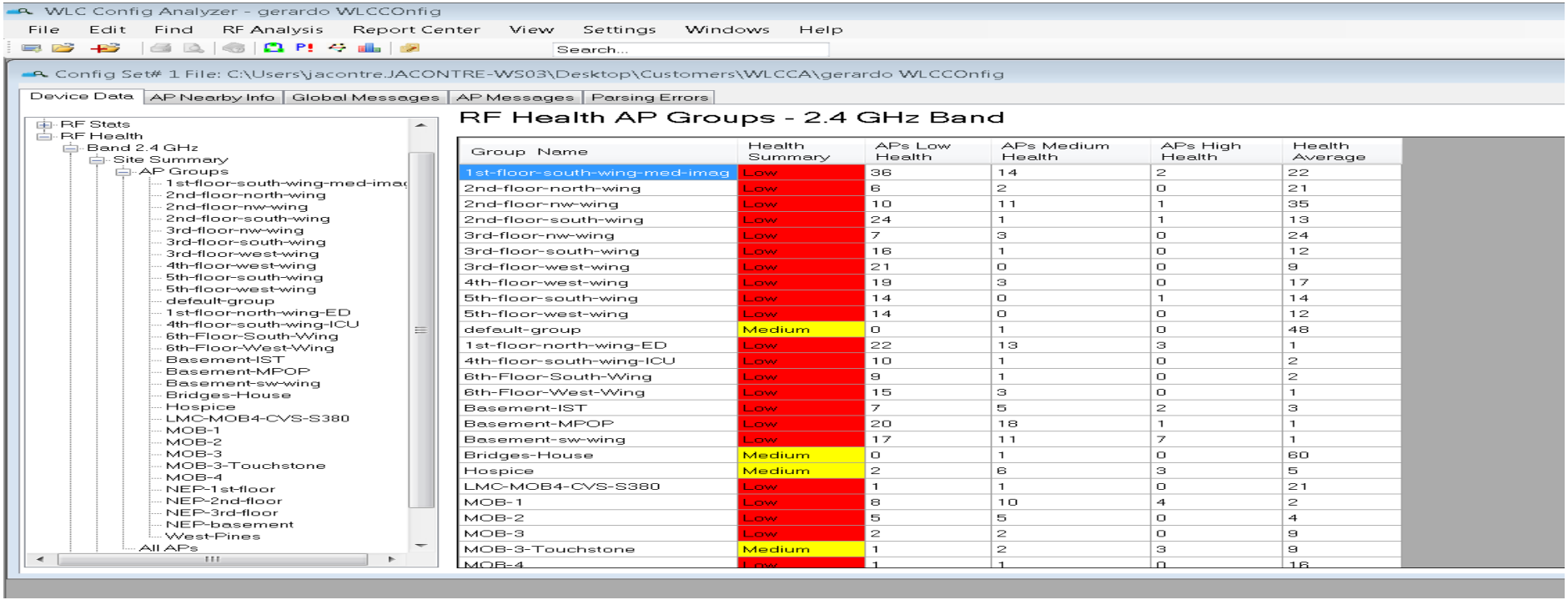
- RF issues
- Client side bugs



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status -RF Analysis WLCCA

WLCCA - now WCAE

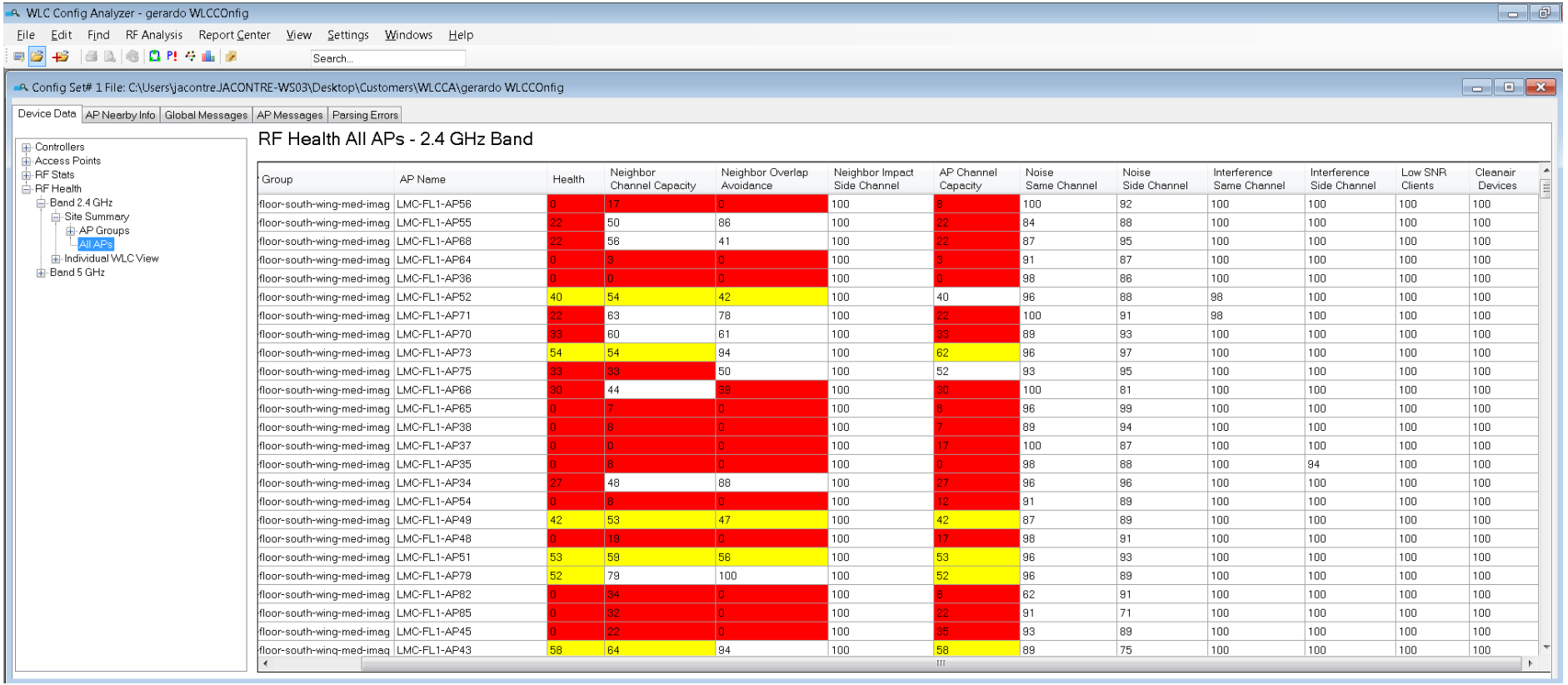


Group Name	Health Summary	APs Low Health	APs Medium Health	APs High Health	Health Average
1st-floor-south-wing-med-imag	Low	36	14	2	22
2nd-floor-north-wing	Low	6	2	0	21
2nd-floor-nw-wing	Low	10	11	1	35
2nd-floor-south-wing	Low	24	1	1	13
3rd-floor-nw-wing	Low	7	3	0	24
3rd-floor-south-wing	Low	16	1	0	12
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

WCAE :https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/212795-wireless-config-analyzer-express.html

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

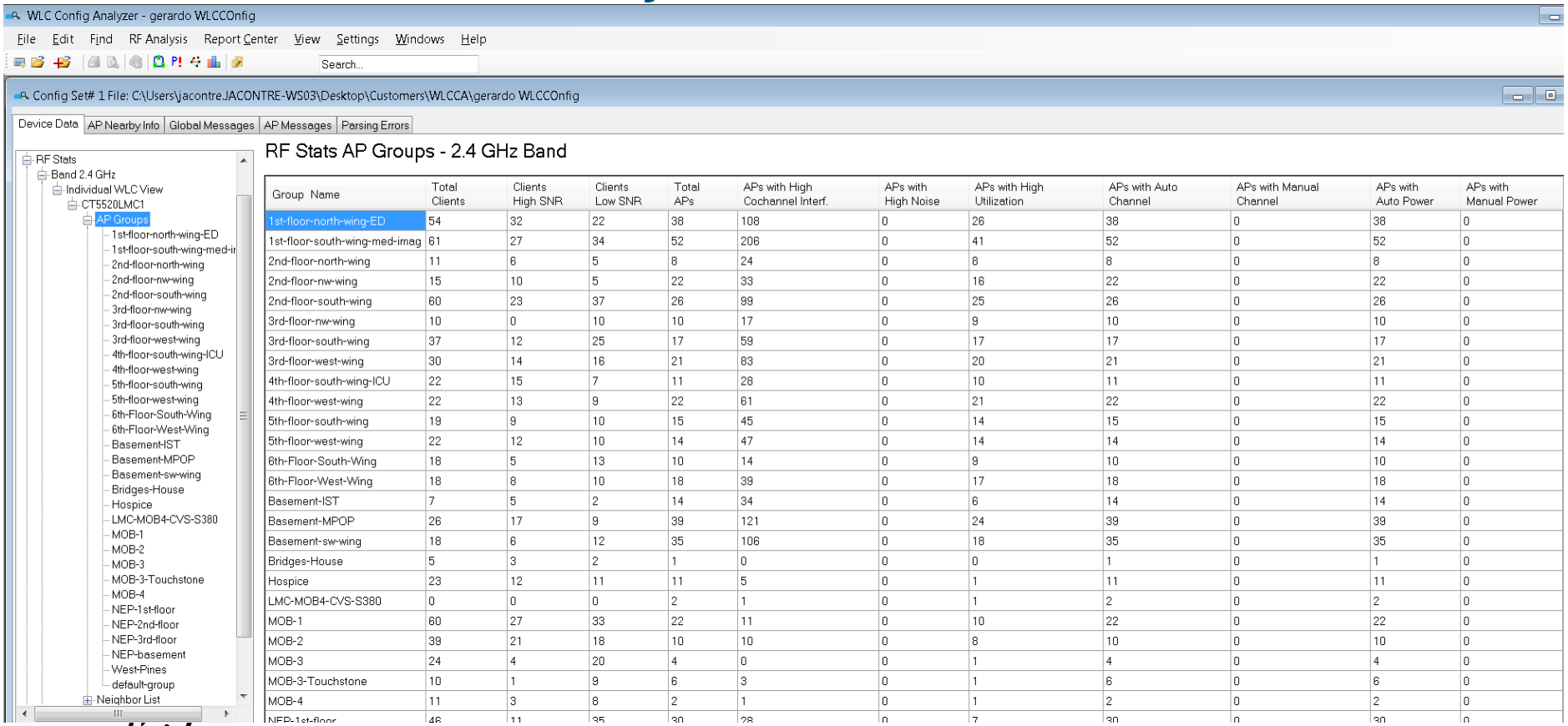
RUN Status -RF Analysis WLCCA



Group	AP Name	Health	Neighbor Channel Capacity	Neighbor Overlap Avoidance	Neighbor Impact Side Channel	AP Channel Capacity	Noise Same Channel	Noise Side Channel	Interference Same Channel	Interference Side Channel	Low SNR Clients	Cleanair Devices
floor-south-wing-med-imag	LMC-FL1-AP56	0	17	0	100	8	100	92	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP55	22	50	86	100	22	84	88	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP68	22	56	41	100	22	87	95	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP64	0	3	0	100	3	91	87	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP36	0	0	0	100	0	98	86	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP52	40	54	42	100	40	96	88	98	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP71	22	63	78	100	22	100	91	98	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP70	33	60	61	100	33	89	93	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP73	54	54	94	100	62	96	97	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP75	33	33	50	100	52	93	95	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP66	30	44	39	100	30	100	81	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP65	0	7	0	100	8	96	99	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP38	0	8	0	100	7	89	94	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP37	0	0	0	100	17	100	87	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP35	0	8	0	100	0	98	88	100	94	100	100
floor-south-wing-med-imag	LMC-FL1-AP34	27	48	88	100	27	96	96	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP54	0	8	0	100	12	91	89	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP49	42	53	47	100	42	87	89	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP48	0	19	0	100	17	98	91	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP51	53	59	56	100	53	96	93	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP79	52	79	100	100	52	96	89	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP82	0	34	0	100	8	62	91	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP85	0	32	0	100	22	91	71	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP45	0	22	0	100	35	93	89	100	100	100	100
floor-south-wing-med-imag	LMC-FL1-AP43	58	64	94	100	58	89	75	100	100	100	100

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

RUN Status -RF Analysis WLCCA



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-IST	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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

De-authenticated Client

- 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)
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

De-authenticated Client

- 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)
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

De-authenticated Client

- Authentication Timeout

  Auth or Key Exchange max-retransmissions reached

```
Retransmit failure for EAPOL-Key M3 to mobile00:1e: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)
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

De-authenticated Client

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


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Issues -Takeaway

- 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 deauth is happening
  - ✓ Packet capture or client logs may be required to see the exact reason
  - ✓ Never forget Radio status and RF conditions

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Troubleshooting -Flex

Client Debugs

- On the FlexConnect AP:

This is pre-8.1!

debug capwap flex

debug capwap client config

debug capwap flexconnect mgmt

debug capwap flexconnect pmk

debug capwap flexconnect cckm

debug capwap flexconnect dot11r

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debugs on Flex APs –AireOS 8.1 New Features

- Client based debugging exist on WLC but such ability was lacking on the AP side.
- Lack of filtering capabilities on debugging information in AP

Specific Flexconnect AP :

debug flexconnect client ap<ap-name> add/delete <addr1> {<addr2> <addr3> <addr4>}

debug flexconnect client ap<ap-name> syslog <server-ip/disable>

For a Flex group :

debug flexconnect client group <group-name>add/delete <addr1> { <addr2> | <addr3> | <addr4>}

debug flexconnectclient group <group-name> syslog <serverip/disable>

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debugs on Flex Aps –Example

(5500-4-82) >debug flexconnect client group ciscolive add 00:40:96:b5:db:d7

Warning! Flex group client debugs will not be enabled on AP where AP specific client debugs are already enabled.

(5500-4-82) >show deb

MAC debugging ..... disabled

Debug Flags Enabled:

Flex-AP Client Debugging ..... disabled

Flex-Group Client Debugging ..... Enabled

Group Name	Syslog IP Address	Mac Addresses
Ciscolive	0.0.0.0	00:40:96:b5:db:d7

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex –802.11

```
*Jan 26 15:27:28.263: (0040.96b5.dbd7): CAPWAP: Central authclient, Not
sending delete mobile to controller

*Jan 26 15:27:28.263: (0040.96b5.dbd7): dot11_mgmt:Setting AID 0 for station
*Jan 26 15:27:28.263: (0040.96b5.dbd7): Reap_Mgmt: Open AuthClient,
auth_type0, auth_algorithm0 fsm_type4

*Jan 26 15:27:28.263: (0040.96b5.dbd7): Reap_Mgmt; Created MN , wlan 2,
association in progress

*Jan 26 15:27:28.263: (0040.96b5.dbd7): SM: ---REAP Open Authentication
0x6E7888C: AuthReq(0)SM:    Assoc(2) --> DONT CHANGE STATE (255)

*Jan 26 15:27:28.263: (0040.96b5.dbd7): dot11_mgmt:FR_SM:
dot11_mgmt_smact_lwapp_reauth_req(): 0040.96b5.dbd7 :: INIT (STOP_FR, 0x0) -
> INIT
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex –802.11

```
(0040.96b5.dbd7): dot11_driver: Dot11Radio1: Rx AssocReq for the client
(0040.96b5.dbd7): SM: ---REAP Open Authentication 0x6E7888C:
AssocReq(1)SM:    Assoc(2) --> DONT CHANGE STATE (255)
(0040.96b5.dbd7): dot11_mgmt: found a valid rsniewith key_mgmtFAC02 and
encrypt_type512
(0040.96b5.dbd7): dot11_mgmt: WLAN MFP=1 WPA2=yes
(0040.96b5.dbd7): dot11_mgmt: Allocated AID 1 for client
(0040.96b5.dbd7): dot11_mgmt: [7E818AA6] send assocresp, status[0] to
dst=0040.96b5.dbd7, aid[1] on Dot11Radio1
(0040.96b5.dbd7): dot11_driver: Dot11Radio1: TxAssocResp to client
0040.96b5.dbd7
(0040.96b5.dbd7): dot11_mgmt: forwarding assocreqto controller
(0040.96b5.dbd7): dot11_mgmt: start assoctimer
(0040.96b5.dbd7): Reap_Mgmt: Stopping assoctimer
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex – 802.11

```
(0040.96b5.dbd7): Reap_Mgmt: Assoc Resp for this station accepted by controller

(0040.96b5.dbd7): capwap: MN FSM cur state = CAPWAP_MN_ST_ADDED, evt=
CAPWAP_MN_EV_ASSOC_RSP

(0040.96b5.dbd7): capwap: MN FSM new state = CAPWAP_MN_ST_ADDED

(0040.96b5.dbd7): CAPWAP_ADD_MN: Reap Flags: 0x0, FlexAclName: , webAclName:

(0040.96b5.dbd7): CAPWAP_ADD_MN: slot 1, wlan 2, vlanId-1, AID 1, encrypt policy 0x1
encrypt_type 0x0000, parent 0000.0000.0000

(0040.96b5.dbd7): CAPWAP_ADD_MN: GatewayIp= 0.0.0.0 GateWayMask 0.0.0.0 Client IP
4.0.16.11 IP-learn-type = 3

(0040.96b5.dbd7): CAPWAP_ADD_MN: Other Flags 0x0,  session_timeout0, Local Switch 0

(0040.96b5.dbd7): CAPWAP_ADD_MN: It is a Non WGB Client

(0040.96b5.dbd7): capwap: MN FSM cur state = CAPWAP_MN_ST_ADDED, evt= CAPWAP_MN_EV_ADD

(0040.96b5.dbd7): capwap: MN FSM new state = CAPWAP_MN_ST_ADDED
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex – 802.11

```
(0040.96b5.dbd7): capwap: MN FSM cur state = CAPWAP_MN_ST_ADDED, evt= CAPWAP_MN_EV_ADD

(0040.96b5.dbd7): capwap: MN FSM new state = CAPWAP_MN_ST_ADDED

(0040.96b5.dbd7): capwap: MN FSM cur state = CAPWAP_MN_ST_ADDED, evt= CAPWAP_MN_EV_ADD_KEY

(0040.96b5.dbd7): capwap: Not a fast-roaming client, plumbing keys with encrypt policy 4,
encrypt type 0x200

(0040.96b5.dbd7): Dot11_Driver: setting client key with encrypt type 0x200

(0040.96b5.dbd7): capwap: MN FSM new state = CAPWAP_MN_ST_ADDED
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex –Address Learning

```
(0040.96b5.dbd7): capwap: MN FSM cur state = CAPWAP_MN_ST_ADDED, evt =
CAPWAP_MN_EV_ADD_DONE

(0040.96b5.dbd7): capwap: MN FSM new state = CAPWAP_MN_ST_ADDED

(0040.96b5.dbd7): DHCP: 'BOOT REPLY' message type: DHCP_OFFER, MAC da: 0000.0004.0200, MAC
sa: 1009.8020.1900, IP da: 192.168.5.250, IP sa: 1.1.1.1, DHCP ciaddr: 0.0.0.0, DHCP
yiaddr: 192.168.5.250, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr:
0040.96b5.dbd7

*Jan 26 15:27:34.783: (0040.96b5.dbd7): DHCP: 'BOOT REPLY' message type: DHCP_ACK, MAC da:
0100.0000.c562, MAC sa: 1d00.c562.1500, IP da: 192.168.5.250, IP sa: 1.1.1.1, DHCP ciaddr:
0.0.0.0, DHCP yiaddr: 192.168.5.250, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP
chaddr: 0040.96b5.dbd7
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs on Flex – Authentication

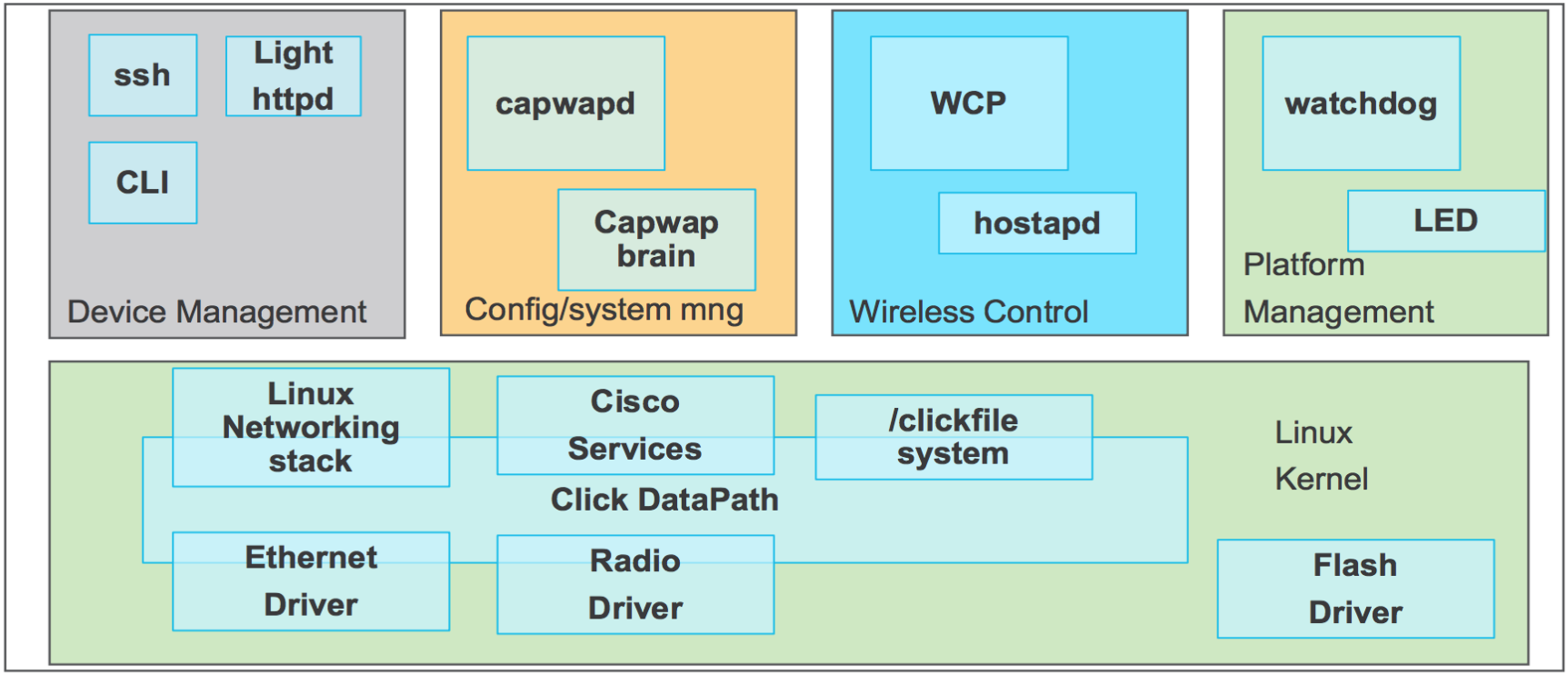
Only on Local-Auth

```
*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_aaa: Received EAPOL packet from client

*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_aaa: eapolver1 type 3 posting event 0x9

*Jan 26 16:09:01.527: (0040.96b5.dbd7): DOT1X_SM: Executing Action [state:
WPAV2_PTK_MSG2_WAIT, event: RECV_EAPOL_KEY_RSP] for client

*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_dot1x: Received wpav2 ptkmsg2

*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_dot1x: verifying PTK msg2 from client

..

*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_dot1x: Starting wpav2 ptkmsg3 to supplicant

*..

*Jan 26 16:09:01.527: (0040.96b5.dbd7): dot11_dot1x: mcst_key_len16 index 1 vlan0
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Troubleshooting
AP COS

AP COS – A Different Architecture (…Linux)



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP COS – Config will look very different from IOS

```
Alpha38003-Ishant#show configuration
AP Name                          : Alpha38003-Ishant
Admin State                      : Enabled
AP Mode                          : Local
AP Submode                       : None
Location                         : default location
Reboot Reason                    : Controller Reload
command
Primary controller name          : Alpha14Controller
Primary controller IP            : 192.168.10.12
Secondary controller name        :
Secondary controller IP          :
Tertiary controller name         :
Tertiary controller IP           :
AP join priority                 : 1
IP Prefer-mode                   : IPv4
CAPWAP UDP-Lite                  : Unconfigured
Last Joined Controller name      : Alpha14Controller
DTLS Encryption State            : Disabled
Discovery Timer                  : 10
Heartbeat Timer                  : 30
CDP State                        : Enabled
Watchdog monitoring              : Enabled
IOX                              : Disabled
RRM State                        : Enabled
LSC State                        : Disabled
SSH State                        : Enabled
AP Username                      : Ishant
Session Timeout                  : 300
Extlog Host                      : 0.0.0.0
Extlog Flags                     : 0
Extlog Status Interval           : 0
Syslog Host                      : 255.255.255.255
Syslog Facility                  : 0
Syslog Level                     : informational
Core Dump TFTP IP Addr           :
Core Dump File Compression       : Disabled
Core Dump Filename               :
Client Trace Status              : Disabled
Client Trace All Clients         : Disabled
Client Trace Filter              : 0x00000000
Client Trace Out ConsoleLog      : Disabled
WLC Link LAG status              : Disabled
AP Link LAG status               : Disabled
AP WSA Mode                      : Disabled
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP COS - Client Information

- Different components shows different Information

#show dot11 clients

```
Alpha38003rdfloor#show dot11 clients
Total dot11 clients: 2
       Client MAC Slot ID WLAN ID AID            WLAN Name RSSI Maxrate WGB
34:36:3B:D4:73:30       1       2   6 Cisco-Live-Melbourne  -51 MCS93SS  No
30:07:4D:60:80:20       1       1   3              alpha14  -50 MCS92SS  No
```

#show controllers dot11Radio 1 client

```
Alpha38003rdfloor#show controllers dot11Radio 1 client
              mac radio vap aid state       encr Maxrate is_wgb_wired      wgb_mac_addr
34:36:3B:D4:73:30     1   1   6   FWD       OPEN MCS93SS        false 00:00:00:00:00:00
30:07:4D:60:80:20     1   0   3   FWD AES_CCM128 MCS92SS        false 00:00:00:00:00:00
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs – 2800/3800 series

- **On COS AP:** config ap client-trace address add <MAC address H.H.H>

```
config ap client-trace filter assoc enable
config ap client-trace filter auth enable
config ap client-trace filter dhcp enable
config ap client-trace filter eap enable
config ap client-trace filter icmp enable

config ap client-trace start
config ap client-trace stop

show ap client-trace status

config ap client-trace output console-log enable
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debugs – 1800 series

- **On COS AP :**

```
debug dot11 client level events addr <mac>
debug dot11 client level errors addr <mac>
debug dot11 client level critical addr <mac>
debug dot11 client level info addr <mac>

debug dot11 client datapath eapol addr <mac>
debug dot11 client datapath dhcp addr <mac>
debug dot11 client datapath arp addr <mac>

Use Slot 0 for 2.4ghz and 1 for 5ghz and appropriate
wlan ID in question

debug dot11 driver slot 0 wlan 1 assoc
debug dot11 driver slot 0 wlan 1 auth
debug dot11 driver slot 0 wlan 1 node
debug dot11 driver slot 0 wlan 1 state
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP COS – Client-Trace Debugs Options

- **config ap client-trace address add MAC**
- **config ap client-trace output console-log enable**
- **config ap client-trace filter {all|assoc|auth| dhcp| eap|icmp|probe } enable|disable**

#show ap client-trace status

```
Client Trace Status      : Started
Client Trace ALL Clients : disable
Client Trace Address     : 00:1e:e5:df:a3:c4
Client Trace Filter      : auth
Client Trace Filter      : assoc
Client Trace Filter      : eap
Client Trace Filter      : dhcp
Client Trace Output      : eventbuf
Client Trace Output      : console-log
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Trace - Trace format

[*02/22/2017 08:54:40.203412] [ap-cos] [00:1e:e5:df:a3:c4] <apr1v2> [U:W]
DOT11_AUTHENTICATION : Retry 0 PwrM 0 Seq 250 (.)

[*02/22/2017 08:54:40.203412]	:	Timestamp
[ap-cos]	:	AP name
[00:1e:e5:df:a3:c4]	:	Client mac
<apr1v2>	:	WLAN interface
[U:W]	:	Direction {U/D}: Subsystem {Wireless, Eth, Click}

DOT11_AUTHENTICATION : Retry 0 PwrM 0 Seq 250 (.)

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Trace - PSK Example

[16:56:13.5199] [1494608173:519910] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:W] DOT11_AUTHENTICATION

[16:56:13.5199] [1494608173:519952] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [D:W] DOT11_AUTHENTICATION

[16:56:13.5209] [1494608173:520946] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:W] DOT11_ASSOC_REQUEST

[16:56:13.5211] [1494608173:521189] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [D:W] DOT11_ASSOC_RESPONSE

[16:56:13.5274] [1494608173:527441] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [D:E] EAPOL_KEY.M1

[16:56:13.5275] [1494608173:527496] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [D:W] EAPOL_KEY.M1

[16:56:13.5286] [1494608173:528666] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:W] EAPOL_KEY.M2

[16:56:13.5287] [1494608173:528738] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [U:E] EAPOL_KEY.M2

[16:56:13.5292] [1494608173:529254] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [D:E] EAPOL_KEY.M3

[16:56:13.5292] [1494608173:529286] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [D:W] EAPOL_KEY.M3

[16:56:13.5305] [1494608173:530565] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:W] EAPOL_KEY.M4

[16:56:13.5306] [1494608173:530628] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [U:E] EAPOL_KEY.M4

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Trace - PSK Example

[16:56:13.6327] [1494608173:632738] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:W] DHCP_REQUEST

[16:56:13.6328] [1494608173:632793] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:C] DHCP_REQUEST

[16:56:13.6328] [1494608173:632861] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [U:C] DHCP_REQUEST

[16:56:13.6328] [1494608173:632893] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [U:E] DHCP_REQUEST

[16:56:13.6329] [1494608173:632910] [CAP3802] [aa:aa:03:00:00:00] <wired0> [U:E] DHCP_REQUEST

[16:56:13.6329] [1494608173:632938] [CAP3802] [ff:ff:ff:ff:ff:ff] <apr1v7> [D:W] DHCP_REQUEST

[16:56:13.6506] [1494608173:650603] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [D:E] DHCP_ACK

[16:56:13.6506] [1494608173:650634] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [D:C] DHCP_ACK

[16:56:13.6507] [1494608173:650694] [CAP3802] [bc:9f:ef:1b:89:ef] <wired0> [D:C] DHCP_ACK

[16:56:13.6507] [1494608173:650733] [CAP3802] [aa:aa:03:00:00:00] <wired0> [U:E] DHCP_ACK

[16:56:13.6507] [1494608173:650747] [CAP3802] [bc:9f:ef:1b:89:ef] <apr1v7> [D:W] DHCP_ACK

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP COS – Key Takeaways

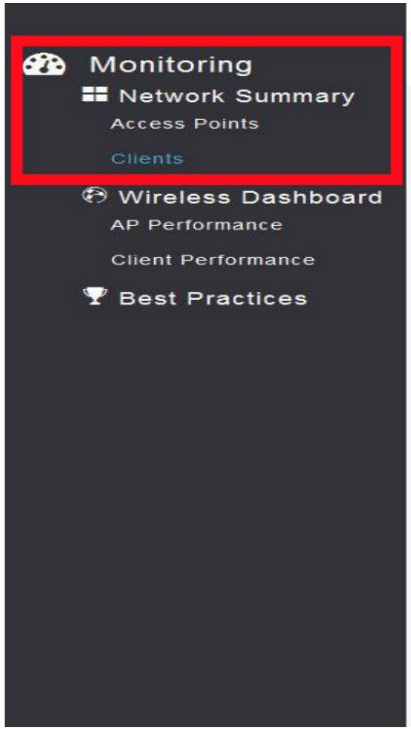
- Know which COS AP type, 3800/2800 vs 1800 series AP. You will need to use different client debugs depending on which AP type used.
- **Show Tech** – best source of complete information on AP health
- Review your AP syslogs, very helpful on AP join or any type of Radio reset/crash “more syslogs <filename>”
- Various show commands can be used to check on client status
  - Show client summary
  - Show controller dot11radio client

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Troubleshooting Using the GUI

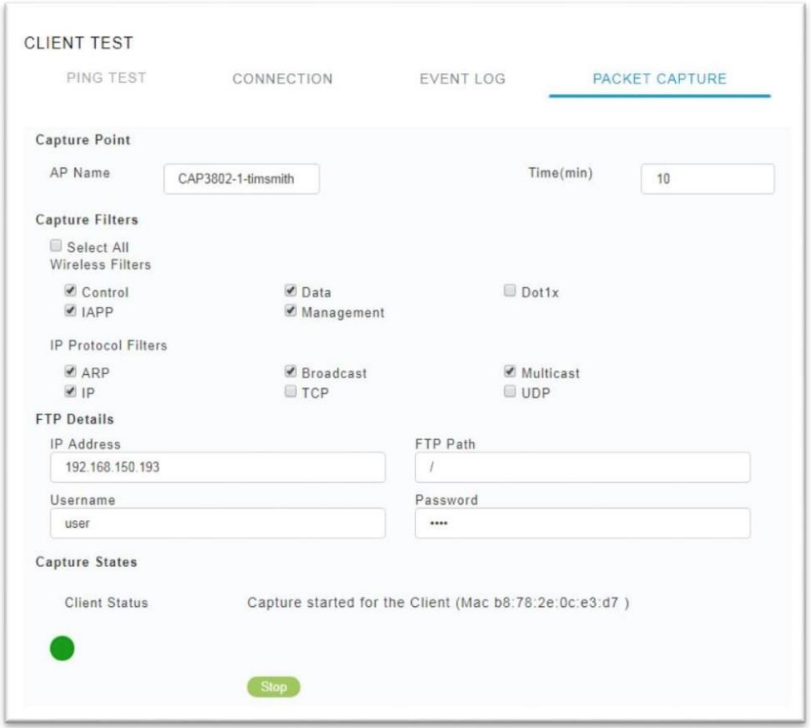
Client Debug Tools - Updated for Release 8.2/8.3

Click on the "HOME" button on the Controller GUI



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

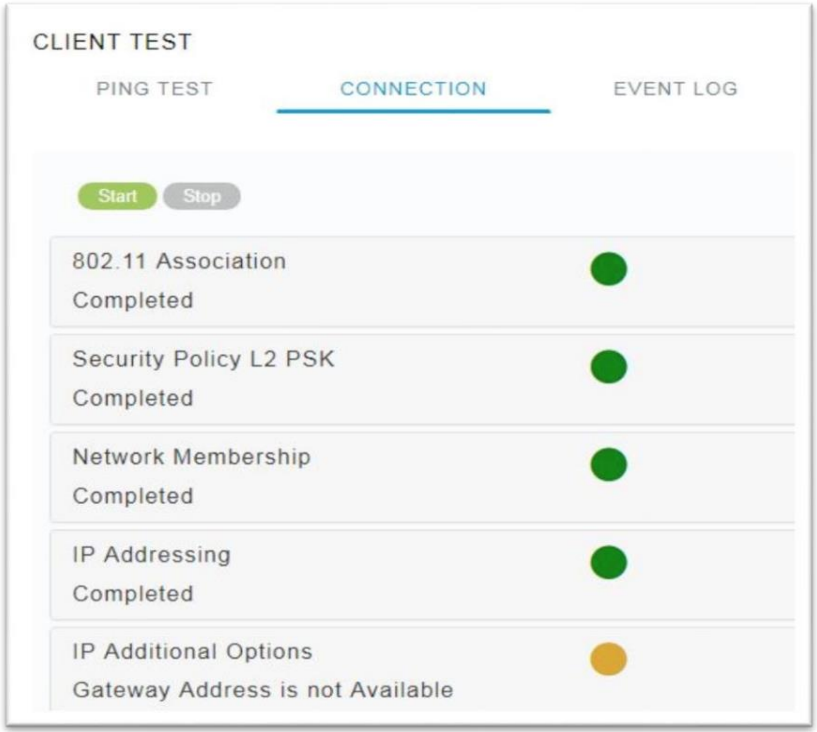
Client Debug Tools - Packet Capture



- 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 are 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 and above

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

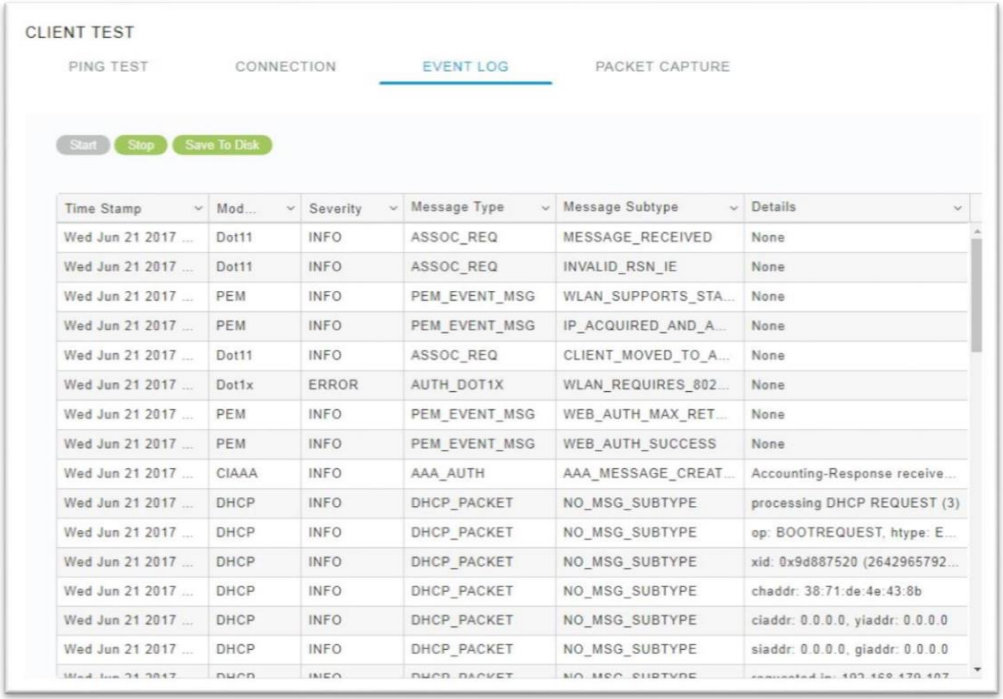
Client Debug Tools - Connection Test



- 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
- 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
- WLC 8.3 and above

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client Debug Tools - Connection Test



Time Stamp	Mod...	Severity	Message Type	Message Subtype	Details
Wed Jun 21 2017 ...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
Wed Jun 21 2017 ...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Wed Jun 21 2017 ...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STA...	None
Wed Jun 21 2017 ...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_A...	None
Wed Jun 21 2017 ...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_TO_A...	None
Wed Jun 21 2017 ...	Dot1x	ERROR	AUTH_DOT1X	WLAN_REQUIRES_802...	None
Wed Jun 21 2017 ...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_MAX_RET...	None
Wed Jun 21 2017 ...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_SUCCESS	None
Wed Jun 21 2017 ...	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_CREAT...	Accounting-Response receive...
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	processing DHCP REQUEST (3)
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	op: BOOTREQUEST, htype: E...
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	xid: 0x9d887520 (2642965792...
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	chaddr: 38:71:de:4e:43:8b
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Wed Jun 21 2017 ...	DHCP	INFO	DHCP_PACKET	NO_MSG_SUBTYPE	siaddr: 0.0.0.0, giaddr: 0.0.0.0

- Event log debugging tool for administrators
  - 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
  - Works on Roaming Clients
  - Option to export captured events to Excel for offline analysis
- WLC 8.3 and above

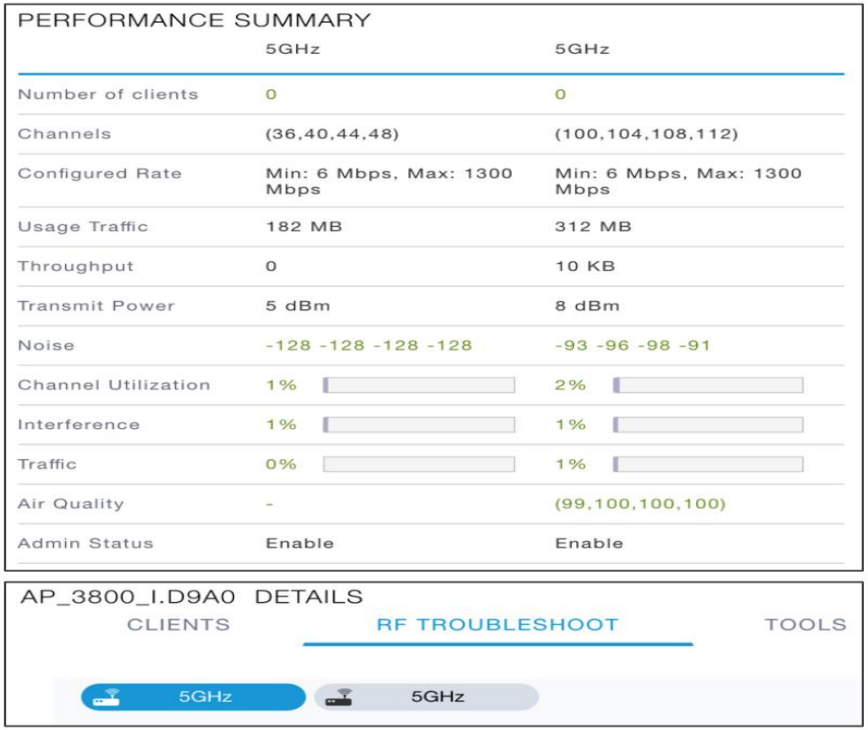
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP View Enhancements

- AP MAC, IP Address, and Serial number
- CDP / LLDP Enhancements
  - <SWITCH><PORT-TYPE><PORT>
- AP Type
- AP Power Status
- AP Group / Flex Group

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP View Enhancements



- Displays Channels and Power levels in use.
- Air Quality for CleanAir AP's
- Performance Metrics for RF Conditions
  - Channel Utilization
  - Interference
  - Traffic
- Flexible Radio Support

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client View Enhancements

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client View Enhancements

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client View Enhancements

NETWORK & QOS

Description	Status
IP Address	192.168.179.109
IPv6 Address	fe80::1ccc:8f8:d906:8a08
VLAN	279
Source Group Tag	N/A
Fastlane Client	No
Mobility Role	Local
WMM	Supported
U-APSD	Disabled
QoS Level	Platinum

SECURITY & POLICY

Description	Status
Policy	RSN (WPA2)
Cipher	CCMP (AES)
Key Management	PSK
EAP Type	N/A
ACL (IP/IPv6)	None/None
mDNS Profile	None
AAA Role	None

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Troubleshooting

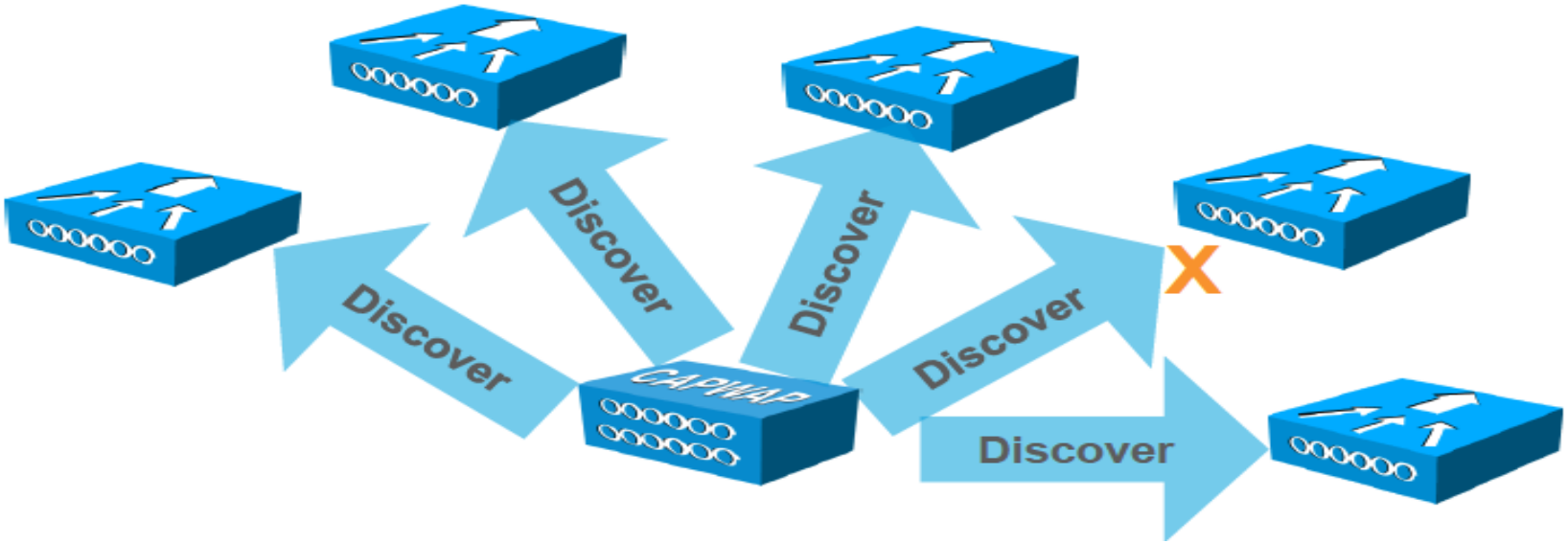
AP Join Process

- WLC Discovery
- DTLS/Join
- Image Download
- Configuration Check
- REG
- More information:

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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

L3 WLC Discovery



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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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>”

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 mesg Sent to 192.168.70.10, Port 5246
*Jan  2 15:41:42.039:           MsgType   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg Sent to 192.168.5.55, Port 5246
*Jan  2 15:41:42.039:           MsgType   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg Sent to 255.255.255.255, Port 5246
*Jan  2 15:41:42.039:           MsgType   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg 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:           MsgType   : CAPWAP_DISCOVERY_RESPONSE
*Jan  2 15:41:42.055: CAPWAP Control mesg 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:           MsgType   : CAPWAP_DISCOVERY_RESPONSE
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Discover/Join –AP Side

```
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Calling wtpGetAcToJoinfrom 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: Apmgrcount=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 Mgrwith 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
sucessfullypeer_ip: 192.168.5.55 peer_port: 5246
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Discover/Join –WLC Side

```
*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: apType: Ox1b 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 Msgelement 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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join –Country Mismatch -AP

```
*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
sucessfullypeer_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
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Join –Country Mismatch -WLC

```
*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.!]
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Lightweight APs

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/sshinto 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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Lightweight APs

Show Commands

- **On the WLC:**
  show msglog
  show traplog
- **On the AP:**
  show tech
  show log
  show capwap client rcb
  show capwap client config
  show capwap reap status

259	Sat May 9 15:48:31 2015	AP Disassociated. Base Radio MAC:a0:cf:5b:6e:f5:a0
260	Sat May 9 15:48:31 2015	AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:a0:cf:5b:6e:f5:a0 Cause=Heartbeat Timeout Status:NA
261	Sat May 9 15:48:31 2015	AP's Interface:0(802.11b) Operation State Down: Base Radio MAC:a0:cf:5b:6e:f5:a0 Cause=Heartbeat Timeout Status:NA

```
MAIB-1142#sh capwap client rcb
AdminState                      :   ADMIN_ENABLED
SwVer                           :   7.6.110.0
NumFilledSlots                  :   2
Name                            :   MAIB-1142
Location                        :   default location
MwarName                        :   Maib5508
MwarApMgrIp                     :   10.105.132.49
MwarHwVer                       :   0.0.0.0
ApMode                          :   Local
ApSubMode                       :   Not Configured
OperationState                  :   UP
CAPWAP Path MTU                 :   1485
LinkAuditing                    :   disabled
AP Rogue Detection Mode         :   Disabled
AP Tcp Mss Adjust               :   Disabled
AP IPv6 TCP MSS Adjust          :   Disabled
Predownload Status              :   None
Auto Immune Status              :   Disabled
RA Guard Status                 :   Enabled
Efficient Upgrade State         :   Disabled
Efficient Upgrade Role          :   None
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Lightweight APs

Debugs to be enabled

- **On the WLC:**

debug mac addr<AP Ethernet/Radio mac>
debug capwap events enable
debug capwap errors enable
debug dtlsall enable
debug pm pkienable

- **On the AP:**

debug dhcpdetail
debug capwap client detail

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Supportability

- **Filtering per AP**
  debug mac addr04:da:d2:4f:f0:50
  debug capwap events enable
  Use radio mac for mac-addr filters

- **For large deployments: CSCul27717**
  Improvements made to dtls/capwap debug output for large AP counts
  Available on latest 7.0/7.4/7.6

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Supportability

APs have a “flight recorder”

```
cap2600i-sw1-033#dir
Directory of flash:/
 2   -rwx 64279    Jan 2 2014 10:32:24 +00:00  event.log
 3   drwx 128      Jan 2 2014 10:26:12 +00:00  configs
 4   -rwx 280      Jan 2 2014 15:41:58 +00:00  lwapp_officeextend.cfg
10   -rwx 352      Jan 2 2014 15:41:52 +00:00  env_vars
 5   -rwx 49168    Jan 3 2014 06:26:30 +00:00  lwapp_non_apspecific_reap.cfg
 7   -rwx 965      Nov 21 2013 15:22:52 +00:00 lwapp_mm_mwar_hash.cfg
 6   -rwx 95008    Jan 2 2014 15:42:08 +00:00  lwapp_reap.cfg
17   -rwx 125501   Nov 20 2013 17:22:48 +00:00 event.r0
13   drwx 192      Dec 20 2012 21:37:52 +00:00 ap3g2-rcvk9w8-mx
11   -rwx 265      May 28 2013 09:58:54 +00:00 lwapp_mobileconcierge.cfg
12   -rwx 66319    Jan 2 2014 10:08:04 +00:00  event.capwap
25   -rwx 7192     Jan 3 2014 06:26:27 +00:00  private-multiple-fs
18   drwx 1792     Jan 2 2014 10:22:48 +00:00  ap3g2-k9w8-mx.152-4.JB3
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Supportability

AP Remote Commands (WLC CLI)

- **Debug AP enable <AP name>**
  Enables AP Remote Debug
  AP Must be associated to WLC
  Redirects AP Console output to WLC session

- **Debug AP command “<command>” <AP name>**
  Output is redirected to WLC session
  AP runs IOS, numerous generic IOS commands available

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Supportability

- Methods of Accessing the AP
  - Console
  - Telnet / SSH
  - No GUI support
  - AP Remote Commands

- Enabling Telnet/SSH
  - WLC CLI: **config ap [telnet/ssh] enable <ap name>**
  - WLC GUI: Wireless > All APs > Select AP > Advanced > Select [telnet/ssh] > Apply

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

AP Supportability

Show Commands (AP CLI or WLC Remote Cmd)

- Show controller Do[0/1] (or Show Tech)
  Must have! Before/During/After event
- Show log
- WLC: show ap eventlog <ap name>
- Show capwap client <?>
- CLI Tips
  Debug capwap console cli
  Debug capwap client no-reload

```
AP#show cap client ?
  callinfo    Lwapp client Call Info
  config      CAPWAP Client NV Config File
  detailrcb   Lwapp client rcb Info
  ha          CAPWAP Client HA parameters
  mn          CAPWAP Client 80211 MN
  rcb         CAPWAP Client RCB
  timers      CAPWAP Client Timers
  traffic     CAPWAP Client 80211 Traffic
```


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility

Mobility—Types

- Legacy –Flat
  - Old style
  - Discriminator is mobility group name

- New –Hierarchical
  - For 7.3, 7.5+ and Converged access
  - Supports large setups, multiple device roles
  - Covered on Converged access troubleshooting

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

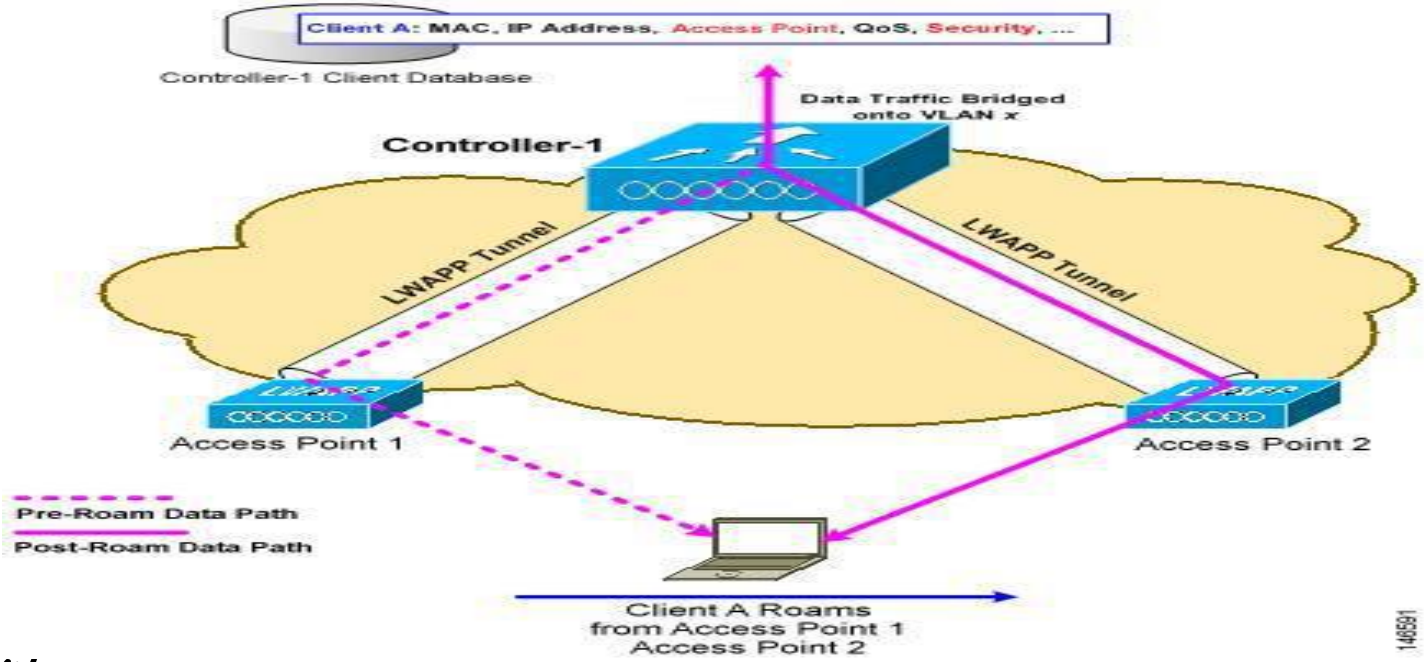
Mobility -Messaging Flow

- 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**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

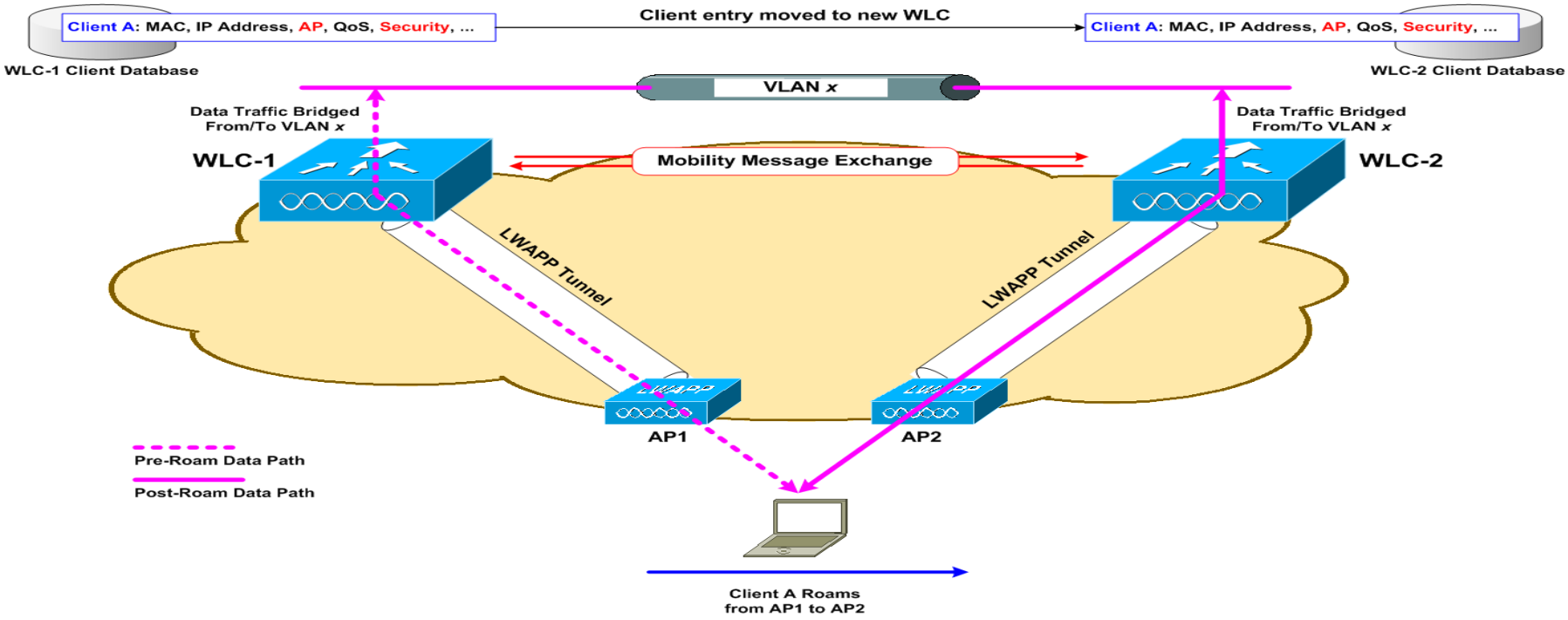
Mobility - Intra-Controller

- Client roams between two APs on the same controller



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

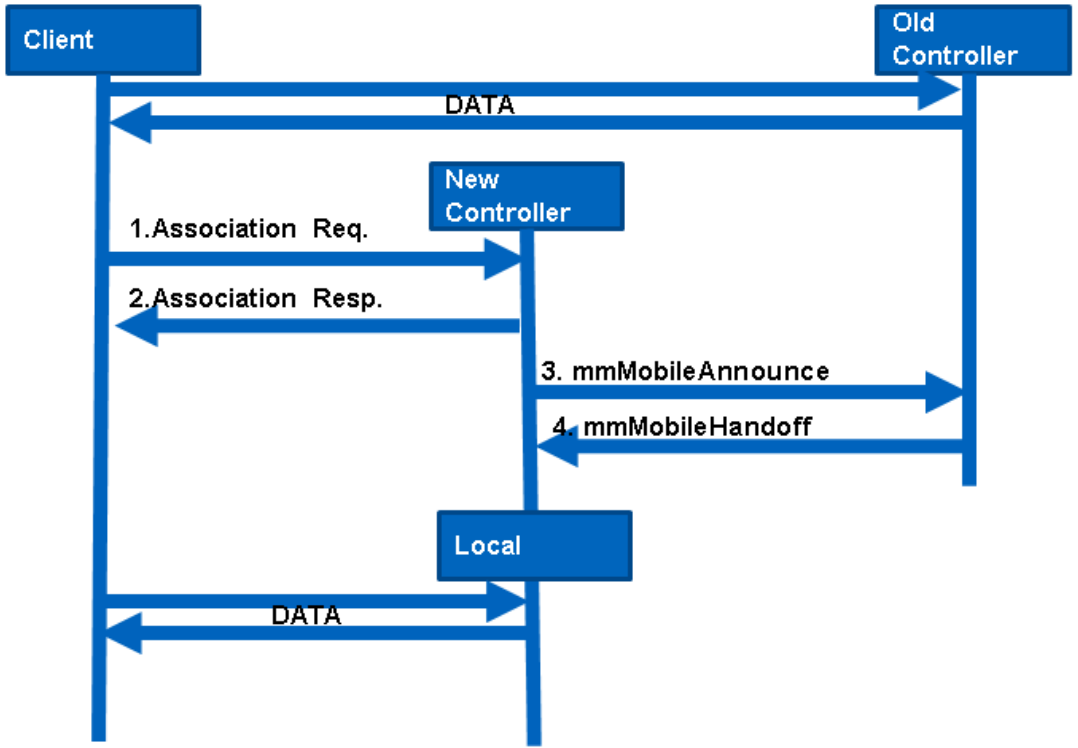
Mobility -Inter-Controller (Layer 2)



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layer 2 Roaming

- Layer 2 roams occur when you move between WLCsand both WLCshave connectivity to the same client subnets. In this case, the client database entry is simply moved to the new WLC.



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility - Layer 2 Inter WLC

Debug Client <Mac Address>

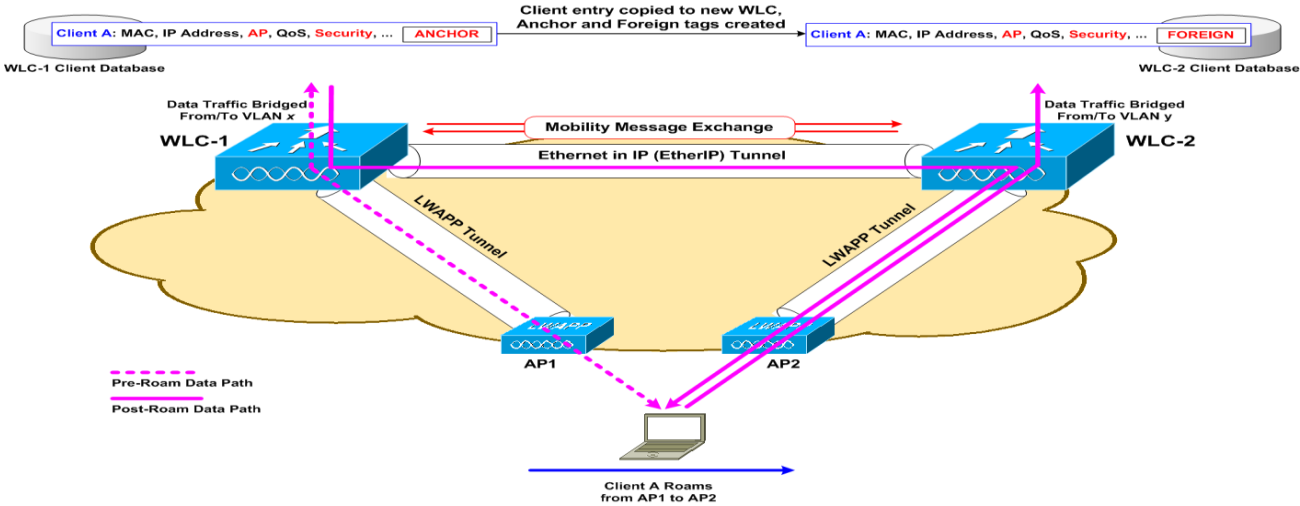
Debug Client <Mac Address>

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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
- **Symmetric**

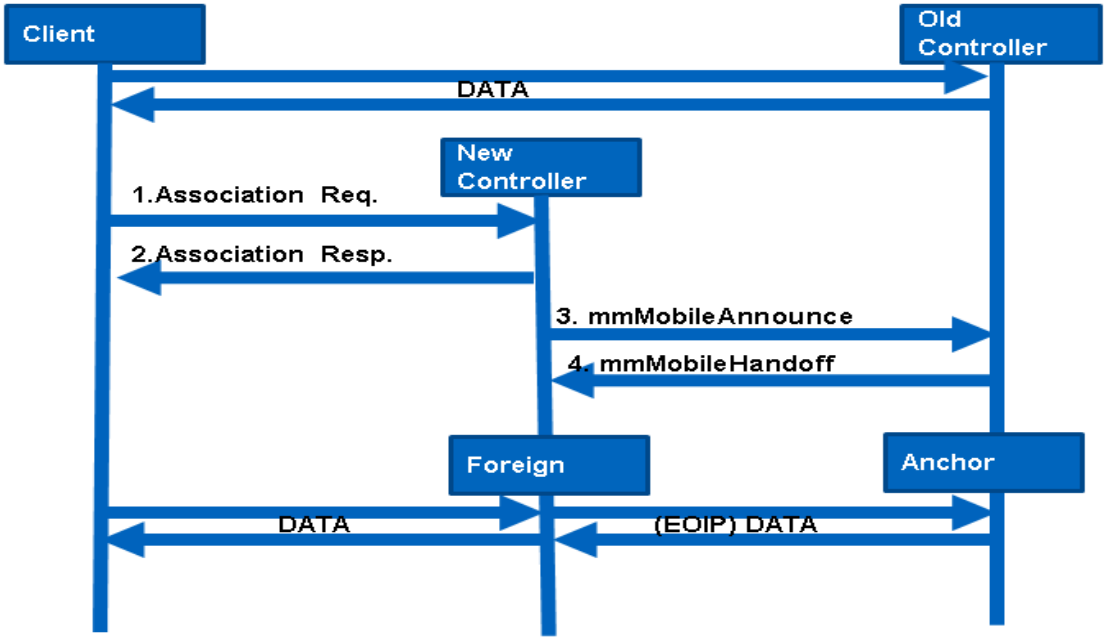
  traffic path



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

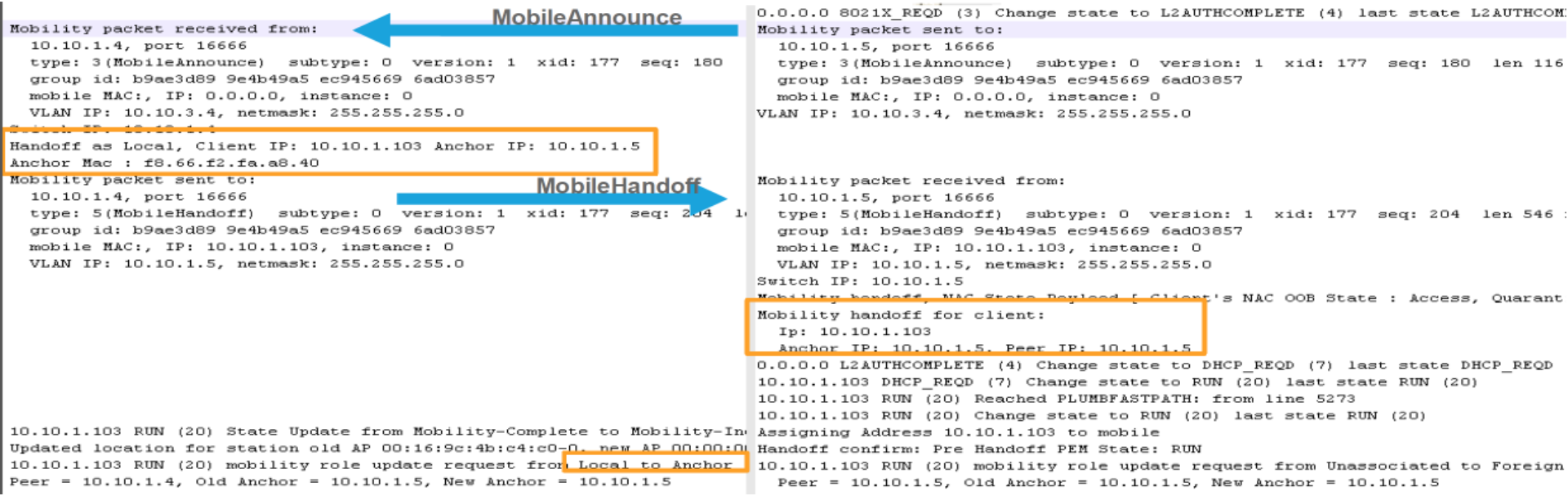


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility - Layer 3 Inter WLC

Debug Client <Mac Address>

Debug Client <Mac Address>



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobility –Typical Problems

- Misconfiguration
  - Wrong policy set

```
*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
mmAnchorExportRcvSsid=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 ExportAnchormobility msg. Delete client.
```

  - Wrong IP/MAC/Mobility name

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.

Ciscolive!

Thank you

cisco
You're
Cisco live!