TOMORROW starts here.

cisco

Cisco live!

Troubleshooting Wireless LANs

BRKEWN-3011

Madhuri C

Senior TAC Engineer - Wireless

Cisco live!

Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- AP Discovery/Join
- WLC Config/Monitoring
- Client Connectivity
- Mobility
- Packet Analysis

Troubleshooting Wireless LANs

- **Software and Support**
- Troubleshooting Basics
- AP Discovery/Join
- WLC Config/Monitoring
- Client Connectivity
- Mobility
- Packet Analysis

Software and Support

- Opening a TAC Service Request
- Cisco Support Model
  - What to expect from TAC
  - How does escalation work?
- WLC Software Trains
  - CCO (ED/MD/AW)
  - Engineering Specials

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

Software and Support

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, 7.4.121.0, 7.6.100.0 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
- 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

Software and Support

WLC Software Trains - CCO

- Escalation builds
  - Used through TAC to deliver urgent fixes before next CCO
  - “Copy” of CCO plus pointed fixes
- Debug image or Test image
  - Diagnostic / validation
- Interim beta builds
  - Early visibility, Public

Software and Support - Takeaways

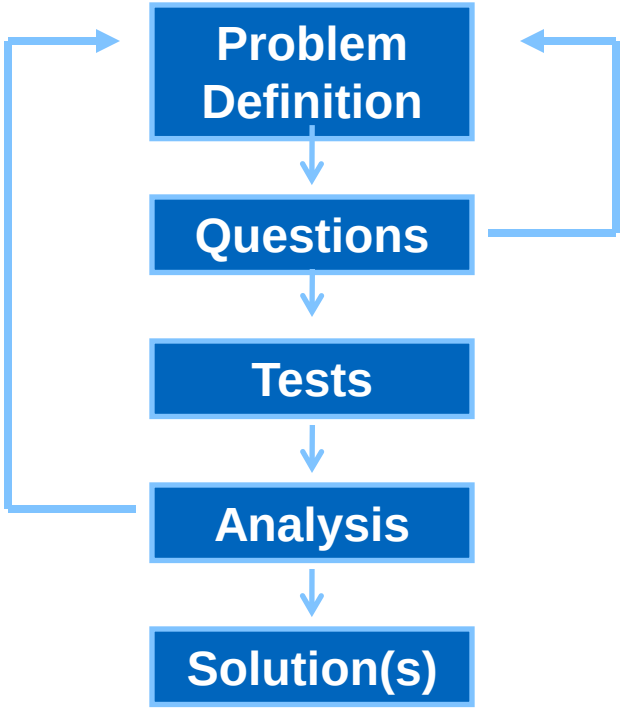
- Have at hand:
  - Show run-config
  - Clear problem description
  - Reproduce the problem
- Client issues
  - Debug client
- Crash
  - Crash file (transfer upload)

Troubleshooting Wireless LANs

- Software and Support
- **Troubleshooting Basics**
- AP Discovery/Join
- WLC Config/Monitoring
- Client Connectivity
- Mobility
- Packet Analysis

Troubleshooting Basics

- Troubleshooting
  - Clearly define the problem
  - Understand any possible triggers
  - Know the expected behaviour
  - 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
  - Reduce scope
  - Bad description: “Client slow to connect”
  - Good description: “Client associations are rejected with **Status 17** several times before they associate successfully.”

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
  - Lastly it could be a bug !!

- Step 3: Know the expected behaviour
  - Know the order of expected behaviour. We can further compare working debugs or packet capture with a non-working scenario.
  - 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 a problem is reproducible in other environments with a known procedure, TAC/BU can facilitate internal testing and proposed fix/workaround verification

Troubleshooting Basics

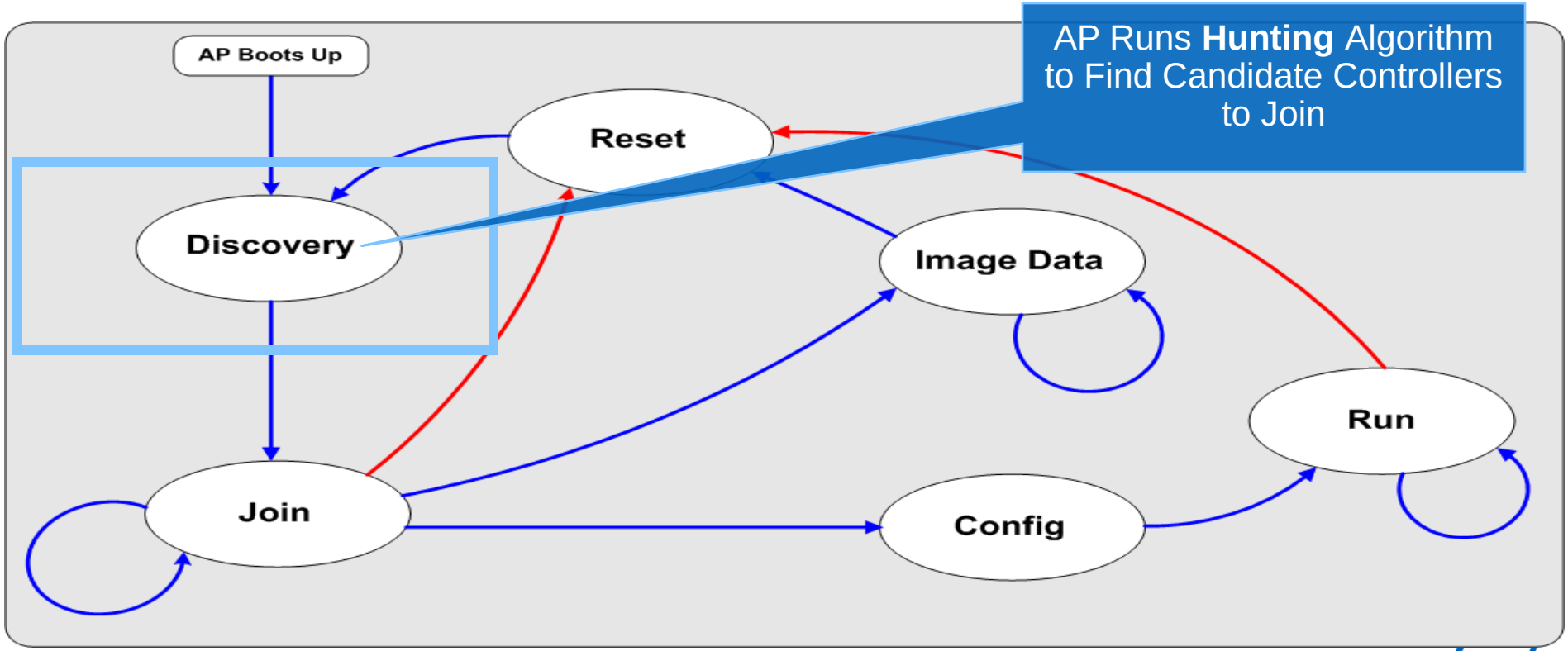
Recommended Tools

- 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
- Wired Packet Capture
  - Example: Wireshark
    - Use for spanned switchports of AP/WLC or client side data
- Spectrum Analyser
  - Spectrum Expert with Card or Clean-Air AP
- The “Client Debug” and logs from WLC, AP
- AP Packet Capture

Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- **AP Discovery/Join**
- WLC Config/Monitoring
- Client Connectivity
- Mobility
- Packet Analysis

AP Discover/Join



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>”

AP Discover/Join

Join Process

- WLCs send Discovery Response back to AP
  - Name, Capacity, AP Count, Master?, AP-MGR, Load per AP-MGR
- AP selects the single best WLC candidate from
  - High Availability Config: Primary/Secondary/Tertiary/Backup
  - Master Controller
  - Greatest available capacity
  - Ratio of total capacity to available capacity
- AP sends single Join Request to best candidate
  - WLC responds with Join Response
  - AP joins and receives config (or downloads image if not correct)

AP Discover/Join

Troubleshooting AP Discover/Join

- "Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)", Document ID 70333
- **Make sure date/time on WLC is accurate (certificates)!**
- From AP

  Debug ip udp

  Debug capwap client [event/error]
- From WLC

  Debug mac addr <AP ethernet mac>

  Debug capwap [event/error/packet] enable

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: Msg Type : **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: Msg Type : 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: Msg Type : 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: Msg Type : **CAPWAP_DISCOVERY_RESPONSE**

*Jan 2 15:41:42.055: CAPWAP Control **mesg Recd from 192.168.5.55**, Port 5246

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: 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 15:41:52.467: %CAPWAP-5-DTLSREQSUCC**:** **DTLS connection created successfully** peer_ip: 192.168.5.55

peer_port: 5246

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: 04:da:d2:4f:f0:50 ApModel: AIR-CAP2602I-E-K9

*spamApTask7: Jan 02 15:35:57.296: **apModel: AIR-CAP2602I-E-K9**

*spamApTask7: Jan 02 15:35:57.296: apType = 27 apModel: AIR-CAP2602I-E-K9

*spamApTask7: Jan 02 15:35:57.296: apType: Ox1b bundleApImageVer: 7.6.100.0

*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 Session established** server (192.168.5.55:5246), client (192.168.5.156:7411)

*spamApTask6: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c **Starting wait join timer** for AP: 192.168.5.156:7411

*spamApTask7: Jan 02 15:36:07.764: 04:da:d2:4f:f0:50 **Join Request from 192.168.5.156:7411**

*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 Join resp: CAPWAP Maximum Msg element len = 83

*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 **Join Response sent to 192.168.5.156:7411**

*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 **CAPWAP State: Join**

AP Join – Country Mismatch - AP

Example scenario

*Jan 3 07:48:36.603: %CAPWAP-3-ERRORLOG: **Selected MWAR '5500-4'(index 0).**

*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 successfully** peer_ip: 192.168.5.54 peer_port: 5246

*Jan 3 07:48:37.467: %CAPWAP-5-SENDJOIN: **sending Join Request** to 192.168.5.54

*Jan 3 07:48:37.467: %CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination.

*Jan 3 07:48:37.467: %CAPWAP-3-ERRORLOG: CAPWAP SM handler: **Failed to process message type 10 state 5**.

*Jan 3 07:48:37.467: %CAPWAP-3-ERRORLOG: Failed to process encrypted capwap packet from 192.168.5.54

*Jan 3 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

*Jan 3 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**

*Jan 3 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.!]

Troubleshooting Lightweight APs

Check the Basics First

- Make sure the AP is getting an address from DHCP server.
- If the AP's address is statically set, ensure it is correctly configured.
- Can the AP and the WLC communicate?
- If pings are successful, ensure the AP has **at least one** method by which to discovery at least a single WLC.
- Check time in WLC is valid.
- Console or telnet/ssh into the controller to run debugs.

Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- AP Discovery/Join
- **WLC Config/Monitoring**
- Client Connectivity
- Mobility
- Packet Analysis

WLC Config/Monitoring

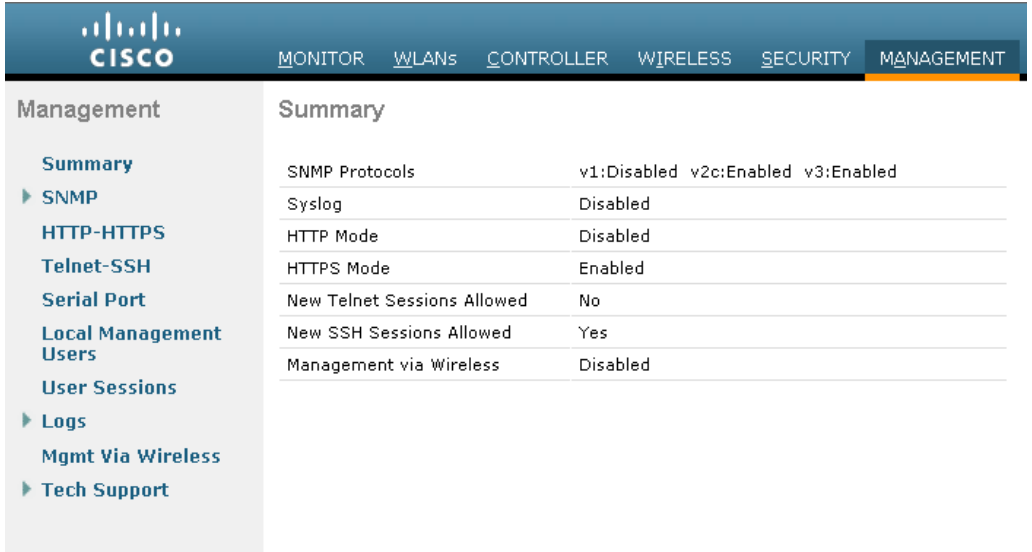
- Supportability
  - WLC
  - AP
- WLANs
- RRM / Radio / RF
- Wireless LAN Controller Config Analyser (WLCCA)

WLC Config/Monitoring

Supportability - WLC

Methods of Management

- GUI
  - HTTPS (E) / HTTP (D)
- CLI
  - Console
  - SSH (E) / Telnet (D)
- SNMP
  - V1 (D) / V2 (E) – Change me!
  - V3 (E) – Change me



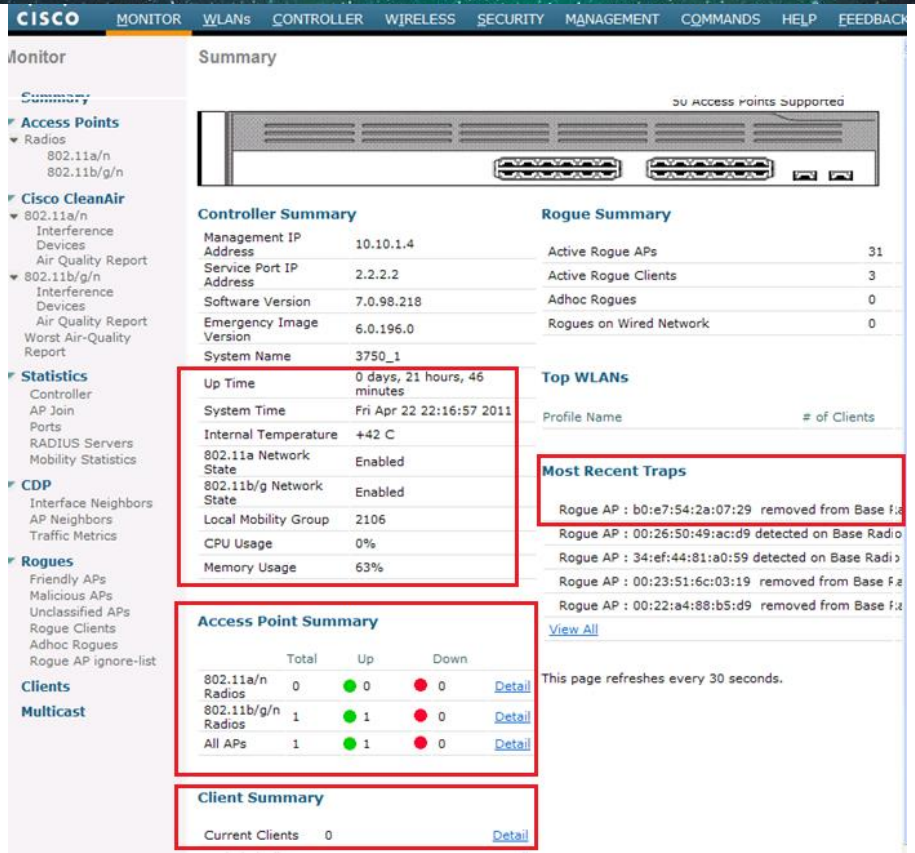
Note: Management Via Wireless Clients (D)

WLC Config/Monitoring

Supportability - WLC

Using the GUI

- Monitor
  - AP/Radio Statistics
  - WLC Statistics
  - Client Details
  - Trap Log



WLC Config/Monitoring

Supportability - WLC

Using the GUI

- Wireless > All APs
  - AP list shows AP Physical UP Time
  - APs are sorted by Controller Associated Time
  - Select AP to see Controller Associated Time

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

All APs

Current Filter: None [Change Filter] [Clear Filter]

Number of APs: 3

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type
APc47d.4f3a.e3d0	AIR-CAP3502E-A-K9	c4:7d:4f:3a:e3:d0	0 d, 00 h 18 m 09 s	Enabled	REG	29	Local	LSC
AP-1140-1	AIR-LAP1142N-A-K9	00:22:90:91:3f:70	5 d, 22 h 02 m 04 s	Enabled	REG	29	Local	MIC
AP001c.58dc.8574	AIR-LAP1131AG-A-K9	00:1c:58:dc:85:74	0 d, 00 h 00 m 00 s	Enabled	Downloading	29	Local	MIC

Time Statistics

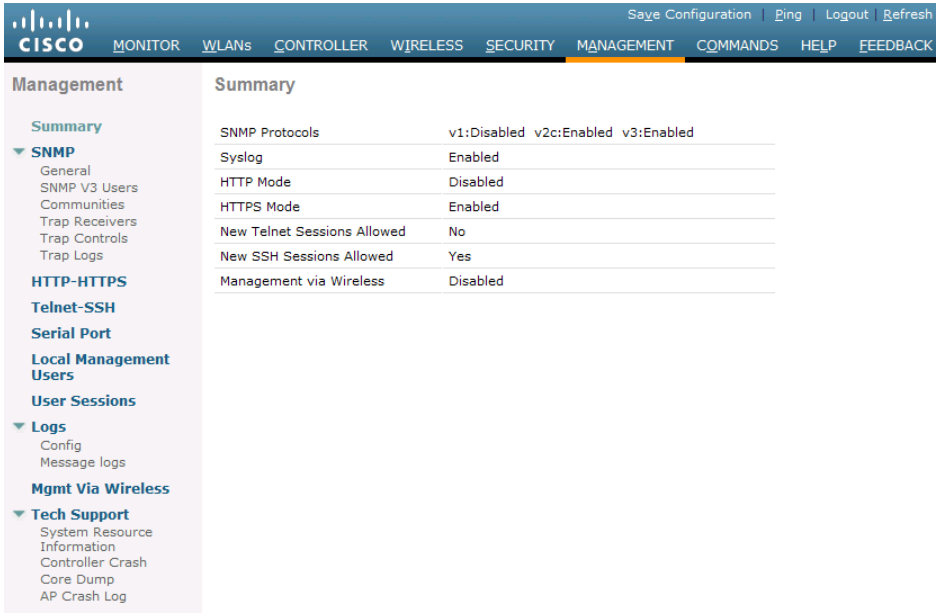
UP Time	5 d, 22 h 02 m 53 s
Controller Associated Time	0 d, 00 h 02 m 02 s
Controller Association Latency	0 d, 00 h 00 m 10 s

WLC Config/Monitoring

Supportability - WLC

Using the GUI

- Management
  - SNMP Config
  - Logs
  - Tech Support



WLC Config/Monitoring

WLC Important Show Commands

- **Show run-config**
  - Must have! No exceptions!
  - “show run-config commands” (like IOS show running-config)
  - “show run-config no-ap” (no AP information added)
- **Show tech-support**
- CLI Tip
  - Log all output
  - **Config Paging Disable**

WLC Config/Monitoring

WLC Important Debugs

- **Debug client <client mac address>**
  - Client Involved? Must Have! No Exceptions
- **Debug capwap <event/error/detail/info> enable**
- CLI Tips
  - Log all output
  - Debugs are session based, they end when session ends
  - "**Config session timeout 60**", sets 60 minute idle timeout
  - **Debug disable-all** (Disables all debugs)

WLC Config/Monitoring

WLC Supportability – Best Practices

- Change default SNMP Parameters
- Configure Syslog for WLC and AP

  !!AP default behavior is to **Broadcast** syslog!!
- Enable Coredump for WLC and AP
- Configure NTP Server for Date/Time

AP Supportability

Supportability

- Methods of Accessing the AP
  - Console
  - Telnet (D) / SSH (D)
  - 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>**
- **Debug AP command “<command>” <AP name>**
  - Enables AP Remote Debug
  - AP Must be associated to WLC
  - Redirects AP Console output to WLC session

AP Supportability

Show Commands

- 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
```

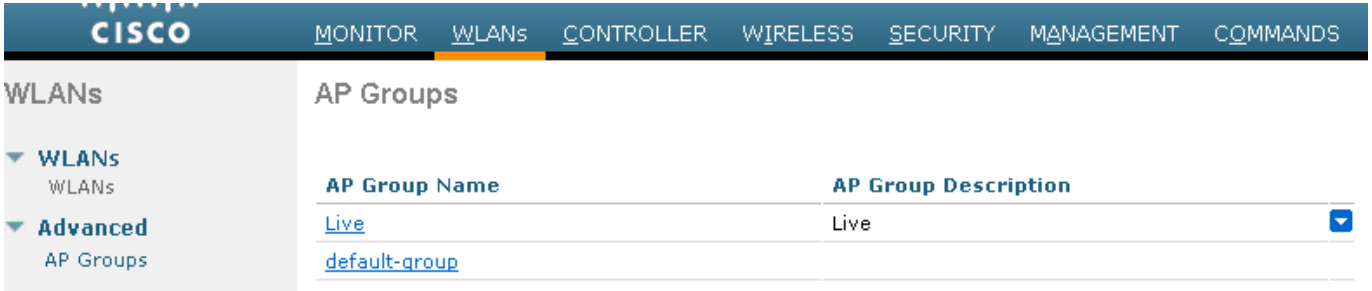
WLC Config/Monitoring

- Supportability
  - WLC
  - AP
- **WLANs**
- RRM / Radio / RF
- Wireless LAN Controller Config Analyser (WLCCA)

WLC Config/Monitoring

WLANs – AP Groups

- AP “Default Group” consists of all WLANs ID 1-16 and cannot be modified
- AP Groups must be created for WLAN ID 17+
- AP Groups override the Interface configured local to the WLAN
- AP Groups override default RF Profiles



WLC Config/Monitoring

WLANs - Tweaks

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'CiscoLive'

< Back

General | Security | QoS | Advanced

Allow AAA Override — Enabled

Coverage Hole Detection — Enabled

Enable Session Timeout — 1800 Session Timeout (secs)

Aironet IE — Enabled

Diagnostic Channel — Enabled

IPv6 Enable [7]

Override Interface ACL — None

P2P Blocking Action — Disabled

Client Exclusion [3] — Enabled — 60 Timeout Value (secs)

Maximum Allowed Clients [9] — 0

Static IP Tunneling [12] — Enabled

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	☐	☐	☐	☐	☑	☑	☑	☐

Scan Defer Time — 100

DHCP

DHCP Server — Override

DHCP Addr. Assignment — Required

Management Frame Protection (MFP)

MFP Client Protection [4] — Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) — 1

802.11b/g/n (1 - 255) — 1

NAC

NAC State — None

Load Balancing and Band Select

Client Load Balancing

Client Band Select [8]

Voice

WLC Config/Monitoring

- Supportability
  - WLC
  - AP
- WLANs
- **RRM / Radio / RF**
- Wireless LAN Controller Config Analyser (WLCCA)

RRM / Radio / RF

There are generally two common scenarios or issues involving RRM

- APs power change frequency (too much or not at all)
  - Nearby APs list meets the general rule of RSSI from 3rd closest AP is better than TPC Power Threshold
  - TPC Tuning may be required
- APs not changing channel
  - Check if other APs are in each others neighbour list
  - Already established channel plan might not change APs without just cause (Sensitivity)

RRM / Radio / RF

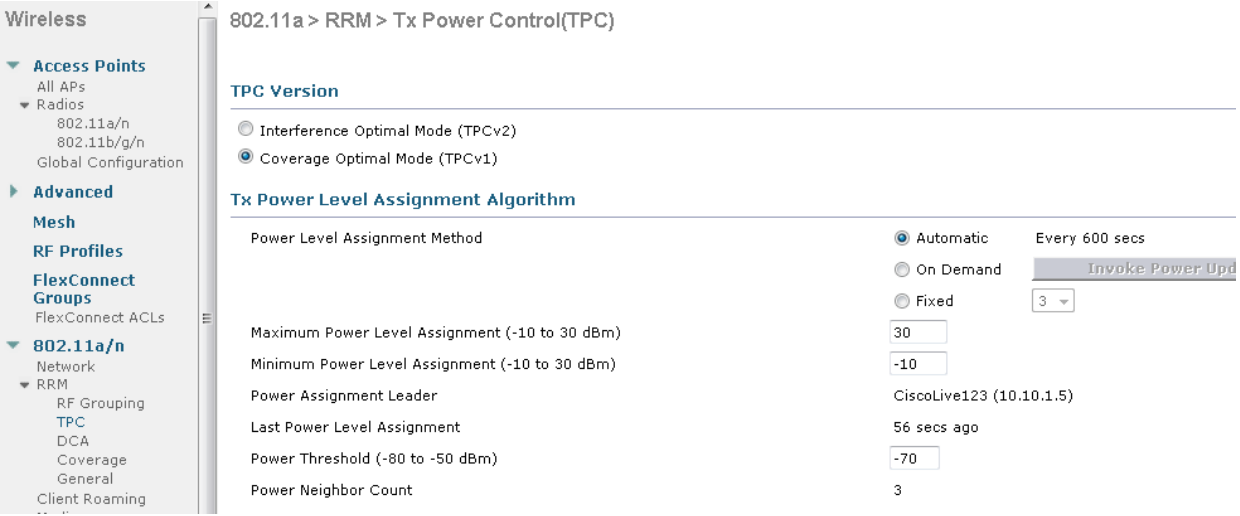
Show AP Auto-RF (In Run-Config)

- **show ap auto-rf [802.11a/b] <AP Name>**
- Load Information
  - Receive Utilisation.. 0 % Rx load to Radio
  - Transmit Utilisation.. 2 % Tx load from Radio
  - Channel Utilisation.. 12 % % Busy
- Nearby APs
  - AP 00:16:9c:4b:c4:c0 slot 0.. -60 dBm on 11 (10.10.1.5)
  - AP 00:26:cb:94:44:c0 slot 0.. -64 dBm on 11 (10.10.1.4)

RRM / Radio / RF

Radio – TPC Tuning

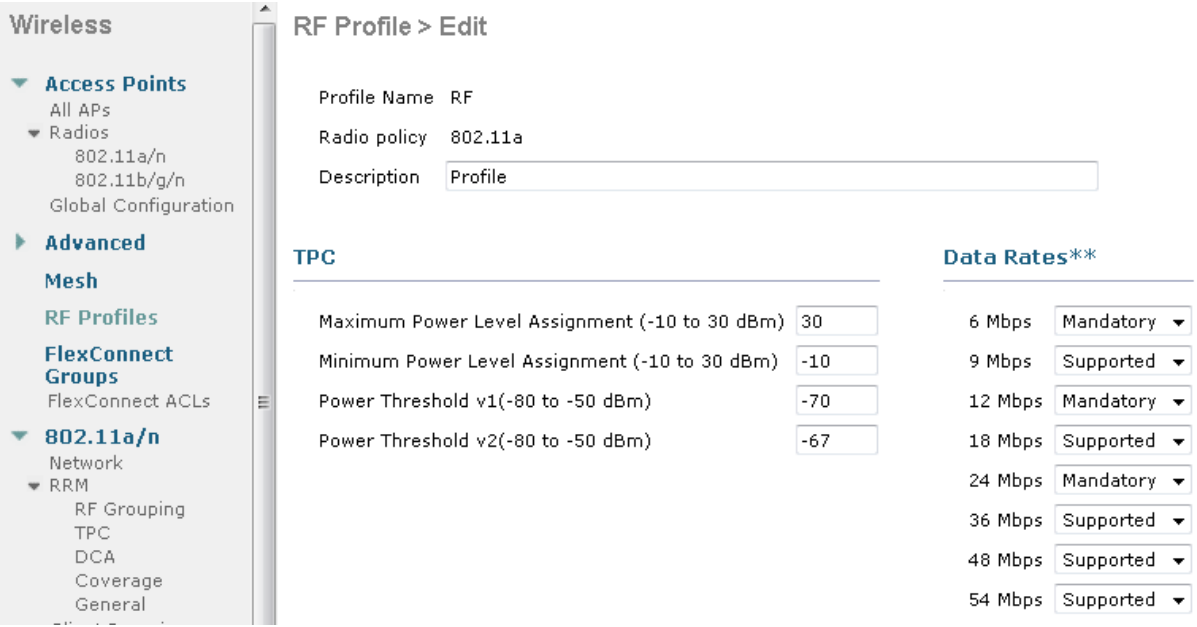
- Power Assignment Leader
- Power Threshold
- Consider Minimum Power Level Assignment



RRM / Radio / RF

Radio – TPC Tuning – RF Profiles

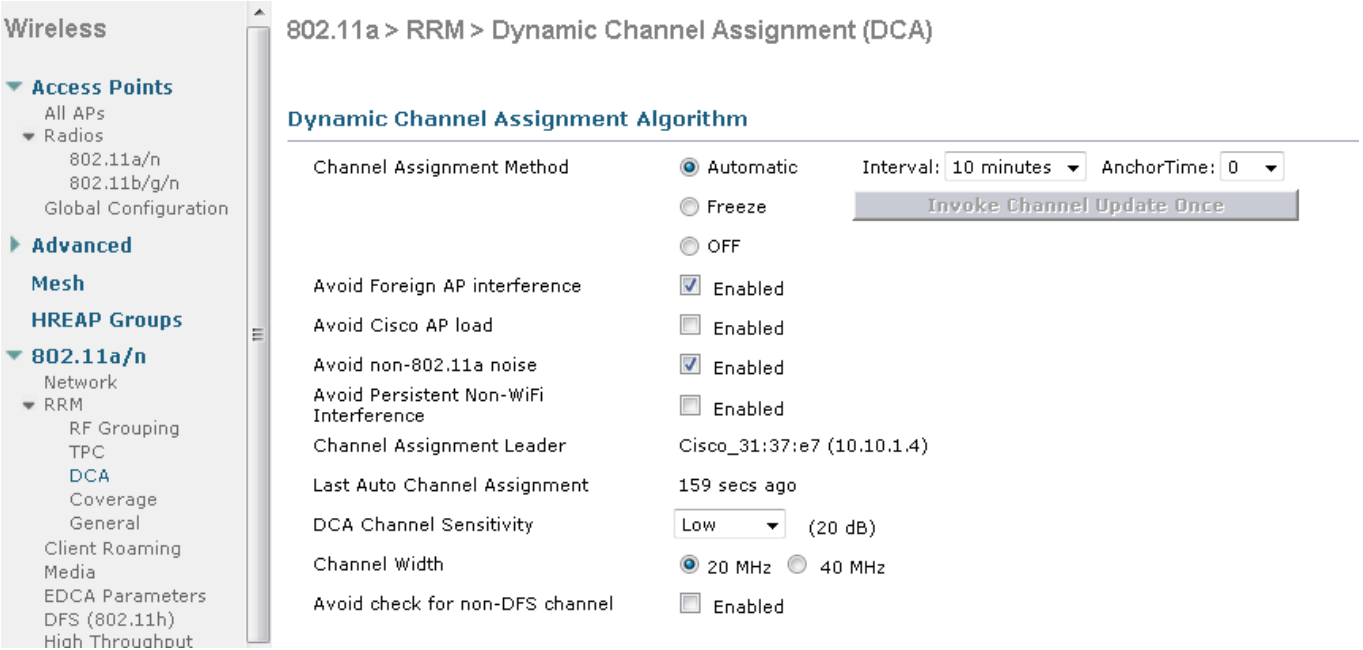
- RF Profiles let you make the same TPC settings but for specific groups of APs



RRM / Radio / RF

DCA Tuning

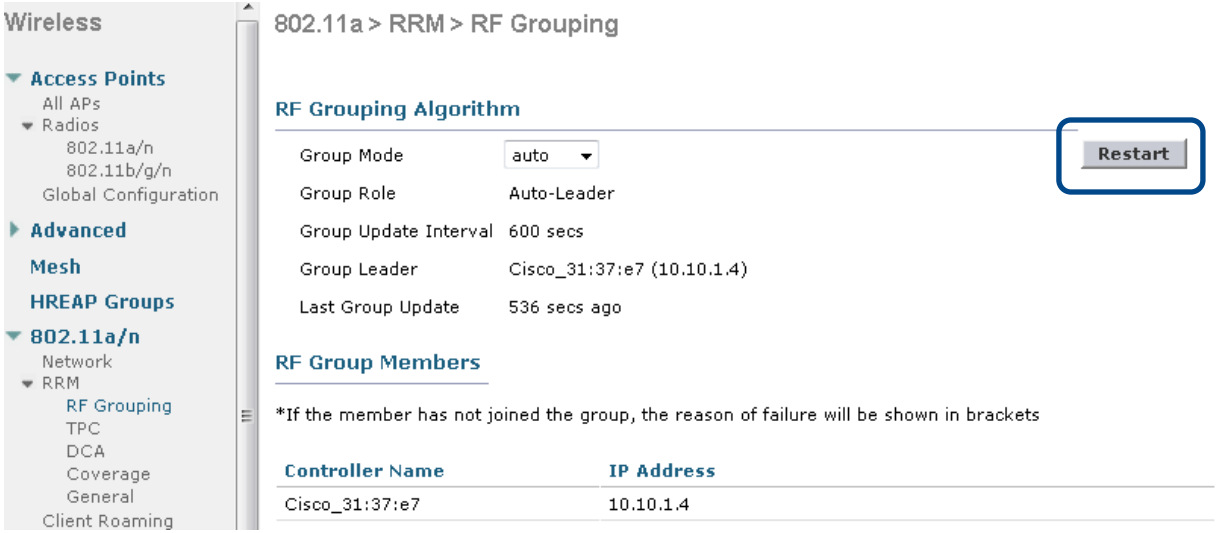
- If channels change too frequently, DCA may need to be made less sensitive or run at longer intervals



RRM / Radio / RF

DCA – STARTUP Mode

- In some large environments with new APs being deployed, STARTUP mode may be beneficial
- Previously this required a WLC REBOOT, but can be accomplished by RF Grouping configuration



DCA Channel Sensitivity Low STARTUP (5 dB)

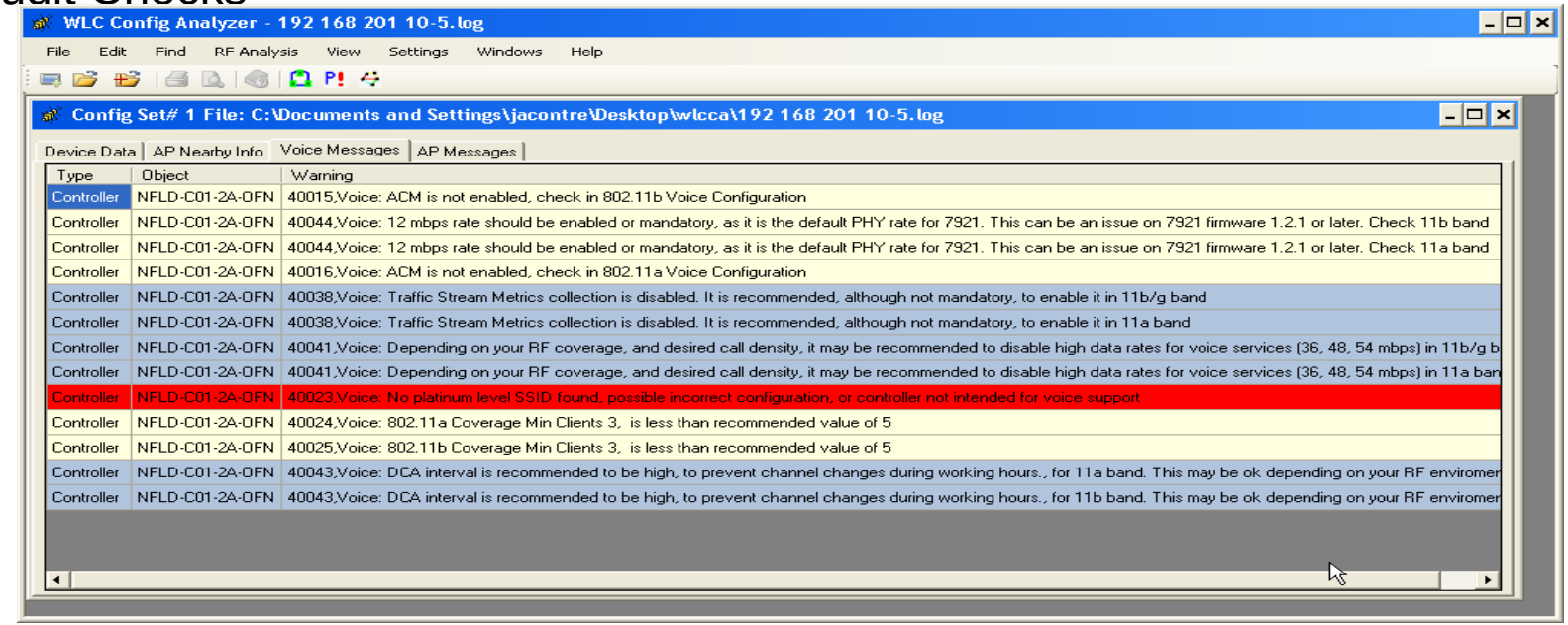
WLC Config/Monitoring

- Supportability
  - WLC
  - AP
- WLANs
- RRM / Radio / RF
- **Wireless LAN Controller Config Analyser (WLCCA)**

WLC Config Analyser (WLCCA)

Support Forums DOC-1373

- Main objective: Save time while analysing configuration files from WLCs
- Audit Checks

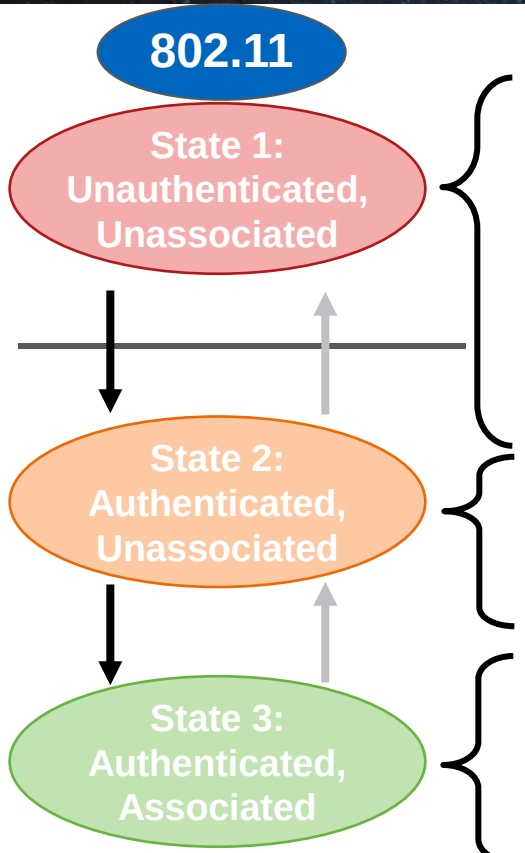


Type	Object	Warning
Controller	NFLD-C01-2A-OFN	40015,Voice: ACM is not enabled, check in 802.11b Voice Configuration
Controller	NFLD-C01-2A-OFN	40044,Voice: 12 mbps rate should be enabled or mandatory, as it is the default PHY rate for 7921. This can be an issue on 7921 firmware 1.2.1 or later. Check 11b band
Controller	NFLD-C01-2A-OFN	40044,Voice: 12 mbps rate should be enabled or mandatory, as it is the default PHY rate for 7921. This can be an issue on 7921 firmware 1.2.1 or later. Check 11a band
Controller	NFLD-C01-2A-OFN	40016,Voice: ACM is not enabled, check in 802.11a Voice Configuration
Controller	NFLD-C01-2A-OFN	40038,Voice: Traffic Stream Metrics collection is disabled. It is recommended, although not mandatory, to enable it in 11b/g band
Controller	NFLD-C01-2A-OFN	40038,Voice: Traffic Stream Metrics collection is disabled. It is recommended, although not mandatory, to enable it in 11a band
Controller	NFLD-C01-2A-OFN	40041,Voice: Depending on your RF coverage, and desired call density, it may be recommended to disable high data rates for voice services (36, 48, 54 mbps) in 11b/g b
Controller	NFLD-C01-2A-OFN	40041,Voice: Depending on your RF coverage, and desired call density, it may be recommended to disable high data rates for voice services (36, 48, 54 mbps) in 11a ban
Controller	NFLD-C01-2A-OFN	40023,Voice: No platinum level SSID found, possible incorrect configuration, or controller not intended for voice support
Controller	NFLD-C01-2A-OFN	40024,Voice: 802.11a Coverage Min Clients 3, is less than recommended value of 5
Controller	NFLD-C01-2A-OFN	40025,Voice: 802.11b Coverage Min Clients 3, is less than recommended value of 5
Controller	NFLD-C01-2A-OFN	40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11a band. This may be ok depending on your RF enviromen
Controller	NFLD-C01-2A-OFN	40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11b band. This may be ok depending on your RF enviromen

Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- AP Discovery/Join
- WLC Config/Monitoring
- **Client Connectivity**
- Mobility
- Packet Analysis

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

AP

802.11 Auth Complete, Not Mandatory

802.11 Assoc Complete

WLC

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)

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

The Client Debug - Walkthrough

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

The Client Debug - Walkthrough

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

Association

```
 Cisco Controller) >debug client 00:16:EA:B2:04:36
 Cisco Controller) >
(Cisco Controller) >
Association received from mobile on AP 00:26:cb:94:44:c0
0.0.0.0 START (0) Changing ACL 'none' (ACL ID 0) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1621)
Applying site-specific IPv6 override for station 00:16:ea:b2:04:36 - vapId 1, site 'default-group', interface '3'
Applying IPv6 Interface Policy for station 00:16:ea:b2:04:36 - vlan 3, interface id 8, interface '3‘

STA - rates (12): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
Processing RSN IE type 48, length 22 for mobile 00:16:ea:b2:04:36

0.0.0.0 START (0) Initializing policy
0.0.0.0 START (0) Change state to AUTHCHECK (2) last state AUTHCHECK (2)
0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state 8021X_REQD (3)
0.0.0.0 8021X_REQD (3) DHCP Not required on AP 00:26:cb:94:44:c0 vapId 1 apVapId 1for this client
0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP 00:26:cb:94:44:c0 vapId 1 apVapId 1
apfMsAssoStateInc
apfPemAddUser2 Changing state for mobile 00:16:ea:b2:04:36 on AP 00:26:cb:94:44:c0 from Idle to Associated
Scheduling deletion of Mobile Station:  (callerId: 49) in 1800 seconds

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

Association

Association received from mobile on **AP 00:26:cb:94:44:c0**
0.0.0.0 START (0) Changing ACL 'none' (ACL ID 0) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1621)
Applying site-specific IPv6 override for station 00:16:ea:b2:04:36 - **vapId 1, site 'default-group', interface '3'**
Applying IPv6 Interface Policy

- Association received
  Association Request, client did not “Roam” (Reassociate)
  AP Base Radio = 00:26:cb:94:44:c0
- vapId 1, site 'default-group', interface '3‘
  vapId = WLAN # (Wlan 1)
  site = AP Group (default-group)
  Interface = Dynamic Interface name (3)
- vlan 3
  Vlan = Vlan # of Dynamic Interface

Association

STA - rates (12): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
Processing **RSN IE type 48**, length 22 for mobile 00:16:ea:b2:04:36

- STA - rates
  Mandatory Rates (>128) = (#-128)/2
  Supported Rates (<128) = #/2
  1m,2m,5.5m,11m,6s,9s,12s,18s,24s,36s,48s,54s
- Processing **RSN IE type 48**
  WPA2-AES
  Processing **WPA IE type 221** = WPA-TKIP

Association

0.0.0.0 START (0) Initializing policy
0.0.0.0 START (0) Change state to AUTHCHECK (2) last state AUTHCHECK (2)
0.0.0.0 AUTHCHECK (2) **Change state to 8021X_REQD** (3) last state 8021X_REQD (3)
0.0.0.0 8021X_REQD (3) DHCP Not required on AP 00:26:cb:94:44:c0 vapId 1 apVapId 1for this client
0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP 00:26:cb:94:44:c0 vapId 1 apVapId 1
apfMsAssoStateInc
apfPemAddUser2 Changing state for mobile 00:16:ea:b2:04:36 on AP 00:26:cb:94:44:c0 from Idle to Associated
Scheduling deletion of Mobile Station: (callerId: 49) in 1800 seconds

- 0.0.0.0 START
  0.0.0.0 = IP we know for client (In this case nothing)
- Change state to 8021X_REQD
  Passed association, moving client to next state: 8021X_REQD
- Scheduling deletion
  Session Time on WLAN (1800 seconds in this case)

Association

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

- **Slot 0** = B/G(2.4) Radio
  Slot 1 = A(5) Radio
- Sending Assoc Response **Status 0** = Success
  Anything other than Status 0 is Failure

Common Assoc Response Failures:
1 – Unknown Reason – Anything not matching defined reason codes
12 – Unknown or Disabled SSID
17 – AP cannot handle any more associations (Load Balancing)
18 – Client is using a datarate that is not allowed
35 – WLAN requires the use of WMM and client does not support it
201 – Voice client attempting to connect to a non-platinum WLAN
202 – Not enough available bandwidth to handle a new voice call (CAC Rejection)

Association Scenario 1 - Roaming

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

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]**
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**

Association Scenario 2 – AAA Filter Failed

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

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

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

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

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

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

Association Scenario 3 – Blacklisted

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

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

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

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

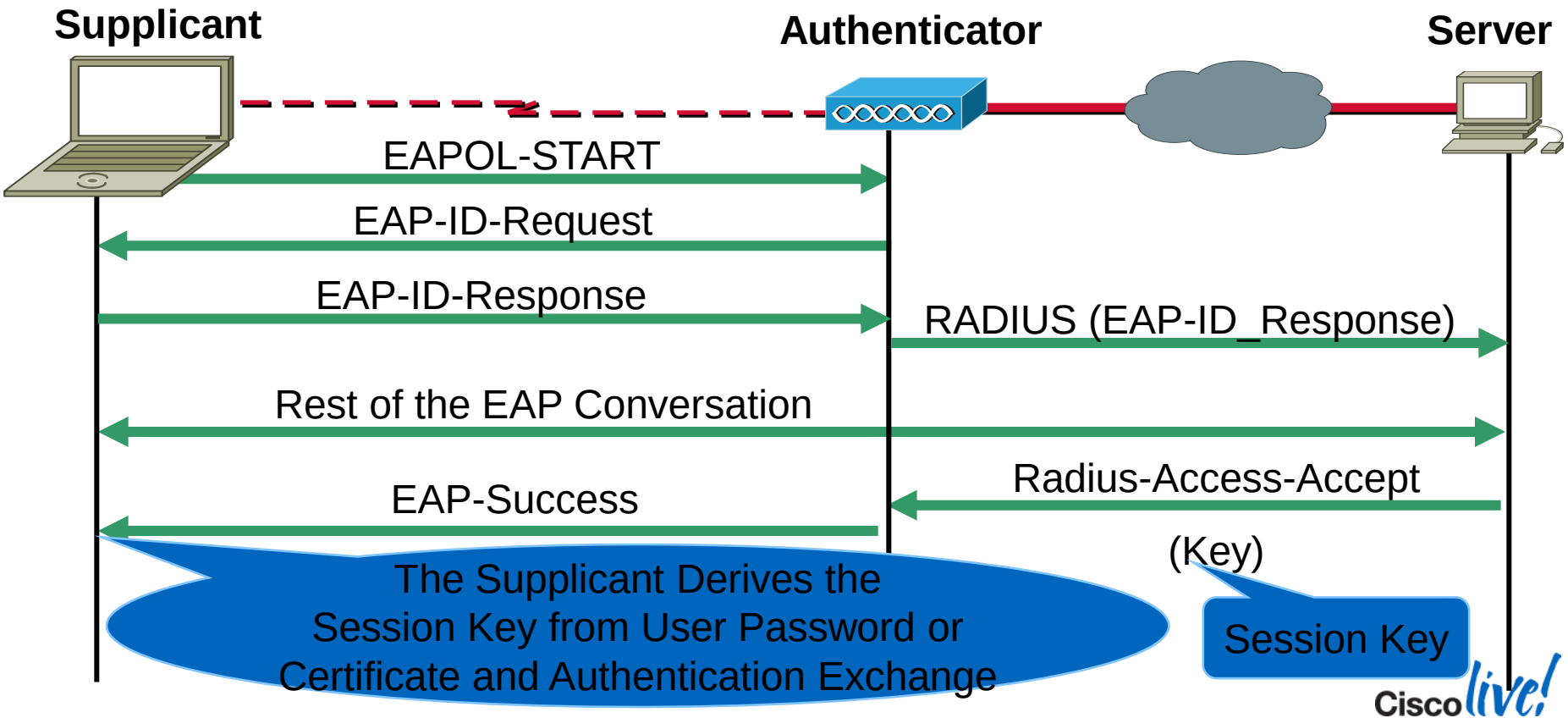
Association - Takeaway

- Association vs. Reassociation
- Debug shows
  AP, Slot, AP-Group, WLAN ID, Interface, Data Rates, Encryption type
- Association Response
  Confirms if Client is associated
  Defines reason if denied
- Further troubleshooting may require Wireless Sniffer or capture at AP Switchport

The Client Debug - Walkthrough

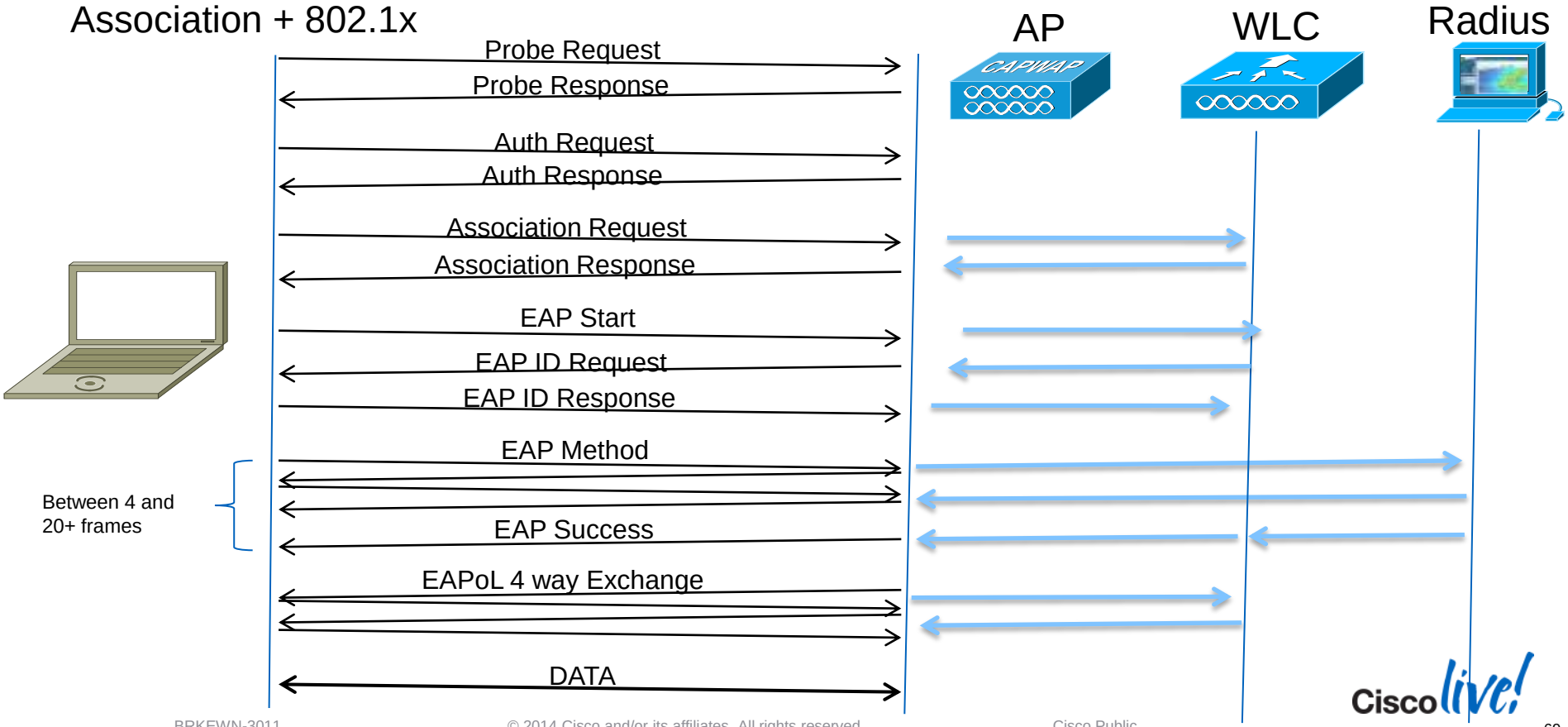
- Association (Start)
- **L2 Authentication (8021X_REQD)**
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc
- Tips and Tricks

802.1X Authentication



802.1X Authentication

Association + 802.1x



802.1x - Successful

```
Dec 16 15:36:07.557: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID 04:da:d2:28:94:ce (status 0)
ApVapId 2 Slot 1
Dec 16 15:36:07.559: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state
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)
Dec 16 15:36:07.566: 00:40:96:b5:db:d7 Received EAPOL START from mobile 00:40:96:b5:db:d7
Dec 16 15:36:07.566: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state

Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received Identity Response (count=2) from mobile 00:40:96:b5:db:d7
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
Dec 16 15:36:07.569: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Authenticating state
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
Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Processing Access-Challenge for mobile 00:40:96:b5:db:d7
Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Entering Backend Auth Req state (id=220) for mobile 00:40:96:b5:db:d7
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
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)
Dec 16 15:36:07.575: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
```

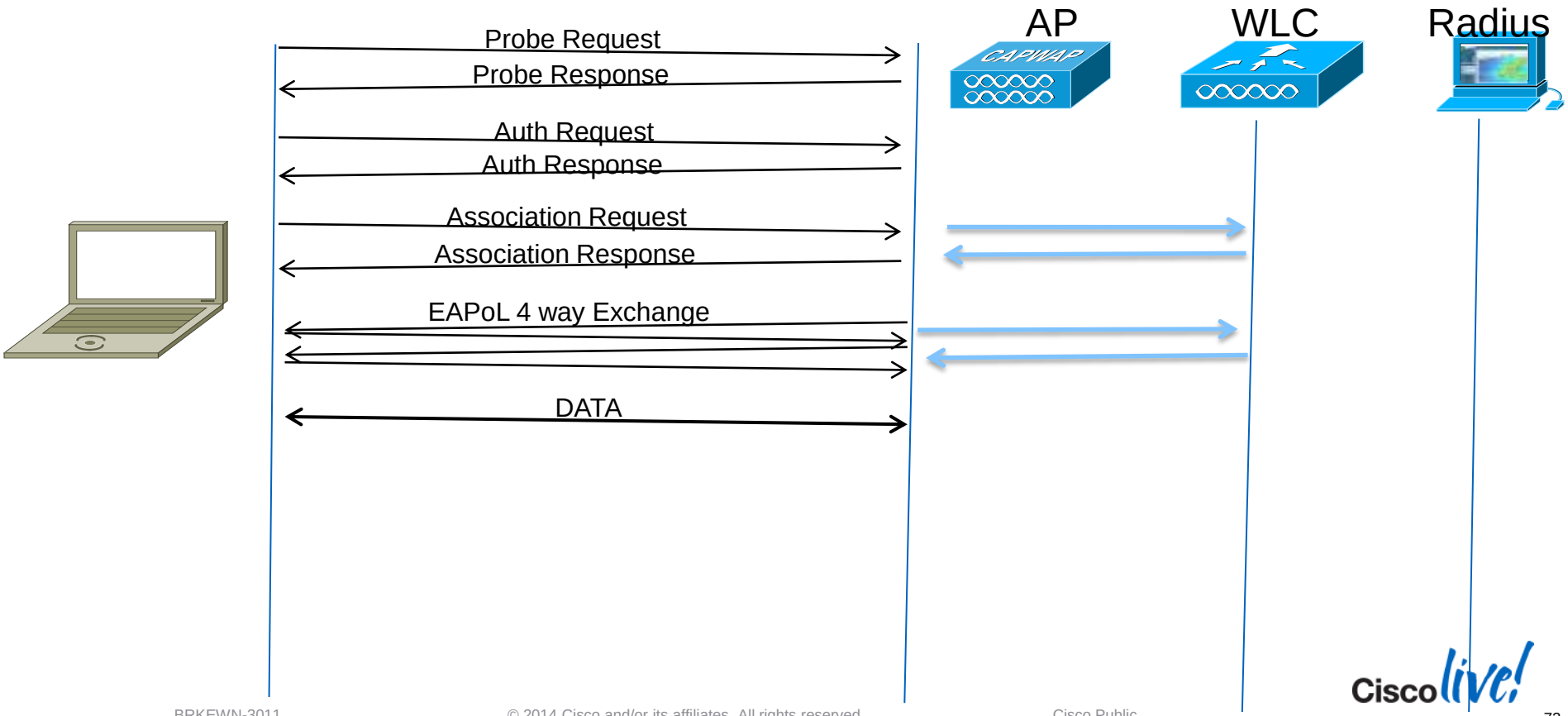
802.1x – Successful (Contd..)

```
Dec 16 15:36:07.575: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
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)
..
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
Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Processing Access-Accept for mobile 00:40:96:b5:db:d7
Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 acl from 255 to 255

Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 Flex acl from 65535 to 65535

Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Username entry (cisco) already exists in name table, length = 253
Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Username entry (cisco) created in mscb for mobile, length = 253
Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Setting re-auth timeout to 1800 seconds, got from WLAN config.
Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Station 00:40:96:b5:db:d7 setting dot1x reauth timeout = 1800
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)
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)
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
```

WPA - PSK Authentication



PSK – Successful scenario

Dec 16 15:30:14.920: 00:40:96:b5:db:d7 **Association received from mobile** on BSSID f8:4f:57:a1:d8:aa
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)
Dec 16 15:30:14.923: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7
Dec 16 15:30:14.924: 00:40:96:b5:db:d7 Initiating RSN PSK to mobile 00:40:96:b5:db:d7
Dec 16 15:30:14.924: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 **into Force Auth state**
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
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
Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7
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
Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7
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
Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7
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
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
Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7
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 Scenario 2 – Wrong Secret

Dec 16 15:25:28.923: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa
Dec 16 15:25:28.925: 00:40:96:b5:db:d7 **Sending Assoc Response** to station on BSSID f8:4f:57:a1:d8:aa (status 0) ApVapId 6 Slot 1
Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7
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
Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7
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
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
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
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
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
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)
Dec 16 15:25:32.020: 00:40:96:b5:db:d7 **Scheduling deletion of Mobile Station:** (callerId: 57) in 10 seconds

PSK Scenario 3 – Client Excluded

Jan 02 11:19:56.190: 68:7f:74:75:f1:cd **Blacklisting (if enabled)** mobile 68:7f:74:75:f1:cd
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)**

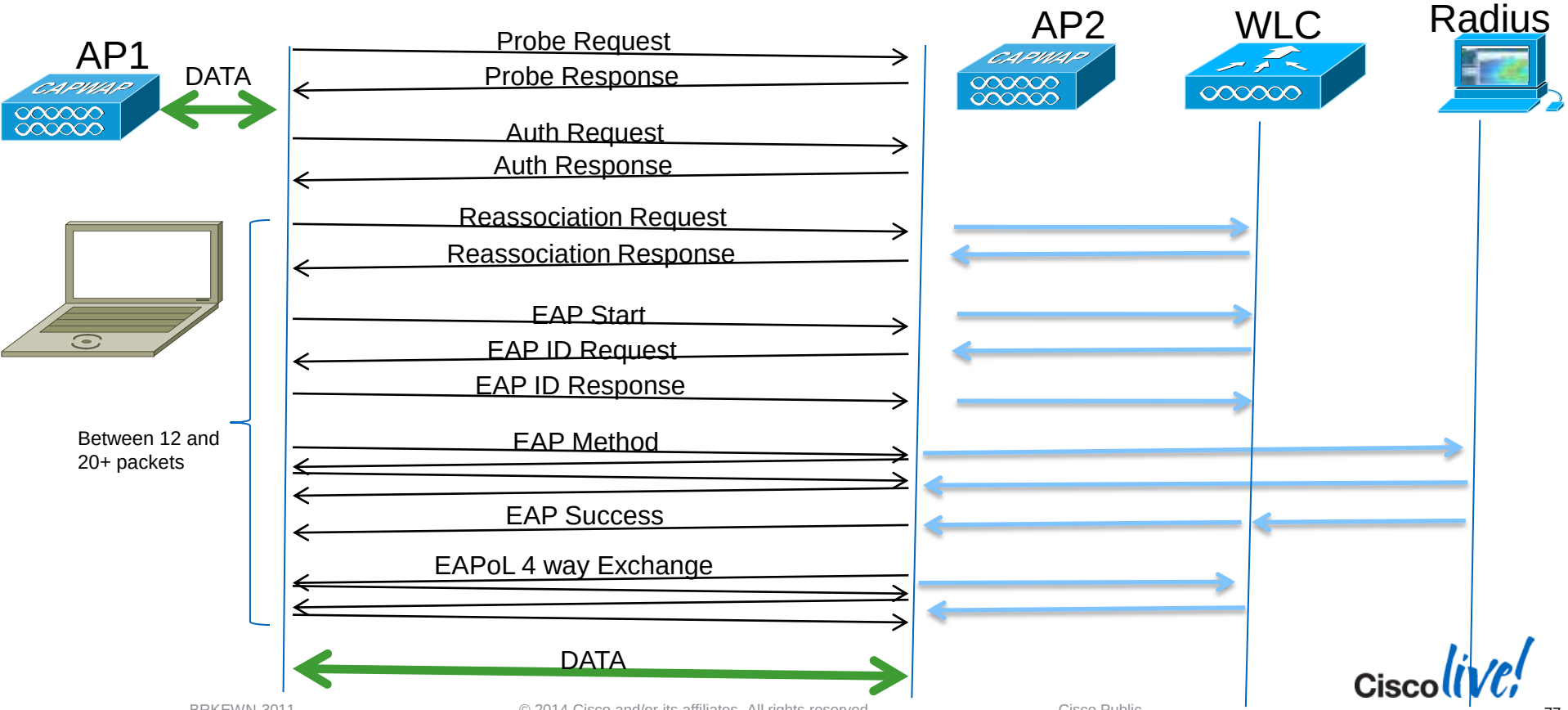
Jan 02 11:19:56.190: 68:7f:74:75:f1:cd **Scheduling deletion of Mobile Station: (callerId: 44) in 10 seconds**
Jan 02 11:19:56.190: 68:7f:74:75:f1:cd 0.0.0.0 8021X_REQD (3) Change state to START (0) last state 8021X_REQD (3)

Jan 02 11:19:56.190: 68:7f:74:75:f1:cd 0.0.0.0 START (0) Reached FAILURE: from line 5274
Jan 02 11:19:56.190: 68:7f:74:75:f1:cd Scheduling deletion of Mobile Station: (callerId: 9) in 10 seconds

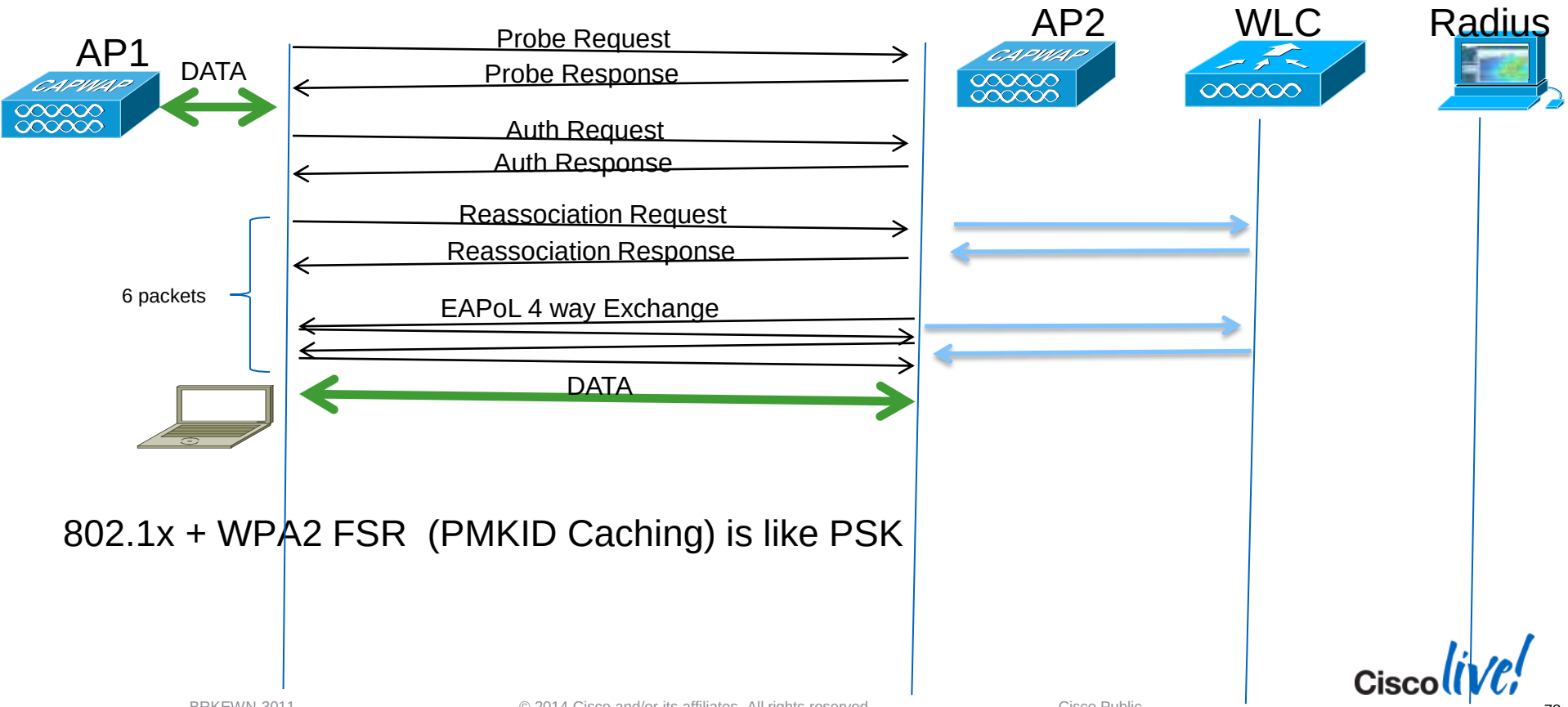
L2 Authentication - Takeaway

- 8021X_REQD means L2 Authentication pending
  Authentication/Encryption has not be established
- In PSK, key is not derived from AAA
- If “Processing Access-Reject”
  AAA/RADIUS Rejected the user (not the WLC)
- If “Processing Access-Accept”
  AAA/Radius Accepted the user
  M1-M4 should follow
- Further Troubleshooting
  Debug aaa [all/event/detail/packet] enable
  Debug dot1x [aaa/packet] enable

802.1X Authentication Roaming

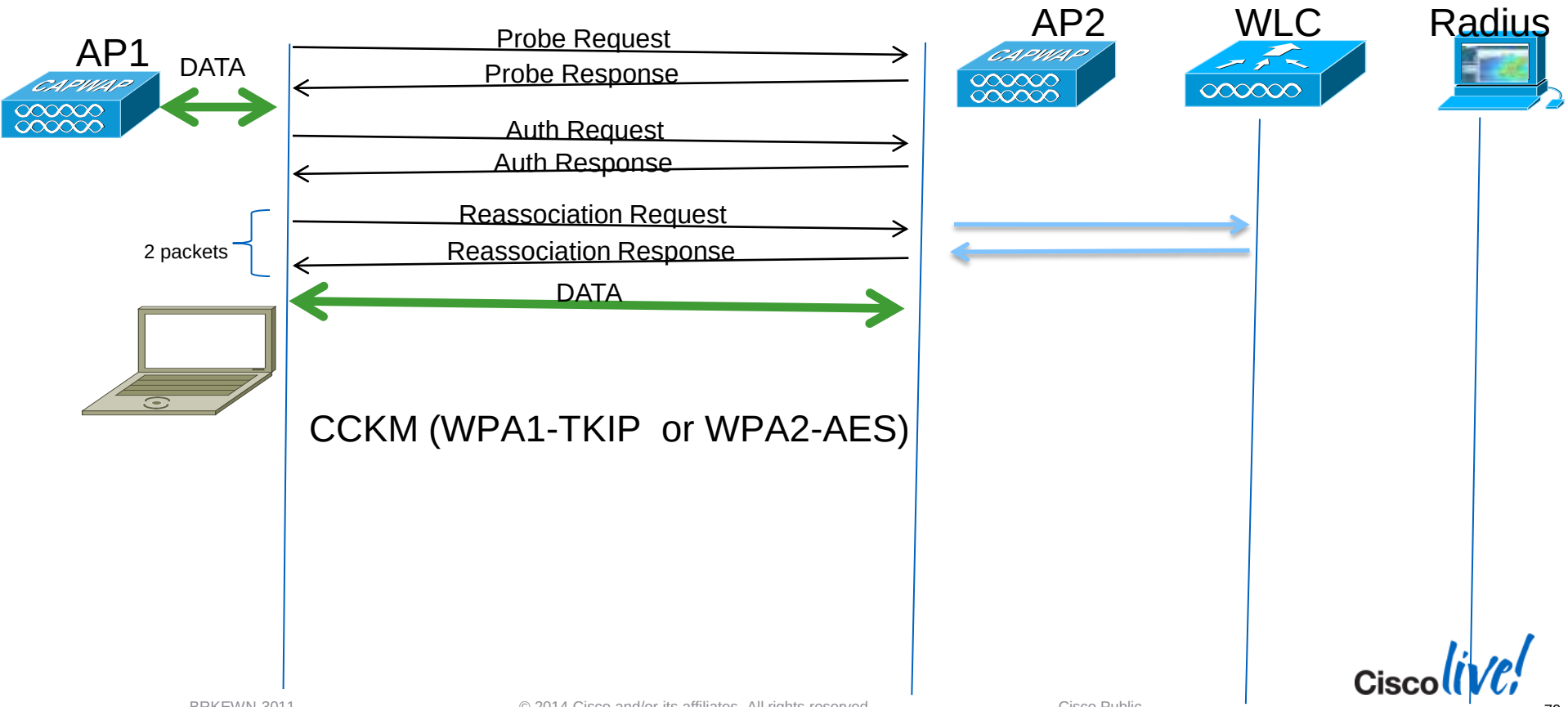


802.1X Authentication Roaming



802.1x + WPA2 FSR (PMKID Caching) is like PSK

802.1X with CCKM Authentication Roaming



Association - FSR

Processing WPA IE type 221, length 22 for mobile 00:16:ea:b2:04:36
CCKM: Mobile is using CCKM
CCKM: Processing REASSOC REQ IE
Including CCKM Response IE (length 62) in Assoc Resp to mobile
Sending Assoc Response to station on BSSID 00:26:cb:94:44:c0 (status 0) Vap Id 6 Slot 1

OR

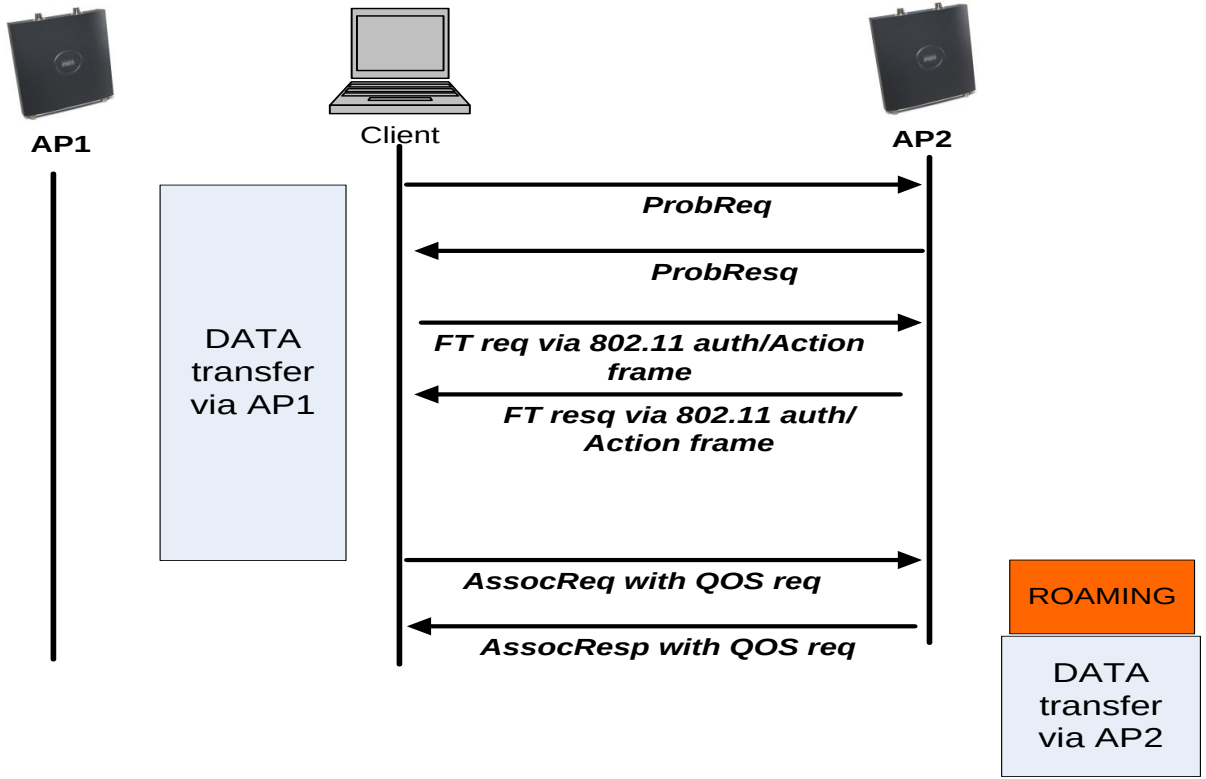
Processing RSN IE type 48, length 22 for mobile 00:16:ea:b2:04:36
Received RSN IE with 1 PMKIDs from mobile 00:16:ea:b2:04:36
Received PMKID: (16)
[0000] cb bc 27 82 88 14 92 fd 3b 88 de 6a eb 49 be c8
Found an entry in the global PMK cache for station
Computed a valid PMKID from global PMK cache for mobile

FSR	aIOS	CUWN
CCKM - WPA	yes	yes
CCKM - WPA2	yes	yes
WPA2 PKC	no	yes
WPA2 "Sticky"	yes	yes*(7.2)

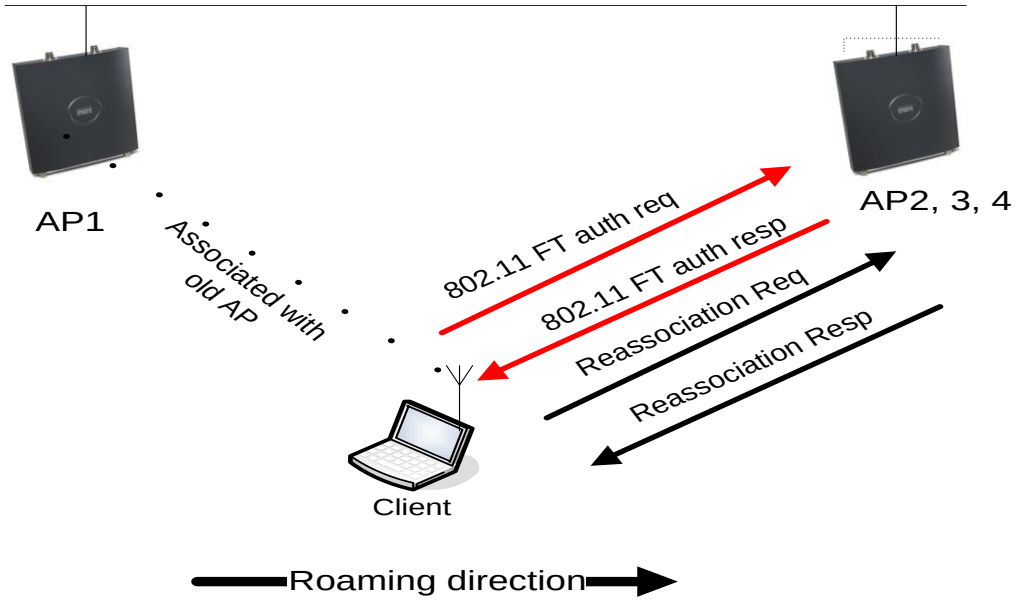
* WPA2 “Sticky” PMKID Caching is now supported in 7.2 WLC Release with limited scale. This at least allows some form of Fast Secure Roaming for “Sticky” clients (like Apple).

802.11r Roaming

WPA2 - .11r Client (Fast Transition)



802.11r Over the Air Roaming

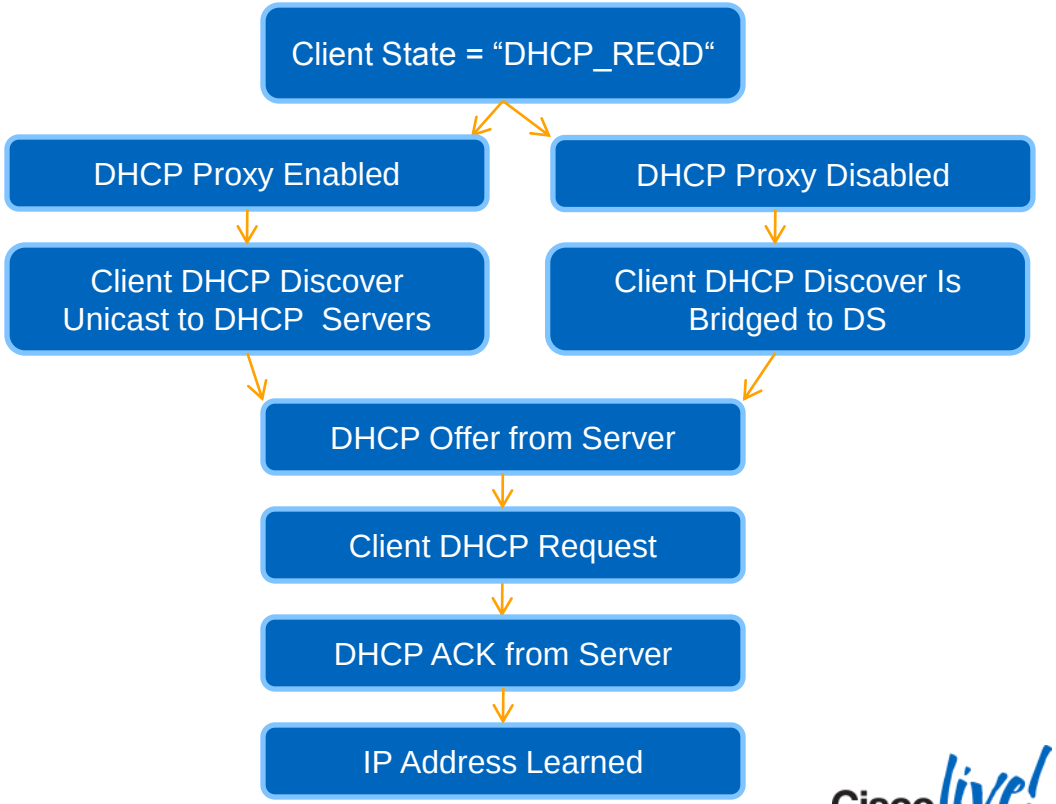


The Client Debug - Walkthrough

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

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



Client DHCP

00:16:ea:b2:04:36 Received EAPOL-key in PTKINITNEGOTIATING state
00:16:ea:b2:04:36 apfMs1xStateInc
00:16:ea:b2:04:36 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
00:16:ea:b2:04:36 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP 00:26:cb:94:44:c0 vapId 3 apVapId 3for this client
00:16:ea:b2:04:36 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:26:cb:94:44:c0 vapId 3 apVapId 3
00:16:ea:b2:04:36 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
00:16:ea:b2:04:36 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 4755, Adding TMP rule
00:16:ea:b2:04:36 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (ACL ID 255)
00:16:ea:b2:04:36 Stopping retransmission timer for mobile 00:16:ea:b2:04:36
00:16:ea:b2:04:36 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
.....
00:16:ea:b2:04:36 DHCP received op **BOOTREQUEST (1)** (len 308,vlan 0, port 29, encap 0xec03)
.....
00:16:ea:b2:04:36 DHCP received op **BOOTREPLY (2)** (len 308,vlan 0, port 29, encap 0xec00)
.....
00:16:ea:b2:04:36 10.10.1.103 DHCP_REQD (7) Change state to RUN (20) last state RUN (20)
00:16:ea:b2:04:36 10.10.1.103 Added NPU entry of type 1, dtlFlags 0x0

DHCP – Process Start

DHCP received op BOOTREQUEST (1) (len 308,vlan 5, port 1, encap 0xec03)
DHCP (encap type 0xec03) mstype 0ff: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:74:75:f1:cd
DHCP ciaddr: 0.0.0.0, yiaddr: **192.168.50.101**
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP server id: **1.1.1.1** rcvd server id: **192.168.0.21**
DHCP received op BOOTREQUEST (1) (len 335,vlan 5, port 1, encap 0xec03)
DHCP (encap type 0xec03) mstype 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 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
```

Client DHCP - Takeaway

- DHCP_REQD means Learning IP State
  Only “Required” if enabled on the WLAN
- If Proxy is enabled
  - Confirm DHCP Server on Interface (or Wlan) is correct
  - DHCP Server may not respond to WLC Proxy (Firewalls?)
- If Proxy is disabled, DHCP is similar to wired client
- Further Troubleshooting
  - If WLC does not show a BOOTREQUEST, confirm the client request arrives to the WLC (packet capture).
  - If issue is believed to be on WLC: **debug dhcp message enable**

The Client Debug - Walkthrough

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

Webauth

*apfReceiveTask: 00:16:ea:b2:04:36 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (ACL ID 255)

***pemReceiveTask: 00:16:ea:b2:04:36 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0**

DHCP Proxy DTL Recv Task: 00:16:ea:b2:04:36 DHCP received op BOOTREQUEST (1) (len 312,vlan 0, port 29, encap 0xec03)

……..

***DHCP Proxy DTL Recv Task: 00:16:ea:b2:04:36 10.10.3.86 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state WEBAUTH_REQD (8)**

*DHCP Proxy DTL Recv Task: 00:16:ea:b2:04:36 10.10.3.86 WEBAUTH_REQD (8) pemAdvanceState2 5170, Adding TMP rule

*DHCP Proxy DTL Recv Task: 00:16:ea:b2:04:36 10.10.3.86 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255)

*DHCP Proxy DTL Recv Task: 00:16:ea:b2:04:36 Assigning Address 10.10.3.86 to mobile

***pemReceiveTask: 00:16:ea:b2:04:36 10.10.3.86 Added NPU entry of type 2, dtlFlags 0x0**

*pemReceiveTask: 00:16:ea:b2:04:36 Sent an XID frame

*apfReceiveTask: 00:16:ea:b2:04:36 Orphan Packet from 10.10.3.86 on mobile

*apfReceiveTask: 00:16:ea:b2:04:36 Orphan Packet from 10.10.3.86 on mobile

***apfReceiveTask: 00:16:ea:b2:04:36 Orphan Packet from 10.10.3.86 on mobile**

……

***emWeb: 00:16:ea:b2:04:36 Username entry (cisco) created for mobile**

*emWeb: 00:16:ea:b2:04:36 10.10.3.86 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)

***emWeb: 00:16:ea:b2:04:36 10.10.3.86 WEBAUTH_NOL3SEC (14) Change state to RUN (20) last state RUN (20)**

*emWeb: 00:16:ea:b2:04:36 Session Timeout is 1800 - starting session timer for the mobile

*emWeb: 00:16:ea:b2:04:36 10.10.3.86 RUN (20) Reached PLUMBFASTPATH: from line 5063

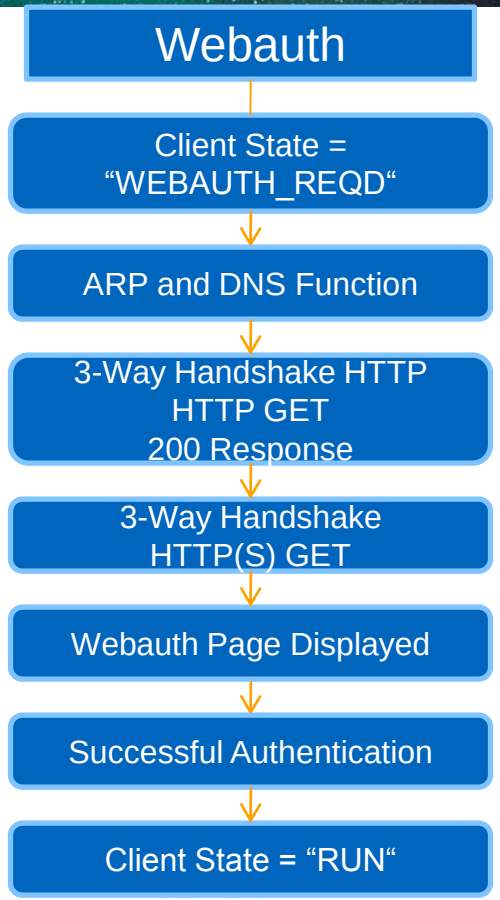
*emWeb: May 17 22:25:16.564: 00:16:ea:b2:04:36 10.10.3.86 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 5006 IPv6 Vlan = 3, IPv6 intf id = 8

*emWeb: May 17 22:25:16.564: 00:16:ea:b2:04:36 10.10.3.86 RUN (20) Successfully plumbed mobile rule (ACL ID 255)

***pemReceiveTask: May 17 22:25:16.578: 00:16:ea:b2:04:36 10.10.3.86 Added NPU entry of type 1, dtlFlags 0x0**

Webauth Redirect

- Client in WEBAUTH_REQD state
- ARP and DNS must be functional
- Client attempts to browse internet
- WLC “Hijacks” the handshake
- Client redirects to Virtual Interface
- Certificate negotiation if applicable
- Webauth page is displayed
- Client authenticates



Confirm ARP and DNS Function

ARP and DNS Function

```
C:\>arp -a

Interface: 10.10.3.217 --- 0x2
  Internet Address      Physical Address      Type
  10.10.3.1             00-00-0c-07-ac-03     dynamic
```

```
C:\>nslookup www.cisco.com
Server:  vnsc-bak.sys.gtei.net
Address:  4.2.2.2

Non-authoritative answer:
Name:    e144.cd.akamaiedge.net
Address:  72.247.200.170
```

No.	Time	Source	Destination	BSS Id	Info
1	0.000000	0.0.0.0	255.255.255.255		DHCP Discover - Transaction ID 0x2c763266
5	3.999592	0.0.0.0	255.255.255.255		DHCP Discover - Transaction ID 0x2c763266
6	5.526812	Cisco_39:b4:10	Broadcast		Who has 10.10.3.1? Tell 10.10.3.85
7	6.074837	1.1.1.1	10.10.3.86		DHCP Offer - Transaction ID 0x2c763266
8	6.075988	0.0.0.0	255.255.255.255		DHCP Request - Transaction ID 0x2c763266
9	6.084963	1.1.1.1	10.10.3.86		DHCP ACK - Transaction ID 0x2c763266
10	6.121845	Intel_b2:04:36	Broadcast		Gratuitous ARP for 10.10.3.86 (Request)
11	6.999304	Intel_b2:04:36	Broadcast		Gratuitous ARP for 10.10.3.86 (Request)
12	7.999355	Intel_b2:04:36	Broadcast		Gratuitous ARP for 10.10.3.86 (Request)
15	9.939419	Intel_b2:04:36	Broadcast		Who has 10.10.3.1? Tell 10.10.3.86
16	9.974065	All-HSRP-router	Intel_b2:04:36		10.10.3.1 is at 00:00:0c:07:ac:03
17	9.983017	Intel_b2:04:36	Broadcast		Who has 10.10.3.1? Tell 10.10.3.86
18	9.986083	All-HSRP-router	Intel_b2:04:36		10.10.3.1 is at 00:00:0c:07:ac:03
62	101.417335	Intel_b2:04:36	Broadcast		Who has 10.10.3.1? Tell 10.10.3.86
63	101.429484	All-HSRP-router	Intel_b2:04:36		10.10.3.1 is at 00:00:0c:07:ac:03
830	287.634442	10.10.3.86	4.2.2.2		Standard query A www.cisco.com
831	287.668517	4.2.2.2	10.10.3.86		Standard query response CNAME www.cisco.com

Capture from Wireless Adapter

3-Way Handshake HTTP GET 200 Response

3-Way Handshake HTTP(S) GET

Webauth Page Displayed

688	274.256556	10.10.3.86	72.247.200.170	msfw-storage > http [SYN] Seq=0 Win=64	
689	274.259856	72.247.200.170	10.10.3.86	http > msfw-storage [SYN, AC[redacted] Ack	
690	274.259872	10.10.3.86	72.247.200.170	msfw-storage > http [ACK] Seq=1 Ack=1 Win=64	
691	274.260005	10.10.3.86	72.247.200.170	GET / HTTP/1.1	
692	274.262927	72.247.200.170	10.10.3.86	http > msfw-storage [ACK] Seq=1 Ack=124	
693	274.262956	72.247.200.170	10.10.3.86	HTTP/1.1 200 OK (text/html)	
694	274.262987	72.247.200.170	10.10.3.86	http > msfw-storage [FIN, ACK] Seq=389	
695	274.263003	10.10.3.86	72.247.200.170	msfw-storage > http [ACK] Seq=1240 Ack=39	
696	274.263131	10.10.3.86	72.247.200.170	msfw-storage > http [RST, ACK] Seq=1240 Ack=39	
703	275.324260	10.10.3.86	1.1.1.1	msfw-replica > https [SYN] Seq=0 Win=64512 Len	
705	275.333365	1.1.1.1	10.10.3.86	https > msfw-replica [SYN, AC[redacted] Ack	
706	275.333412	10.10.3.86	1.1.1.1	msfw-replica > https [ACK] Seq=1 Ack=1	
722	275.371821	10.10.3.86	1.1.1.1	Client Hello	
723	275.375061	1.1.1.1	10.10.3.86	https > msfw-replica [ACK] Seq=1 Ack=78	
724	275.375149	1.1.1.1	10.10.3.86	Server Hello, Certificate, Server Hello Don	
725	275.376268	10.10.3.86	1.1.1.1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
726	275.401100	1.1.1.1	10.10.3.86	Change Cipher Spec, Encrypted Handshake Message	
727	275.565962	10.10.3.86	1.1.1.1	msfw-replica > https [ACK] Seq=268 Ack=53 Win	
728	275.797061	10.10.3.86	1.1.1.1	msfw-replica > https [FIN, ACK] Seq=268 Ac	
729	275.800133	1.1.1.1	10.10.3.86	Encrypted Alert	
730	275.800183	10.10.3.86	1.1.1.1	msfw-replica > https [RST, ACK] Seq=269	
731	275.800253	1.1.1.1	10.10.3.86	https > msfw-replica [FIN, ACK] Seq=782 Ac	
732	275.800284	10.10.3.86	1.1.1.1	msfw-replica > https [RST] Seq=269 Win=0 Len=0	
740	278.350361	10.10.3.86	1.1.1.1	rapi > https [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1	
741	278.353676	1.1.1.1	10.10.3.86	https > rapi [SYN, ACK] Seq=0 Ack=1 Win=5560 Len=0 MSS=1390 SACK_PERM=1	
742	278.353724	10.10.3.86	1.1.1.1	rapi > https [ACK] Seq=1 Ack=1 Win=64512 Len=0	
743	278.354808	10.10.3.86	1.1.1.1	Client Hello	
744	278.359783	1.1.1.1	10.10.3.86	https > rapi [ACK] Seq=1 Ack=110 Win=5560 Len=0	
745	278.359872	1.1.1.1	10.10.3.86	Server Hello, Change Cipher Spec, Encrypted Handshake Message	
746	278.360766	10.10.3.86	1.1.1.1	Change Cipher Spec, Encrypted Handshake Message	

```
0120  65 22 3e 3c 4d 45 54 41  20 68 74 74 70 2d 65 71   e"><META  http-eq
0130  75 69 76 3d 22 45 78 70  69 72 65 73 22 20 63 6f   uiv="Exp ires" co
0140  6e 74 65 6e 74 3d 22 2d  31 22 3e 3c 4d 45 54 41   ntent="- 1"><META
0150  20 68 74 74 70 2d 65 71  75 69 76 3d 22 72 65 66    http-eq uiv="ref
0160  72 65 73 68 22 20 63 6f  6e 74 65 6e 74 3d 22 31   resh" co ntent="1
0170  3b 20 55 52 4c 3d 68 74  74 70 73 3a 2f 2f 31 2e   ; URL=ht tps://1.
0180  31 2e 31 2e 31 2f 6c 6f  67 69 6e 2e 68 74 6d 6c   1.1.1/lo gin.html
0190  3f 72 65 64 69 72 65 63  74 3d 77 77 77 2e 63 69   ?redirec t=www.ci
01a0  73 63 6f 2e 63 6f 6d 2f  22 3e 3c 2f 48 45 41 44   sco.com/ "></HEAD
01b0  3e 3c 2f 48 54 4d 4c 3e  0d 0a                     ></HTML> ..
```

WLC Responding with SYN, ACK

Redirect to Virtual Interface Comes from Here

WLC Responding with SYN, ACK

Client Is Talking to Webauth….

Address for Client to Redirect to (Virtual IP/Name)

Webauth - Takeaway

- If WEBAUTH_REQD, then not authenticated
  Only traffic allowed is DHCP, ARP, DNS, Pre-Auth ACL.
- If not redirected, can client browse to virtual IP?
- Cert issue? Consider disabling HTTPS for HTTP webauth
- Most common scenario involves ARP/DNS failure
  Must confirm that client actually sends TCP SYN (http) to IP
- If proven that TCP SYN is sent and WLC does not SYN ACK, then there may be a WLC side problem
  debug client <MAC Address>
  debug webauth enable <client ip address>

The Client Debug - Walkthrough

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

Run State

- RUN State is the Client Traffic Forwarding State
- Client is Connected and should be functional

10.10.3.82 **DHCP_REQD (7) Change state to RUN (20)** last state RUN (20)
10.10.3.82 RUN (20) Reached PLUMBFASTPATH: from line 5273
10.10.3.82 **Added NPU entry of type 1**, dtlFlags 0x0

OR

10.10.3.86 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)
10.10.3.86 **WEBAUTH_NOL3SEC (14) Change state to RUN** (20) last state RUN (20)
Session Timeout is 1800 - starting session timer for the mobile
10.10.3.86 RUN (20) Reached PLUMBFASTPATH: from line 5063
10.10.3.86 **Added NPU entry of type 1**, dtlFlags 0x0

The Client Debug - Walkthrough

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

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 s
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)
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)

Deauthentication - 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
  - Packet capture or client logs may be require to see exact reason

The Client Debug - Walkthrough

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

Tips and Tricks

- Collect a client debug for an extended duration
  Several roams, deauths, failures, etc…
- Use an enhanced text editor with filter or “find all”
  I use Notepad++
- Find All
  “Association Received” (will also pull reassociations)
  “Assoc Resp”
  “Access-Reject”
  “timeoutEvt”

Tips and Tricks

File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?

wlcdebug-5-17-11.txt

```
496 *Dot1x_NW_MsgTask_0: May 17 22:16:19.033: 00:16:ea:b2:04:36 Scheduling deletion of Mobile Station:  (callerId: 65) in 10 sec
497 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Association received from mobile on AP 00:16:9c:4b:c4:c0
498 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 0.0.0.0 8021X_REQD (3) Changing ACL 'none' (ACL ID 255) ===> 'none'
499 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Applying site-specific IPv6 override for station 00:16:ea:b2:04:36
500 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Applying IPv6 Interface Policy for station 00:16:ea:b2:04:36 - vlar
501 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 STA - rates (8): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
502 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 STA - rates (12): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
503 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Processing RSN IE type 48, length 22 for mobile 00:16:ea:b2:04:36
504 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Received RSN IE with 0 PMKIDs from mobile 00:16:ea:b2:04:36
505 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 0.0.0.0 8021X_REQD (3) Initializing policy
506 *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 0.0.0.0 8021X_REQD (3) Change state to AUTHCHECK (2) last state 802
```

Find result - 32 hits

```
Search "association re" (32 hits in 1 files)
  C:\wlcdebug-5-17-11.txt (32 hits)
    Line 55: *apfMsConnTask_0: May 17 22:13:36.674: 00:16:ea:b2:04:36 Association received from mobile on AP 00:26:cb:94:44:c0
    Line 276: *apfMsConnTask_0: May 17 22:16:08.719: 00:16:ea:b2:04:36 Association received from mobile on AP 00:26:cb:94:44:c0
    Line 361: *apfMsConnTask_0: May 17 22:16:17.559: 00:16:ea:b2:04:36 Reassociation received from mobile on AP 00:16:9c:4b:c4:c0
    Line 395: *apfMsConnTask_0: May 17 22:16:18.046: 00:16:ea:b2:04:36 Reassociation received from mobile on AP 00:16:9c:4b:c4:c0
    Line 427: *apfMsConnTask_0: May 17 22:16:18.459: 00:16:ea:b2:04:36 Reassociation received from mobile on AP 00:3a:98:48:dd:40
    Line 462: *apfMsConnTask_0: May 17 22:16:18.920: 00:16:ea:b2:04:36 Reassociation received from mobile on AP 00:16:9c:4b:c4:c0
    Line 497: *apfMsConnTask_0: May 17 22:16:19.361: 00:16:ea:b2:04:36 Association received from mobile on AP 00:16:9c:4b:c4:c0
    Line 530: *apfMsConnTask_0: May 17 22:16:23.139: 00:16:ea:b2:04:36 Association received from mobile on AP 00:3a:98:48:dd:40
```

Normal text file | 262685 chars 267737 bytes 2527 lines | Ln : 497 Col : 72 Sel : 14 (14 bytes) in 1 ranges | Dos\Windows | ANSI | INS

Tips and Tricks

File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?

wlcdebug-5-17-11.txt

```
1499 *Dot1x_NW_MsgTask_0: May 17 22:19:08.621: 00:16:ea:b2:04:36 Entering Backend Auth Req state (id=9) for mobile 00:16:ea:b2:04:36
1500 *Dot1x_NW_MsgTask_0: May 17 22:19:08.621: 00:16:ea:b2:04:36 Sending EAP Request from AAA to mobile 00:16:ea:b2:04:36 (EAP Id 9)
1501 *Dot1x_NW_MsgTask_0: May 17 22:19:08.685: 00:16:ea:b2:04:36 Received EAPOL EAPPKT from mobile 00:16:ea:b2:04:36
1502 *Dot1x_NW_MsgTask_0: May 17 22:19:08.686: 00:16:ea:b2:04:36 Received EAP Response from mobile 00:16:ea:b2:04:36 (EAP Id 9, EAP Type
1503 *Dot1x_NW_MsgTask_0: May 17 22:19:08.686: 00:16:ea:b2:04:36 Entering Backend Auth Response state for mobile 00:16:ea:b2:04:36
1504 *Dot1x_NW_MsgTask_0: May 17 22:19:08.687: 00:16:ea:b2:04:36 Processing Access-Reject for mobile 00:16:ea:b2:04:36
1505 *Dot1x_NW_MsgTask_0: May 17 22:19:08.687: 00:16:ea:b2:04:36 CCKM: Sending cache delete
1506 *Dot1x_NW_MsgTask_0: May 17 22:19:08.687: 00:16:ea:b2:04:36 PMK: Sending cache delete
1507 *Dot1x_NW_MsgTask_0: May 17 22:19:08.688: 00:16:ea:b2:04:36 Removing PMK cache entry for station 00:16:ea:b2:04:36
1508 *Dot1x_NW_MsgTask_0: May 17 22:19:08.688: 00:16:ea:b2:04:36 Removing PMK cache due to EAP-Failure for mobile 00:16:ea:b2:04:36 (EAI
1509 *Dot1x_NW_MsgTask_0: May 17 22:19:08.688: 00:16:ea:b2:04:36 Sending EAP-Failure to mobile 00:16:ea:b2:04:36 (EAP Id 9)
1510 *Dot1x_NW_MsgTask_0: May 17 22:19:08.688: 00:16:ea:b2:04:36 Entering Backend Auth Failure state (id=9) for mobile 00:16:ea:b2:04:36
1511 *Dot1x_NW_MsgTask_0: May 17 22:19:08.689: 00:16:ea:b2:04:36 Setting quiet timer for 5 seconds for mobile 00:16:ea:b2:04:36
1512 *Dot1x_NW_MsgTask_0: May 17 22:19:08.689: 00:16:ea:b2:04:36 dot1x - moving mobile 00:16:ea:b2:04:36 into Unknown state
1513 *osapiBsnTimer: May 17 22:19:13.592: 00:16:ea:b2:04:36 802.1x 'quiteWhile' Timer expired for station 00:16:ea:b2:04:36 and for mess
```

Find result - 2 hits

```
Search "Access-a" (2 hits in 1 files)
  C:\wlcdebug-5-17-11.txt (2 hits)
    Line 1248: *Dot1x_NW_MsgTask_0: May 17 22:18:27.623: 00:16:ea:b2:04:36 Processing Access-Accept for mobile 00:16:ea:b2:04:36
    Line 1564: *Dot1x_NW_MsgTask_0: May 17 22:19:13.828: 00:16:ea:b2:04:36 Processing Access-Accept for mobile 00:16:ea:b2:04:36
Search "access-r" (1 hits in 1 files)
  C:\wlcdebug-5-17-11.txt (1 hits)
    Line 1504: *Dot1x_NW_MsgTask_0: May 17 22:19:08.687: 00:16:ea:b2:04:36 Processing Access-Reject for mobile 00:16:ea:b2:04:36
```

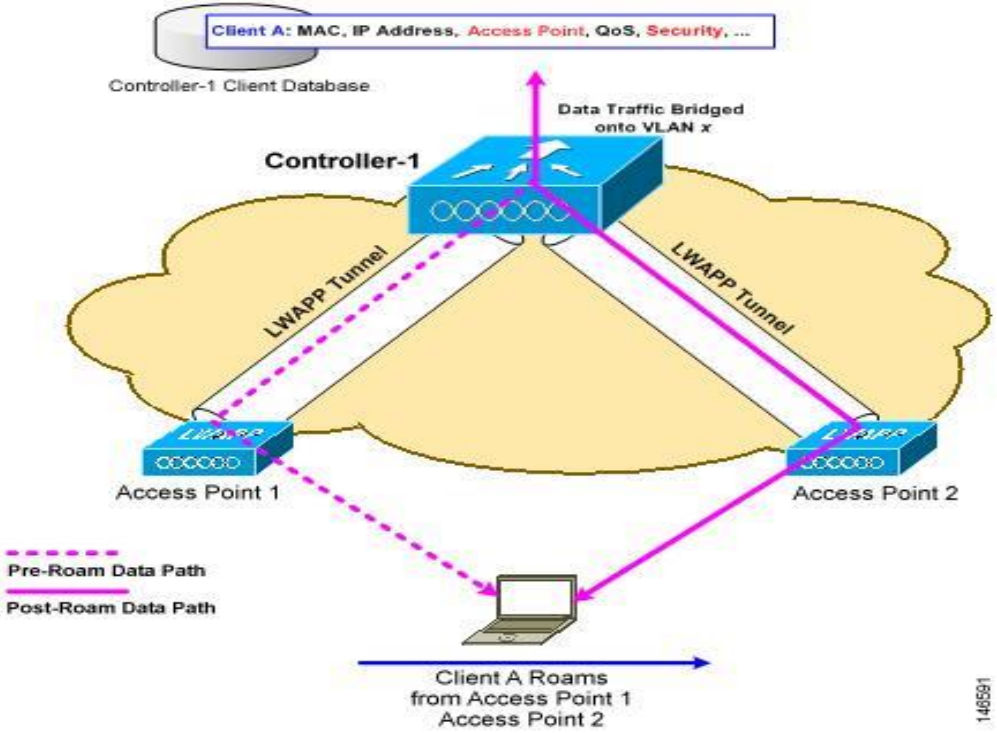
Normal text file | 262685 chars 267737 bytes 2527 lines | Ln : 1504 Col : 80 Sel : 8 (8 bytes) in 1 ranges | Dos\Windows | ANSI | INS

Troubleshooting Wireless LANs

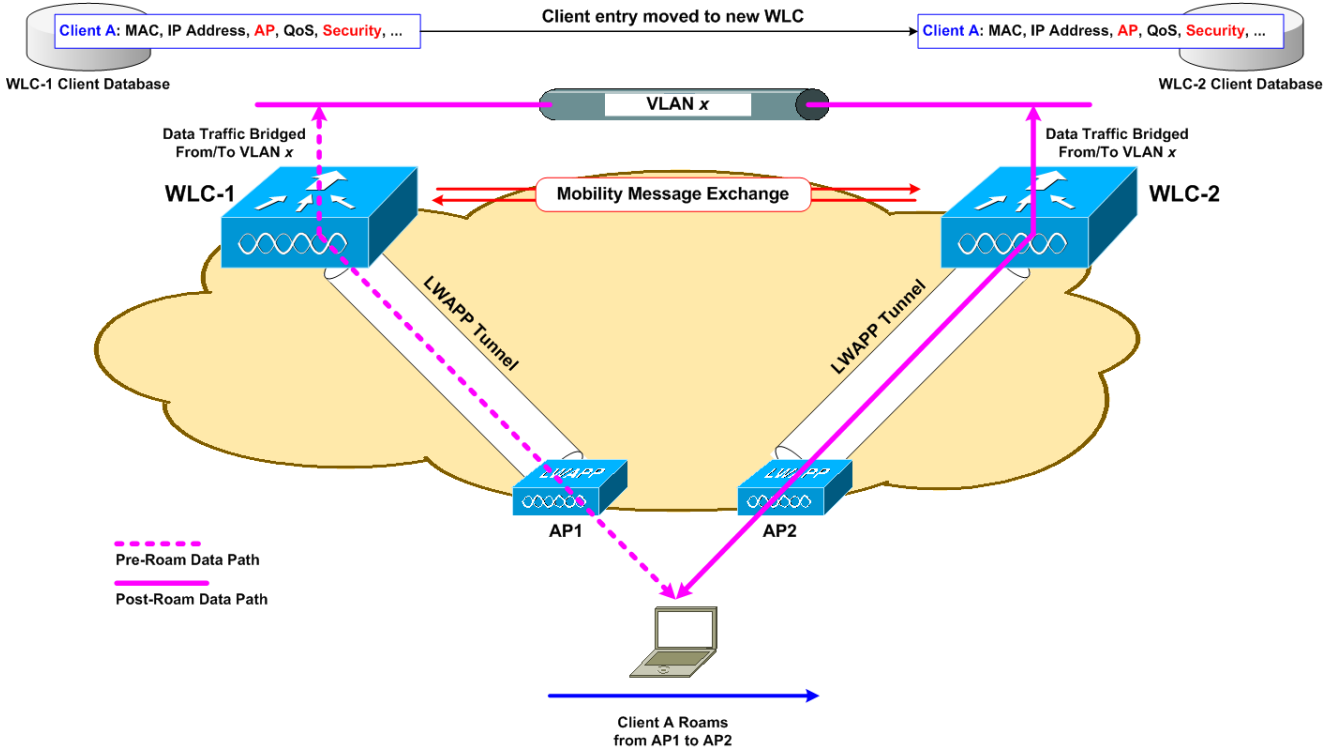
- Software and Support
- Troubleshooting Basics
- AP Discovery/Join
- WLC Config/Monitoring
- Client Connectivity
- **Mobility**
- Packet Analysis

Mobility—Intra-Controller

Client Roams Between Two APs on the Same Controller



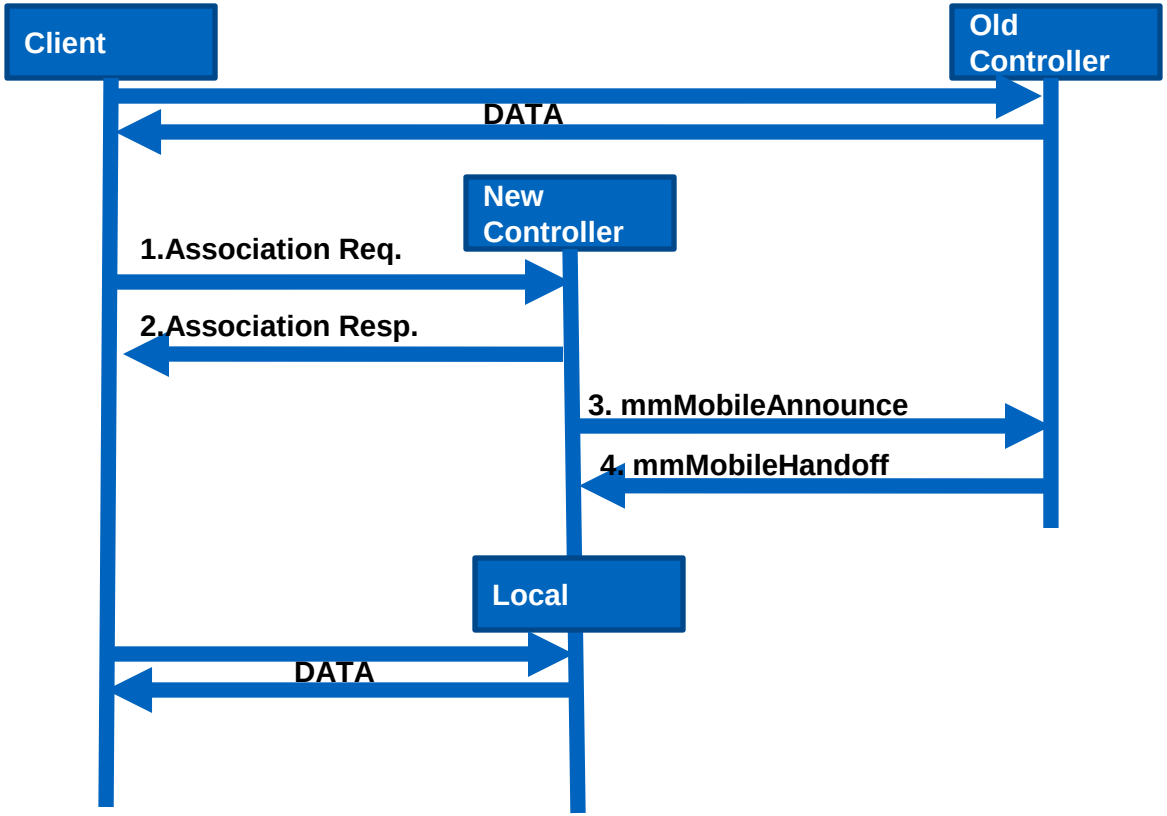
Mobility—Inter-Controller (Layer 2)



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— L2 Inter WLC



Mobility— L2 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

MobileAnnounce

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

```
0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPL
Mobility query, PEM State: L2AUTHCOMPLETE
........
Mobility packet sent to:
  10.10.1.4, port 16666
  type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 71  seq: 118  len 116 fla
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC: , IP: 0.0.0.0, instance: 0
  VLAN IP: 10.10.3.5, netmask: 255.255.255.0
........
0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state DHCP_REQD (7)
0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
........
```

MobileHandoff

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

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

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

Mobility handoff, NAC State Payload [ Client's NAC OOB State : Access, Quarantin
Mobility handoff for client:
Ip: 10.10.3.235
Anchor IP: 0.0.0.0, Peer IP: 10.10.1.4
```

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

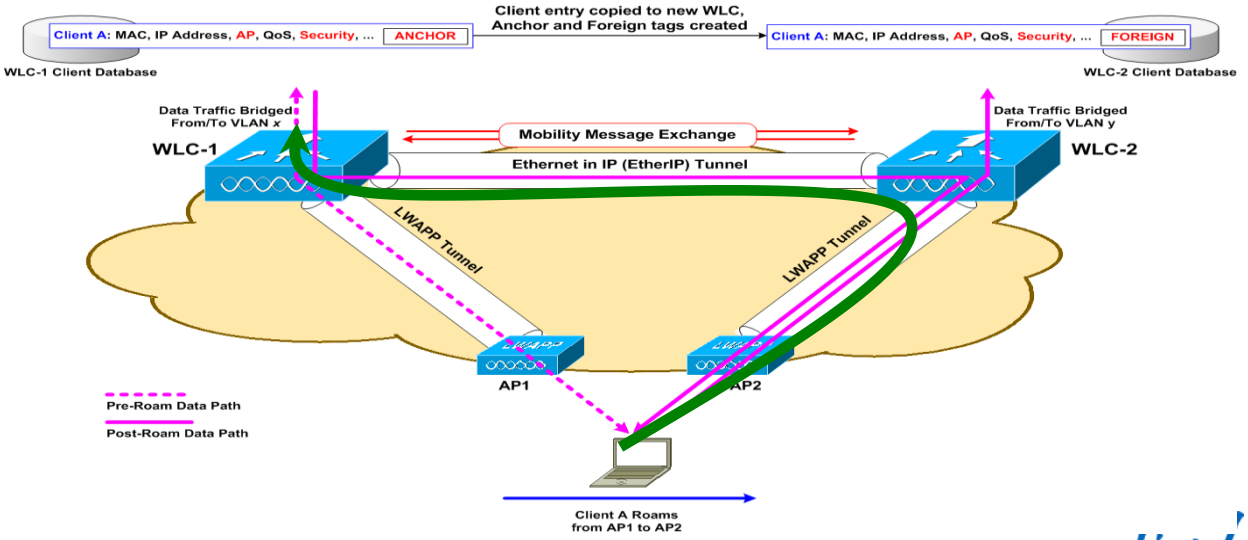
```
10.10.3.235 DHCP_REQD (7) Change state to RUN (20) last state RUN (20)
........
10.10.3.235 RUN (20) mobility role update request from Unassociated to Local
= 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5
10.10.3.235 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete,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

Mobility—Layer 3

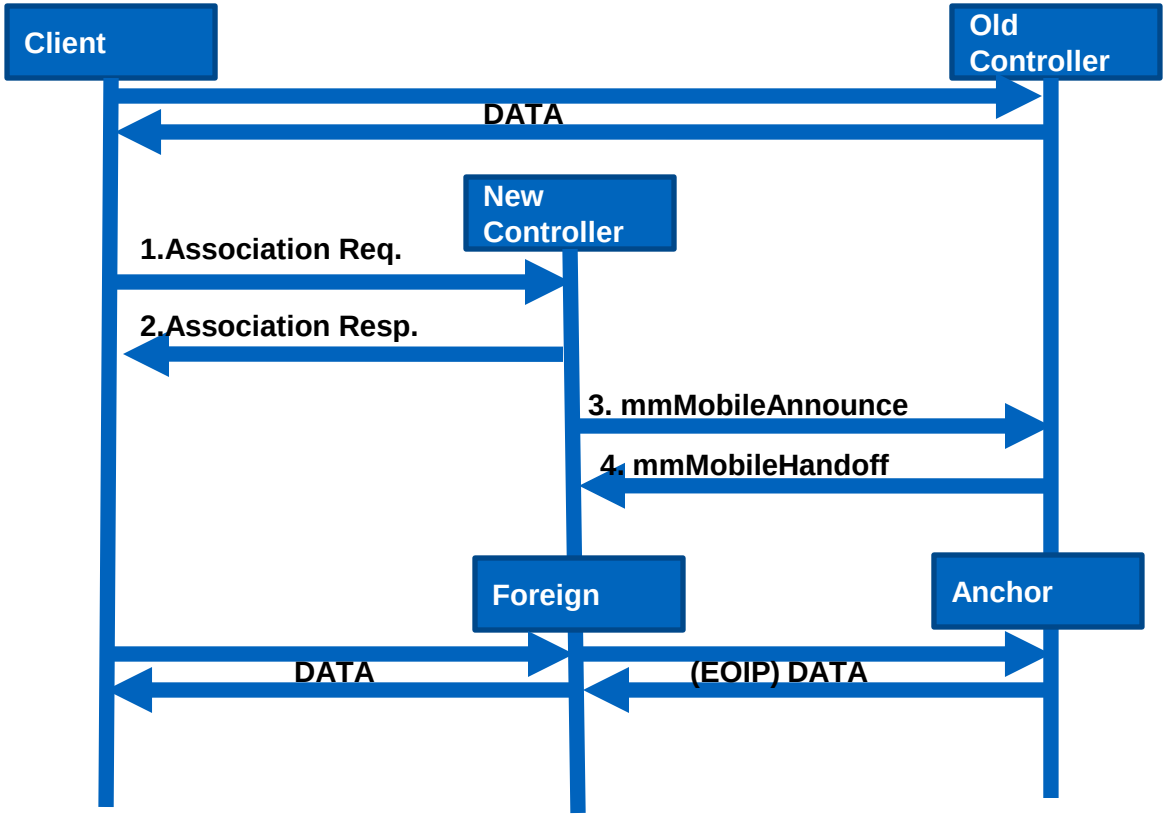
Layer 3 roaming (a.k.a. **anchor/foreign**)

New WLC does not have an interface on the subnet the client is on

New WLC will tell the old WLC to forward all client traffic to the new WLC



Mobility— L3 Inter WLC



Mobility— L3 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

MobileAnnounce

```
Mobility packet received from:
  10.10.1.4, port 16666
  type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 177  seq: 180
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 0.0.0.0, instance: 0
  VLAN IP: 10.10.3.4, netmask: 255.255.255.0
Switch IP: 10.10.1.1
Handoff as Local, Client IP: 10.10.1.103 Anchor IP: 10.10.1.5
Anchor Mac : f8.66.f2.fa.a8.40
Mobility packet sent to:
  10.10.1.4, port 16666
  type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 177  seq: 204  l
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 10.10.1.103, instance: 0
  VLAN IP: 10.10.1.5, netmask: 255.255.255.0
```

MobileHandoff

```
10.10.1.103 RUN (20) State Update from Mobility-Complete to Mobility-In
Updated location for station old AP 00:16:9c:4b:c4:c0-0, new AP 00:00:0
10.10.1.103 RUN (20) mobility role update request from Local to Anchor
Peer = 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5
```

```
0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMP
Mobility packet sent to:
  10.10.1.5, port 16666
  type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 177  seq: 180  len 116
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 0.0.0.0, instance: 0
VLAN IP: 10.10.3.4, netmask: 255.255.255.0
```

```
Mobility packet received from:
  10.10.1.5, port 16666
  type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 177  seq: 204  len 546 f
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 10.10.1.103, instance: 0
  VLAN IP: 10.10.1.5, netmask: 255.255.255.0
Switch IP: 10.10.1.5
Mobility handoff, NAC State Payload [ Client's NAC OOB State : Access, Quaranti
Mobility handoff for client:
  Ip: 10.10.1.103
  Anchor IP: 10.10.1.5, Peer IP: 10.10.1.5
0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state DHCP_REQD (
10.10.1.103 DHCP_REQD (7) Change state to RUN (20) last state RUN (20)
10.10.1.103 RUN (20) Reached PLUMBFASTPATH: from line 5273
10.10.1.103 RUN (20) Change state to RUN (20) last state RUN (20)
Assigning Address 10.10.1.103 to mobile
Handoff confirm: Pre Handoff PEM State: RUN
10.10.1.103 RUN (20) mobility role update request from Unassociated to Foreign
  Peer = 10.10.1.5, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5
```

Mobility— L3 Inter WLC

Debug Client <Mac Address>

Debug Mobility Handoff Enable

Anchor

```
10.10.1.103 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete,
  mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED

Mobility Response: IP 10.10.1.103 code Handoff Indication (2)
   reason Client handoff successful - anchor released (1), PEM State RUN, Role Anchor
Set symmetric mobility tunnel for as in Anchor role
10.10.1.103 Added NPU entry of type 1, dtlFlags 0x1
Sending a gratuitous ARP for 10.10.1.103, VLAN Id 0

(Cisco Controller) >show client detail
Client MAC Address..............................
AP MAC Address..................................... 00:00:00:00:00:00
Mobility State..................................... Anchor
Mobility Foreign IP Address....................... 10.10.1.4
```

Foreign

```
10.10.1.103 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete,
    mobility role=Foreign, client state=APF_MS_STATE_ASSOC
10.10.1.103 RUN (20) Change state to RUN (20) last state F
Configured Anchor for mobile. Sending Igmp query
Mobility Response: IP 10.10.1.103 code Handoff (1),
    reason Handoff success (0), PEM State RUN, Role Foreign(3)
Set symmetric mobility tunnel for as in Foreign role
10.10.1.103 Added NPU entry of type 1, dtlFlags 0x1

(Cisco Controller) >show client detail
Client MAC Address..............................
AP MAC Address..................................... 00:26:cb:94:44:c0
Mobility State..................................... Foreign
Mobility Anchor IP Address........................ 10.10.1.5
```

Mobility Group vs. Mobility Domain

- Mobility Group - WLCs with the same group name
  - L2/L3 Handoff
  - Auto Anchoring
  - Fast Secure Roaming
  - APs get all of these as a Discover candidate

Local Mobility Group group

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

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

Local Mobility Group group

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

Mobility Data/Control Path

- Sent between all WLCs, by member with lowest MAC
  - Control Path = UDP 16666 (30 Seconds)
  - Data Path = EoIP Protocol 97 (10 Seconds)
  - debug mobility keep-alive enable <IP Address>

```
09:07:01.397: UDP Keepalive received from::
09:07:01.397:   10.10.1.4, port 16666
09:07:01.397:   type: 20(MobilityPingRequest)  subtype: 0  version: 1  xid: 52  seq: 52  len 41 flags 1
09:07:01.397:   group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
09:07:01.397: UDP Keepalive sent to::
09:07:01.397:   10.10.1.4, port 16666
09:07:01.397:   type: 21(MobilityPingReply)  subtype: 0  version: 1  xid: 52  seq: 74  len 41 flags 0
09:07:01.397:   group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
 May 22 09:07:11.397: EOIP Keepalive received from: 10.10.1.4
 May 22 09:07:11.397:  version : 02, opcode : ETHOIP_OP_REQ sequence no. 22 peerStatus: 1
 May 22 09:07:11.397: EOIP Keepalive sent to: 10.10.1.4
 May 22 09:07:11.397:  version : 02, opcode : ETHOIP_OP_RESP sequence no. 22 peerStatus: 0
 May 22 09:07:21.397: EOIP Keepalive received from: 10.10.1.4
 May 22 09:07:21.397:  version : 02, opcode : ETHOIP_OP_REQ sequence no. 23 peerStatus: 1
 May 22 09:07:21.397: EOIP Keepalive sent to: 10.10.1.4
 May 22 09:07:21.397:  version : 02, opcode : ETHOIP_OP_RESP sequence no. 23 peerStatus: 0
 May 22 09:07:31.398: EOIP Keepalive received from: 10.10.1.4
 May 22 09:07:31.398:  version : 02, opcode : ETHOIP_OP_REQ sequence no. 24 peerStatus: 1
 May 22 09:07:31.398: EOIP Keepalive sent to: 10.10.1.4
 May 22 09:07:31.398:  version : 02, opcode : ETHOIP_OP_RESP sequence no. 24 peerStatus: 0
09:07:31.398: UDP Keepalive received from::
09:07:31.398:   10.10.1.4, port 16666
09:07:31.398:   type: 20(MobilityPingRequest)  subtype: 0  version: 1  xid: 53  seq: 53  len 41 flags 1
09:07:31.398:   group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
09:07:31.398:  Highest Mobility Version supported  2
09:07:31.398: UDP Keepalive sent to::
09:07:31.398:   10.10.1.4, port 16666
09:07:31.398:   type: 21(MobilityPingReply)  subtype: 0  version: 1  xid: 53  seq: 75  len 41 flags 0
09:07:31.398:   group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
```

Troubleshooting Wireless LANs

- Software and Support
- Troubleshooting Basics
- AP Discovery/Join
- WLC Config/Monitoring
- Client Connectivity
- Mobility
- **Packet Analysis**

Wireshark Tutorial

- Default Wireshark view might look like this:

Unfiltered_call_trace.pkt - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

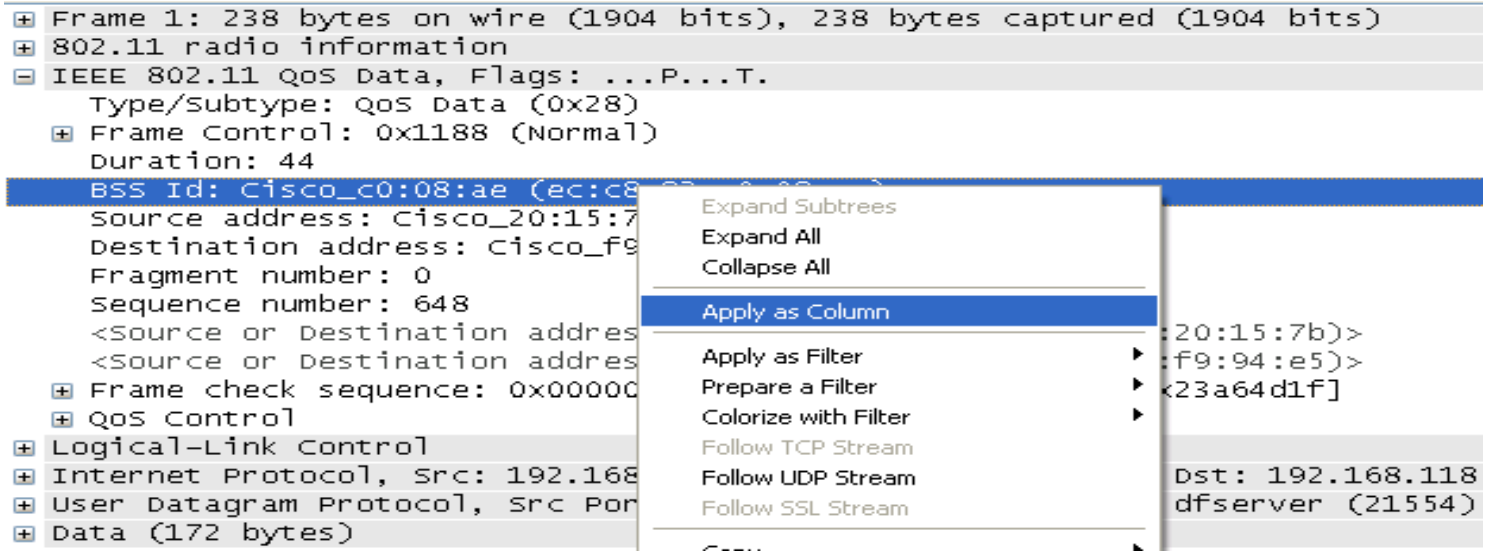
Filter: Expression... Clear Apply

No.	Time	Source	Destination	Info
61	0.204835892	Cisco_f9:94:e5	Cisco_20:15:7b	QoS Data, SN=630, FN=0, Flags=..m.R.F.C [retransmitted]
62	0.204839707		Cisco_c0:08:ae (RA)	Acknowledgement, Flags=...P....C
63	0.205097199	192.168.118.100	192.168.118.102	Source port: dfserver Destination port: 30528
64	0.205469132	Cisco_f9:94:e5	Cisco_20:15:7b	QoS Data, SN=631, FN=0, Flags=....R.F.C [retransmitted]
65	0.205474854		Cisco_c0:08:ae (RA)	Acknowledgement, Flags=...P....C
66	0.223968506	192.168.118.102	192.168.118.100	Source port: 30528 Destination port: dfserver
67	0.223972321		Cisco_20:15:7b (RA)	Acknowledgement, Flags=.....C
68	0.224212647	192.168.118.100	192.168.118.102	Source port: dfserver Destination port: 30528
69	0.224214554		Cisco_c0:08:ae (RA)	Acknowledgement, Flags=...P....C
70	0.243968964	192.168.118.102	192.168.118.100	Source port: 30528 Destination port: dfserver
71	0.243972779		Cisco_20:15:7b (RA)	Acknowledgement, Flags=.....C
72	0.244344712	Cisco_20:15:7b	Cisco_f9:94:e5	QoS Data, SN=661, FN=0, Flags=...PR..TC [retransmitted]
73	0.244348526		Cisco_20:15:7b (RA)	Acknowledgement, Flags=.....C
74	0.244350434	192.168.118.100	192.168.118.102	Source port: dfserver Destination port: 30528
75	0.244583130	Cisco_f9:94:e5	Cisco_20:15:7b	QoS Data, SN=633, FN=0, Flags=....R.F.C [retransmitted]
76	0.244588852		Cisco_c0:08:ae (RA)	Acknowledgement, Flags=...P....C
77	0.263969422	192.168.118.102	192.168.118.100	Source port: 30528 Destination port: dfserver
78	0.263975144		Cisco_20:15:7b (RA)	Acknowledgement, Flags=.....C
79	0.264211655	192.168.118.100	192.168.118.102	Source port: dfserver Destination port: 30528
80	0.264215470		Cisco_c0:08:ae (RA)	Acknowledgement, Flags=...P....C
81	0.280082703	Cisco_c0:08:ae	Broadcast	Beacon frame, SN=4082, FN=0, Flags=.....C, BI=100, SSI
82	0.280088425	192.168.118.102	192.168.118.100	Source port: 30528 Destination port: dfserver
83	0.280088425		Cisco_20:15:7b (RA)	Acknowledgement, Flags= C

File: "C:\Documents and Settings\weterry\Deskt... Packets: 7204 Displayed: 7204 Marked: 0 Load time: 0:00.140

Wireshark Tutorial

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



Wireshark Tutorial

- Within seconds your wireshark can also have:

Destination	BSS Id	Priority	Data Rate	Channel	Signal Strength	EOSP	Info
192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	48000000	149	100	End of service	Source
Cisco_20:15:7b	ec:c8:82:c0:08:ae	3	48000000	149	100	End of service	QoS Dat
192.168.118.100	ec:c8:82:c0:08:ae	6	24000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
Cisco_20:15:7b	ec:c8:82:c0:08:ae	3	48000000	149	100	End of service	QoS Dat
Cisco_c0:08:ae (			24000000	149	100		Acknowl
192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	48000000	149	100	Service period	Source
Cisco_c0:08:ae (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	48000000	149	100	End of service	Source
Cisco_c0:08:ae (			24000000	149	100		Acknowl
192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	48000000	149	100	End of service	Source
Cisco_c0:08:ae (			24000000	149	100		Acknowl
Cisco_c0:08:ae	ec:c8:82:c0:08:ae	0	24000000	149	100		QoS Nul
Cisco_20:15:7b (			24000000	149	100		Acknowl
Cisco_20:15:7b	ec:c8:82:c0:08:ae	7	48000000	149	100	End of service	QoS Nul
Cisco_c0:08:ae (			24000000	149	100		Acknowl
192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	54000000	149	100	End of service	Source
Cisco_c0:08:ae (			24000000	149	100		Acknowl
Broadcast	ec:c8:82:c0:08:ae		6000000	149	100		Beacon
192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source
Cisco_20:15:7b (			24000000	149	100		Acknowl
192.168.118.102	ec:c8:82:c0:08:ae	3	54000000	149	100	Service period	Source

ıred (fra... | Packets: 7204 Displayed: 7204 Marked: 0 Load time: 0:00.156

Wireshark Tutorial

- Filtering data is just as easy

Filter: wlan.bssid == ec:c8:82:c0:08:ae Expression... Clear Apply

No.	Time	Source	Destination	BSS Id	Priority	Data Rate	Channel	Signal Strength	EOSP	Info
41	0.1439	192.168.118.102	192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source port: 305
43	0.1440	192.168.118.100	192.168.118.102	ec:c8:82:c0:08:ae	3	54000000	149	100	End o	Source port: dfs
44	0.1446	Cisco_f9:94:e5	Cisco_20:15:7b	ec:c8:82:c0:08:ae	3	54000000	149	100	End o	QoS Data, SN=628
46	0.1638	192.168.118.102	192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source port: 305
48	0.1641	192.168.118.100	192.168.118.102	ec:c8:82:c0:08:ae	3	54000000	149	100	End o	Source port: dfs
50	0.1773	192.168.118.102	192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	99		Source port: 305
52	0.1777	Cisco_c0:08:ae	Broadcast	ec:c8:82:c0:08:ae		6000000	149	100		Beacon frame, SN
53	0.1777	Cisco_c0:08:ae	Cisco_20:15:7b	ec:c8:82:c0:08:ae	7	54000000	149	100	End o	QoS Null functio
55	0.2039	192.168.118.102	192.168.118.100	ec:c8:82:c0:08:ae	6	54000000	149	100		Source port: 305
57	0.2043	Cisco_20:15:7b	Cisco_f9:94:e5	ec:c8:82:c0:08:ae	6	24000000	149	99		QoS Data, SN=659

```
⊞ 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 (0x08)
  ⊞ Frame Control: 0x0080 (Norma
    Duration: 0
    Destination address: Broadca
    Source address: Cisco_c0:08:
    <Source or Destination addre                    ff:ff)>
    <Source or Destination addre
    BSS Id: Cisco_c0:08:ae (ec:c
    Fragment number: 0
    Sequence number: 4080
  ⊞ Frame check sequence: 0x0000
⊞ IEEE 802.11 wireless LAN manag
```

- Expand Subtrees
- Expand All
- Collapse All
- Apply as Column
- Apply as Filter ▸
  - Selected
  - Not Selected
  - ... and Selected
  - ... or Selected
  - ... and not Selected
  - ... or not Selected
- Prepare a Filter ▸
- Colorize with Filter ▸
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream

Wireshark Tutorial - CAPWAP

- User data is encapsulated in CAPWAP

Filter: (capwap) Expression... Clear Apply

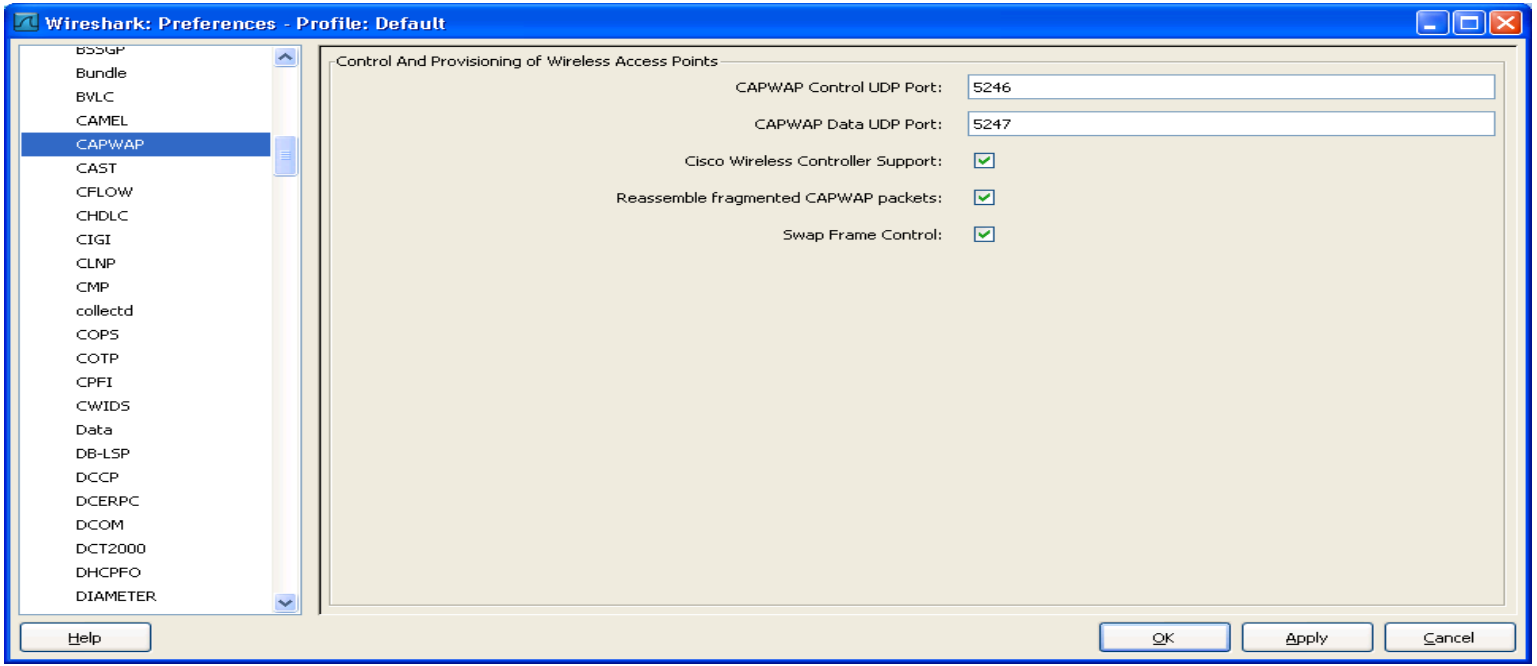
No.	Time	Source	Destination	BSS Id	Info
6471	713.2344	Cisco_07:68:30	HonHaiPr_da:83:76	00:1c:b1:07:68:30	Association Request,
6473	713.2738	b1:07:68:30:0c:ee	Homag_00:00:1c	e6:da:83:76:ff:ff	Fragmented IEEE 802.
6474	713.2745	b1:07:68:30:0c:ee	Homag_00:00:1c	e6:da:83:76:ff:ff	Fragmented IEEE 802.
6476	713.3316	ff:ff:ff:ff:00:03	MS-NLB-PhysServer-08_00:0	08:00:00:02:1c:4b	Fragmented IEEE 802.
6478	713.7592	b1:07:68:30:0c:ee	Homag_00:00:1c	e6:da:83:76:ff:ff	Fragmented IEEE 802.
6479	713.7592	ff:ff:ff:ff:00:03	MS-NLB-PhysServer-08_00:0	08:00:00:01:0c:ee	Fragmented IEEE 802.
6481	713.7595	Cisco_07:68:30	HonHaiPr_da:83:76	9c:4e:20:24:77:43	Association Request,
6482	714.2311	b1:07:68:30:00:00	PciCompo_00:00:1c	00:00:00:00:00:1c	Fragmented IEEE 802.

```
⊞ Frame 6471: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)
⊞ Ethernet II, Src: Cisco_31:37:e7 (88:43:e1:31:37:e7), Dst: Cisco_dc:85:74 (00:1c:58:dc:85:74)
⊞ Internet Protocol, Src: 10.10.1.14 (10.10.1.14), Dst: 10.10.1.161 (10.10.1.161)
⊞ User Datagram Protocol, Src Port: capwap-data (5247), Dst Port: 51289 (51289)
⊞ Control And Provisioning of Wireless Access Points
⊞ IEEE 802.11 Association Request, Flags: ....R...
⊞ IEEE 802.11 wireless LAN management frame
⊞ [Malformed Packet: IEEE 802.11]
```

Wireshark Tutorial

- Wireshark can also de-encapsulate CAPWAP DATA

  Edit > Preference > Protocols > CAPWAP



Wireshark Tutorial

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

Filter: (capwap) && (wlan.bssid == 00:1c:b1:07:68:30) Expression... Clear Apply

No.	Time	Source	Destination	BSS Id	Info
6478	713.7592	10.10.3.32	10.10.3.255	00:1c:b1:07:68:30	Echo (ping) request
6481	713.7595	Cisco_24:77:43	HonHaiPr_da:83:76	00:1c:b1:07:68:30	Data, SN=0, FN=0, Fla
6482	714.2311	00:00:00_00:00:00	Cisco_07:68:30	00:1c:b1:07:68:30	Probe Request, SN=0,
6483	714.2747	HonHaiPr_da:83:76	Broadcast	00:1c:b1:07:68:30	Gratuitous ARP for 10
6488	714.7591	10.10.3.32	10.10.3.255	00:1c:b1:07:68:30	Echo (ping) request
6491	714.7596	Cisco_24:77:43	HonHaiPr_da:83:76	00:1c:b1:07:68:30	Data, SN=0, FN=0, Fla
6492	715.3237	10.10.3.32	239.255.255.250	00:1c:b1:07:68:30	M-SEARCH * HTTP/1.1
6495	715.3384	HonHaiPr_da:83:76	Broadcast	00:1c:b1:07:68:30	Who has 10.10.3.1? T

```
⊞ Frame 6478: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
⊞ Ethernet II, Src: Cisco_dc:85:74 (00:1c:58:dc:85:74), Dst: Cisco_31:37:e7 (88:43:e1:31:37:e7)
⊞ 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
```

Packet Capture – Sniffer Mode AP

- Select channel to Sniff
- Select destination for traffic

802.11b/g/n Cisco APs > Configure

General

AP Name	AP8843.e103.bda2
Admin Status	Enable
Operational Status	UP
Slot #	0

Sniffer Channel Assignment

Sniff	☑
Channel	6
Server IP Address	10.10.3.217

RF Channel Assignment

Packet Capture – Sniffer Mode AP

- Omnipeek has a Remote Adapter to capture this data
- Wireshark, just capture network adapter

  NOTE: Wireshark does not open the port UDP 5000

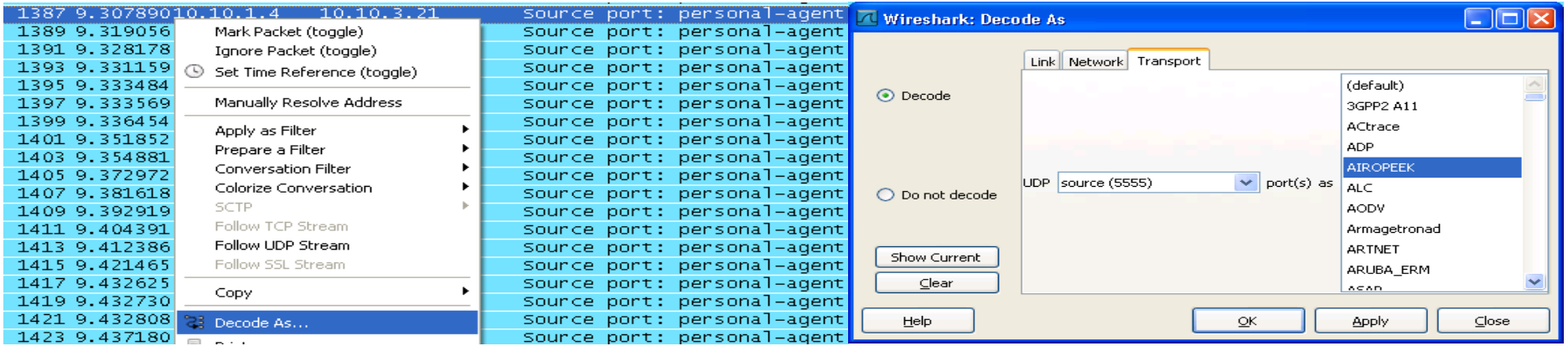
  PC will send ICMP Unreachables

Filter: Expression... Clear Apply

No.	Time	Source	Destination	BSS Id	Info
1353	9.147979	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1354	9.148017	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1355	9.164847	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1356	9.164925	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1357	9.174637	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1358	9.174698	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1359	9.187766	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1360	9.187839	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1361	9.199622	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1362	9.199673	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1363	9.202995	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1364	9.203025	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1365	9.212584	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main
1366	9.212639	10.10.3.217	10.10.1.4		Destination unreachable (Port unreachable)
1367	9.212718	10.10.1.4	10.10.3.21		Source port: personal-agent Destination port: commplex-main

Packet Capture – Sniffer Mode AP

- With wireshark, filter !icmp.type == 3
- Data (UDP 5000) still not intelligible yet
  - Decode as Airopeek



Packet Capture – Sniffer Mode AP

Filter: (((!icmp.type == 3))) && (wlan.bssid == 00:13:10:94:b1:38) Expression... Clear Apply

No.	Time	Source	Destination	BSS Id	Info
908	7.407936	Apple_41:75:76	Cisco-Li_94:b1:38	00:13:10:94:b1:38	Null function (No data), SN=2918, F
912	7.408402	Apple_41:75:76	IPv6mcast_00:00:00:fb	00:13:10:94:b1:38	Data, SN=2919, FN=0, Flags=.p.....T
930	7.447019	Apple_41:75:76	Cisco-Li_94:b1:38	00:13:10:94:b1:38	Null function (No data), SN=2920, F
934	7.447464	Apple_41:75:76	IPv4mcast_00:00:fb	00:13:10:94:b1:38	Data, SN=709, FN=0, Flags=.pm...F.C
936	7.448667	Apple_41:75:76	IPv6mcast_00:00:00:fb	00:13:10:94:b1:38	Data, SN=710, FN=0, Flags=.p....F..
953	7.549848	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=711, FN=0, Flags=.
981	7.652088	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=712, FN=0, Flags=.
1003	7.754447	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=713, FN=0, Flags=.
1033	7.856970	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=714, FN=0, Flags=.
1061	7.959369	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=715, FN=0, Flags=.
1086	8.061752	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=716, FN=0, Flags=.
1110	8.162600	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=717, FN=0, Flags=.
1132	8.265532	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=718, FN=0, Flags=.
1160	8.368230	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=719, FN=0, Flags=.
1216	8.573799	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=721, FN=0, Flags=.
1246	8.675197	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=722, FN=0, Flags=.
1270	8.778398	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=723, FN=0, Flags=.
1292	8.880925	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=724, FN=0, Flags=.
1314	8.983597	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=725, FN=0, Flags=.
1337	9.085730	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=726, FN=0, Flags=.
1359	9.187766	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=727, FN=0, Flags=.
1383	9.290083	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=728, FN=0, Flags=.
1409	9.392919	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=729, FN=0, Flags=.
1441	9.495297	Cisco-Li_94:b1:38	Broadcast	00:13:10:94:b1:38	Beacon frame, SN=730, FN=0, Flags=.

Key- Takeaways

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




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CISCO™