

What You Make Possible

















TOMORROW starts here.



2

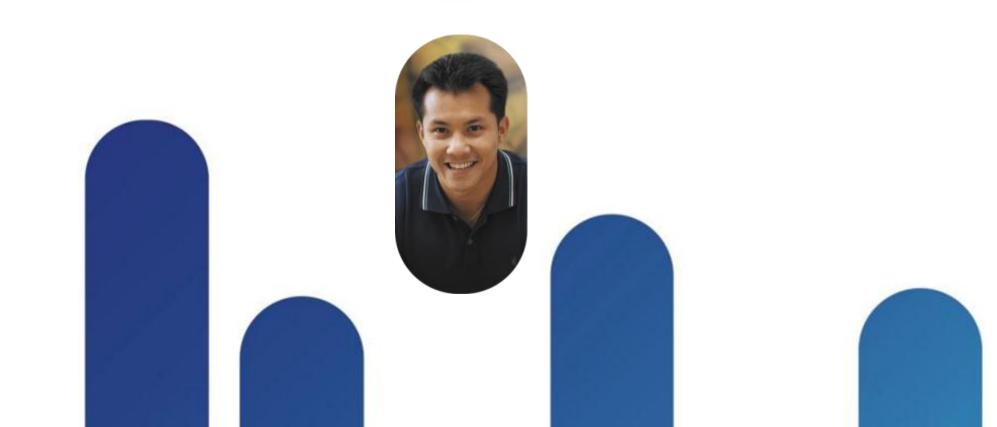
Troubleshooting Wireless LANs

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





Basic Concepts







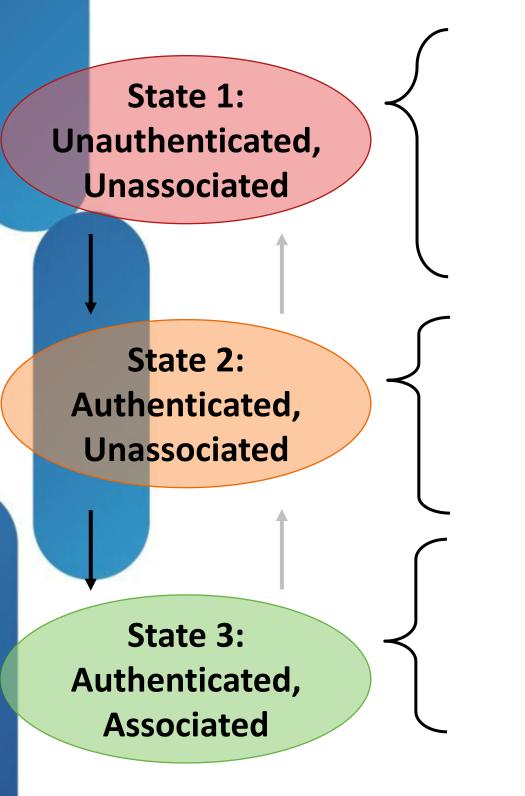


Key Concepts

- 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

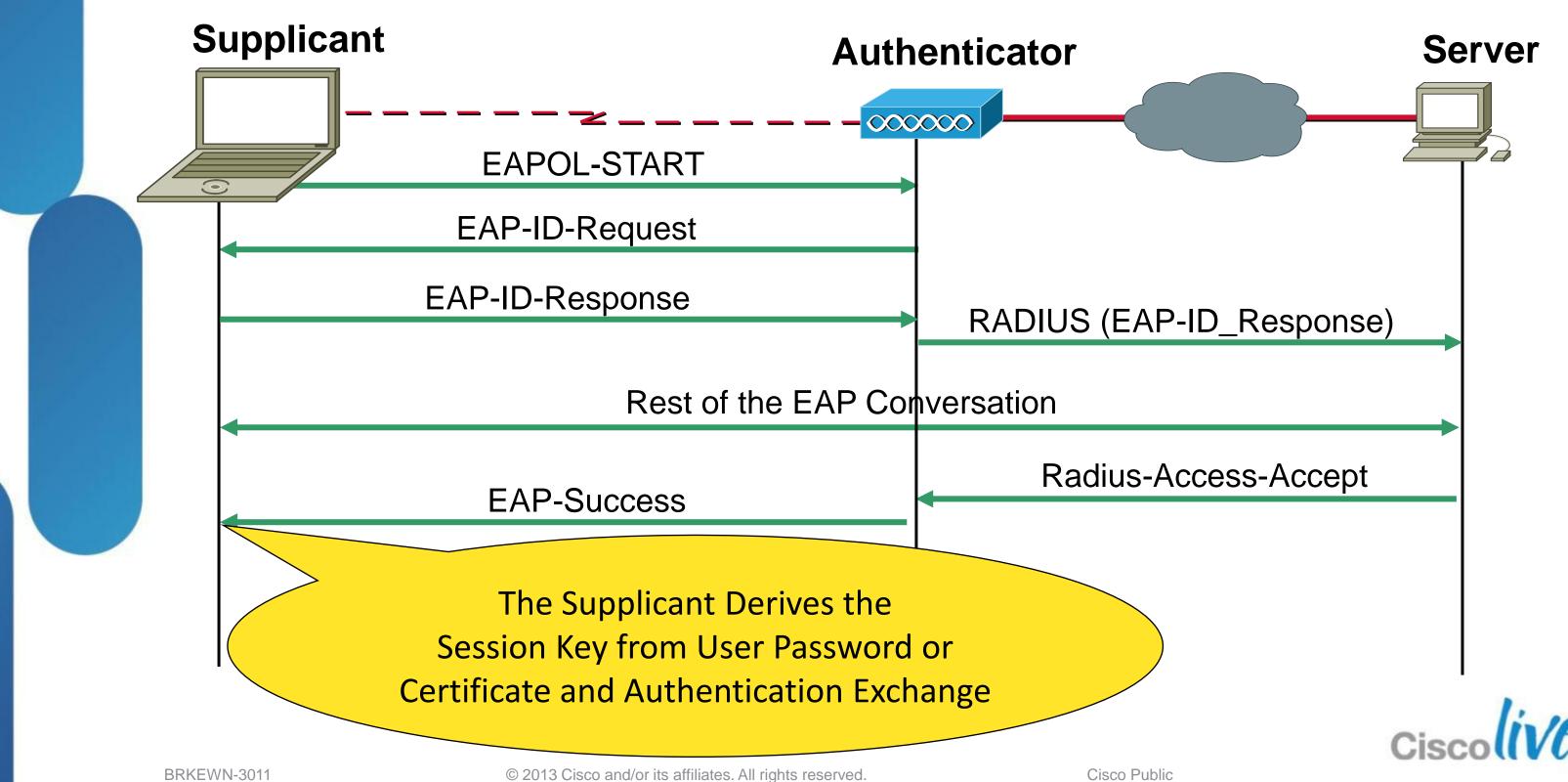


- Listen for Beacons 1.
- Probe Request/Response 2.
- <u>Authentication Request/Response</u>
- **Association Request** 4.
- **Association Response** 5.
- (Optional: EAPOL Authentication) 6.
- (Optional: Encrypt Data) 7.
- Move User Data 8.

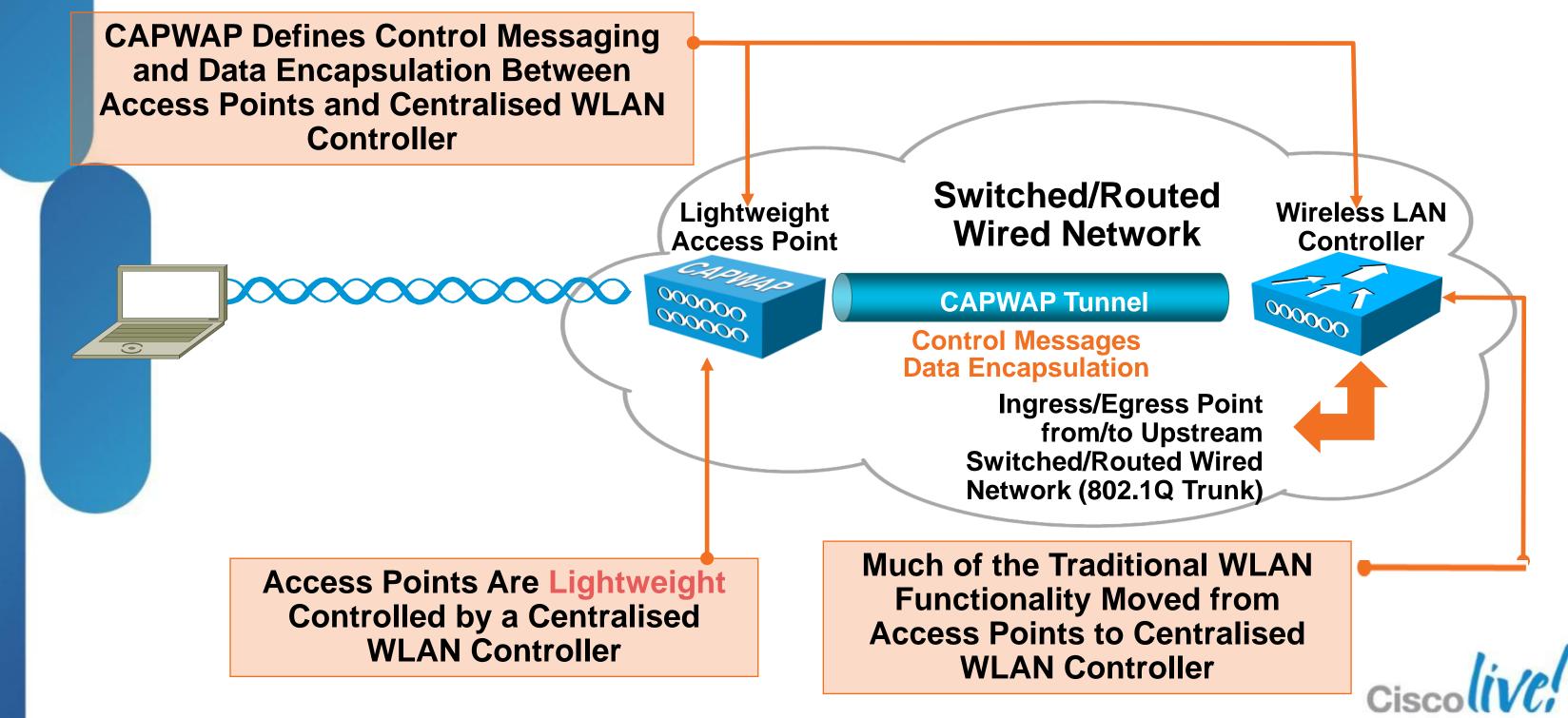




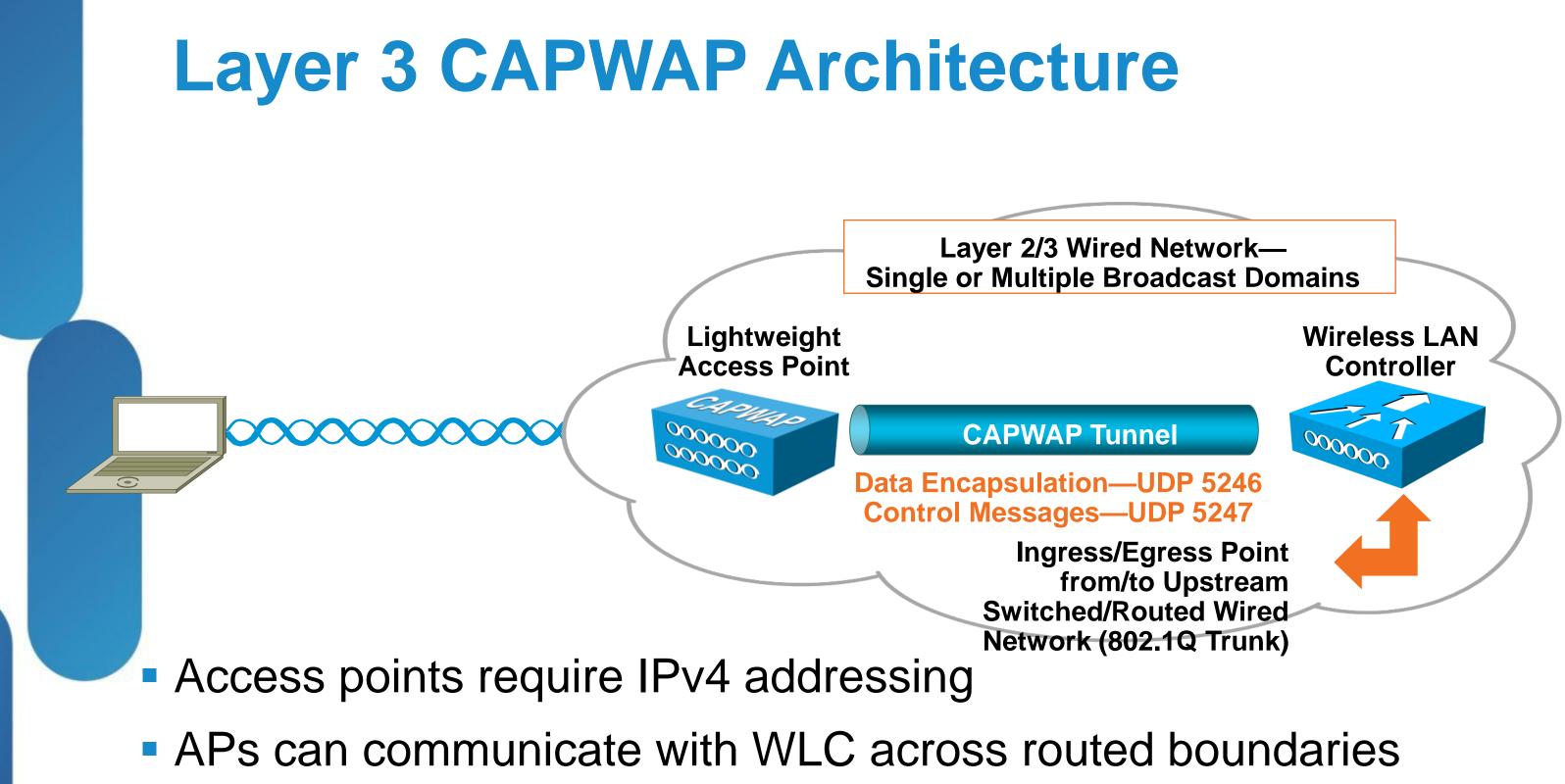
802.1X Authentication



Cisco Centralised WLAN Model











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

Description	LWAPP	
Fragmentation/ Re-assembly	Relies on IPv4	
Path-MTU Discovery	Not Supported	C
Control Channel Encryption between AP and WLC	Yes (Using AES)	
Data Channel Encryption between AP and WLC	No	
UDP Ports	12222(Data), 12223(Ctrl)	



CAPWAP

CAPWAP Itself Does Both

Has a Robust P-MTU Discovery Mechanism, Can also Detect Dynamic MTU Changes

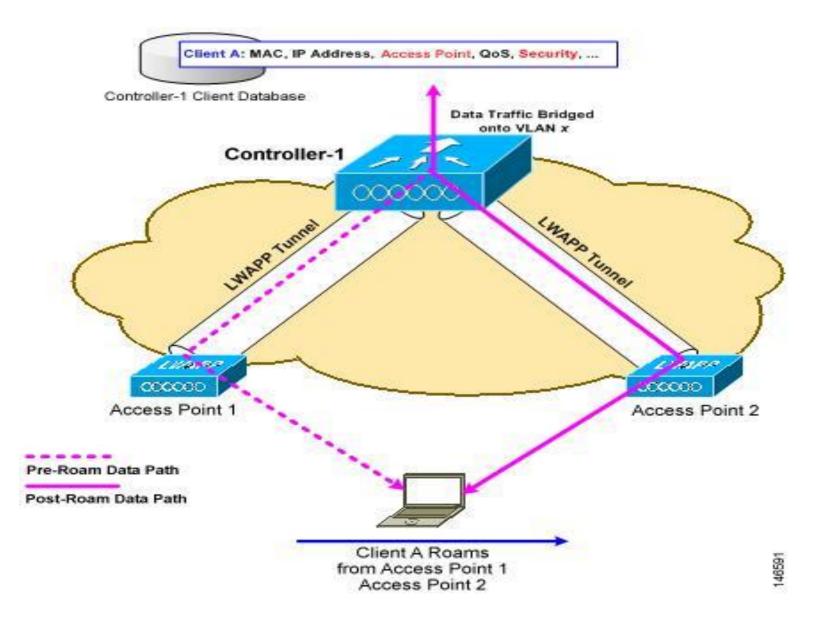
Yes (Using DTLS)

Yes (Using DTLS)

5246 (Ctrl) 5247 (Data)

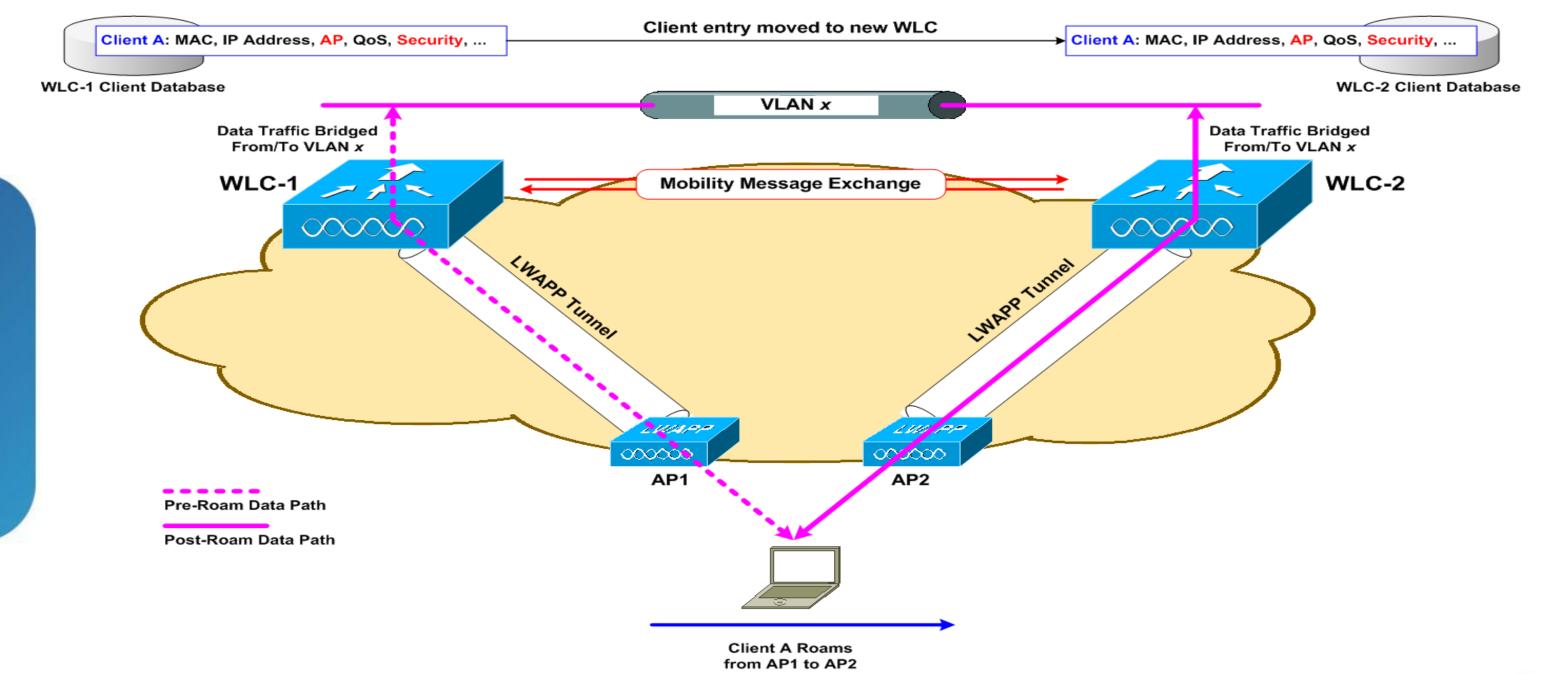
Mobility—Intra-Controller

Client roams between two APs on the same controller





Mobility—Inter-Controller (Layer 2)

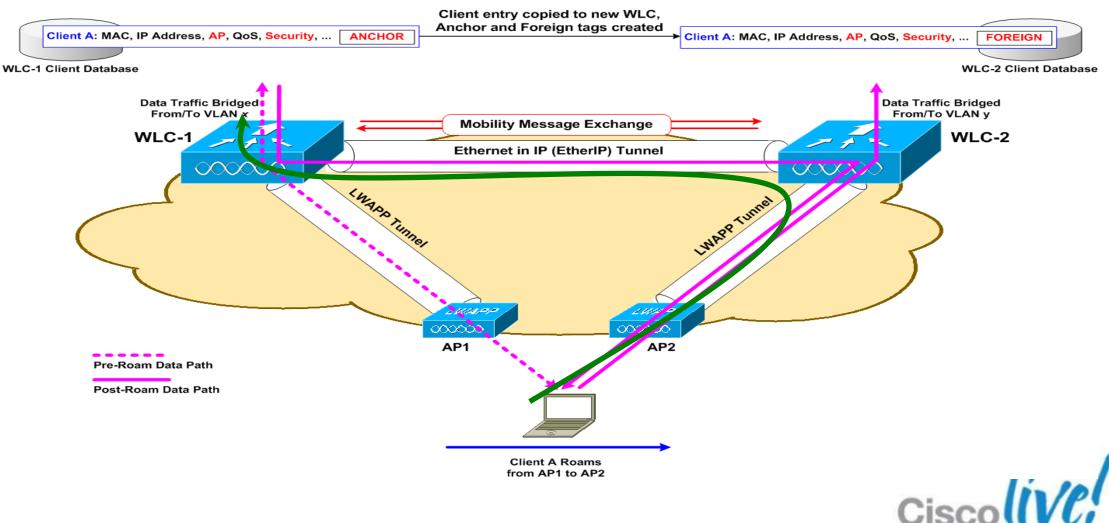






Mobility—Inter-Controller (Layer 3)

- 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 Client A: MAC, IP Address, AP, QoS, Security, ... ANCHOR
- Asymmetric traffic path established (deprecated)
- Symmetric traffic path





Radio Resource Management Refresher

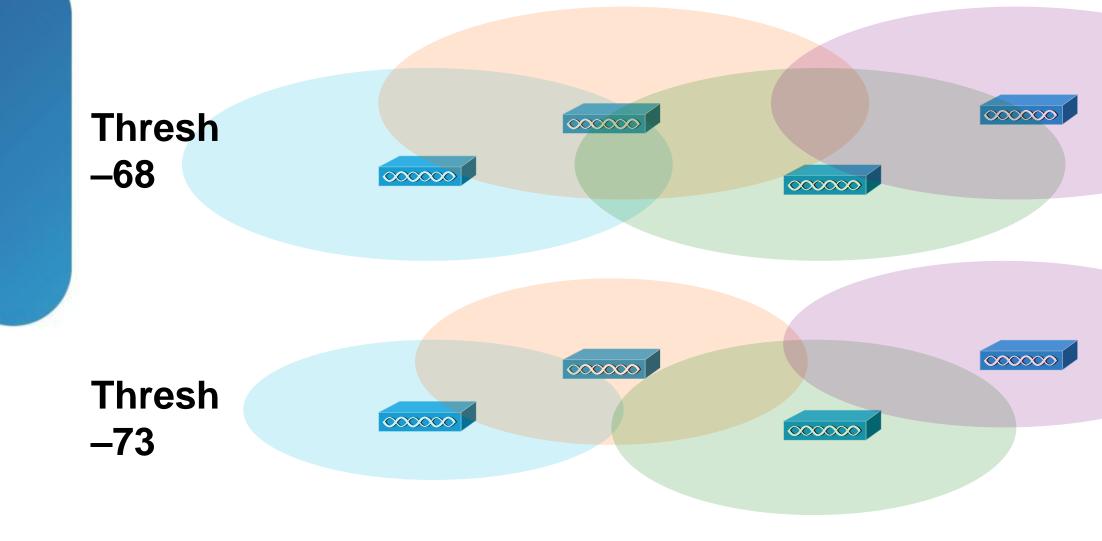
- Dynamic Channel Assignment (DCA)
 - Selects channels for the radios to use
- Transmit Power Control (**TPC**)
 - Adjusts radio power level for the radios to use
- Coverage Hole Detection and Mitigation (CHDM)
 - Detects coverage holes, by identifying clients from which we are receiving a poor signal, and accordingly **increases** radio power, to compensate





Radio Resource Management – auto RF

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



Default: -70 dBm

Use lower values for high density deployments



PEM - Client Forwarding

Name	Description
RUN	Normal Client Traffic For
DHCP_REQ	IP Learning State. One Packet from to CPU in Order to Learn the IP
WEBAUTH_REQ	Web Authentication Pe
8021X_REQ	802.1x Authentication Tak

orwarding m this Client Is Sent P Address Used ending king Place



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)

os nbers

2.1 instead (RFC 5737) oup name



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









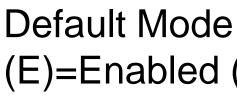
Supportability

- 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



Methods of Management

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



(E)=Enabled (D)=Disabled



Using the GUI

Monitor

AP/Radio Statistics

WLC Statistics

Client Details

Trap Log

uluilu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS
Monitor		Summa	rv	

Summary

Access Points

 Radios 802.11a/n 802.11b/g/n

Cisco CleanAir

♥ 802.11a/n Interference Devices

Air Quality Report 802.11b/g/n Interference Devices Air Quality Report Worst Air-Quality

Report Statistics Controller

AP Join Ports RADIUS Servers Mobility Statistics

CDP

Interface Neighbors AP Neighbors Traffic Metrics

Rogues

Friendly APs Malicious APs Unclassified APs Rogue Clients Adhoc Rogues Rogue AP ignore-list

Clients

Multicast

Summary 50 Access Points Supported Software Version 10.10.1.4 Address 31 Software Version 7.0.98.218 Berry Version 6.0.196.0 System Name 3750_1 Up Time 0 days, 21 hours, 46 Minutes 700 WLANS System Time Fri Apr 22 22:16:57 2011 Internal Temperature +42 C 802.11b/g Network Enabled State Bobled B02.11b/g Network Enabled Local Mobility Group 2106							nfiguration <u>P</u> i	ng Lo <u>q</u> o		
States Points Supported Supported Controller Summary Rogue Summary Management IP 10.10.1.4 Address 10.10.1.4 Service Port IP 2.2.2.2 Address Adhoc Rogues 0 Service Port IP 2.2.2.2 Active Rogue APs 31 System Name 3750_1 Controller Summary Adhoc Rogues 0 System Name 3750_1 Controller Summary Active Rogue APs 31 System Time Fri Apr 22 22:16:57 2011 Profile Name # of Clients Internal Temperature 442 C Solution of Summary S	<u>W</u> LANs <u>C</u>	ONTROL	LER W	<u>I</u> RELESS	SECURIT	Y M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	FEEDBACH	
Controller Summary Management IP 10.10.1.4 Rogue Summary Management IP 10.10.1.4 Active Rogue APs 31 Service Port IP 2.2.2.2 Active Rogue Clients 3 Software Version 7.0.98.218 Adocess 0 Berergency Image 6.0.196.0 Rogues on Wired Network 0 System Name 3750_1 0 Rogues on Wired Network 0 System Time Fri Apr 22 22:16:57 2011 Top WLANS Profile Name # of Clients Sol2.115/g Network Enabled Bost Recent Traps 802:115/second from Base Rogue AP : b0:27:54:2a:07:29 removed from Base Rogue AP : b0:27:54:2a:07:29 removed from Base Rogue AP : b0:23:51:6c:31:9 removed from Base Rogue AP : b0:23:51:56:31:9 removed from Base Rogue AP : b0:23:51:56:31:9 removed from Base Rogue AP : 00:23:51:56:31:9 removed from Base Rogue AP : 00:23:51:56:31:9 removed from Base Rogue AP : 00:23:51:56:31:9 removed from Base Rogue AP : 00:22:61:50:49:ac:03 detected on Base Rad Rogue AP : 00:23:51:56:31:9 removed from Base Rogue AP : 00:23:51:56:31:9 removed from Base <td>Summary</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Summary									
Controller Summary Rogue Summary Management IP 10.10.1.4 Address 31 Service Port IP 2.2.2.2 Active Rogue Clients 3 Address 0 Bagues Allow Rogues 0 Software Version 7.0.98.218 Adoc Rogues 0 Beregency Image 6.0.196.0 Rogues on Wired Network 0 System Name 3750_1 0 0 Up Time 0 days, 21 hours, 46 minutes Fri Apr 22 22:16:57 2011 Profile Name # of Clients System Time Fri Apr 22 22:16:57 2011 Profile Name # of Clients Most Recent Traps 802.113 Metwork Enabled Rogue AP : 00:27:54:28:07:29 removed from Base Rogue AP : 00:23:51:60:319 removed from Base Rogue AP : 00:23:51:60:319 removed from Base Rogue AP : 00:23:51:56:319 removed from Base Core Spoint Summary Total Up Down Rogue AP : 00:23:51:56:319 removed from Base 802:11b/g/n 1 0 Detail This page refreshes every 30 seconds. 802:11b/g/n 1 0 Detail This page refreshes every 30 seconds. 802:11b/g/n 1 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>FO Assess Daint</td> <td></td> <td></td>							FO Assess Daint			
Controller Summary Rogue Summary Management IP 0.10.1.4 Active Rogue APs 31 Address 10.10.1.4 Active Rogue Clients 3 Software Version 7.0.98.218 Address 0 Emergency Image 6.0.196.0 Rogues on Wired Network 0 System Name 3750_1 0 Rogues on Wired Network 0 System Time Fri Apr 22 22:16:57 2011 Profile Name ≠ of Clients Notst Recent Traps 802.11b/g Network Enabled Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:34:88:b5:d9 removed from Base Rogue AP : 00:22:34:88:b5:d9 removed from Base Radios 0 0 Detail This page refreshes every 30 seconds. 802.11b/g/n 1 0 Detail This page refreshes every 30 seconds. 802.11b/g/n 1 0 Detail This page refreshes every 30 seconds. 802.11b/g/n 1 0 Detail This page refreshes every 30 sec	3333399000	9333933339333393	aaggaaaaaa		9900990999999999		SU ACCess Point			
Controller Summary Rogue Summary Management IP 10.10.1.4 Active Rogue APs 31 Address 2.2.2.2 Active Rogue Clients 3 Software Version 7.0.98.218 Address 0 Emergency Image 6.0.196.0 Rogues on Wired Network 0 System Name 3750_1 0 Rogues on Wired Network 0 System Time Fri Apr 22 22:16:57 2011 Profile Name ≠ of Clients Notst Recent Traps 802.11b/g Network Enabled Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:34:88:b5:d9 removed from Base Rogue AP : 00:22:34:88:b5:d9 removed from Base Radios 0 0 Detail This page refreshes every 30 seconds. 802.11b/g/n 1 0 Detail Radios 0 Detail This page refreshes every 30 seconds.	11111111111	100000000000000000000000000000000000000			000000000000000000000000000000000000000			000000000000000000000000000000000000000		
Management IP 10.10.1.4 Active Rogue APs 31 Address 31 Active Rogue Clients 31 Address 7.0.98.218 Adhoc Rogues 0 Software Version 7.0.98.218 Adhoc Rogues 0 System Name 3750_1 Rogues on Wired Network 0 System Name 3750_1 Top WLANS 0 System Time Fri Apr 22 22:16:57 2011 Top WLANS # of Clients System Name Fri Apr 22 22:16:57 2011 Profile Name # of Clients Internal Temperature +42 C # of Clients # of Clients S02.11a Network Enabled # of Clients # of Clients Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 re										
Management IP 10.10.1.4 Active Rogue APs 31 Address 31 Active Rogue Clients 31 Address 7.0.98.218 Adhoc Rogues 0 Software Version 7.0.98.218 Adhoc Rogues 0 System Name 3750_1 Rogues on Wired Network 0 System Name 3750_1 Top WLANS 0 System Time Fri Apr 22 22:16:57 2011 Top WLANS # of Clients System Name Fri Apr 22 22:16:57 2011 Profile Name # of Clients Internal Temperature +42 C # of Clients # of Clients S02.11a Network Enabled # of Clients # of Clients Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 re	Controller	Summa	EV/			Poque Summary	,			
Address 2.2.2.2 Active Rogue Aps 31 Address 2.2.2.2 Active Rogue Clients 3 Software Version 7.0.98.218 Addoc Rogues 0 Regrency Image 6.0.196.0 Rogues on Wird Network 0 Version 0 days, 21 hours, 46 minutes 70 0 Address 0 System Name 3750_1 Top WLANS 70 0 Profile Name # of Clients System Time Fri Apr 22 22:16:57 2011 Profile Name # of Clients Profile Name # of Clients Soluar Name 376 Enabled Profile Name # of Clients Soluar Name 53% Enabled Profile Name # of Clients Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:22:50:49:ac:d9 detected on Base Rad CPU Usage 0% Rogue AP : 00:22:51:6:ci:03:19 removed from Base Rogue AP : 00:22:51:51:6c:03:19 removed from Base Rogue AP : 00:22:51:6:ci:03:19 removed from Base Rodius N 0 0 Detail Madress 1 1 0 Detail Address 2 0 Detail <t< td=""><td></td><td></td><td>-</td><td></td><td></td><td>Kogue Summary</td><td></td><td></td><td></td></t<>			-			Kogue Summary				
Address 2.2.2.2 Active Rogue Clients 3 Software Version 7.0,98.218 Adhoc Rogues 0 System Name 3750_1 0 0 Up Time 0 days, 21 hours, 46 minutes 0 0 System Name 3750_1 Top WLANs 0 Up Time 0 days, 21 hours, 46 minutes Top WLANs 0 System Time Fri Apr 22 22:16:57 2011 The Mark State Profile Name # of Clients 802.11a Network Enabled Most Recent Traps Rogue AP : b0:e7:54:2a:07:29 removed from Base CPU Usage 0% Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : b0:23:51:6c:03:19 removed from Base Rogue AP : b0:23:51:61:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:1b/g/n 1 1 0 Detail All APs 1 1 0 Detail All APs 1 0 Detail Client Summary Current Clients 0 Detail Current Clients 0 Detail This page refreshes every 30 seconds.	Address					Active Rogue APs			31	
Boundation of the product of the p		IP	2.2.2.2	2		Active Rogue Client	s			
Version 0.00130.0 System Name 3750_1 Up Time 0 days, 21 hours, 46 minutes System Time Fri Apr 22 22:16:57 2011 Internal Temperature +42 C 802.11a Network Enabled State Enabled 802.11b/g Network Enabled State Enabled Local Mobility Group 2106 CPU Usage 0% Memory Usage 63% Access Point Summary Total Total Up No Detail Radios 0 0 802.11b/g/n 1 0 All APs 1 1 Current Clients 0 Current Clients 0 Current Clients 0 Detail			7.0.98.	.218		_				
Up Time 0 days, 21 hours, 46 minutes Top WLANS System Time Fri Apr 22 22:16:57 2011 Profile Name # of Clients Memory Usage Enabled Most Recent Traps CPU Usage 0% Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Rogue AP : 00:22:351:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Radios 0 0 Detail 802.11b/g/n 1 0 Detail 802.11b/g/n 1 0 Detail		mage	6.0.196	5.0		Rogues on Wired Ne	etwork		0	
op Time minutes prinutes profile Name # of Clients System Time Fri Apr 22 22:16:57 2011 Profile Name # of Clients Internal Temperature +42 C Profile Name # of Clients 802.11a Network Enabled Enabled Most Recent Traps 802.11b/g Network Enabled Rogue AP : b0:e7:54:2a:07:29 removed from Base Local Mobility Group 2106 Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad CPU Usage 0% Rogue AP : 00:23:51:6c:03:19 removed from Base Memory Usage 63% Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Nost Recent Traps 802.11b/g/n 1 0 Detail Radios 1 1 0 Detail All APs 1 0 Detail Current Clients 0 Detail Detail Excluded Clients 0 Detail Detail	System Nam	e	3750_1	1						
Internal Temperature +42 C 802.11a Network Enabled State Enabled S02.11b/g Network Enabled Local Mobility Group 2106 CPU Usage 0% Memory Usage 63% Access Point Summary Fotal View All Mage refreshes every 30 seconds. 802.11b/g/n 1 0 Radios 0 0 802.11b/g/n 1 0 All APs 1 1 Current Clients 0 Detail Excluded Clients 0 Detail Excluded Clients 0 Detail	Up Time				Top WLANs					
Internal Temperature +42 C 802.11a Network State Enabled 802.11b/g Network State Enabled Local Mobility Group 2106 CPU Usage 0% 63% Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:20:24:48:b5:d9 removed from Base Rogue AP : 00:20:24:48	System Time	9	Fri Apr	22 22:16:57	7 2011	Profile Name # of Clients				
State Enabled 802.11b/g Network Enabled Local Mobility Group 2106 CPU Usage 0% Memory Usage 63% Access Point Summary Fodu Total Up Down 802.11b/g/n 1 Radios 0 Rodius Lib/g/n 1 All APs 1 1 0 Detail Current Clients 0 Detail Excluded Clients 0 Detail Current Clients 0 Detail Excluded Clients 0 Detail Excluded Clients 0 Detail Most Recent Traps Rogue AP : b0:e7:54:2a:07:29 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:20:a4:88:b5:d9 removed from Base Rogue AP	Internal Tem	perature	+42 C							
802.11b/g Network State Enabled Local Mobility Group 2106 CPU Usage 0% Memory Usage 63% Access Point Summary Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Network 802.11a/n 0 0 802.11b/g/n 1 0 802.11b/g/n 1 0 All APs 1 1 Current Clients 0 Detail Excluded Clients 0 Detail		work	Enable	d		Most Recent Traps				
Local Mobility Group 2106 Rogue AP : b0:e7:54:2a:07:29 removed from Base CPU Usage 0% Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Memory Usage 63% Rogue AP : 00:23:51:6c:03:19 removed from Base Access Point Summary Image: Comparison of the pown Rogue AP : 00:22:a4:88:b5:d9 removed from Base 802.11a/n 0 Detail View All 802.11b/g/n 1 0 Detail 802.11b/g/n 1 0 Detail All APs 1 1 0 Client Summary Detail Excluded Clients 0 0 Detail Detail This page refreshes every 30 seconds.	802.11b/g N	etwork	Enable	d						
CPU Usage 0% Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad Memory Usage 63% Rogue AP : 00:23:51:6c:03:19 removed from Base Access Point Summary Total Up Down 802.11a/n 0 0 Detail 802.11b/g/n 1 0 Detail 802.11b/g/n 1 0 Detail All APs 1 0 Detail Client Summary Detail Detail Current Clients 0 Detail Excluded Clients 0 Detail		Group	2106			Rogue AP : b0:e7:54:2a:07:29 removed from Base F				
Memory Usage 63% Rogue AP : 00:23:51:6c:03:19 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Rogue AP : 00:22:a4:88:b5:d9 removed from Base Memory Usage Total Up Down S02.11a/n Radios 0 0 Detail 802.11b/g/n Radios 1 0 Detail All APs 1 0 Detail Client Summary Detail Detail Current Clients 0 Detail Excluded Clients 0 Detail	CPU Usage		0%			Rogue AP : 00:26:50:49:ac:d9 detected on Base Rad				
Access Point Summary Rogue AP : 00:22:a4:88:b5:d9 removed from Base Note of the second sec	Memory Usa	ge	63%			Rogue AP : 34:ef:	44:81:a0:59 de	tected on E	Base Radio	
Total Up Down 802.11a/n 0 0 0 Detail 802.11b/g/n 1 1 0 Detail 802.11b/g/n 1 1 0 Detail All APs 1 1 0 Detail Client Summary Detail Detail Excluded Clients 0 Detail						-				
Total Up Down 802.11a/n Radios 0 0 0 Detail 802.11b/g/n Radios 1 1 0 Detail All APs 1 1 0 Detail Client Summary Current Clients 0 Detail Excluded Clients 0 Detail	Access Poi	nt Sumi	mary			_	:a4:88:b5:d9 re	emoved fro	om Base Ra	
802.11a/n Radios 0 0 Detail 802.11b/g/n Radios 1 1 0 Detail All APs 1 1 0 Detail		in our	, and the second s			View All				
Radios 0 0 Detail 802.11b/g/n 1 1 0 All APs 1 1 0 Detail Client Summary Current Clients 0 Detail Excluded Clients 0 Detail		Total	Up	Down						
Radios 1 1 0 Detail All APs 1 1 0 Detail Client Summary Current Clients 0 Detail Excluded Clients 0 Detail		0	• 0	• •	Detail	This page refreshes	every 30 second	is.		
All APs 1 • 1 • 0 Detail Client Summary Current Clients 0 Detail Excluded Clients 0 Detail		1	• 1	• 0	Detail					
Current Clients 0 Detail Excluded Clients 0 Detail		1	• 1	• 0	Detail					
Excluded Clients 0 Detail	Client Sum	mary								
	Current Clier	nts 0			<u>Detail</u>					
Disabled Clients 0 Detail	Excluded Clie	ents 0			<u>Detail</u>					
	Disabled Clie	ents O			<u>Detail</u>					
									1 00	

					Sa <u>v</u> e Co	nfiguration <u>P</u> i	ng Lo <u>a</u> c	out <u>R</u> efresh	
<u>W</u> LANS <u>C</u> ON	NTROLLI	ER W <u>I</u> RE	ELESS	<u>S</u> ECURIT	Y M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
Summary								•	
10000000000000000	0000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	300000000000000000000000000000000000000	000000000000000000000000000000000000000	50 Access Point	s Supporte	ed	
	000000000000			000000000000000000000000000000000000000			000000000000000000000000000000000000000		
								-	
Controller Su		У			Rogue Summary	,			
Management IP Address		10.10.1.4			Active Rogue APs			31	
Service Port IP Address		2.2.2.2			Active Rogue Client	s		3	
Software Versio		7.0.98.218	3		Adhoc Rogues			0	
Emergency Ima Version	age	6.0.196.0			Rogues on Wired Ne	etwork		0	
System Name		3750_1							
Up Time		0 days, 21 hours, 46 minutes			Top WLANs				
System Time		Fri Apr 22	22:16:5	57 2011	Profile Name # of Clients				
Internal Tempe		+42 C							
802.11a Networ State		Enabled			Most Recent Traps				
802.11b/g Netw State	vork	Enabled							
Local Mobility G	Group	2106			Rogue AP : b0:e7:54:2a:07:29 removed from Base R Rogue AP : 00:26:50:49:ac:d9 detected on Base Radio				
CPU Usage		0%			Rogue AP : 34:ef:44:81:a0:59 detected on Base Radio				
Memory Usage		63%			Rogue AP : 00:23				
					Rogue AP : 00:22:a4:88:b5:d9 removed from Base R				
Access Point	Summ	nary			View All				
Тс	otal	Up	Down	1					
802.11a/n Radios 0		0	0	Detail	This page refreshes	every 30 second	ls.		
802.11b/g/n 1 Radios 1		1 (0	Detail					
All APs 1		1	0	Detail					
Client Course									
Client Summ	ary								
Current Clients	0			<u>Detail</u>				_	
Excluded Client				Detail					
Disabled Client	s O			<u>Detail</u>					
								10	

		50 140		650UD1			ng Logout <u>R</u> efre		
		LER W	IRELESS	<u>S</u> ECURIT	Y M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBAC		
Summary									
						50 Access Point	s Supported		
	999999999999999999			088888888888888888888888888888888888888					
30000300000	1000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	(1917)			n la		
				4-2-					
Controller	Summa	ry			Rogue Summary	,			
Managemen Address	t IP	10.10.1	.4		Active Rogue APs		31		
Service Port Address	t IP	2.2.2.2			Active Rogue Client	ts	3		
Software Ve	ersion	7.0.98.	218		Adhoc Rogues		0		
Emergency Version	Image	6.0.196	.0		Rogues on Wired N	etwork	0		
System Nan	ne	3750_1							
Up Time		0 days, minutes	21 hours,	46	Top WLANs				
System Tim	e	Fri Apr	22 22:16:5	7 2011	Profile Name		# of Clients		
Internal Ten	nperature	+42 C							
802.11a Net State	twork	Enabled	ł		Most Recent Traps				
802.11b/g N State	letwork	Enabled	ł		-				
Local Mobilit	ty Group	2106					emoved from Base R		
CPU Usage		0%					tected on Base Radi		
Memory Usa	age	63%					tected on Base Radio		
					-		emoved from Base R emoved from Base R		
Access Po	int Sum	mary			View All		emoved from base k		
	Total	Up	Down		VICKIM				
802.11a/n Radios	0	• o	• 0	Detail	This page refreshes	every 30 second	ds.		
802.11b/g/n Radios	1	• 1	• 0	Detail					
All APs	1	• 1	• 0	Detail					
Client Sum	nmary								
Current Clie	ents O			Detail					
Excluded Cli	ients 0			Detail					
Disabled Cli	ents 0			Detail			-		
							lin 10		

Cisco

Using the GUI

AP Name	AP Model	AP MAC	AP Up Time
AP8843.e103.bda2	AIR-LAP1242G-A-K9	88:43:e1:03:bd:a2	0 d, 22 h 25 m 45 s

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)

Time Statistics

UP Time

Controller Associated Time Controller Association Latency

0 d, 22 h 26 m 49 s 0 d, 14 h 51 m 20 s 0 d, 00 h 04 m 12 s

Using the GUI

Management **SNMP** Config Logs **Tech Support**

					Sa <u>v</u> e Co	nfiguration <u>P</u> ii	ng Log	out <u>R</u> efresh
	TOR <u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	Sumn	nary						
Summary	SNMP	Protocols	v1:I	Disabled v2c:	Enabled v3:Enable	ed		
SNMP	Syslog	I	Ena	bled				
General SNMP V3 Users	HTTP N	Mode	Disa	abled				
Communities	HTTPS	Mode	Ena	bled				
Trap Receivers Trap Controls	New Te	elnet Sessions Allo	wed No					
Trap Logs	New S	SH Sessions Allow	ed Yes					
HTTP-HTTPS	Manag	ement via Wireles	s Disa	abled				
Telnet-SSH								
Serial Port								
Local Manageme Users	nt							
User Sessions								
 Logs Config Message logs 								
Mgmt Via Wirele	55							
 Tech Support System Resource Information Controller Crash Core Dump AP Crash Log 								



- 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**



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>



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

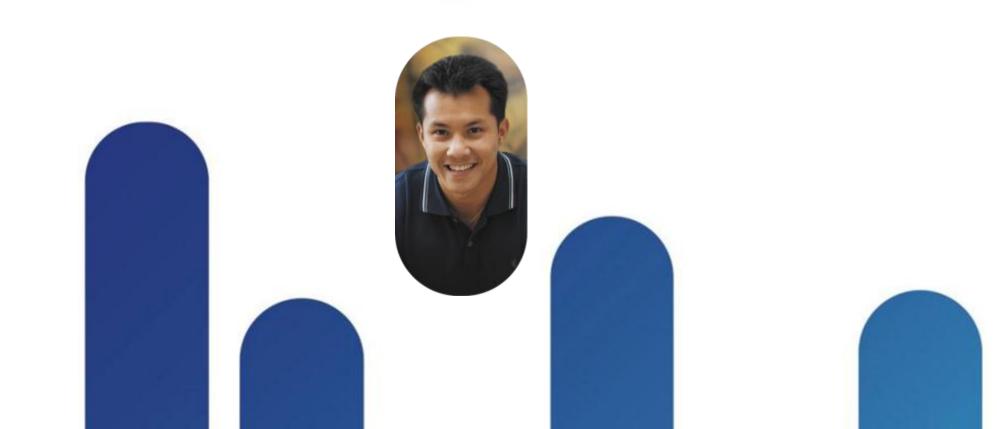
Debug capwap client no-reload

AP#show cap	client
callinfo	Lwapp
config	CAPWA
detailrcb	Lwapp
ha	CAPWi
mn	CAPWi
rcb	CAPWI
timers	CAPWI
traffic	CAPWi

L.	£	
p (client (Call Info
AP	Client	NV Config File
p (client r	cb Info
AP	Client	HA parameters
AP	Client	80211 MN
AP	Client	RCB
AP	Client	Timers
ÅP	Client	80211 Traffic



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

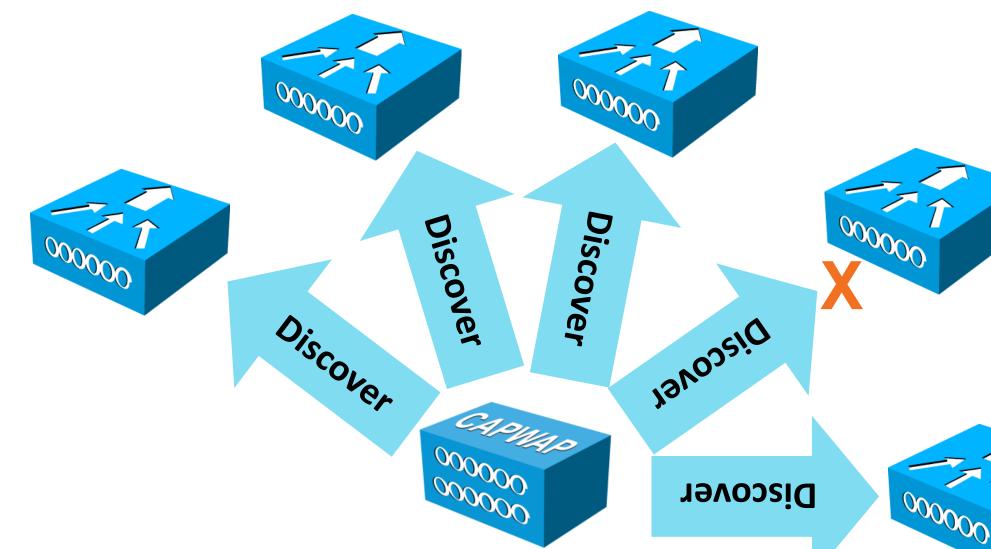
- Discovery broadcast on local subnet
- Locally-stored controller IP addresses 2.
- DHCP vendor specific option 43 3.
- DNS resolution of: 4.
 - "CISCO-CAPWAP-CONTROLLER.localdomain"
 - "CISCO-LWAPP-CONTROLLER.localdomain"
- If no controller found, start over 5.

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

BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved.

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

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

This Last Step Provides the Whole System with Automatic AP/WLC Load-Balancing Note: **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







Cisco Public

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 errors detail info packet payload hexdump

Configures	debug	of	CAPWAP	ever
Configures	debug	of	CAPWAP	erro
Configures	debug	of	CAPWAP	deta
Configures	debug	of	CAPWAP	info
Configures	debug	of	CAPWAP	pacl
Configures	debug	of	CAPWAP	pay.
Configures	debug	of	CAPWAP	pay!

nts and state ors ail o ket loads loads



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 05:02:18.949: DTLS connection not found, creating new connection for 192:168:100:103 (41824) 192:168:100:4 (5246)
- *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 07:44:55.779: DTLS connection not found, creating new connection for 192:168:100:104 (41825) 192:168:100:4 (5246)

*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

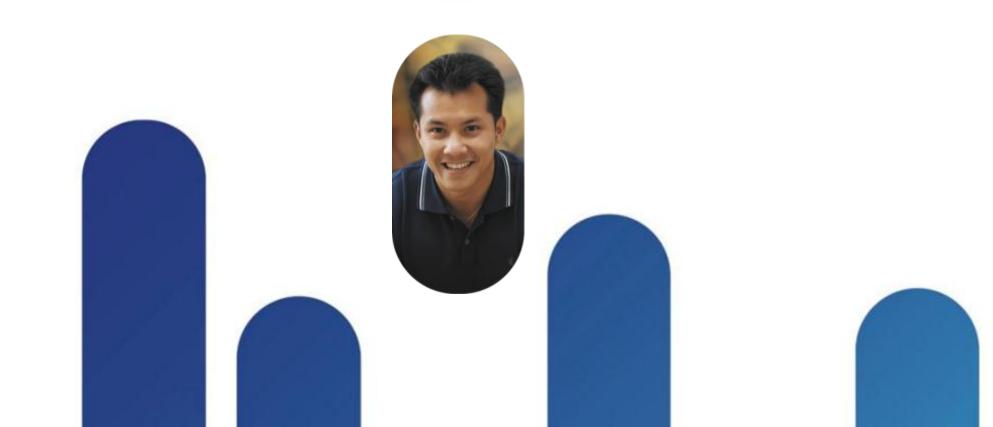
*Jan 09 07:44:56.713: 00:17:df:a8:bf:00 Join Request from 192.168.100.104:41825 *Jan 09 07:44:56.714: 00:17:df:a8:bf:00 In AAA state 'Idle' for AP 00:17:df:a8:bf:00 *Jan 09 07:44:56.714: 00:17:df:a8:bf:00 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.100.104:41825

*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

File Edit View Favorite				
🌏 Back 🝷 🕥 👻 💌	🔁 🏠 🔎 Search 🤺 Favorites	ं 🥝 🔗 - 🚵 🔳 - 🗖] 🖹 🋍 😫 🥾	
ddress 🙋 https://192.168	3.145.10/screens/frameset.html			•
				Sa <u>v</u> e Configuration <u>P</u> ing
CISCO	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER W <u>I</u> RELESS <u>s</u> ec	URITY M <u>A</u> NAGEMENT C <u>I</u>	<u>o</u> mmands he <u>l</u> p
Monitor	Clients > Detail			< Back Link Test
			-	
Summary Access Points	Client Properties		AP Properties	
 Statistics 	MAC Address	00:1c:10:e8:1a:f0	AP Address	00:21:1c:7a:40:50
► CDP	IP Address	192.168.145.103	AP Nome	LAP1240-2
Roques	Client Type	Regular		802.11g
Clients	User Name	Kegulai	WLAN Profile	open
Multicast	Oser Name Port Number	8	Status	Associated
			Association ID	2
	Interface	management -	802,11 Authenticatio	
	VLAN ID	0		on Shared Key
	CCX Version	Not Supported	Reason Code	-
	E2E Version	Not Supported	Status Code	13
	Mobility Role	Local	CF Pollable	Not Implemented
	Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
	Policy Manager State Management Frame	RUN	Short Preamble	Implemented
	Protection	No	PBCC	Not Implemented
	Security Information		Channel Agility	Not Implemented
	Security Policy Completed	Yes	Timeout	1800
	Policy Type	N/A	WEP State	WEP Disable
		None		
	EAP Type NAC State	N/A Access		

show client detail

© 2013 Cisco and/or its affiliates. All rights reserved.

	- 🗆	×
Go	Links	>>
-	<u>R</u> efres	ь
gout	<u>N</u> enies	
_		
Remo	ve	
		-
et		



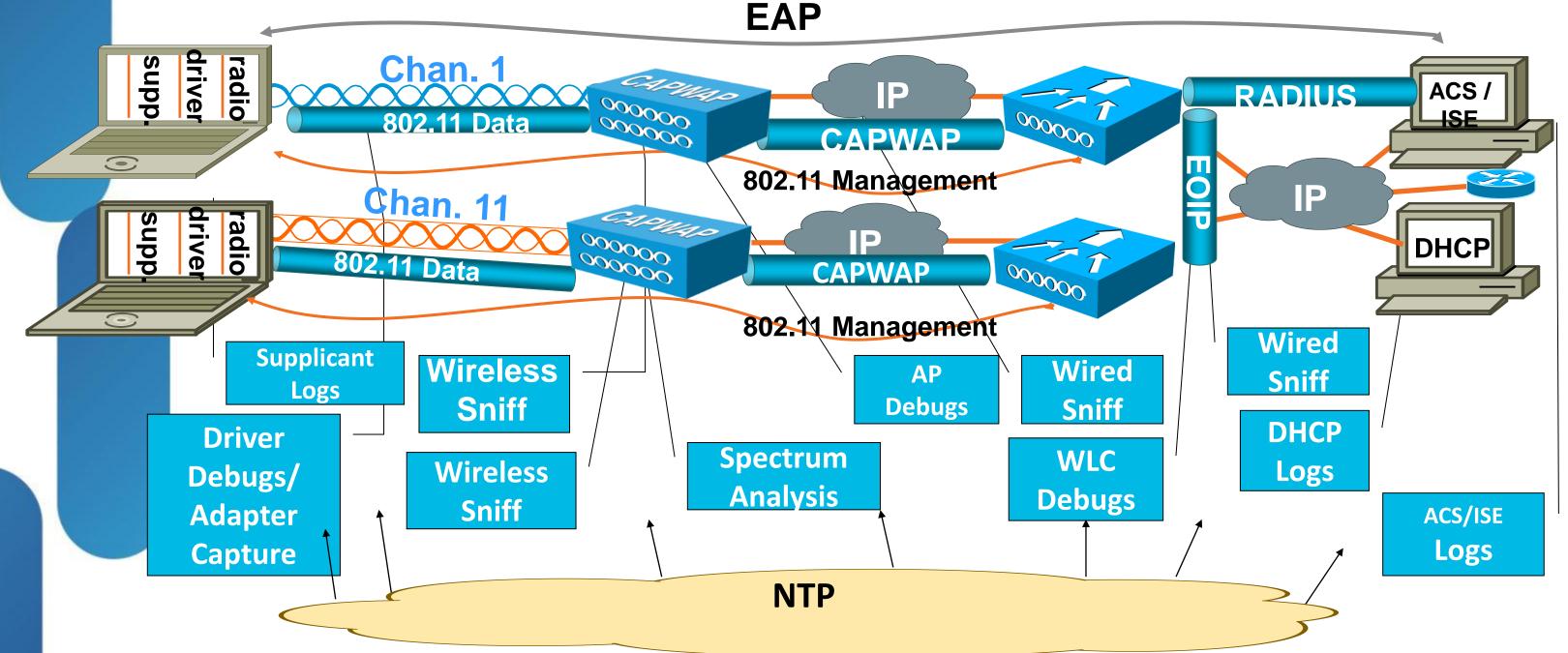


Client Connectivity

- Unified Wireless Network: Troubleshoot Client Issues Document ID: 107585
- Configuration Issues
 - -SSID/Security Mismatch
 - Disabled WLAN
 - Unsupported Data-Rates
 - Disabled Clients
 - -Radio Preambles
- Cisco Features Issues with Third Party Clients -Aironet IE, MFP

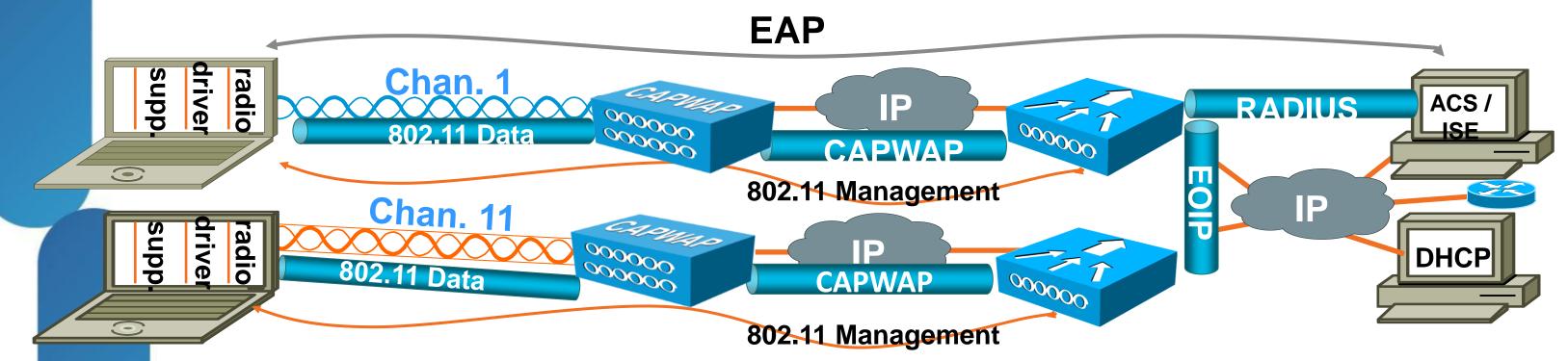


Complexity of a Wireless Network





Supplicant logs



-WZC supplicant log:

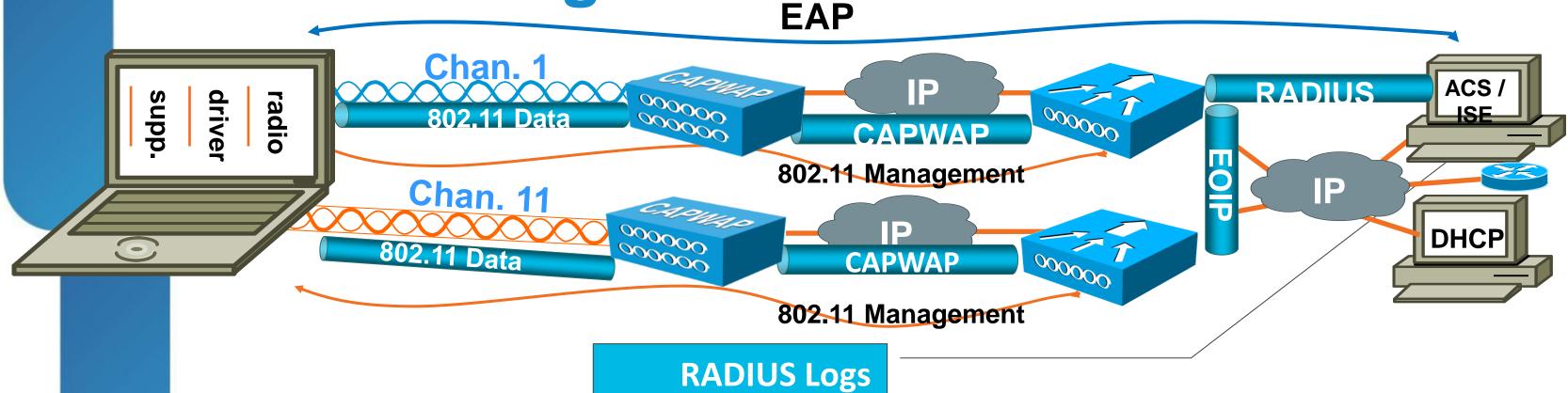
netsh ras set tracing * enabled — logs in c:\windows\tracing see http://www.microsoft.com/technet/network/wifi/wlansupp.mspx -PROSet supplicant log: under hklm\software\intel\wireless\settings 1xconfigdbg=wwxyz; 1xDebugLevel=dword:0x18;1xLogLevel=dword:0x18 logs in c:\ (subject to change without warning)

-ADU: see CSCsi16921

-CSSC/AnyConnect: see Log Packager utility on cisco.com



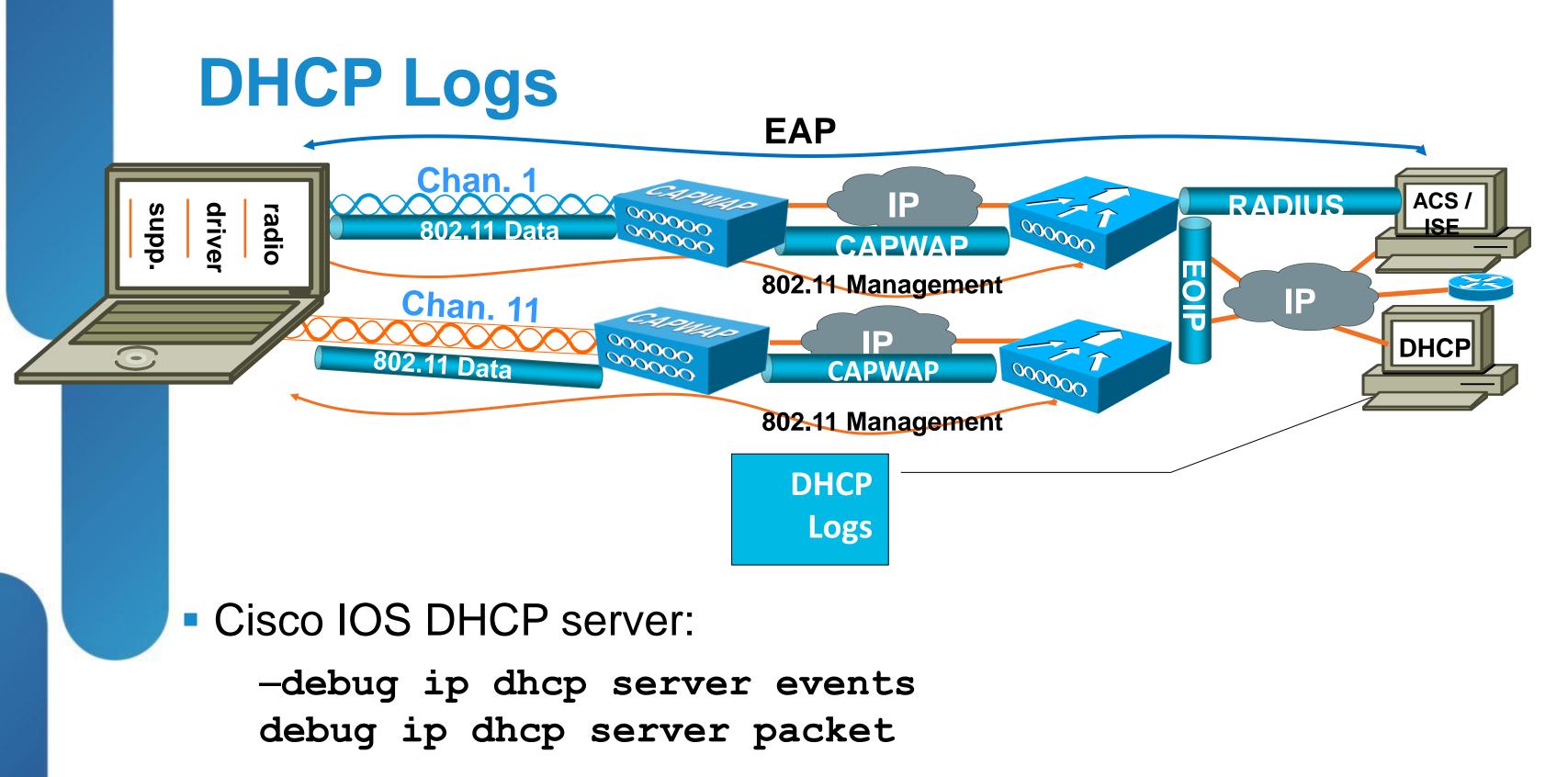
RADIUS Logs



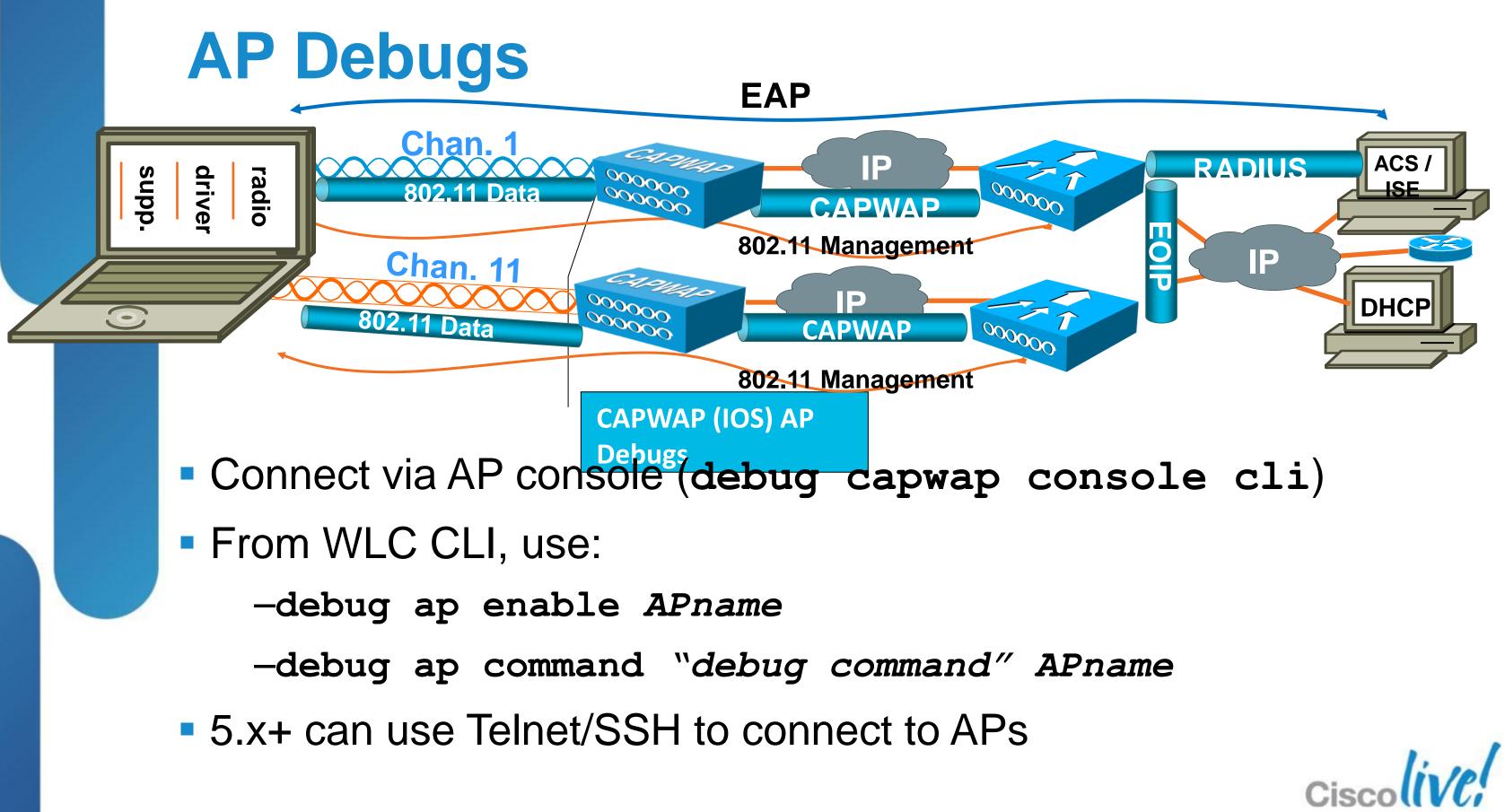
See Monitoring and Reporting section on ACS 5.x or ISE NTP sync your ACS/ISE!

© 2013 Cisco and/or its affiliates. All rights reserved.









AP Debugs

By default, radio debugs appear only on the console. To see radio debugs in your telnet/ssh/WLC CLI session, use the command

debug dot11 dot11radiox print printf where x is 0 or 1

Useful radio debugs: debug dot11 dot11radiox trace print {mgmt, keys, client, beacon, rcv, xmt} (beacon, rcv & xmt can be extremely verbose!)



Client Debug debug client <mac address>

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

(Cisco Controller) > show debug

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 ffiliates. All rights reserved



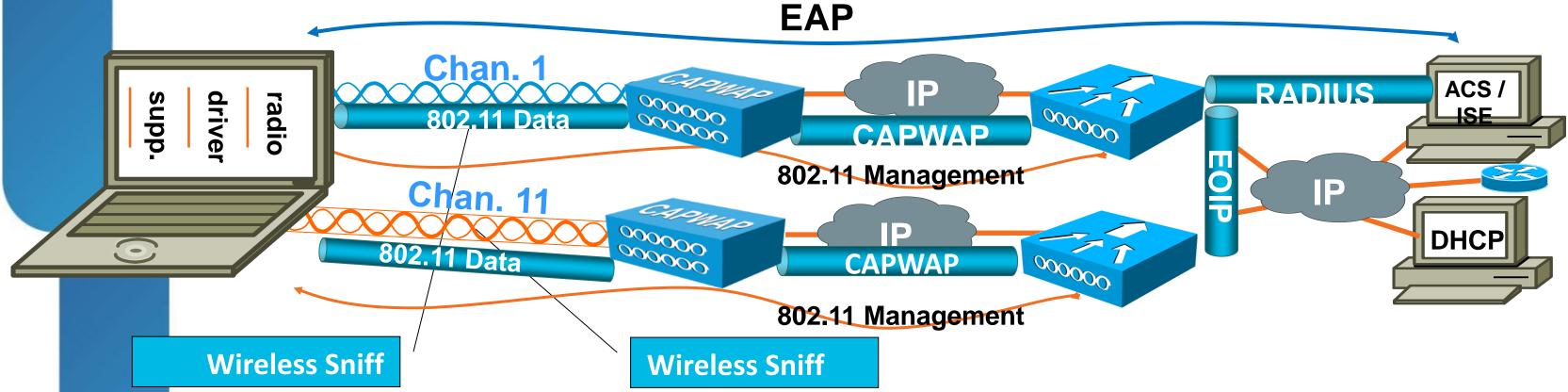
WLC Debugs

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



Wireless Sniff



- Good options (Windows PCs):
 - -Omnipeek from Wildpackets (Linksys WUSB600N, CB21AG,..) -Wireshark with CACE Technologies AirPcap adapters
 - USB adapters nice for multichannel sniff
 - -AirMagnet

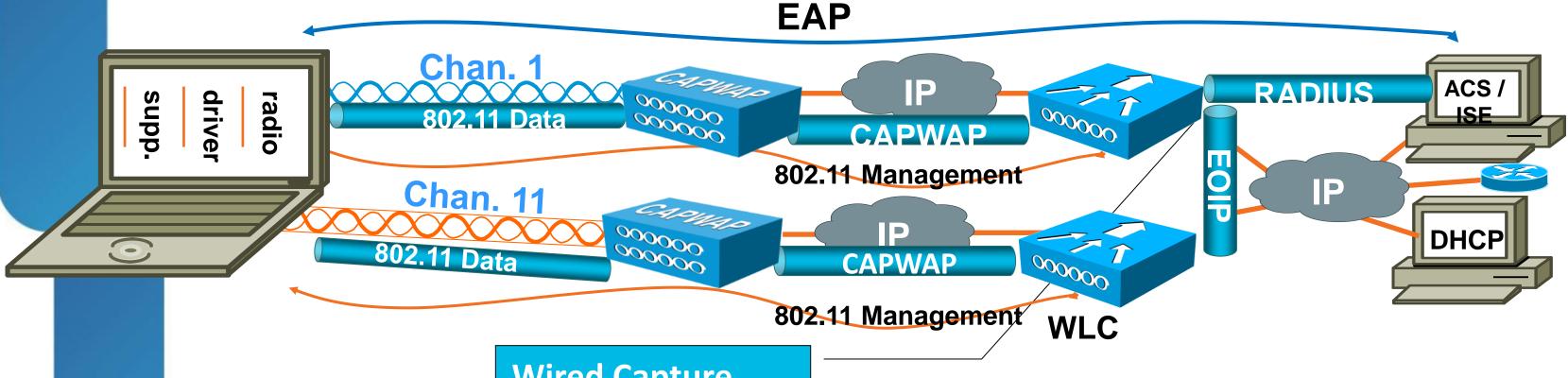


Wireless Sniff - Some Tips

- 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



- Wired Capture
- 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

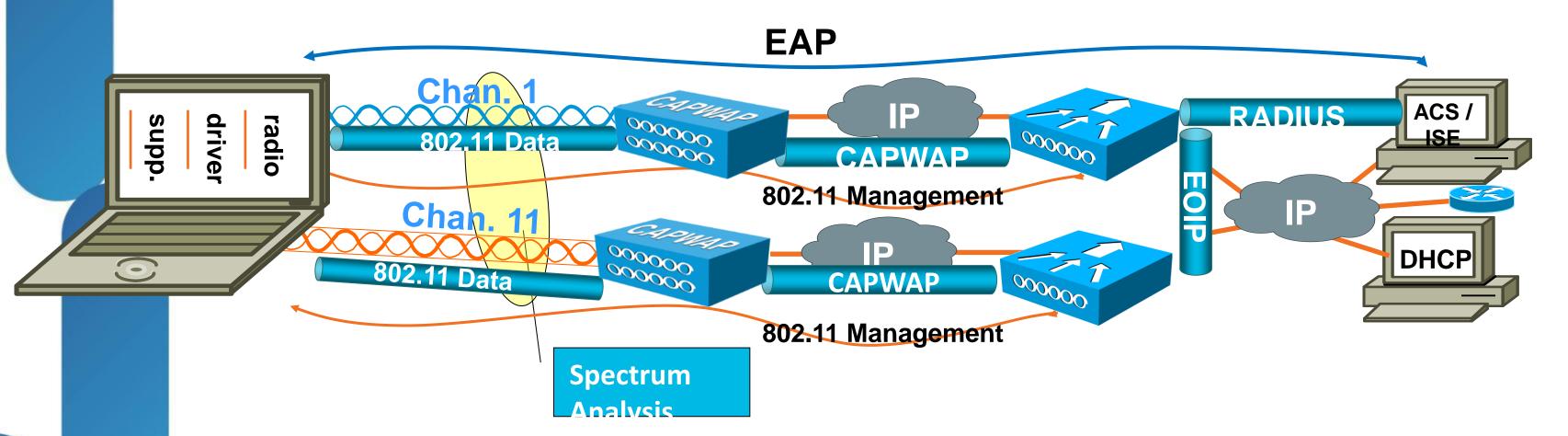
• NTP sync your sniffers!

BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved



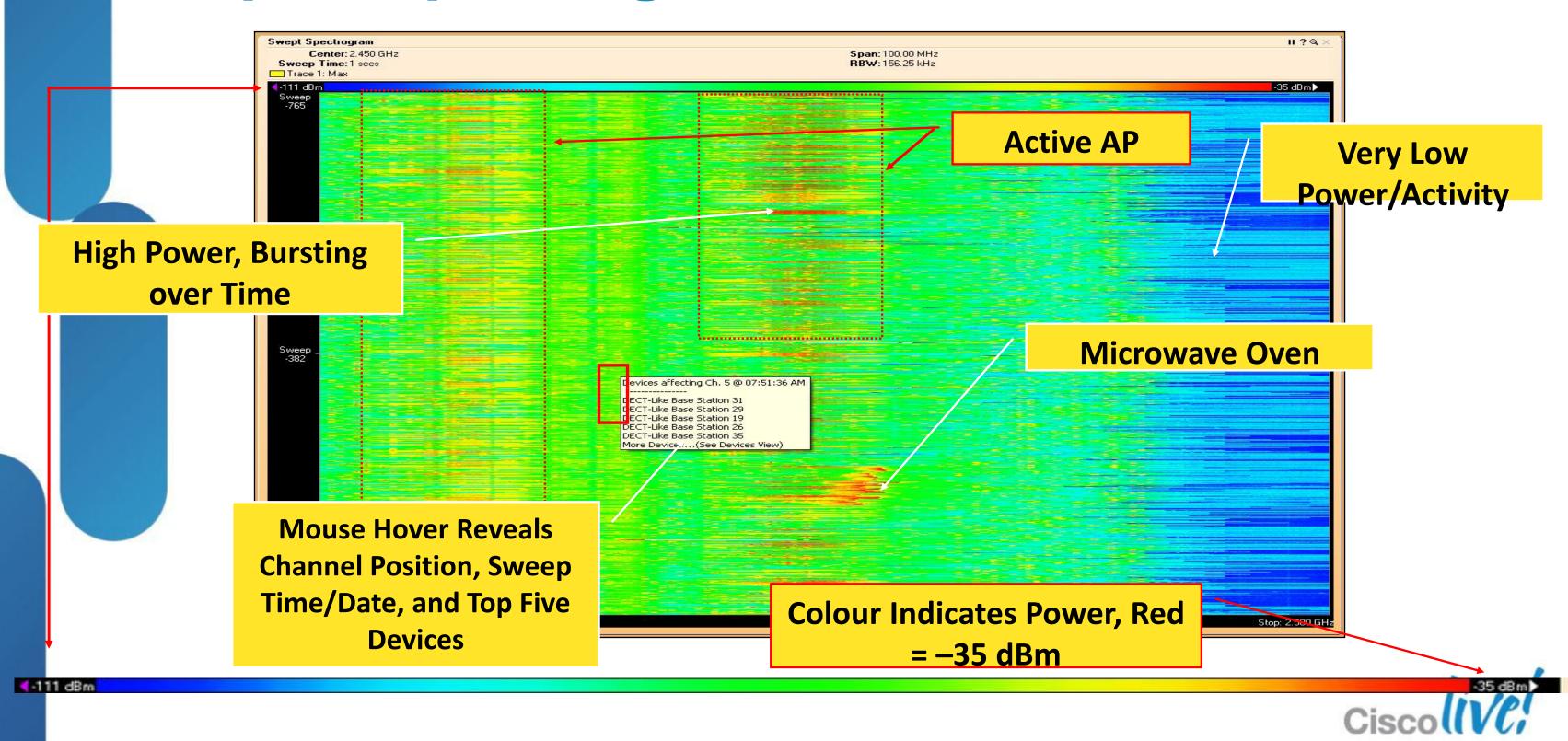
Spectrum Analysis



- 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

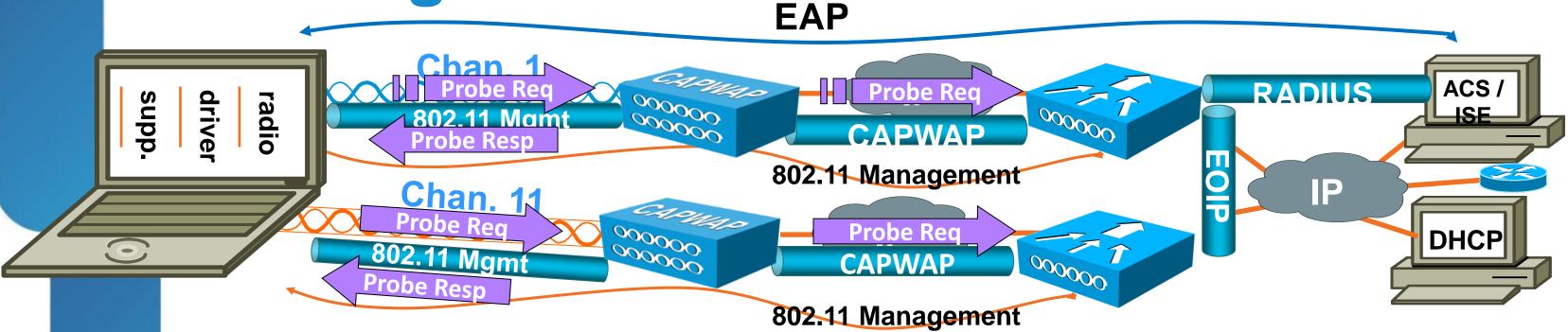


SpEx Tips

- 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



Probing



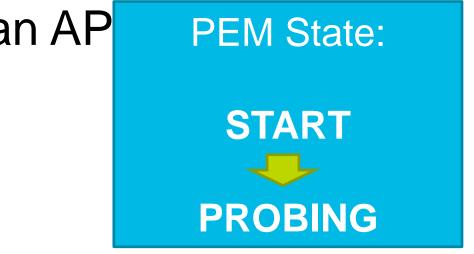
1. Client probes for the SSID

- 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

BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved.





Probing

	Source	Destination	Protocol	Info	Size	RSSI	Rate
:37.815670013	C15C0_92	Broadcast	IEEE 802	Probe Request, SN=138, FN=0, SSID: "	45	58	6.0
:37.816028594	Cisco_8e	Cisco_92	IEEE 802	Probe Response, SN=2629, FN=0, BI=100, SSID: """"",	209	52	6.0

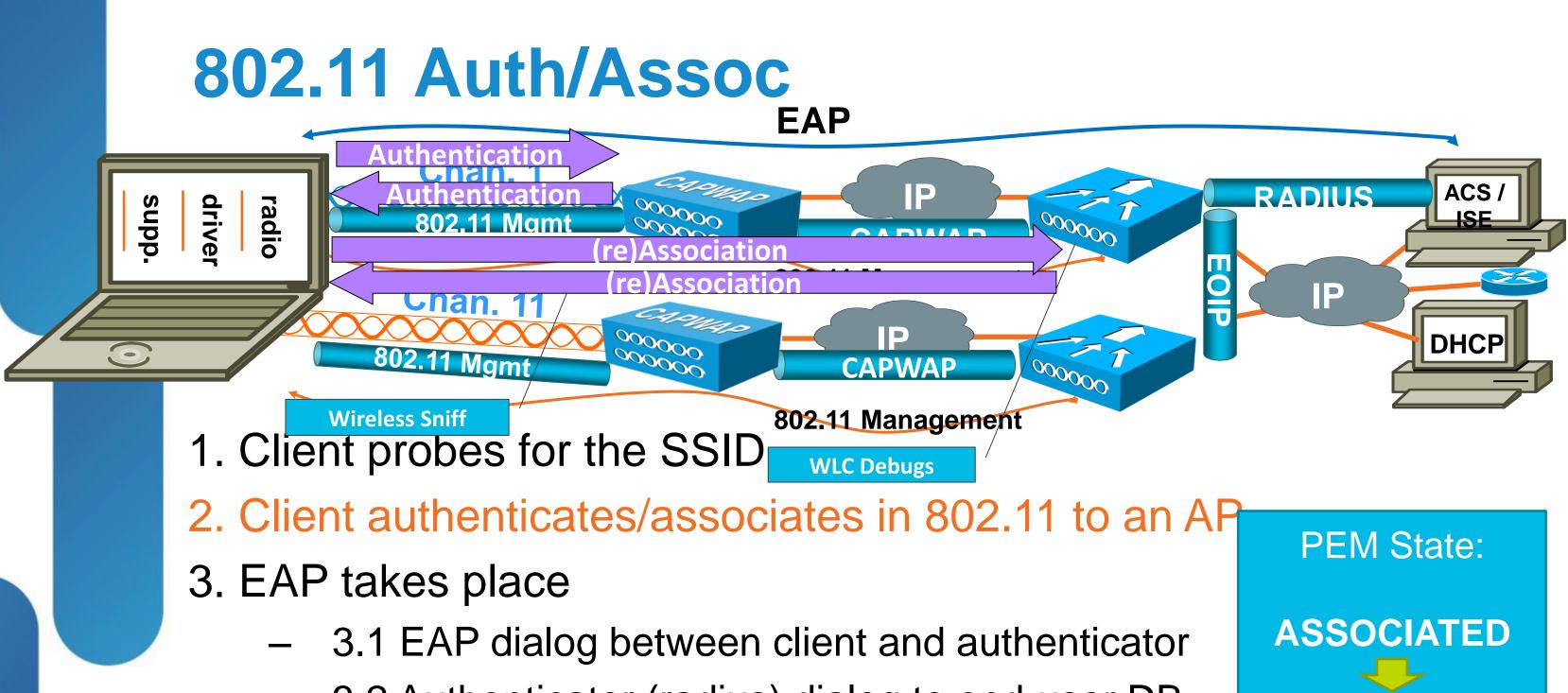
- Clients broadcasts a probe for the SSID of interest
- AP unicasts back a probe response
- Probe response includes interesting facts (information elements) about the service
 - Tagged parameters (169 bytes) ∃ SSID parameter set: " Supported Rates: 6.0(B) 9.0 12.0(B) 18.0 24.0(B) 36.0 48.0 54.0 Country Information: Country Code: US. Any Environment QBSS 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.





- 3.2 Authenticator (radius) dialog to end-user DB
- 4. DHCP address negotiation
- 5. Client reaches RUN state

BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved.

8021X REQD

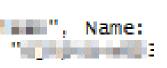


802.11 Auth/Assoc

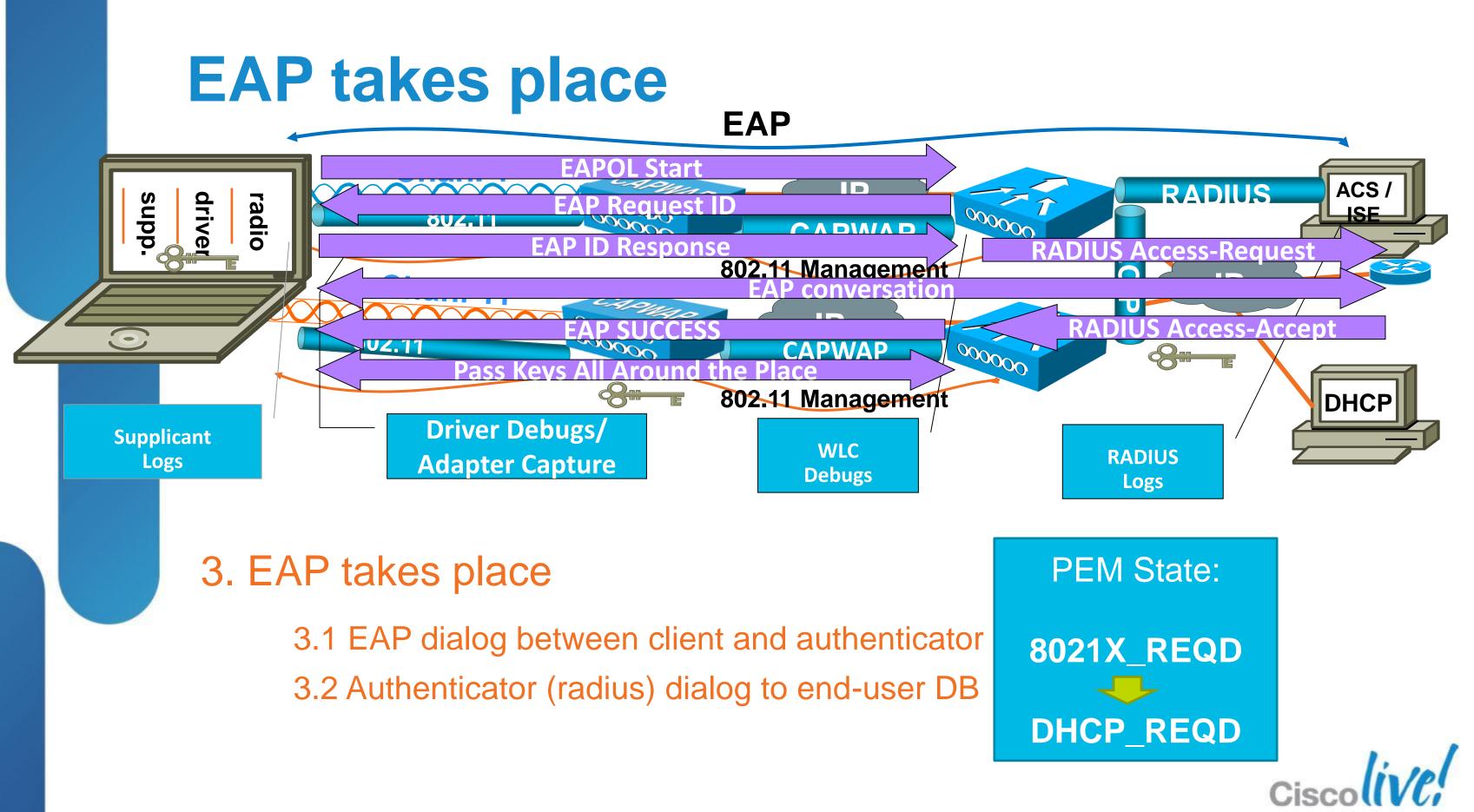
```
25 05:30:36 IntelCor_7; Cisco_83:5 IEEE 802 Authentication, SN=209, FN=0
26 05:30:36 IntelCor_7; Cisco_83:5 IEEE 802 Authentication, SN=209, FN=0
27 05:30:36 IntelCor_7; Cisco_83:5 IEEE 802 Association Request, SN=210, FN=0, SSID: " Mame:
28 05:30:36 Cisco_83:5 IntelCor_7 IEEE 802 Association Response, SN=3262, FN=0, Name: " _____ E
```

- 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





30	63	1.0
30	62	1.0
91	62	1.0
123	33	11.0



Wireshark Capture of MS-PEAP (WPA2)

# .	Time	Source	Destination	Protocol	Info	Size	RSS
	11:16:26.547979				Request, Identity [RFC3748]	71	
	11:16:26.945640				Response, Identity [RFC3748]	60	
	11:16:26.961292				Request, PEAP [Palekar]	24	
	11:16:27.574427				Client Hello	128	
5	11:16:27.579089	Cisco_36	IntelCor_3e:	EAP	Request, PEAP [Pa]ekar]	1030	
6	11:16:27.599226	IntelCor	Cisco_36:a2:	EAP	Response, PEAP [Palekar]	60	
7	11:16:27.603239	Cisco_36	IntelCor_3e:	TLSV1	Server Hello, Certificate, Server Hello Done	945	
8	11:16:27.773854	IntelCor	Cisco_36:a2:	TLSV1	Client Key Exchange, Change Cipher Spec, Encrypted Handsh	354	
9	11:16:27.805694	Cisco_36	IntelCor_3e:	TLSV1	Change Cipher Spec, Encrypted Handshake Message	87	
10	11:16:27.848802	IntelCor	Cisco_36:a2:	EAP	Response, PEAP [Palekar]	60	
11	11:16:27.852007	Cisco_36	IntelCor_3e:	TLSV1	Application Data	77	
12	11:16:27.951994	IntelCor	Cisco_36:a2:	TLSV1	Application Data, Application Data	114	
13	11:16:27.955152	Cisco_36	IntelCor_3e:	TLSV1	Application Data	93	
14	11:16:28.088598	IntelCor	Cisco_36:a2:	TLSV1	Application Data, Application Data	162	
15	11:16:28.110353	Cisco_36	IntelCor_3e:	TLSV1	Application Data	109	
16	11:16:28.151837	IntelCor	Cisco_36:a2:	TLSV1	Application Data, Application Data	98	
17	11:16:28.154869	Cisco_36	IntelCor_3e:	TLSV1	Application Data	61	
18	11:16:28.189439	IntelCor	Cisco_36:a2:	TLSV1	Application Data, Application Data	98	
19	11:16:28.194497	Cisco_36	IntelCor_3e:	EAP	Success	22	
20	11:16:28.194909	Cisco_36	IntelCor_3e:	EAPOL	Key	135	
21	11:16:28.294394	IntelCor	Cisco_36:a2:	EAPOL	Key	133	
22	11:16:28.297998	Cisco_36	IntelCor_3e:	EAPOL	Key	193	
23	11:16:28.312797	IntelCor	Cisco_36:a2:	EAPOL	Key	113	
-24	11:16:28.435178	0.0.0.0	255.255.255.	DHCP	DHCP Request - Transaction ID 0x56fe92f0	378	





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 ld 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

·· ·· ·· cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ON	TROLLER W <u>I</u> RELESS	<u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Monitor	Clients > Detail						
Summary Access Points 	Client Properties			~	P Properties		
Cisco CleanAir	MAC Address	00:0e:9b:47:3e:06			AP Address		00:22:90:92:af:70
Statistics	IP Address	0.0.0.0			AP Name		L1140
► CDP	Client Type	Regular			АР Туре		802.11b
▶ Rogues	User Name	bad_user			WLAN Profile		CL2012
Clients	Port Number	29			Status		Associated
Multicast	Interface	vlan69			Association ID		1
	VLAN ID	0			802.11 Authent	ication	Open System
	CCX Version	CCXv1			Reason Code		1
	E2E Version	Not Supported			Status Code		0
	Mobility Role	Local			CF Pollable		Not Implemented
	Mobility Peer IP Address	N/A			CF Poll Request	:	Not Implemented
	Policy Manager State	8021X_REQD			Short Preamble		Implemented
	Management rrame Protection	No			PBCC		Not Implemented
	UpTime (Sec)	160			Channel Agility		Not Implemented
	Power Save Mode	OFF			Timeout		1800
	Current TxRateSet	11.0			WEP State		WEP Enable
	Data RateSet	1.0,2.0,5.5,11.0	11				
	Security Information						
	Security Policy Completed	No					
	Policy Type	802.1×					
	Encryption Cipher	CCMP (AES)					
	ЕАР Туре	РЕАР					

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





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 received = 2

[TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 59) 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=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 12 mobile 00:13:ce:57:2b:84 received = 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]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * sendRadiusMessage:2494 Successful transmission of Authentication Packet (id 66) to 10.48.76.71:1812, proxy state 00:13:ce:57:2b:84-ce:57 [TIME]: * radiusProcessQueue:2735 Max retransmission of Access-Request (id 66) to 10.48.76.71 reached for mobile 00:13:ce:57:2b:84 [TIME]: * sendAAAError:323 Returning AAA Error 'Timeout' (-5) for mobile 00:13:ce:57:2b:84

AAA connectivity failure will generate an SNMP trap

218	Thu Jan 5 13:47:33 2012	RADIUS server 10.48.76.71:1812 deactivated in global list
219	Thu Jan 5 13:47:33 2012	RADIUS server 10.48.76.71:1812 failed to respond to request (ID 14) fo

In the WLC GUI, Go to: Management | SNMP → Trap Logs



or client 00:00:00:3d:00:00 / user 'unknown'





Verify Complete 802.11/ **802.1X Connectivity**

debug 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	10.48.76.71	
Shared Secret Format	ASCII 🗸	
Shared Secret	***	Make Sure t
Confirm Shared Secret	***	Shared Secr
Кеу Wrap	(Designed for FIPS custo	
Port Number	1812	Select the Correct
Server Status	Enabled 🖵 🖛	(Common Ports Are
Support for RFC 3576	Enabled 🖵	Status Must
Server Timeout	2 seconds 🖛	Be Enabled
Network User	🖾 Enable 🛛 🖛 🛶 🛶 🛶	
Management	🜌 Enable	
IPSec	🔲 Enable	Network User Auth Ha Server to Be Used Glo

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

BRKEWN-3011

the Correct ret Is Input

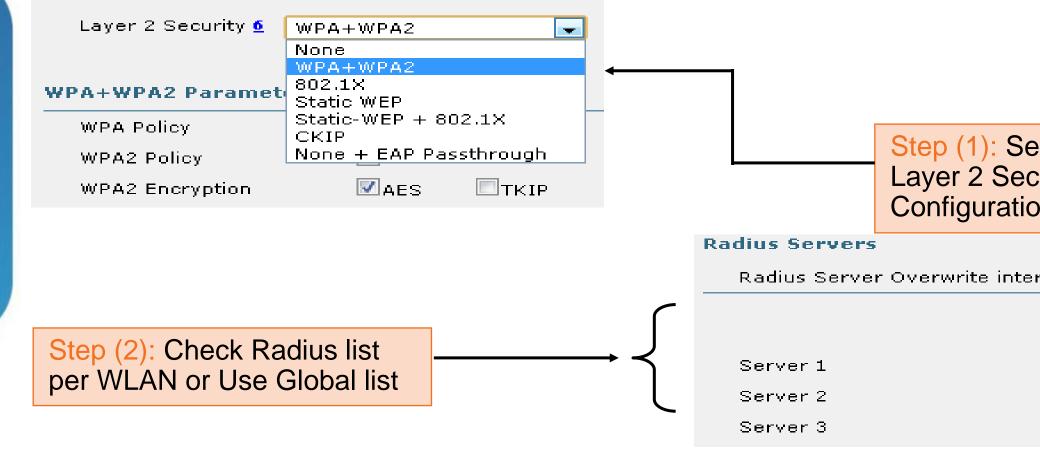
RADIUS Port e 1812 and 1645)

> **Timeout May** Be too Short

as to Be Enabled for This AAA obally, Otherwise, Select on WLAN

Troubleshooting 802.1X

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



In the WLC GUI, Go to: WLANs | WLANs | WLANs and Then Select Edit for the WLAN of Interest

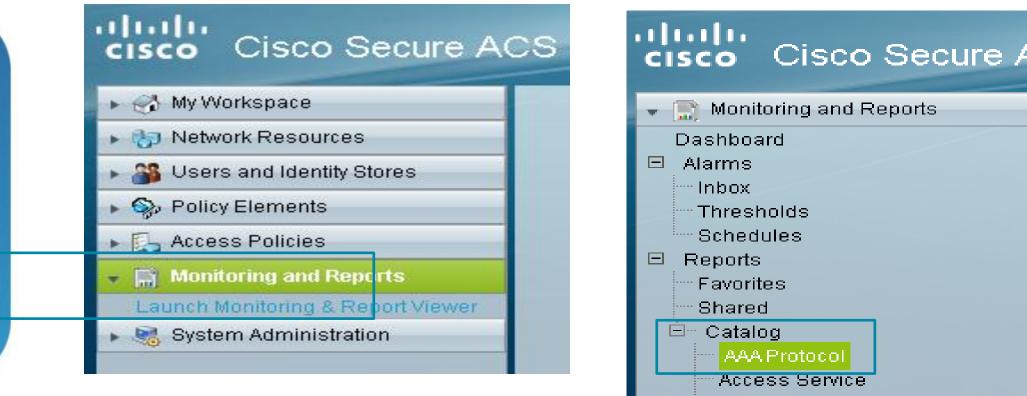
BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved.

elect t curity on	he Desired	
rface	Enabled	
	Authenticatio	n Servers 1, Port:1812 -

Troubleshooting 802.1X – ACS 5.x

Enabled Logging in your ACS 5.x server to identify where issues might lie with backend authentication



ACS Instance

Failure Reason

Endpoint



4	ACS View						
	Monitoring & Reports > Reports > Catalog > AAA						
		Report	ts				
		Filter:	Go				
			Report Name				
		\bigcirc	AAA Diagnostics				
		\bigcirc	Authentication Trend				
		\bigcirc	RADIUS Accounting				
		\odot	RADIUS Authentication				
		\bigcirc	TACACS Accounting				
		\bigcirc	TACACS Authentication				
		\bigcirc	TACACS Authorization				



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?



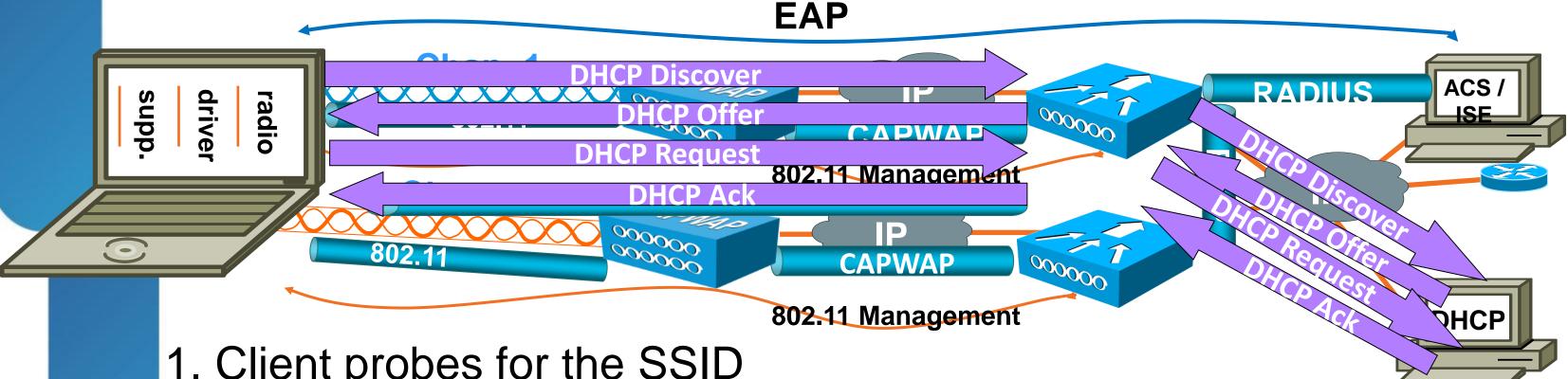
802.1X – Common issues

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? \rightarrow 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 BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved

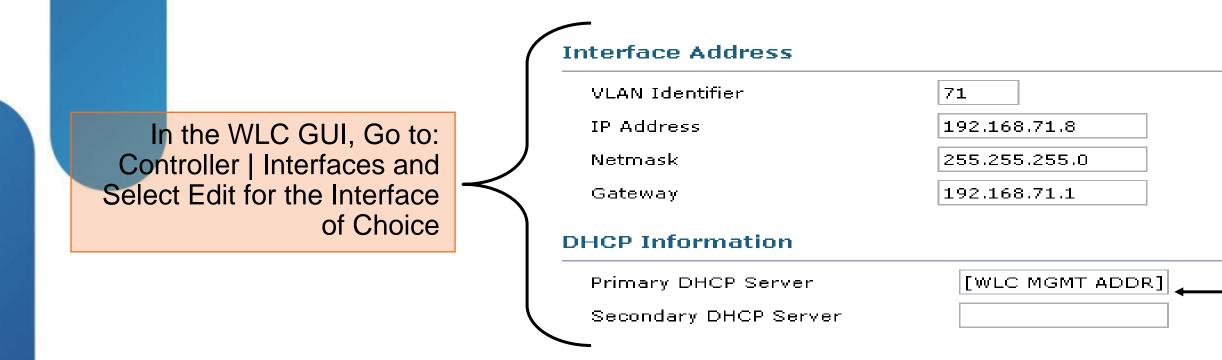
PEM State: DHCP REQD RUN



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:



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

Client IP Provisioning via DHCP

debug 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





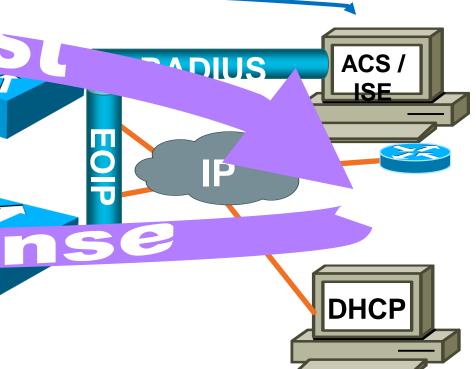
PING Succeeds!! EAP 000000 driver radio 000000 qqu 200000 802.11 Management Chan. 11 $\mathbf{\Theta}$ 802.11 Management

- 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

BRKEWN-3011

© 2013 Cisco and/or its affiliates. All rights reserved.



PEM State:

RUN

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
 - -<u>http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g/7_0</u> /english/deployment/guide/7925dply.pdf
- 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

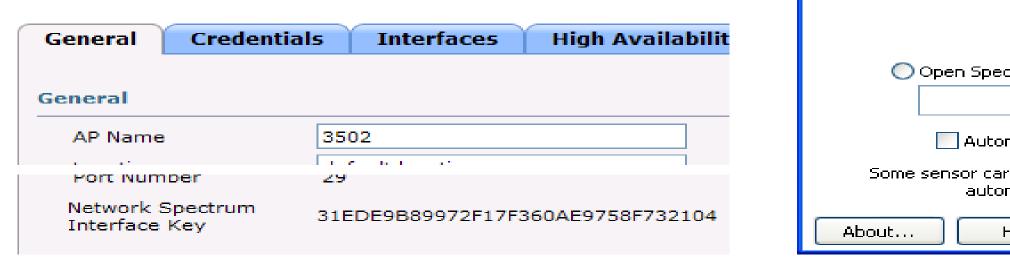
- Clean Air APs can be used in lieu of Spectrum Card for **Spectrum Analysis**
 - AP can be placed in SE-Connect mode for full functionality
 - AP in local mode can be used now for Spectrum Analysis of current channel



Spectrum Expert with Clean Air

- Obtain Spectrum Key
- Connect to Remote Sensor





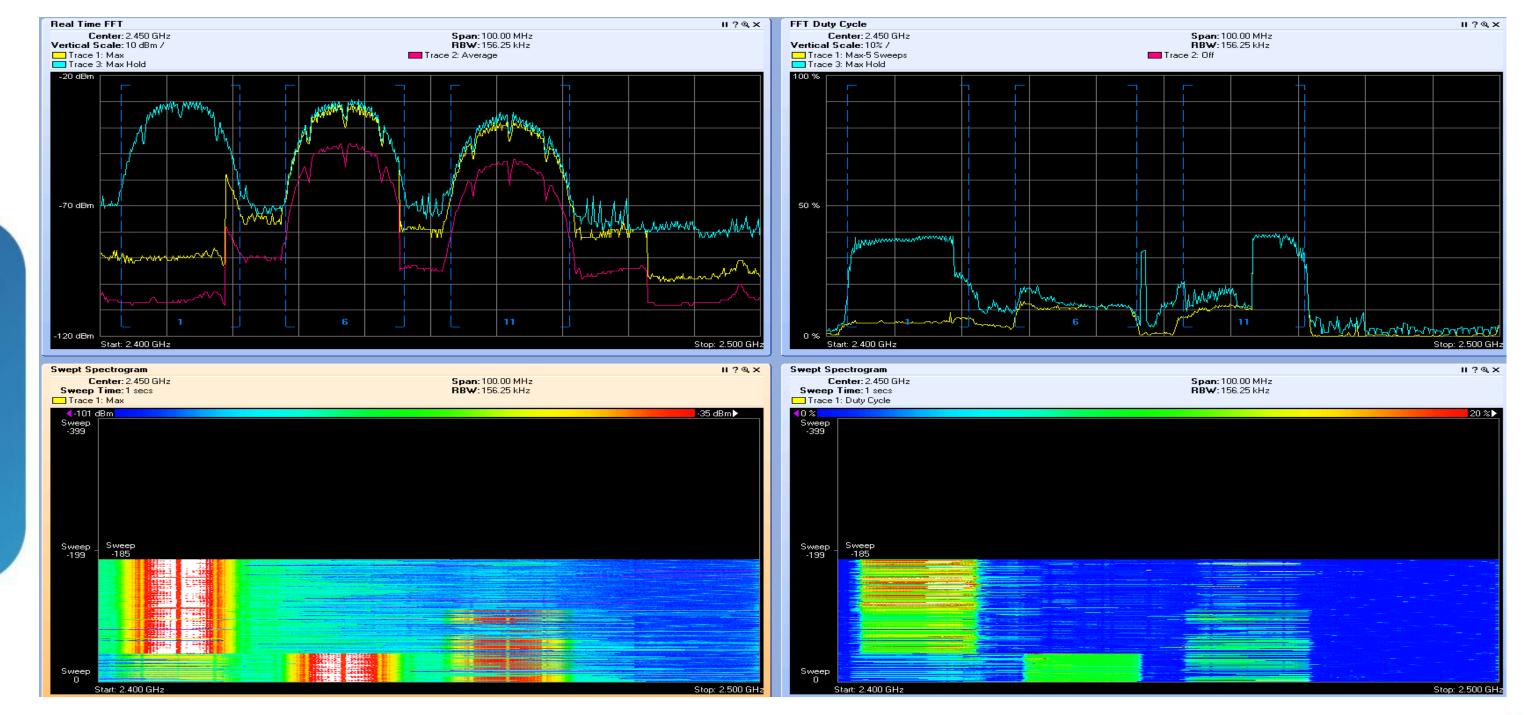


Connect to Sensor

t to Sensor				
C	SCO			
O Sensor Card with Int	ernal Antenna			
O Sensor Card with Ex	ternal Antenna			
Remote Sensor:				
IP Address	10 . 10 . 2 . 57			
Radio	⊙b/g/n ⊖a/n			
Кеу	31EDE9B89972F17F360AE [,]			
Open Spectrum Cap	ture File:			
	Browse			
Automatically use this sensor next time				
me sensor cards may select external vs. internal antenna automatically in lieu of above setting.				
t Help	OK Cancel			



Spectrum Expert with Clean Air







Summary

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



Q & A









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
- 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





communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button. www.ciscoliveaustralia.com/portal/login.ww



Don't forget to activate your Cisco Live 365 account for access to all session material,



CISCO

