What You Make Possible
Troubleshooting Wireless LANs
BRKEWN-3011
Troubleshooting Wireless LANs

- Basic Concepts
- Best Practices
- Supportability
- AP Troubleshooting
- Troubleshooting Clients
- Voice over WiFi
- SE-Connect - Clean Air
Basic Concepts
Key Concepts

- 802.11/802.1X/WPA
- Cisco Unified Architecture/CAPWAP
- Cisco Unified Client Mobility
- Radio Resource Management (RRM)
- Client states
Steps to Building an 802.11 Connection

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

State 1: Unauthenticated, Unassociated
State 2: Authenticated, Unassociated
State 3: Authenticated, Associated
802.1X Authentication

The Supplicant Derives the Session Key from User Password or Certificate and Authentication Exchange
Cisco Centralised WLAN Model

CAPWAP Defines Control Messaging and Data Encapsulation Between Access Points and Centralised WLAN Controller

Access Points Are Lightweight Controlled by a Centralised WLAN Controller

Much of the Traditional WLAN Functionality Moved from Access Points to Centralised WLAN Controller

Switched/Routed Wired Network

Ingress/Egress Point from/to Upstream Switched/Routed Wired Network (802.1Q Trunk)

Lightweight Access Point

CAPWAP Tunnel

Control Messages
Data Encapsulation

Wireless LAN Controller
Layer 3 CAPWAP Architecture

- Access points require IPv4 addressing
- APs can communicate with WLC across routed boundaries
CAPWAP

- Protocol starting with 5.2 for controllers and APs
- IETF Standard
- Support encryption of control and data planes
- L3 only
- Controllers still support LWAPP Discovery, Join, Image states to migrate APs
- Fragmentation and reassembly done in protocol, not in IP level
## Differences between LWAPP and CAPWAP

<table>
<thead>
<tr>
<th>Description</th>
<th>LWAPP</th>
<th>CAPWAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmentation/ Re-assemble</td>
<td>Relies on IPv4</td>
<td>CAPWAP Itself Does Both</td>
</tr>
<tr>
<td>Path-MTU Discovery</td>
<td>Not Supported</td>
<td>Has a Robust P-MTU Discovery Mechanism, Can also Detect Dynamic MTU Changes</td>
</tr>
<tr>
<td>Control Channel Encryption between AP and WLC</td>
<td>Yes (Using AES)</td>
<td>Yes (Using DTLS)</td>
</tr>
<tr>
<td>Data Channel Encryption between AP and WLC</td>
<td>No</td>
<td>Yes (Using DTLS)</td>
</tr>
<tr>
<td>UDP Ports</td>
<td>12222(Data), 12223(Ctrl)</td>
<td>5246 (Ctrl) 5247 (Data)</td>
</tr>
</tbody>
</table>
Mobility—Intra-Controller

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

- Asymmetric traffic path established (deprecated)

- Symmetric traffic path
Radio Resource Management Refresher

- Dynamic Channel Assignment (DCA)
  - Selects channels for the radios to use

- Transmit Power Control (TPC)
  - Adjusts radio power level for the radios to use

- Coverage Hole Detection and Mitigation (CHDM)
  - Detects coverage holes, by identifying clients from which we are receiving a poor signal, and accordingly increases radio power, to compensate
Radio Resource Management – auto RF

- config advanced 802.11[a|b] tx-power-control-thresh is the master fader for radio power (values in -60 to -80 dBm — lower values for denser installations)

<table>
<thead>
<tr>
<th>Thresh</th>
<th>Default: -70 dBm</th>
<th>Use lower values for high density deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td>-68</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-73</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## PEM - Client Forwarding

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUN</td>
<td>Normal Client Traffic Forwarding</td>
</tr>
<tr>
<td>DHCP_REQ</td>
<td>IP Learning State. One Packet from this Client Is Sent to CPU in Order to Learn the IP Address Used</td>
</tr>
<tr>
<td>WEBAUTH_REQ</td>
<td>Web Authentication Pending</td>
</tr>
<tr>
<td>8021X_REQ</td>
<td>802.1x Authentication Taking Place</td>
</tr>
</tbody>
</table>
Best Practices
Best Practices - RF

- Site survey, in case of doubts, **site survey**, after installation, **site survey** …
- Site survey **must** be meaningful
  - Same device types, coverage band, intended service
- Reduce unneeded WLANs
- Use BandSelect only on WLANs with mixed clients
Best Practices - RF

- Turn off lowest data rates when possible (more bandwidth, less channel utilisation, etc)
- Fine tune AutoRF (depending on density)
- Avoid aggressive load balancing, unless high-density and never use with voice
Best Practices - Network

- Do not use STP on controllers
- Filter VLANs toward WLC that are not in use
- LAG config on switch side must be consistent
- If no LAG, one AP manager per physical port
- Use multicast mode
Best Practices - Network

For fastest failover, AP ports should be configured for:

- Local mode:
  - `spanningtree portfast` and `switchport mode access`

- H-REAP / FlexConnect mode:
  - `spanningtree portfast` and `switchport mode access`
  - `spanningtree portfast trunk` and `switchport mode trunk` (VLAN support)
Best Practices - Mobility

- Do not create unnecessary **big** mobility groups
- Same virtual gateway address across all members
- VG address should **not** be routable
  - address 1.1.1.1 has been allocated, use 192.0.2.1 instead (RFC 5737)
- Same CAPWAP mode, symmetric setting, group name
- Use symmetric mobility (only option as of 5.2)
Best Practices - Security

- Increase RADIUS timeout (e.g. 5 seconds)
- Change SNMPv3 users
- Increase EAP identity timeout, not EAP retries!
- Increase AP authentication threshold
- NTP: must have for context-aware/location, MFP, debugging
Best Practices - Administration

- Back up before upgrade
- Downgrade is not supported (no longer true since XML configuration in 4.2+)
- Always set controller name on AP for join process
- Enable and set syslog server on APs
- Enable telnet/SSH and set up local credentials on AP
- Make sure AP name is representative of location
Supportability
Supportability

- WLC Supportability
  - Methods of Management
  - Using the GUI
  - Important Show Commands (CLI)
  - Important Debug Commands (CLI)
  - Best Practices

- AP Supportability
  - Methods of Accessing the AP
  - Important Show Commands
WLC Supportability

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

Default Mode
(E)=Enabled (D)=Disabled
WLC Supportability

Using the GUI

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

Using the GUI

- Wireless > All APs
  - AP list shows AP Physical UP Time
  - APs are sorted by Controller Associated Time
  - Check bottom of AP list for any recent AP disruptions
  - Select AP to see Controller Associated Time (duration)
WLC Supportability

Using the GUI

- Management
- SNMP Config
- Logs
- Tech Support
WLC Supportability

Important Show Commands (CLI)

- Show run-config
  - “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 Supportability

Important Debugs (CLI)

- Debug client <client mac address>
- 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 mac addr <mac address>
WLC Supportability

Best Practices

- Change default SNMP Parameters
- Configure Syslog for WLC and AP
- Enable Coredump for WLC and AP
- Configure NTP Server for Date/Time
AP 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

Default Mode
(E)=Enabled (D)=Disabled
AP Supportability

AP Remote Commands (WLC CLI)

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

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

Show Commands (AP CLI or WLC Remote Cmd)

- Show controller Do[0/1] (or Show Tech)
- Show log
- WLC: show ap eventlog <ap name>
- Show capwap client <?>

Debug capwap console cli
Debug capwap client no-reload
AP Troubleshooting
AP Troubleshooting

- Typical problems
  - Discovery/Join
  - Time set at WLC
  - Regulatory domain issues
  - Debug
AP Join Troubleshooting

- First, the AP must **hunt** for the IP addresses of possible WLCs to join
- Next, the AP sends **discover** messages to all the WLCs, to find out which ones are alive
- Then the AP picks the best WLC and tries to **join** it
- For details, see the “Controlling Lightweight Access Points” section of the WLC configuration guide.
L3 WLC Address Hunting

AP Goes Through the Following Steps to Compile a Single List of WLAN Controllers

1. Discovery broadcast on local subnet
2. Locally-stored controller IP addresses
3. DHCP vendor specific option 43
4. DNS resolution of:
   - “CISCO-CAPWAP-CONTROLLER.localdomain”
   - “CISCO-LWAPP-CONTROLLER.localdomain”
5. If no controller found, start over

Note: The Actual Order of This Process Is Irrelevant Because Each AP Goes Through All Steps Before Proceeding to the Next Phase. Some Steps May Never Happen

L3 WLC Discovery

AP Tries to Send Discover Messages to All the WLC Addresses that Its Hunting Process Turned Up
Discovery Algorithm

- Once a list of WLAN controllers is compiled, the AP sends a unicast CAPWAP discovery request message to each of the controllers in the list.
- WLAN controllers receiving the CAPWAP discovery messages respond with a discovery response.
- Discovery response contain important information:
  - Controller name, controller type, AP capacity, current AP load, master controller status, AP-manager IP address(es).
- AP waits for its discovery interval to expire, then selects a controller and sends a join request to that controller.
WLAN Controller Selection Algorithm

The AP Selects the Controller to Join using the Following Criteria

1. If the AP has been configured with primary, secondary, and/or tertiary controller, the AP will attempt to join these first
2. Attempt to join a WLAN controller configured as a master controller
3. Attempt to join the WLAN controller with the greatest excess AP capacity

Note: This Last Step Provides the Whole System with Automatic AP/WLC Load-Balancing Functionality
WLAN Controller Join Process
Mutual Authentication

- AP CAPWAP Join request contains the AP’s signed X.509 certificate
- WLAN controller validates the certificate before sending an CAPWAP join response
  - Manufacture Installed Certificate (MIC) all Cisco Aironet APs manufactured after July 18, 2005
  - Self-Signed Certificate (SSC) - Lightweight upgraded Cisco Aironet APs manufactured prior to July 18, 2005
  - SSC APs must be authorised on the WLAN controller
WLAN Controller Join Process
Mutual Authentication

- If AP is validated, the WLAN controller sends the CAPWAP join response which contains the controller’s signed X.509 certificate.
- If the AP validates the WLAN controller, it will download firmware (if necessary) and then request its configuration from the WLAN controller.
Troubleshooting Lightweight APs

- Can the AP and the WLC communicate?
- Make sure the AP is getting an address from DHCP (check the DHCP server leases for the AP’s MAC address)
- If the AP’s address is statically set, ensure it is correctly configured
- Try pinging the AP from the controller
- If pings are successful, ensure the AP has at least one method by which to discovery at least a single WLC
- Console or telnet/ssh into the controller to run debugs
Set the WLC’s Time

- Make sure each controller has the correct time set
- Check the WLC’s time:
  - (WLC_CLI) >show time
- Manually set the time:
  - (WLC_CLI) >config time manual <MM/DD/YY> <HH:MM:SS>
- Or, use NTP:
  - (WLC_CLI) >config time ntp server <Index> <IP Address>
  - (WLC_CLI) >config time ntp interval <3600 - 604800 sec>
Does Regulatory Domain Matter? Yes!

(WLC_CLI) >debug mac addr 00:12:80:ad:7a:9c
(WLC_CLI) >debug capwap events enable

[TIME]: * spamVerifyRegDomain:6202 AP 00:12:80:ad:7a:9c 80211bg
Regulatory Domain (-A) does not match with country (BE) reg. domain -BE for slot 0

[TIME]: DEBU CTRLR spamVerifyRegDomain:6167 spamVerifyRegDomain
RegDomain set for slot 1 code 0 regstring -A regDfromCb -E

[TIME]: * spamVerifyRegDomain:6202 AP 00:12:80:ad:7a:9c 80211a
Regulatory Domain (-A) does not match with country (BE) reg. domain -BE for slot 1

[TIME]: DEBU CTRLR spamVerifyRegDomain:6210 spamVerifyRegDomain AP
RegDomain check for the country BE failed

[TIME]: * spamProcessConfigRequest:1730 AP 00:12:80:ad:7a:9c: Regulatory Domain check Completely FAILED. The AP will not be allowed to join.

▪ The fix?
  Make sure you match your APs’ regulatory domain with your WLCs.
  RRM will use the lowest common denominator for channels

▪ How do you know how to make sure you do?
  Search CCO for Wireless LAN Compliance Status
CAPWAP Troubleshooting

- WLC side debug commands:

(Cisco Controller) >debug capwap ?

- events: Configures debug of CAPWAP events and state
- errors: Configures debug of CAPWAP errors
- detail: Configures debug of CAPWAP detail
- info: Configures debug of CAPWAP info
- packet: Configures debug of CAPWAP packet
- payload: Configures debug of CAPWAP payloads
- hexdump: Configures debug of CAPWAP payloads
CAPWAP Troubleshooting

- Useful CAPWAP join debugs:
  - debug dhcp
  - debug ip udp
  - debug capwap client {config, error, event, detail, packet}
  - debug dtls client {error, event}
CAPWAP Join

(Cisco Controller) > debug capwap events enable  
*Jan 09 05:02:07.952: 00:17:df:a8:bf:00 Discovery Request from 192.168.100.103:41824  
*Jan 09 05:02:07.952: 00:17:df:a8:bf:00 Join Priority Processing status = 0, Incoming Ap's Priority 1, MaxLrads = 6, joined Aps =0  
*Jan 09 05:02:07.952: 00:17:df:a8:bf:00 Discovery Response sent to 192.168.100.103:41824  
*Jan 09 05:02:19.881: DTLS connection established  
*Jan 09 05:02:19.881: DTLS Session established server (192.168.100.4:5246), client (192.168.100.103:41824)  
*Jan 09 05:02:19.881: Starting wait join timer for DTLS connection 0xc332dbc!, AP: 192.168.100.103:41824  
*Jan 09 05:02:19.884: 00:17:df:a8:bf:00 Join Request from 192.168.100.103:41824  
*Jan 09 05:02:19.884: DTL Adding AP 3 - 192.168.100.103  
*Jan 09 05:02:19.884: Join Version: = 84057344  
*Jan 09 05:02:19.885: Join resp: CAPWAP Maximum Msg element len = 91  
*Jan 09 05:02:19.885: CAPWAP State: Configure
CAPWAP Failure

*Jan 09 07:44:45.781: 00:17:df:a8:bf:00 Discovery Request from 192.168.100.104:41825
*Jan 09 07:44:45.781: 00:17:df:a8:bf:00 Join Priority Processing status = 0, Incoming Ap's Priority 1, MaxLrads = 6, joined Aps = 0
*Jan 09 07:44:45.781: 00:17:df:a8:bf:00 Discovery Response sent to 192.168.100.104:41825
*Jan 09 07:44:56.710: DTLS connection established
*Jan 09 07:44:56.710: DTLS Session established server (192.168.100.4:5246), client (192.168.100.104:41825)
*Jan 09 07:44:56.710: Starting wait join timer for DTLS connection 0xc332dbc!, AP: 192.168.100.104:41825
*Jan 09 07:44:56.713: 00:17:df:a8:bf:00 Join Request from 192.168.100.104:41825
*Jan 09 07:44:56.714: 00:17:df:a8:bf:00 In AAA state 'Idle' for AP 00:17:df:a8:bf:00
*Jan 09 07:44:56.714: 00:17:df:a8:bf:00 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.100.104:41825
*Jan 09 07:44:56.714: Failed to process CAPWAP packet from 192.168.100.104:41825
*Jan 09 07:44:56.715: Disconnecting DTLS session 0xc332dbc for AP 00:17:df:a8:bf:00 (192:168:100:104/41825)
*Jan 09 07:44:56.715: CAPWAP State: Dtls tear down
Troubleshooting Clients
Troubleshooting Clients

- Connectivity issues
- Logs/Debugs
- Wireless/Wired Sniff
- Spectrum Analysis
- Each Step Explained
Connectivity Issues

- Typical problem: **client(s) can not connect to the network**
- Where to look (assuming basic steps were already taken): policy manager state and status

CLI: `show client detail <MAC>`
Client Connectivity


- **Configuration Issues**
  - SSID/Security Mismatch
  - Disabled WLAN
  - Unsupported Data-Rates
  - Disabled Clients
  - Radio Preambles

- **Cisco Features - Issues with Third Party Clients**
  - Aironet IE, MFP
Complexity of a Wireless Network

- **EAP**
- **Supplicant Logs**
- **Driver Debugs/Adapter Capture**
- **Wireless Sniff**
- **Wireless Sniff**
- **Spectrum Analysis**
- **AP Debugs**
- **Wired Sniff**
- **WLC Debugs**
- **DHCP Logs**
- **ACS/ISE Logs**

- **Chan. 1**
  - 802.11 Data
  - CAPWAP
  - 802.11 Management

- **Chan. 11**
  - 802.11 Data
  - CAPWAP
  - 802.11 Management

- **DHCP**
- **ACO / ISE**
- **CAPWAP**
- **EOIP**
- **RADIUS**
- **NTP**
Supplicant logs

-WZC supplicant log:

```
netsh ras set tracing * enabled
```
logs in c:\windows\tracing

see http://www.microsoft.com/technet/network/wifi/wlansupp.mspx

-PROSet supplicant log: under hklm\software\intel\wireless\settings

```
1xconfigdbg=wwxyz; 1xDebugLevel=dword:0x18; 1xLogLevel=dword:0x18
```
logs in c:\ (subject to change without warning)

-ADU: see CSCsi16921
-CSSC/AnyConnect: see Log Packager utility on cisco.com
RADIUS Logs

- See Monitoring and Reporting section on ACS 5.x or ISE
- NTP sync your ACS/ISE!
© 2013 Cisco and/or its affiliates. All rights reserved.

Cisco IOS DHCP server:
- `debug ip dhcp server events`
- `debug ip dhcp server packet`
AP Debugs

- Connect via AP console (`debug capwap console cli`)
- From WLC CLI, use:
  - `debug ap enable APname`
  - `debug ap command “debug command” APname`
- 5.x+ can use Telnet/SSH to connect to APs
By default, radio debugs appear only on the console. To see radio debugs in your telnet/ssh/WLC CLI session, use the command

```
dump dot11 dot11radio x print printf
```

where x is 0 or 1

Useful radio debugs:

```
dump dot11 dot11radio x trace print {mgmt, keys, client, beacon, rcv, xmt}
```

(beacon, rcv & xmt can be extremely verbose!)
Client Debug

d debug client <mac address>

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

(Cisco Controller) >show debug

MAC address ............................... 00:16:ea:b2:04:36

Debug Flags Enabled:

dhcp packet enabled
dot11 mobile enabled
dot11 state enabled
dot1x events enabled
dot1x states enabled
pem events enabled
pem state enabled
CCKM client debug enabled
WLC Debugs

- More general client debugging options:
  - `debug dot11`
  - `debug dot1x`
  - `debug aaa` (= use for RADIUS troubleshooting)
  - `debug pem`
  - `debug mobility handoff` (= roaming)
  - `debug dhcp`

- Use `debug client <MACaddr>` to filter on a single client
Good options (Windows PCs):

- Omnipeek from Wildpackets (Linksys WUSB600N, CB21AG,..)
- Wireshark with CACE Technologies AirPcap adapters
  USB adapters nice for multichannel sniff
- AirMagnet
Wireless Sniff - Some Tips

- One packet capture per wireless channel
- Multi-channel capture using multiple adapters
- Take unfiltered captures
- Cut a new file every 20–30 MB
- Do not display updated packet during capture
- NTP sync everything
Wired Sniff

- When capturing from trunk ports, best to capture with 802.1q tags (watch out for packets in the wrong VLANs). You may need to touch driver config to see the VLAN information
- Cut new file every 20/30 MB; don’t display packet updates in real time
- NTP sync your sniffers!
Use spectrum analysis to capture RF spectrum behaviour—necessary to identify/track down non-802.11 interference sources

Cisco’s product: **Spectrum Expert**
(Standalone or CleanAir AP in SE-Mode)
SpEx Spectrogram

- Mouse Hover Reveals Channel Position, Sweep Time/Date, and Top Five Devices
- Active AP
- Very Low Power/Activity
- Microwave Oven
- Colour Indicates Power, Red = -35 dBm
- High Power, Bursting over Time
SpEx Tips

- When capturing, be sure to have an 802.11 adapter installed, enabled, but configured not to associate to a WLAN
  - Spectrum expert cannot identify 802.11 devices (MAC address, etc.) without an 802.11 adapter’s aid

- **NTP sync your Spectrum Expert host!**

- **Always use external antenna**

- **If searching for Interferers, good idea to turn off your wireless network**
1. Client probes for the SSID
2. Client authenticates/associates in 802.11 to an AP
3. EAP takes place
   3.1 EAP dialog between client and authenticator
   3.2 Authenticator (radius) dialog to end-user DB
4. DHCP address negotiation
5. Client reaches RUN state
Probing

- Clients broadcasts a probe for the SSID of interest
- AP unicasts back a probe response
- Probe response includes interesting facts (information elements) about the service

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
<th>Size</th>
<th>RSSI</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>137.815670013 Cisco_92</td>
<td>Broadcast Cisco_92</td>
<td>IEEE 802 Probe Request, SSID: &quot;&quot;</td>
<td>45</td>
<td>58</td>
<td>6.0</td>
<td></td>
</tr>
<tr>
<td>137.816028594 Cisco_80</td>
<td>Cisco_92</td>
<td>IEEE 802 Probe Response, SSID: &quot;&quot;</td>
<td>209</td>
<td>52</td>
<td>6.0</td>
<td></td>
</tr>
</tbody>
</table>

Tagged parameters (169 bytes)
- SSID parameter set: ""
- Supported Rates: 6.0(8) 9.0 12.0(8) 18.0 24.0(8) 36.0 48.0 54.0
- QoS Load Element
- Cisco unknown 1 + Device Name
- Reserved tag number: Tag 150 Len 6
- Vendor Specific: WPA
- Vendor Specific: Aironet Unknown
Problems at Probing Stage

- What if the client never sends out a probe?
  - Is it configured for the SSID of interest?

- What if the AP doesn’t send back the probe response?
  - Is it (WLC) configured for the SSID of interest?
  - Do you have RF coverage from this AP? (can you see beacons from it?)

- What if the client never moves beyond probing?
  - Does it like the IEs that the AP is sending out?
  - Try different crypto settings; disable Aironet extensions;
  - try different basic rates; etc.
802.11 Auth/Assoc

1. Client probes for the SSID
2. Client authenticates/associates in 802.11 to an AP
3. EAP takes place
   - 3.1 EAP dialog between client and authenticator
   - 3.2 Authenticator (radius) dialog to end-user DB
4. DHCP address negotiation
5. Client reaches RUN state
802.11 Auth/Assoc

- Client and AP authenticate to each other (normally just open authentication nowadays, some devices don’t even do this)
- Client tries to associate to the AP, hopefully gets a status=0 (successful) response
- What if unsuccessful?
  - Check status code
  - Run debugs on WLC
3. EAP takes place

3.1 EAP dialog between client and authenticator
3.2 Authenticator (radius) dialog to end-user DB
## Wireshark Capture of MS-PEAP (WPA2)

<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
<th>Size</th>
<th>RSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11:16:27.427249</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Request, Identity [RFC3748]</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>11:16:27.505640</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>EAP</td>
<td>Response, Identity [RFC3748]</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>11:16:27.895869</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Request, PEAP [Palekar]</td>
<td>1040</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>11:16:27.928226</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>EAP</td>
<td>Request, PEAP [Palekar]</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>11:16:27.961292</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Request, PEAP [Palekar]</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>11:16:27.974427</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>SSL</td>
<td>Client Hello</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>11:16:27.979089</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Request, PEAP [Palekar]</td>
<td>451</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>11:16:27.982266</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>EAP</td>
<td>Request, PEAP [Palekar]</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>11:16:28.005694</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Response, PEAP [Palekar]</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>11:16:28.048802</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>EAP</td>
<td>Response, PEAP [Palekar]</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11:16:28.052007</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>11:16:28.951994</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>11:16:28.955152</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>11:16:28.988898</td>
<td>IntelCor_3c</td>
<td>Cisco_36</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>11:16:28.103138</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>11:16:28.151817</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>11:16:28.154869</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>11:16:28.189439</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>11:16:28.194497</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>TLSv1</td>
<td>Application Data</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>11:16:28.194909</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Success</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>11:16:28.294394</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Success</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>11:16:28.297998</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Success</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>11:16:28.317797</td>
<td>Cisco_36</td>
<td>IntelCor_3c</td>
<td>EAP</td>
<td>Success</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>11:16:28.435178</td>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP Request - Transaction ID 0x56fe92f0</td>
<td>378</td>
<td></td>
</tr>
</tbody>
</table>
Failed 802.1X Client Authentication

debug dot1x events—Username/Password Failure
(WLC_CLI) >debug mac addr 00:13:ce:57:2b:84
(WLC_CLI) >debug dot1x events enable

[TIME]: * dot1x_auth_txReqId:2827 Sending EAP-Request/Identity to mobile 00:13:ce:57:2b:84 (EAP Id 1)

[TIME]: * dot1x_authsm_capture_supp:675 Received EAPOL START from mobile 00:13:ce:57:2b:84

[TIME]: * dot1x_handle_eapsupp:1962 Received Identity Response (count=n) from mobile 00:13:ce:57:2b:84

<SNIP> Series of 802.1X EAP Requests/Responses </SNIP>

[TIME]: * dot1x_process_aaa:898 Processing Access-Challenge for mobile 00:13:ce:57:2b:84

[TIME]: * dot1x_bauthsm_txReq:465 Sending EAP Request from AAA to mobile 00:13:ce:57:2b:84 (EAP Id 14)

[TIME]: * dot1x_handle_eapsupp:1997 Received EAP Response from mobile 00:13:ce:57:2b:84 (EAP Id 14, EAP Type 25)

[TIME]: * dot1x_process_aaa:928 Processing Access-Reject for mobile 00:13:ce:57:2b:84

[TIME]: * dot1x_auth_txCannedFail:2865 Sending EAP-Failure to mobile 00:13:ce:57:2b:84 (EAP Id 14)
### Check Client Record for Details

**In the WLC GUI, Go to:** Monitor | Clients and Select Details for the Client of Choice

<table>
<thead>
<tr>
<th>Client Properties</th>
<th>AP Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>AP Address</td>
</tr>
<tr>
<td>00:0b:9b:47:3e:06</td>
<td>00:22:90:92:af:70</td>
</tr>
<tr>
<td>IP Address</td>
<td>AP Name</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>LL149</td>
</tr>
<tr>
<td>Client Type</td>
<td>AP Type</td>
</tr>
<tr>
<td>Regular</td>
<td>802.11b</td>
</tr>
<tr>
<td>User Name</td>
<td>WLAN Profile</td>
</tr>
<tr>
<td>bad_user</td>
<td>CL2012</td>
</tr>
<tr>
<td>Port Number</td>
<td>Status</td>
</tr>
<tr>
<td>29</td>
<td>Associated</td>
</tr>
<tr>
<td>Interface</td>
<td>Association ID</td>
</tr>
<tr>
<td>vlan69</td>
<td>1</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>802.11 Authentication</td>
</tr>
<tr>
<td>0</td>
<td>Open System</td>
</tr>
<tr>
<td>CCX Version</td>
<td>Reason Code</td>
</tr>
<tr>
<td>CCXv1</td>
<td>1</td>
</tr>
<tr>
<td>ESE Version</td>
<td>Status Code</td>
</tr>
<tr>
<td>Not Supported</td>
<td>0</td>
</tr>
<tr>
<td>Mobility Role</td>
<td>CF Reliable</td>
</tr>
<tr>
<td>Local</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Mobility Peer IP Address</td>
<td>CF Poll Request</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Policy Manager State</td>
<td>Short Preamble</td>
</tr>
<tr>
<td>8021X_REQD</td>
<td>Implemented</td>
</tr>
<tr>
<td>Management Frame Protection</td>
<td>PBCG</td>
</tr>
<tr>
<td>No</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>UpTime (Sec)</td>
<td>Channel Agility</td>
</tr>
<tr>
<td>160</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Power Save Mode</td>
<td>Timeout</td>
</tr>
<tr>
<td>OFF</td>
<td>1800</td>
</tr>
<tr>
<td>Current TxRateSet</td>
<td>WEP State</td>
</tr>
<tr>
<td>11.0</td>
<td>WEP Enable</td>
</tr>
<tr>
<td>Data Rate Set</td>
<td></td>
</tr>
<tr>
<td>1,6,2,0,5,6,11.0</td>
<td></td>
</tr>
</tbody>
</table>

**Security Information**

- Security Policy Completed: No
- Policy Type: 802.1x
- Encryption Cipher: CCMP (AES)
- EAP Type: PEAP
Successful 802.1X Client Authentication

debug aaa events
(WLC_CLI) >debug mac addr 00:13:ce:57:2b:84
(WLC_CLI) >debug aaa events enable

[TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 49) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57

[TIME]: DEBU CTRLR processIncomingMessages:3480 ****Enter processIncomingMessages: response code=11

[TIME]: DEBU CTRLR processRadiusResponse:3053 ****Enter processRadiusResponse: response code=11

[TIME]: * processRadiusResponse:3325 Access-Challenge received from RADIUS server 10.48.76.71 for mobile 00:13:ce:57:2b:84 receiveId = 2


[TIME]: DEBU CTRLR processIncomingMessages:3480 ****Enter processIncomingMessages: response code=2

[TIME]: DEBU CTRLR processRadiusResponse:3053 ****Enter processRadiusResponse: response code=2

[TIME]: * processRadiusResponse:3325 Access-Accept received from RADIUS server 10.48.76.71 for mobile 00:13:ce:57:2b:84 receiveId = 2
Failed 802.1X Client Authentication

debug aaa events - AAA Server Unreachable

(Cisco Controller) > debug mac addr 00:13:ce:57:2b:84
(Cisco Controller) > debug aaa events enable


[TIME]: * sendAAAError:323 Returning AAA Error 'Timeout' (-5) for mobile 00:13:ce:57:2b:84

- AAA connectivity failure will generate an SNMP trap

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>210</td>
<td>RADIUS server 10.40.76.71:1012 deactivated in global list</td>
</tr>
<tr>
<td>219</td>
<td>RADIUS server 10.48.76.71:1812 failed to respond to request (ID 14) for client 00:00:00:3d:00:00 / user 'unknown'</td>
</tr>
</tbody>
</table>

In the WLC GUI, Go to: Management | SNMP | Trap Logs
Verify Complete 802.11/802.1X Connectivity

duild pem state

(WLC_CLI) > debug mac addr 00:13:ce:57:2b:84
(WLC_CLI) > debug pem state enable

[TIME]: pem_api.c:1780 - State Update 00:13:ce:57:2b:84 from RUN (20) to START (0)
[TIME]: pem_api.c:1836 - State Update 00:13:ce:57:2b:84 from START (0) to AUTHCHECK (2)
[TIME]: pem_api.c:1859 - State Update 00:13:ce:57:2b:84 from AUTHCHECK (2) to 8021X_REQD (3)
[TIME]: pem_api.c:3977 - State Update 00:13:ce:57:2b:84 from 8021X_REQD (3) to L2AUTHCOMPLETE (4)
[TIME]: pem_api.c:4152 - State Update 00:13:ce:57:2b:84 from L2AUTHCOMPLETE (4) to RUN (20)
Troubleshooting 802.1X

- Make sure the RADIUS server is properly configured

RADIUS Authentication Servers > Edit

- Server Index: 1
- Server Address: 10.46.76.71
- Shared Secret Format: ASCII
- Shared Secret: ***
- Confirm Shared Secret: ***
- Key Wrap
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576
- Server Timeout: 2 seconds
- Network User Management: Enabled
- IPSec

Make Sure the Correct Shared Secret Is Input
Select the Correct RADIUS Port (Common Ports Are 1812 and 1645)
Status Must Be Enabled
Timeout May Be too Short
Network User Auth Has to Be Enabled for This AAA Server to Be Used Globally, Otherwise, Select on WLAN

In the WLC GUI, Go to: Security | AAA | RADIUS Authentication and Then Select Edit or New
Troubleshooting 802.1X

- Make sure the proper security policy is enabled for both encryption and authentication.

Step (1): Select the Desired Layer 2 Security Configuration

Step (2): Check Radius list per WLAN or Use Global list

In the WLC GUI, Go to: WLANs | WLANs | WLANs and Then Select Edit for the WLAN of Interest
Troubleshooting 802.1X – ACS 5.x

- Enabled Logging in your ACS 5.x server to identify where issues might lie with backend authentication
802.1X – Common issues

- **SSL Handshake failure** (e.g. PEAP, EAP-TLS)
  - Verify the certificate trust settings on the client side
  - For EAP-TLS, the ACS must also trust the client certificate

- **User unknown or wrong password / unsupported auth method**
  - Correct Access-Service / Identity Store?
802.1X – Common issues

- **Unknown NAS**
  - ACS ignores RADIUS requests coming from non configured AAA clients
  - What is the source IP address of the RADIUS traffic sent by the WLC?
  - Static routes on WLC? → Service Port
DHCP Succeeds

1. Client probes for the SSID
2. Client authenticates/associates in 802.11 to an AP
3. EAP takes place
   - 3.1 EAP dialog between client and authenticator
   - 3.2 authenticator (radius) dialog to end-user DB
4. DHCP address negotiation
5. Client reaches RUN state
Troubleshooting DHCP

If Clients Aren’t Getting Addresses Properly via DHCP, Ensure:

- Clients are not configured for static addressing
- DHCP scopes are properly configured (either external or internal DHCP)
- **External servers**: need to support DHCP proxy—if they don’t, turn on DHCP bridging:
  - `(WLC_CLI) > config dhcp proxy disable`
- **Internal DHCP server**: after properly configuring the WLC’s scopes, each interface needs to have the WLC’s management IP as its DHCP server IP address, as below:

<table>
<thead>
<tr>
<th>VLAN Identifier</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>192.168.71.8</td>
<td>255.255.255.0</td>
<td>192.168.71.1</td>
</tr>
</tbody>
</table>

For Internal DHCP, Input the WLC’s Management IP Address Here

In the WLC GUI, Go to: Controller | Interfaces and Select Edit for the Interface of Choice
Client IP Provisioning via DHCP

debuge dhcp message

(WLC_CLI) >debug mac addr 00:13:ce:57:2b:84
(WLC_CLI) >debug dhcp message enable

[TIME]: dhcp option: received DHCP DISCOVER msg

[TIME]: Forwarding DHCP packet (332 octets) from 00:13:ce:57:2b:84

-- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 20.20.20.1

[TIME]: dhcp option: received DHCP OFFER msg

[TIME]: dhcp option: server id = 20.20.20.1

[TIME]: dhcp option: netmask = 255.255.255.0

[TIME]: dhcp option: gateway = 20.20.20.1

[TIME]: dhcp option: received DHCP REQUEST msg

[TIME]: dhcp option: requested ip = 20.20.20.113

[TIME]: dhcp option: server id = 1.1.1.1

[TIME]: Forwarding DHCP packet (340 octets) from 00:13:ce:57:2b:84

-- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 20.20.20.1

[TIME]: dhcp option: received DHCP ACK msg
PING Succeeds!!

1. Client probes for the SSID
2. Client authenticates/associates in 802.11 to an AP
3. EAP takes place
   - 3.1 EAP dialog between client and authenticator
   - 3.2 authenticator (radius) dialog to end-user DB
4. DHCP address negotiation
5. Client reaches RUN state
802.11n Speeds

- **Troubleshoot 802.11n Speeds Document ID: 112055**
- **Configuration Issues**
  - 11n Support Enabled
  - WMM is Allowed or Required
  - Open or WPA2-AES
  - 5Ghz Channel Width
  - 2.4Ghz does not support 40-Mhz Channels
Voice over WiFi
VoWiFi

- Wireless IP Phone Deployment Guide

- Best Practices
  - -67 dBm signal with 20-30% cell overlap
  - 802.11A
  - CCKM for Fastest Roaming
  - Avoid designs where AP is seen at superb signal, but drops off instantly
VoWiFi - Troubleshooting

- Must know if problem occurs during roaming events or when no association change takes place
- If no change in connection
  - Interference, coverage loss, end to end QOS missing/issue
- If during roaming event
  - How long did the roam take?
  - Does the client associate to another AP again within seconds?
  - Does the client associate to the same AP again?
VoWiFi - Troubleshooting

- Define a reproducible area where you believe you have perfect voice coverage but have problems
- Place phone in Neighbour List Mode (On a call)
  - Real Time current AP RSSI and candidate list
  - Confirm AP as next best candidate is realistically a good candidate
  - Confirm devices roams to correct candidate where the intended design specifies
- Watch out for sudden drops in coverage
VoWiFi - Debugs

- Phone can Trace (debug) to file or syslog
  - Recommend USB Connection and SYSLOG
  - Configured via GUI
  - Enable Debug level for Kernel, WLAN MGR, WLAN Driver

- WLC Debugs
  - Debug client <mac>
  - Debug cac all enable

- Wireless Packet Captures
SE-Connect - Clean Air
SE-Connect

- Clean Air APs can be used in lieu of Spectrum Card for Spectrum Analysis
  - AP can be placed in SE-Connect mode for full functionality
  - AP in local mode can be used now for Spectrum Analysis of current channel
Spectrum Expert with Clean Air

- Obtain Spectrum Key
- Connect to Remote Sensor
Spectrum Expert with Clean Air
Summary

- Basic Concepts
- Best Practices
- Supportability
- AP Troubleshooting
- Troubleshooting Clients
- Voice over WiFi
- SE-Connect - Clean Air
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 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](http://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 8 March 12:00pm-2:00pm

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.