TOMORROW starts here.
Troubleshooting Wireless LANs
BRKEWN-3011

Javier Contreras Albesa
WNG – Escalation Technical Leader
Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- We do we start?
- Client Troubleshooting
- AP Troubleshooting
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
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
Cisco Support Model - Escalation

- **TAC Escalation Process**
  - Multi-Tier support resources within a technology
  - TAC to engage resources (TAC/BU) when appropriate
  - SR ownership might not change hands

- **Customer Escalation Process**
  - Raise SR priority (S1/S2)
  - Engage account team
  - Your satisfaction is important to the Cisco TAC. If you have concerns about the progress of your case, please contact your regional TAC.
Software and Support

WLC Software Trains - CCO

- CCO - Cisco.com release
  - 7.0.240.0, 7.3.112.0, 7.4.120.0, etc…
  - Full test cycle
  - Classified as ED when posted

- AssureWave
  - AW validation results are available at: http://www.cisco.com/go/assurewave
  - Results available 4 weeks after CCO
  - Only specific releases will be AW tested
Software and Support

WLC Software Trains - CCO

- **MD**
  - MD tag represents stable releases for mass adoption
  - MD tag will be considered on CCO after AW release validation, 10 weeks in field and TAC/Escalation signoff

- **Escalation builds**
  - Used through TAC to deliver urgent fixes before next CCO
  - Supported by TAC
  - “Copy” of CCO plus pointed fixes

- **Interim MR beta builds**
  - Early visibility on next MR release
  - Public
Software and Support - Takeaways

- Have at hand:
  - Sh run
  - Clear problem description
  - Problem reproduction if known

- Client issues
  - Deb client

- Crash
  - Crash file (transfer upload…)

Wireless Troubleshooting
Troubleshooting Basics

- Troubleshooting 101
  - Clearly define the problem
  - Understand any possible triggers
  - Know the expected behavior
  - Reproducibility
  - Do not jump into conclusions
Troubleshooting Basics

- Troubleshooting is an art with no right or wrong procedure, but best with a logical methodology.

- Step 1: Define the problem
  - TOP point
    - 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
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 can mean root cause isolation

- **Step 3: Know the expected behavior**
  - If you know the order of expected behavior that is failing, defining where the behavior 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”
Troubleshooting Basics

- **Step 4: Reproducibility**
  - Any problem that has a known procedure to reproduce (or frequently randomly occurs) should be easy 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 much easier to work in development, test fix and deliver with lower impact to end customer
  - Test will be conducted to isolate RCA

- **Step 5: Fix -> Internal**
  - Validate RCA
  - Develop Fix
  - Test for solution, intersection
Troubleshooting Tools

- **Wireless Sniffer**
  - Example: Linksys USB600N with Omnipeek
    - TAC can publish Omnipeek-RA if you have compatible HW
    - Windows 7 with Netmon 3.4 [https://supportforums.cisco.com/docs/DOC-16398](https://supportforums.cisco.com/docs/DOC-16398)
    - Mac OS X 10.6+ [https://supportforums.cisco.com/docs/DOC-19212](https://supportforums.cisco.com/docs/DOC-19212)

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

- **Spectrum Analyzer**
  - Spectrum Expert with Card or Clean-Air AP

- **The “Debug client”**

- **AP Packet Capture**
Where do we start?
Where do we start?

- Client can’t connect....
Client Troubleshooting
Reducing Scope is everything. State is key point:
# Understanding the Client State

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8021X_REQD</td>
<td>802.1x (L2) Authentication Pending</td>
</tr>
<tr>
<td>DHCP_REQD</td>
<td>IP Learning State</td>
</tr>
<tr>
<td>WEBAUTH_REQD</td>
<td>Web (L3) Authentication Pending</td>
</tr>
<tr>
<td>RUN</td>
<td>Client Traffic Forwarding</td>
</tr>
</tbody>
</table>

(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)
The Client Debug

- A multi-debug macro that goes over all 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

- dhcp packet enabled
- dot11 mobile enabled
- dot11 state enabled
dot1x events enabled
dot1x states enabled
- pem events enabled
- pem state enabled
- CCKM client debug enabled
Steps to Building an 802.11 Connection

1. Listen for Beacons
2. Probe Request
3. Probe Response
4. Authentication Request
5. Authentication Response
6. Association Request
7. Association Response
8. (Optional: EAPOL Authentication)
9. (Optional: Encrypt Data)
10. Move User Data

State 1: Unauthenticated, Unassociated
State 2: Authenticated, Unassociated
State 3: Authenticated, Associated
Client States- Walkthrough

- **START (0)** Change state to **AUTHCHECK (2)** last state **START (0)**
- **AUTHCHECK (2)** Change state to **8021X_REQD (3)** last state **AUTHCHECK (2)**
- **8021X_REQD (3)** Change state to **L2AUTHCOMPLETE (4)** last state **8021X_REQD (3)**
- **DHCP_REQD (7)** last state **L2AUTHCOMPLETE (4)**
- **DHCP_REQD (7)** Change state to **RUN (20)** last state **DHCP_REQD (7)**
WLC Architecture (5500)
Client traffic, not RUN

- Multicore CPU (Control)
- Multicore CPU (Data)
- PCIe Switch
- I/O Subsystem
- AP
- Client

Network

Slow Path

Fast Path

Service Port
WLC Architecture (5500)
Client traffic, RUN

- **Multicore CPU (Control)**
- **Multicore CPU (Data)**
- **PCIe Switch**
- **I/O Subsystem**
- **Service Port**
- **Network**
- **Slow Path**
- **Fast Path**
- **CAPWAP Control**
- **Client Traffic**

**Diagram Notes:**
- Client traffic is divided into Slow Path and Fast Path.
- The Slow Path includes CAPWAP Control and Client Traffic.
- The Fast Path includes Multicore CPU (Control) and Multicore CPU (Data).
Client States- Walkthrough

- **Association (Start)**
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
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 - vlan 50, interface id 14, interface 'vlan50'

processSsidIE  statusCode is 0 and status is 0
processSsidIE  ssid_done_flag is 0 finish_flag is 0
STA - rates (8): 130 132 139 12 150 24 36 0 0 0 0 0 0
suppRates  statusCode is 0 and gotSuppRatesElement is 1
STA - rates (12): 130 132 139 12 150 24 36 48 72 96 108 0 0 0
extSuppRates  statusCode is 0 and gotExtSuppRatesElement is 0.0.0.0

0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 apfPemAddUser2 (apf_policy.c:333) Changing state for mobile 00:1c:58:8e:a5:84 on AP 00:3a:9a:a8:ac:d0 from Idle to Associate

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

*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
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 - vlan 50, interface id 14, interface 'vlan50'

  processSsidIE statusCode is 0 and status is 0
  processSsidIE ssid_done_flag is 0 finish_flag is 0
  STA - rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
  suppRates statusCode is 0 and gotSuppRatesElement is 1
  STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
  extSuppRates statusCode is 0 and gotExtSuppRatesElement is 1


*apfMsConnTask_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
  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 Scheduling deletion of Mobile Station: (callerId: 20) in 10 seconds


Association – CCKM failed

*apfMsConnTask_1: Mar 01 11:03:36.686: 64:00:f1:79:a9:39 Reassociation received from mobile on AP a0:cf:5b:fa:df:60
*apfMsConnTask_1: Mar 01 11:03:36.686: 64:00:f1:79:a9:39 172.25.3.179 RUN (20) Changing ACL 'none' (ACL ID 255) ===>
'none' (ACL ID 255) --- (caller apf_policy.c:1621)
*apfMsConnTask_1: Mar 01 11:03:36.686: 64:00:f1:79:a9:39 Applying site-specific IPv6 override for station 64:00:f1:79:a9:39
- vapId 1, site 'default-group', interface 'voip'
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 Applying IPv6 Interface Policy for station 64:00:f1:79:a9:39 - vlan 25, interface id 11, interface 'voip'
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 STA - rates (0): 152 36 48 72 96 108 0 0 0 0 0 0 0 0 0 0
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 STA - rates (6): 152 36 48 72 96 108 0 0 0 0 0 0 0 0 0 0
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 Processing RSN IE type 48, length 22 for mobile 64:00:f1:79:a9:39
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 Received RSN IE with 0 PMKIDs from mobile 64:00:f1:79:a9:39
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 CCKM: Processing REASSOC REQ IE
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 CCKM: Failed to validate REASSOC REQ IE
*apfMsConnTask_1: Mar 01 11:03:36.687: 64:00:f1:79:a9:39 Sending Assoc Response to station on BSSID a0:cf:5b:fa:df:60
(status 1) ApVapId 1 Slot 0
Association – Data rates failed

*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 Applying site-specific Local Bridging override for station 00:23:a7:00:46:a1 - vapId 6, site 'default-group', interface 'bp_secure1'
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 Applying Local Bridging Interface Policy for station 00:23:a7:00:46:a1 - vlan 510, interface id 12, interface 'bp_secure1'
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 processSsidIE statusCode is 0 and status is 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 processSsidIE ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 STA - rates (4): 36 48 72 108 0 0 0 0 0 0 0 0 0 0 0 0 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 suppRates statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 STA - rates (8): 36 48 72 108 12 18 24 96 0 0 0 0 0 0 0 0
*apfMsConnTask_6: Sep 12 15:17:48.686: 00:23:a7:00:46:a1 extSuppRates statusCode is 18 and gotExtSuppRatesElement is 0
*apfMsConnTask_6: Sep 12 15:17:48.686: 00:23:a7:00:46:a1 Sending Assoc Response to station on BSSID 08:d0:9f:be:0f:b0 (status 18) ApVapId 6 Slot 1
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
*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
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

```plaintext
>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]=205
```

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

Be careful
Client States- Walkthrough

- Association (Start)
- **L2 Authentication (8021X_REQD)**
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
PSK authentication

- Probe Request
- Probe Response
- Auth Request
- Auth Response
- Association Request
- Association Response
- EAPoL 4 way Exchange
- DATA

AP -> WLC

Radius
PSK – Successfull

*apfMsConnTask_1: Dec 16 15:30:14.920: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa
*apfMsConnTask_1: Dec 16 15:30:14.921: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:aa (status 0)
*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 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:aa (status 0)

*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 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 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 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 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)
PSK – Wrong secret

*apfMsConnTask_1: Dec 16 15:25:28.923: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa

*apfMsConnTask_1: Dec 16 15:25:28.925: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:aa (status 0)


*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Starting key exchange to mobile 00:40:96:b5:db:d7, data packets will be dropped

*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7 config 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 deauth count 2

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

*dot1xMsgTask: Dec 16 15:25:32.020: 00:40:96:b5:db:d7 Scheduling deletion of Mobile Station: (callerId: 57) in 10 seconds
PSK – Wrong secret - excluded


*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
802.1X Authentication

Between 4 and 20+ frames

Probe Request
Probe Response

Auth Request
Auth Response

Association Request
Association Response

EAP Start

EAP ID Request
EAP ID Response

EAP Method

EAP Success

EAPoL 4 way Exchange

DATA

AP

WLC

Radius

Between 4 and 20+ frames
Sending Assoc Response to station on BSSID 04:da:28:94:ce (status 0)

Sending EAP-Request/Identity to mobile 00:40:96:b5:db:d7 (EAP Id 1)

Sending EAP-Request/Identity to mobile 00:40:96:b5:db:d7 (EAP Id 2)

Received EAP Response packet with mismatching id (currentId=2, eapid=1) from mobile 00:40:96:b5:db:d7

Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7

EAP State update from Connecting to Authenticating for mobile 00:40:96:b5:db:d7

Sending EAP Request from AAA to mobile 00:40:96:b5:db:d7 (EAP Id 220)

WARNING: updated EAP-Identifier 2 ==> 220 for STA

Sending EAP Request from AAA to mobile 00:40:96:b5:db:d7 (EAP Id 220)

Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7

Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
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 Auth Response state for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 acl from 255 to 255

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 Flex acl from 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-auth timeout to 1800 seconds, got from WLAN config.
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Station 00:40:96:b5:db:d7 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Creating a PKC PMKID Cache entry for station 00:40:96:b5:db:d7 (RSN 2)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 Sending EAP-Success to mobile 00:40:96:b5:db:d7 (EAP Id 228)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 00:40:96:b5:db:d7
**802.1x – EAP ID timeout**

*apfMsConnTask_1: Dec 16 14:55:03.127: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:ae (status 0) ApVapId 2 Slot 1

*apfMsConnTask_1: Dec 16 14:55:03.127: 00:40:96:b5:db:d7 Updating AID for REAP AP Client f8:4f:57:a1:d8:a0 - AID ===> 1
*Dot1x_NW_MsgTask_7: Dec 16 14:55:03.129: 00:40:96:b5:db:d7 Station 00:40:96:b5:db:d7 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_7: Dec 16 14:55:03.129: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state
*Dot1x_NW_MsgTask_7: Dec 16 14:55:03.129: 00:40:96:b5:db:d7 Sending EAP-Request/Identity to mobile 00:40:96:b5:db:d7 (EAP Id 1)
Client States- Walkthrough

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
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 broadcast out VLAN
  IP helper or other means required
DHCP

*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Local, client state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5752, Adding TMP rule
*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, Local Bridging Vlan = 50, Local Bridging intf id = 12
*apfReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Jan 02 10:45:27.476: 68:7f:74:75:f1:cd 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
DHCP – Process Start

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

DHCP selected relay 1 - 192.168.50.1 (local address 192.168.50.15, gateway 192.168.50.1, VLAN 50, port 1)
DHCP transmitting DHCP DISCOVER (1)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP xid: 0xa504e3 (10814691), secs: 0, flags: 0
DHCP chaddr: 68:7f:74:75:f1:cd
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP siaddr: 0.0.0.0, giaddr: 192.168.50.15
DHCP sending REQUEST to 192.168.50.1 (len 350, port 1, vlan 50)
DHCP – Offer

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

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

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

192.168.50.101 WEBAUTH_REQD (8) pemAdvanceState2 6662, Adding TMP rule
192.168.50.101 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0
IPv4 A
Plumbing web-auth redirect rule due to user logout
Assigning Address 192.168.50.101 to mobile
DHCP – Rejected

DHCP transmitting DHCP REQUEST (3)
DHCP  op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP  xid: 0xf3a2fca6 (4087544998), secs: 3, flags: 0
DHCP  chaddr: d0:b3:3f:33:1c:88
DHCP  ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP  siaddr: 0.0.0.0, giaddr: 10.87.193.2
DHCP  requested ip: 10.65.8.177
DHCP sending REQUEST to 10.87.193.1 (len 374, port 1, vlan 703)
DHCP selecting relay 2 - control block settings:
  dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
  dhcpGateway: 0.0.0.0, dhcpRelay: 10.87.193.2 VLAN: 703
DHCP selected relay 2 - NONE

DHCP received op BOOTREPLY (2) (len 308,vlan 703, port 1, encap 0xec00)
DHCP sending REPLY to STA (len 402, port 1, vlan 701)
DHCP transmitting DHCP NAK (6)
DHCP  op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 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
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 talk before validating DHCP

- Up to client to realize their address is not valid for the subnet

- DHCP Required on WLAN modifies it
DHCP Required - Caveats

- 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
  - Client may hold until DHCP half-lease time

```
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
```
Client States- Walkthrough

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
Webauth- Walkthrough

Client

1. Association

Controller

2. Authenticate
   - Mac Auth
   - (Access Reject)

Radius

Captive Portal

3. Association Response

4. DHCP

5. HTTP Request

Redirection

To Captive portal: ap_mac, switch_url (controller auth url), redirect(original url), statusCode (result code from wlc), wlan (SSID user is connected), user_mac

Only in mac auth
Webauth- Walkthrough

Sign up page (web user)
URL points to controller
Username/password pre-populated with expected values

Authenticate
Username/pass

Access Accept
Redirection URL

Redirect to splash page
Portal/Network Access

Final Customized page to client

User Form Submit

Client
Controller
Radius
Captive Portal
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, dtlFlags 0x0

Preparing redirect URL according to configured Web-Auth type
Checking custom-web config for WLAN ID:2
unable to get the hostName for virtual IP, using virtual IP =1.1.1.1
Global status is enabled, checking on web-auth type
Web-auth type Internal, no further redirection needed. Presenting default login page to user
http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma" content="
http_response_msg_body2 is ""></HEAD></HTML>

parser host is 192.168.0.45
- parser path is /
added redirect=, URL is now https://1.1.1.1/login.html?
str1 is now https://1.1.1.1/login.html?redirect=192.168.0.45/
clen string is Content-Length: 302
Message to be sent is
   HTTP/1.1 200 OK
Location: https://1.1.1.1/login.html?redirect=192.168.0.45/
Content-Type: text/html
Content-Length: 302
<HTML><HEAD><TITLE>
send data length=428
Webauth Redirect – IPv6

webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- str1 is now

*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- Message to be sent is
HTTP/1.1 200 OK
Content-Type: text/html
Content-L
Webauth Redirect

- Login page requested over https

*emWeb: Jan 02 10:45:53.334: ewaURLHook: Entering:url=/login.html, virtIp = 1.1.1.1, ssl_connection=1, secureweb=1

...
Webauth Success

*emWeb: Jan 02 10:46:42.904:
ewaURLHook: Entering:url=/login.html, virtIp = 1.1.1.1, ssl_connection=1, secureweb=1

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


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

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

- Server IP must be allowed on the preauth ACL... otherwise, loop!


..

*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser host is 192.168.0.21

NEXT:

*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- parser host is 192.168.0.21
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- added redirect=, URL is now

...*

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”
Webauth Take aways

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

- ARP/DNS must work before you can do anything

- Additional debug needed
  - debug web-auth redirect enable mac XX

- Client side capture/logs may be needed
Client States- Walkthrough

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
RUN status

- RUN means: client has completed all required policy states
- “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 6076
  *dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Adding Fast Path rule
  *dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Fast Path rule (contd...) 802.1P = 5, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 101, Local Bridging intf id = 18
  *dot1xMsgTask: Nov 05 14:35:11.841: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255)
  pemReceiveTask: Nov 05 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, dtlFlags 0x0
RUN status - Typical Problems

- Random Disconnections – Radio Reset
  - There are normal radio resets: Channel changes, old packet purge, 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: Cnt 0, Last Ret: 0, Fails: 0, Recvry Status: Stalled NO, In Prog NO
      Code/Count: 37/00010 84D7 51/00021 F25E 52/00012 F25E 54/00002 84D6
      Code/Count: 62/00067 F25F 67/00001 0
RUN status - Typical Problems

- Environmental trigger
  - Typical high channel utilization

```
ap2600-sw1-0-31#sh cont d0 | b QBS
QBSS Load: 0xFE Tx 0 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
```
RUN status - Typical Problems

- Poor Performance
  - RF issues
  - Client side bugs
Client States- Walkthrough

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
Deauthenticated 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)
Deauthenticated 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 Deauth**
  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)
  ```
Deauthenticated Client

- Authentication Timeout
  Auth or Key Exchange max-retransmissions reached

  Retransmit failure for EAPOL-Key M3 to mobile 00:1e:8c:0f:a4:57, retransmit count 3, mscb deauth count 0
  Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller 1x_ptsm.c:534)

- AP Radio Reset (Power/Channel)
  AP disasassociates clients but WLC does not delete entry

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


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

*dot1xMsgTask: Oct 22 15:32:53.056: 24:77:03:c2:8a:20 Sent Deauthenticate to mobile on BSSID 20:3a:07:e4:c8:f0 slot 0(caller 1x_ptsm.c:570)
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 require to see exact reason
  Never forget Radio status and RF conditions
AP Troubleshooting
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
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
AP Supportability

- Filtering per AP
  - debug mac addr 04:da:d2:4f:f0:50
  - debug capwap events enable
  - Use radio mac

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

- APs have “flight recorder”

cap2600i-sw1-033#dir
Directory of flash: /

- rw 64279 Jan 2 2014 10:32:24 +00:00 event.log
- rwx 128 Jan 2 2014 10:26:12 +00:00 configs
- rwx 280 Jan 2 2014 15:41:58 +00:00 lwapp_officeextend.cfg
- rwx 352 Jan 2 2014 15:41:52 +00:00 env_vars
- rwx 49168 Jan 3 2014 06:26:30 +00:00 lwapp_non_apspecific_reap.cfg
- rwx 965 Nov 21 2013 15:22:52 +00:00 lwapp_mm_mwar_hash.cfg
- rwx 49168 Jan 2 2014 15:42:08 +00:00 lwapp_reap.cfg
- drwx 125501 Nov 20 2013 17:22:48 +00:00 event.r0
- drwx 192 Dec 20 2012 21:37:52 +00:00 ap3g2-rcvk9w8-mx
- rwx 265 May 28 2013 09:58:54 +00:00 lwapp_mobileconcierge.cfg
- rwx 66319 Jan 2 2014 10:08:04 +00:00 event.capwap
- rwx 7192 Jan 3 2014 06:26:27 +00:00 private-multiple-fs
- drwx 1792 Jan 2 2014 10:22:48 +00:00 ap3g2-k9w8-mx.152-4.JB3
AP Discover/Join

- Typical source for problems
- Main idea: you must always have discovery mechanism
- AP is social animal
AP Discover/Join

AP Runs **Hunting** Algorithm to Find Candidate Controllers to Join

Diagram:
- **Discovery**
- **Reset**
- **Image Data**
- **Join**
- **Config**
- **Run**
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>”
L3 WLC Discovery

AP Tries to Send Discover Messages to All the WLC Addresses that Its Hunting Process Turned Up
AP Discover/Join – AP Side

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

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

*Jan 2 15:41:52.467: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.5.55 peer_port: 5246
AP Discover/Join – WLC Side

*spamApTask7: Jan 02 15:35:57.296: apType = 27 apModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apType: 0x1b bundleApImageVer: 7.6.100.0
*spamApTask7: Jan 02 15:35:57.296: version:7 release:6 maint:100 build:0
*spamApTask7: Jan 02 15:35:57.296: 04:da:d2:4f:f0:50 Discovery Response sent to 192.168.5.156 port 7411
*spamApTask6: 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
Troubleshooting Lightweight APs

Check the Basics First

- 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 the AP from the controller (not for mesh until 7.4!)
- If pings are successful, ensure the AP has at least one method by which to discovery at least a single WLC
- Check that default GW in AP is valid
- Check time in WLC is valid
- Console or telnet/ssh into the controller to run debugs
*Jan 3 07:48:36.603: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-4'(index 0).
*Jan 3 07:48:36.603: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Jan 3 07:48:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.5.54 peer_port: 5246
*Jan 3 07:48:37.467: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.5.54 peer_port: 5246
*Jan 3 07:48:37.467: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.5.54
*Jan 3 07:48:37.467: %CAPWAP-3-ERRORLOG: 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


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
Mobility—Intra-Controller

- Client roams between two APs on the same controller
Mobility—Inter-Controller (Layer 2)
Mobility—Inter-Controller (Layer 2)

- Client roams between two APs that are connected to two different controllers
- Client connects to a WLAN on a controller that has a different controller as a WLAN anchor Layer 2 roaming:
  - New WLC has an interface configured on the same network as WLC the client is coming from
  - Client session information completely transferred from old WLC to new WLC, and client entry is deleted from old WLC
Mobility - 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
Mobility - Supported Scenarios

- Clients can roam between two APs that are configured as one of the following modes:
  - Local
  - H-REAP / FlexConnect
    - Locally-switched WLAN
    - Centrally-switched WLAN
    - APs part of the same H-REAP group joined to the same WLC for OKC / CCKM

- Roaming is not supported between Local and H-REAP mode APs.

- Mobility is based on VLAN ID as of version 7.2:
  - VLAN tagging is required for roaming to work!
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

- Mobility Domain - WLCs in the mobility list
  - L2/L3 Handoff
  - Auto Anchoring
Mobility - Messaging Flow

- When a client connects to a WLC for the first time, the following happens:
  - New WLC sends MOBILE_ANNOUNCE to all controllers in the mobility group when client connects (note: if possible, configure multicast mobility to lower CPU load and handoff times)
  - Old WLC sends HANDOFF_REQUEST, telling the new WLC I have an entry for this client, here is the client status
  - New WLC sends HANDOFF_REPLY, telling the old WLC OK
Mobility—L2 Inter WLC

0.0.0.0 8021X_REQ (3) Change state to LAUTHCOMPLETE (4) last state L2AUTHCOMPLETE
Mobility query, PEF State: L2AUTHCOMPLETE

........

Mobility packet sent to:
10.10.1.4, port 16666

0.0.0.0 LAUTHCOMPLETE (4) Change state to DHCP_REQ (7) last state DHCP_REQ (7)
0.0.0.0 Added NPU entry of type 9, dtflFlags 0x0

........

Mobility packet received from:
10.10.1.5, port 16668

0.0.0.0.0 8021X_REQ (3) State Update from Mobility-Complete to Mobility-Incomplete,........

10.10.3.235 8021X_REQ (3) Mobility role update request from Local to Handoff
Peer = 0.0.0.0, Old Anchor = 10.10.1.5, New Anchor = 0.0.0.0

Clearing Address 10.10.3.235 on mobile
spfMnProcessDeleteMobile (mpn mn:0:542) Expiring Mobile!  

Debug Client <Mac Address>

Debug Mobility Handoff Enable

BRKEWN-3011  © 2014 Cisco and/or its affiliates. All rights reserved.  Cisco Public
Mobility—L3 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

Mobility packet received from:
10.10.1.4, port 16566
type: 3 (MobilityAnnounce) subtype: 0 version: 1 xid: 177 seq: 180
group id: b9e3d89 9e4b49a5 ec945669 6ad36857
mob WLC: IP: 0.0.0.0, instance: 0
VLAN IP: 10.10.3.4, netmask: 255.255.255.0

Handoff as Local, Client IP: 10.10.1.103 Anchor IP: 10.10.1.5
Anchor Mac: f0.86.32.fa.a0.40

Mobility packet sent to:
10.10.1.5, port 16566
type: 5 (MobilityHandoff) subtype: 0 version: 1 xid: 177 seq: 204

Mobility packet received from:
10.10.1.5, port 16566
type: 3 (MobilityAnnounce) subtype: 0 version: 1 xid: 177 seq: 180

Mobility packet sent to:
10.10.1.5, port 16566
type: 5 (MobilityHandoff) subtype: 0 version: 1 xid: 177 seq: 204

0.0.0.0 802.1X_REQ (3) Change state to L2AUTHCOMPLTE (4) last state L2AUTHCOMM

0.0.0.0 802.1X_REQ (3) Change state to L2AUTHCOMPLTE (4) last state L2AUTHCOMM

0.0.0.0 802.1X_REQ (3) Change state to L2AUTHCOMPLTE (4) last state L2AUTHCOMM

0.0.0.0 802.1X_REQ (3) Change state to L2AUTHCOMPLTE (4) last state L2AUTHCOMM

10.10.1.103 RUN (20) State Update from Mobility-Complete to Mobility-In
Updated location for station old AP 00:16:3c:4b:4c:00- new AP 00:03:01-02
10.10.1.103 RUN (20) mobility role update request from Local to Anchor
Peer = 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5

10.10.1.103 RUN (20) State Update from Mobility-Complete to Mobility-In
Updated location for station old AP 00:16:3c:4b:4c:00- new AP 00:03:01-02
10.10.1.103 RUN (20) mobility role update request from Local to Anchor
Peer = 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5

0.0.0.0 802.1X_REQ (3) Change state to L2AUTHCOMPLTE (4) last state L2AUTHCOMM

BRKEWN-3011 © 2014 Cisco and/or its affiliates. All rights reserved.
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 mmAnchorExportRcv Ssid=webauth Security Policy=0x2050

  - Wrong IP/MAC/Mobility name
Other Troubleshooting Tools
Wireshark Tips

- Default Wireshark view might look like this:
Wireshark Tips

- Newer versions of Wireshark have a feature for “Apply as Column”
  This will take any decodable parameter and make a column
Wireshark Tips

- Within seconds your wireshark can also have:
Wireshark Tips

- Filtering data is just as easy

Frame 52: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits)
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........

Type/Subtype: Beacon frame (0x00)

- Frame Control: 0x0008 (Normal)
- Duration: 0
- Destination address: Broadcast
- Source address: Cisco_c0:08:ae
- BSSID: Cisco_c0:08:ae
- Fragment number: 0
- Sequence number: 4080
- Frame check sequence: 0x0000

IEEE 802.11 Wireless LAN management

Filter: wlan.bssid -- ec:c8:82:c0:08:ae
Wireshark Tips

- You can also create coloring rules
Wireshark Tips - CAPWAP

- For wired capture, user data is encapsulated in CAPWAP
Wireshark Tips

- Wireshark can also de-encapsulate CAPWAP DATA
  Edit > Preference > Protocols > CAPWAP
Wireshark Tips

- With CAPWAP de-encapsulated you can see all the packets to/from client (between AP and WLC)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>BSS Id</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>6478</td>
<td>713.759210.10.3.32</td>
<td>10.10.3.255</td>
<td></td>
<td></td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>6481</td>
<td>713.7595Cisco_24:77:43</td>
<td>HonHaiPr_da:83:76</td>
<td>00:1c:b1:07:68:30</td>
<td>Data, SN-0, FN-0, Fla</td>
<td></td>
</tr>
<tr>
<td>6482</td>
<td>714.231100:00:00_00:00:00</td>
<td>Cisco_07:68:30</td>
<td>00:1c:b1:07:68:30</td>
<td>Probe Request, SN-0,</td>
<td></td>
</tr>
<tr>
<td>6483</td>
<td>714.2747HonHaiPr_da:83:76</td>
<td>Broadcast</td>
<td>00:1c:b1:07:68:30</td>
<td>Gratuitous ARP for 10</td>
<td></td>
</tr>
<tr>
<td>6484</td>
<td>714.759110.10.3.32</td>
<td>10.10.3.255</td>
<td></td>
<td></td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>6491</td>
<td>714.7596Cisco_24:77:43</td>
<td>HonHaiPr_da:83:76</td>
<td>00:1c:b1:07:68:30</td>
<td>Data, SN-0, FN-0, Fla</td>
<td></td>
</tr>
<tr>
<td>6492</td>
<td>715.323710.10.3.32</td>
<td>239.255.255.250</td>
<td>00:1c:b1:07:68:30</td>
<td>M-SEARCH # HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>6495</td>
<td>715.3384HonHaiPr_da:83:76</td>
<td>Broadcast</td>
<td>00:1c:b1:07:68:30</td>
<td>Who has 10.10.3.1? T</td>
<td></td>
</tr>
</tbody>
</table>

- Frame 6478: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
- Internet Protocol, Src: 10.10.1.161 (10.10.1.161), Dst: 10.10.1.14 (10.10.1.14)
- User Datagram Protocol, Src Port: 51289 (51289), Dst Port: capwap-data (5247)
- Control And Provisioning of Wireless Access Points
- IEEE 802.11 Data, Flags: .......T
- Logical-Link Control
- Internet Protocol, Src: 10.10.3.32 (10.10.3.32), Dst: 10.10.3.255 (10.10.3.255)
- Internet Control Message Protocol
Wireshark Tips

- IO Graph can be used to detect anomalies
WLC Config Analyzer (WLCCA)

Support Forums DOC-1373

- Main objective: Save time while analyzing configuration files from WLCs
- Audit Checks
WLC Config Analyzer (WLCCA)

Secondary objective: Carry out RF analysis
WLC Config Analyzer (WLCCA)

- RF groups—non voice
WLC Config Analyzer (WLCCA)

- RF Problem finder – RF Index
Spectrum Expert

- SE-Connect or Local Mode
- Obtain Spectrum Key
- Connect to Remote Sensor

All APs > Details for 3502

<table>
<thead>
<tr>
<th>General</th>
<th>Credentials</th>
<th>Interfaces</th>
<th>High Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP Name</td>
<td>3502</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td>29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Spectrum Interface Key</td>
<td>31ED9B89972F17F360AE9758F732104</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Connect to Sensor

- Sensor Card with Internal Antenna
- Sensor Card with External Antenna
- Remote Sensor

IP Address: 10.10.2.57
Radio: b/g/n
Key: 31ED9B89972F17F360AE9758F732104

Some sensor cards may select external vs. internal antenna automatically in lieu of above setting.
Spectrum Expert with Clean Air
AP Packet Capture

- 7.3 and higher
- AP redirect of traffic sent/received by specific clients
- It works during normal operation
- You must know the AP names beforehand
- Limited use for encrypted WLAN (as of 7.6)
- Capture is done at AP radio driver level, not over the air
AP Packet Dump – FTP Server Required

- Feature requires use of a standard FTP server running on a network server, workstation, or laptop i.e. IIS, Filezilla, WS FTP, 3CD, etc.
- FTP server needs to be accessible by the APs capturing packets *not* the controller
- Multiple simultaneous file upload connections will be initiated to the FTP server
  - One for the AP designated in the start command
  - One for each AP that is an RF neighbor of the AP designated in the start command – *on the same controller only*
- File name format example: `3602-15508-223042013_160038.pcap`
AP Packet Capture

- Configuration:
  > config ap packet-dump classifier data enable
  > config ap packet-dump classifier control enable
  > config ap packet-dump ftp serverip 192.168.0.45 path /Public/temp username XX password YY

>config ap packet-dump start 68:7f:74:75:f1:cd cap2600i-sw1-033

Client Mac Address............................... 68:7f:74:75:f1:cd
FTP Server IP.................................... 192.168.0.45
FTP Server Path.................................. /Public/temp
FTP Server Username.............................. XX
Buffer Size for Capture.......................... 2048 KB
Packet Capture Time.............................. 10 Minutes
Packet Truncate Length............................ Unspecified
Packet Capture Classifier......................... 802.11 Data
Packet Capture Classifier......................... 802.11 Control

>config ap packet-dump stop
AP Packet Capture

- Result is wireshark capture type at FTP server
AP Sniffer Mode

- Non-Servicing radios
- AP directs all traffic to receiving station
- Omnipeek can process the encapsulated traffic for analysis, use Cisco Remote Adapter
- Wireshark may display incorrect content, even if using PEEK protocol decoder
### AP Sniffer Mode

- Capture can be saved as libpcap for later analysis

---

<table>
<thead>
<tr>
<th>Packet Source</th>
<th>Destination</th>
<th>BSSID</th>
<th>Frame Type</th>
<th>Signal</th>
<th>Data Rate</th>
<th>Timestamp</th>
<th>Relative Time</th>
<th>Protocol</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>11752</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>65</td>
<td>1000</td>
<td>265</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11759</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>16</td>
<td>1000</td>
<td>233</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11764</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>1000</td>
<td>1000</td>
<td>265</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11755</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11766</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11757</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11758</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11760</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11761</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11762</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11763</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11764</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11765</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11766</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11767</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11768</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11769</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11770</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11771</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11772</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11773</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11774</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11775</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11776</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11777</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11778</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11779</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11780</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
<tr>
<td>11781</td>
<td>08:01:01:02:47:1F:10</td>
<td>F7</td>
<td>1</td>
<td>171</td>
<td>1000</td>
<td>273</td>
<td>109:01:71:27:000</td>
<td>Beacon</td>
<td>FC360366</td>
</tr>
</tbody>
</table>
Key- Takeaways

- Troubleshooting is a process
- Don’t jump into conclusions
- Main client tool -> debug client + state machine
- Multiple tools available without much effort
  - WLC side debugs
  - AP debugs
  - AP sniffer mode, Packet capture
  - SE mode
  - WLCCA
Call to Action…

Visit the World of Solutions:-

- Cisco Campus
- Walk-in Labs
- Technical Solutions Clinics

- Meet the Engineer

- **Lunch Time Table Topics**, held in the main Catering Hall

- **Recommended Reading**: For reading material and further resources for this session, please visit [www.pearson-books.com/CLMilan2014](http://www.pearson-books.com/CLMilan2014)
Complete Your Online Session Evaluation

- Complete your online session evaluation
- Complete four session evaluations and the overall conference evaluation to receive your Cisco Live T-shirt