Troubleshooting 802.11 Wireless LANs with Centralized Controllers

Tom Koenig
Wireless Product Manager
APAC
tk@cisco.com

Troubleshooting 802.11 Wireless LANs Agenda

- **Review: Cisco’s Unified Architecture**
- **Debugging and Troubleshooting**
    - **Wireless LAN Controllers (WLCs)**
    - **Access Points**
- **Tools you should know about…**

Review: Cisco’s Unified Architecture

Review: Cisco's Unified Architecture Agenda

- **Cisco Centralized WLAN Model**

- **Split MAC and Local MAC**

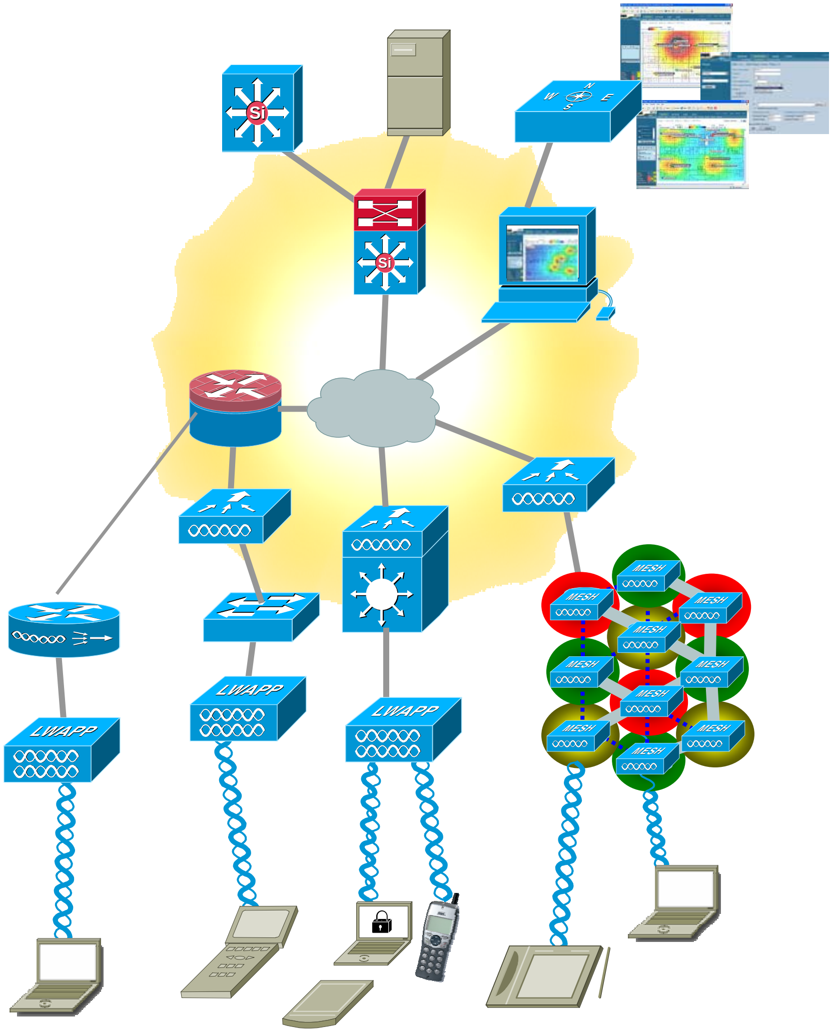
- **LWAPP Architecture**
    - **Layer-2**
    - **Layer-3**

But first…

Marketing slides!!!

Cisco Unified Wireless Network

End-to-End, Unified – Only Cisco



Unified Advanced Services

Unified cellular and Wi-Fi VoIP. Advanced threat detection, identity networking, location-based security, asset tracking and guest access.

World-Class Network Management

Same level of security, scalability, reliability, ease of deployment, and management for wireless LANs as wired LANs.

Network Unification

Integration into all major switching and routing platforms. Secure innovative WLAN controllers.

Mobility Platform

Ubiquitous network access in all environments. Enhanced productivity. Proven platform with large install base and 63% market share. Plug and Play.

Client Devices

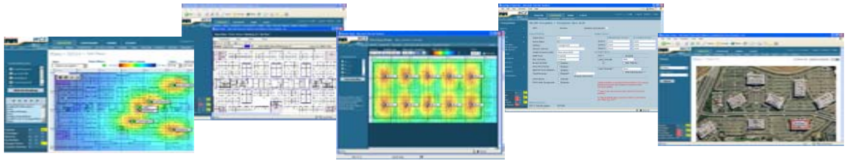
90% of Wi-Fi silicon is Cisco Compatible Certified. “Out-of-the-Box” wireless security.

Cisco Unified Wireless Network
Product Portfolio

Cisco Self-Defending Network

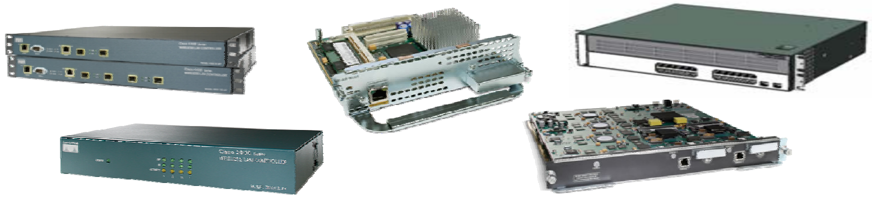
Unified Advanced Services

Unified built-in support of leading edge applications - not an after thought. Cisco Wireless Location Appliance, Cisco WCS, SDN, NAC, Wi-Fi phones, and RF firewalls.



World-Class Network Management

World Class NMS that visualizes and helps secure your air space. Cisco Wireless Control System (WCS)



Network Unification

4400- and 2000-Series WLAN Controllers, Catalyst 6500 Series WiSM, Network Module for Integrated Services Routers, and new Catalyst 3750G Integrated WLC

Mobility Platform

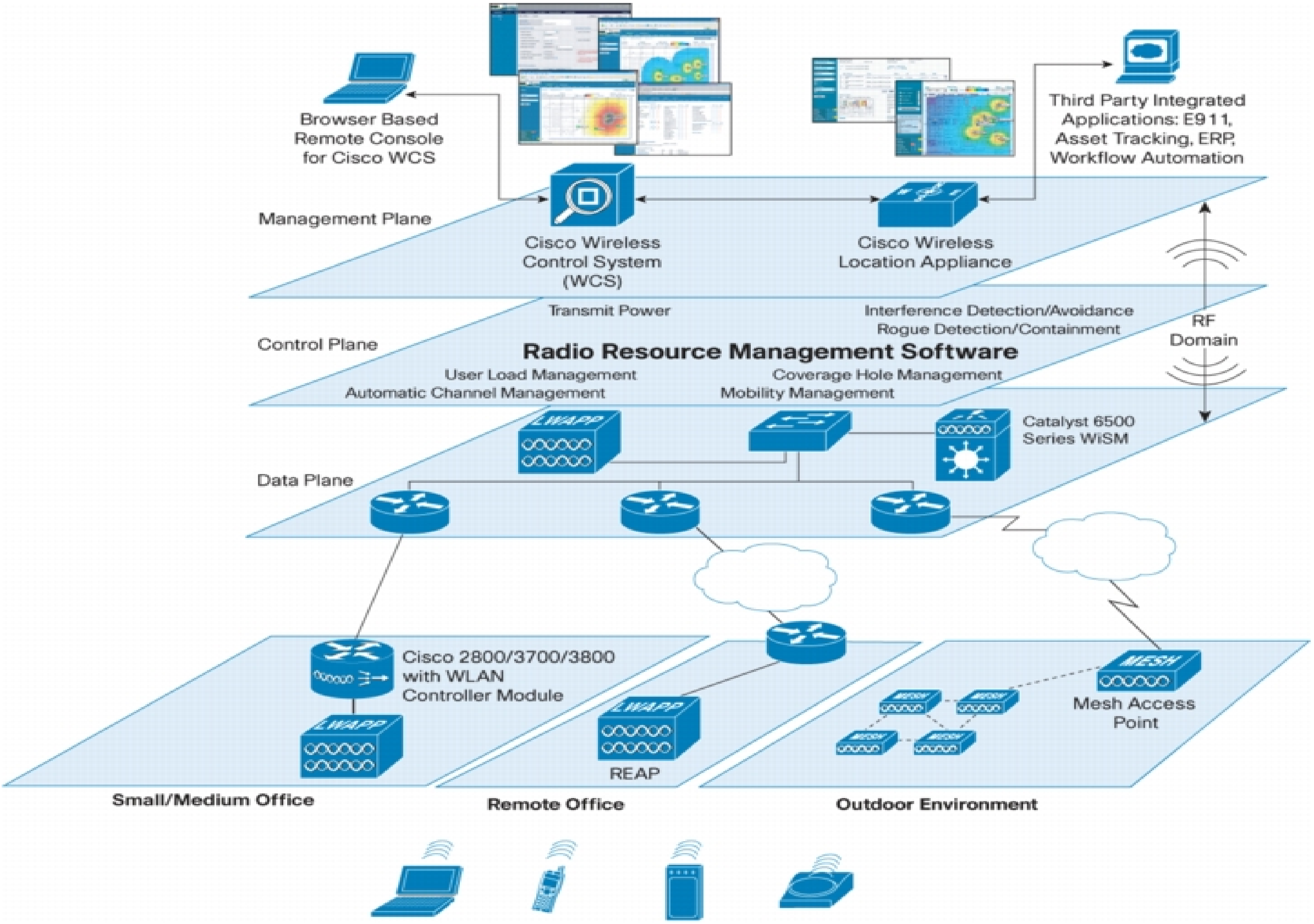
APs dynamically configured and managed through LWAPP. Cisco Aironet Access Points: 1500, 1300, 1240AG, 1230AG, 1130AG, 1100, and 1000.

Cisco Compatible

Client Devices

Secure clients that work out of the box. Cisco Compatible and Cisco Aironet client devices.

Enterprise-Wide RF Intelligence
Pervasive, Easy-to-Use, Unified with Wired Network

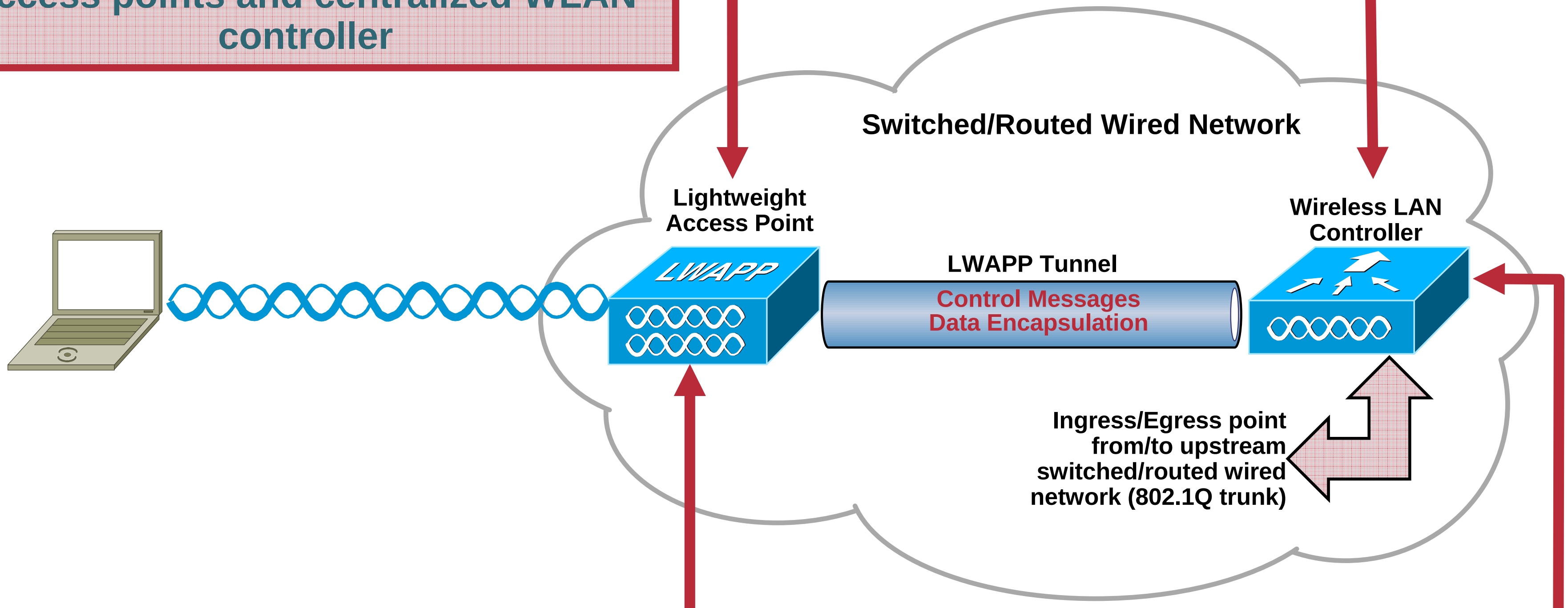


Now…

… back to your regularly scheduled presentation.

Cisco Centralized WLAN Model

LWAPP defines control messaging and data encapsulation between access points and centralized WLAN controller


Switched/Routed Wired Network
Lightweight Access Point
LWAPP
Wireless LAN Controller
LWAPP Tunnel
Control Messages
Data Encapsulation
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

Access Points are “lightweight”—controlled by a centralized WLAN controller

Much of the traditional WLAN functionality moved from access points to centralized WLAN controller

Cisco Centralized WLAN Model

LWAPP carries all communication between access point and controller

L2 or L3 transport

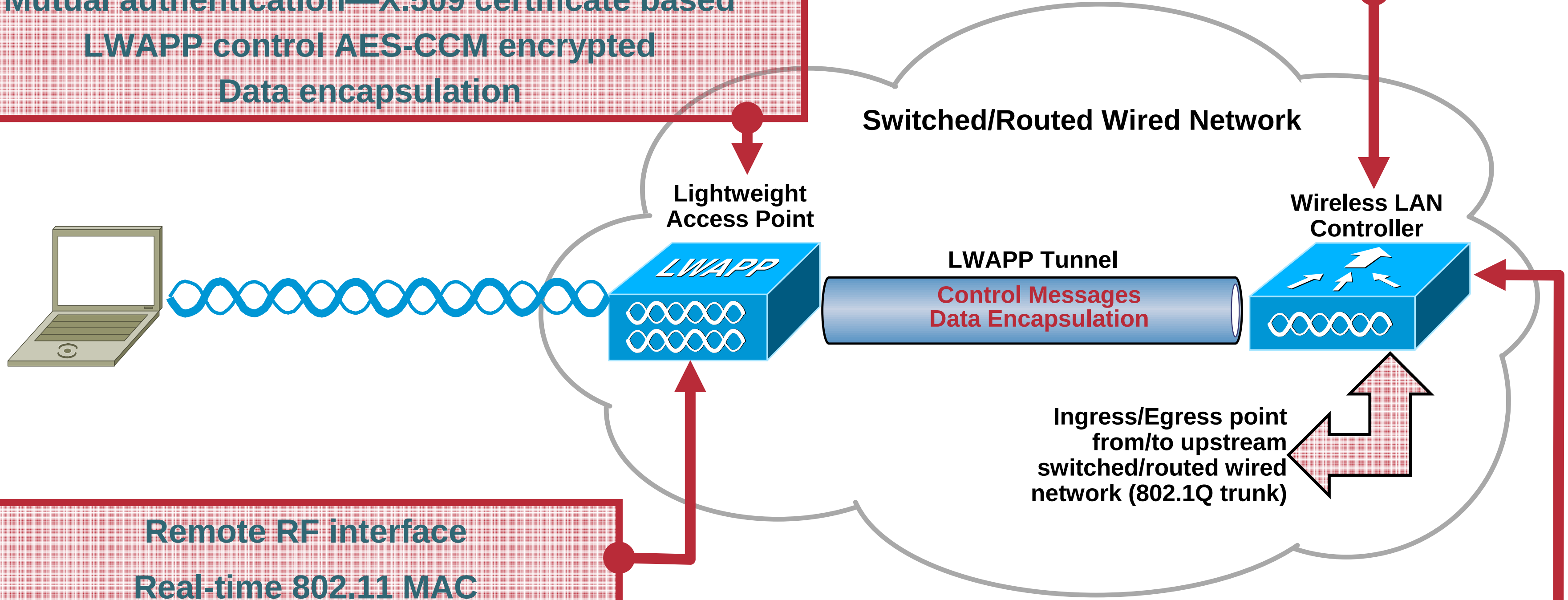
Mutual authentication—X.509 certificate based

LWAPP control AES-CCM encrypted

Data encapsulation

Radio resource management

Mobility management


Switched/Routed Wired Network
Lightweight Access Point
LWAPP
Wireless LAN Controller
LWAPP Tunnel
Control Messages
Data Encapsulation
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

Remote RF interface

Real-time 802.11 MAC

RF spectral analysis

WLAN IDS Signature analysis

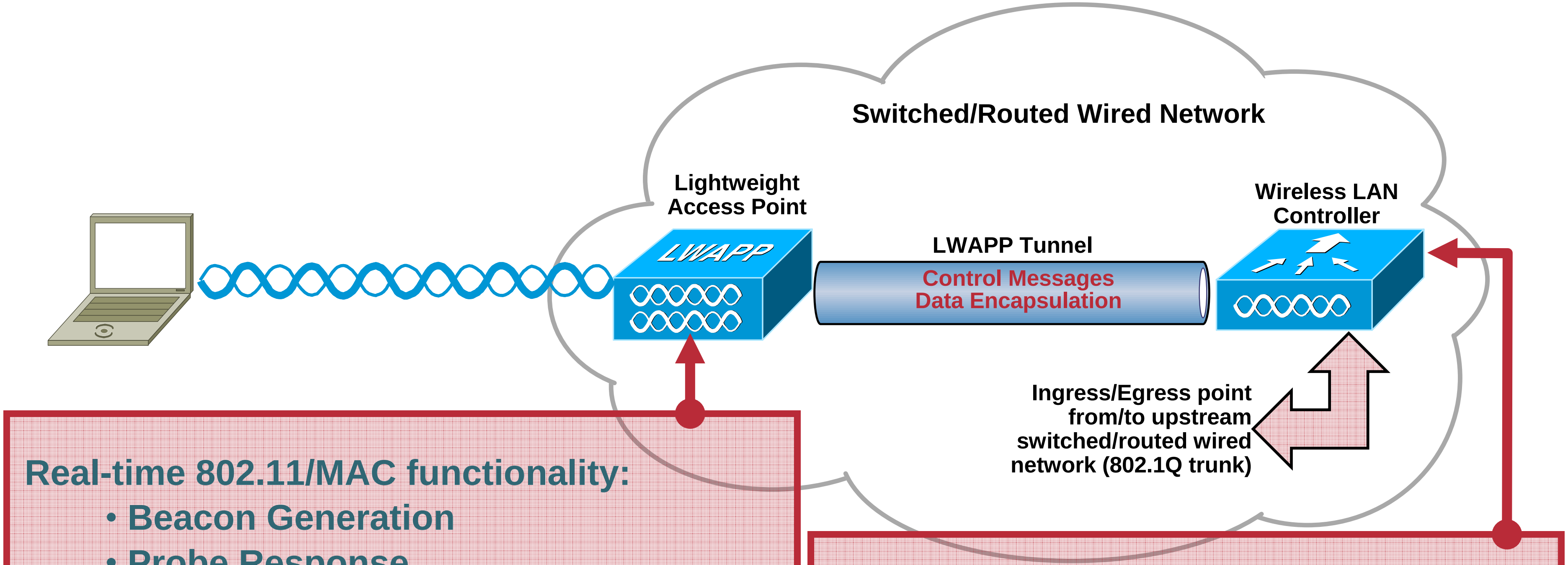
Security management

QoS policies enforcement

Centralized configuration, firmware management

Northbound management interfaces

Division of Labor—Split MAC


Switched/Routed Wired Network
Lightweight Access Point
LWAPP
LWAPP Tunnel
Control Messages
Data Encapsulation
Wireless LAN Controller
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

Real-time 802.11/MAC functionality:

- Beacon Generation
- Probe Response
- Power management/Packet buffering
- 802.11e/WMM scheduling, queueing
- MAC layer data encryption/decryption
- 802.11 control messages

Data encapsulation/de-encapsulation

Fragmentation/De-fragmentation

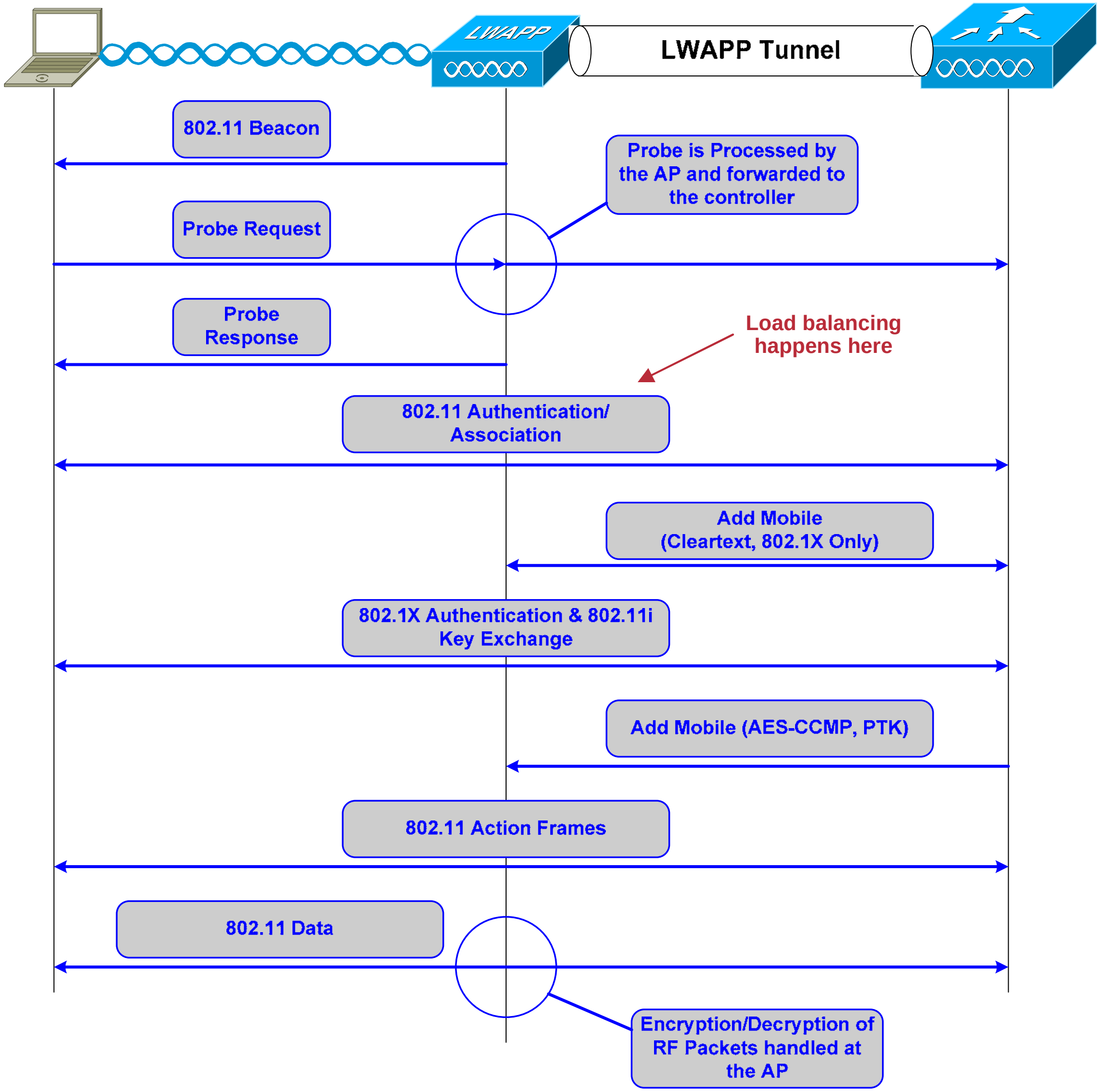
Non real-time 802.11/MAC functionality:

- Assoc/Disassoc/Reassoc
- 802.11e/WMM resource reservation
- 802.1X/EAP
- Key management

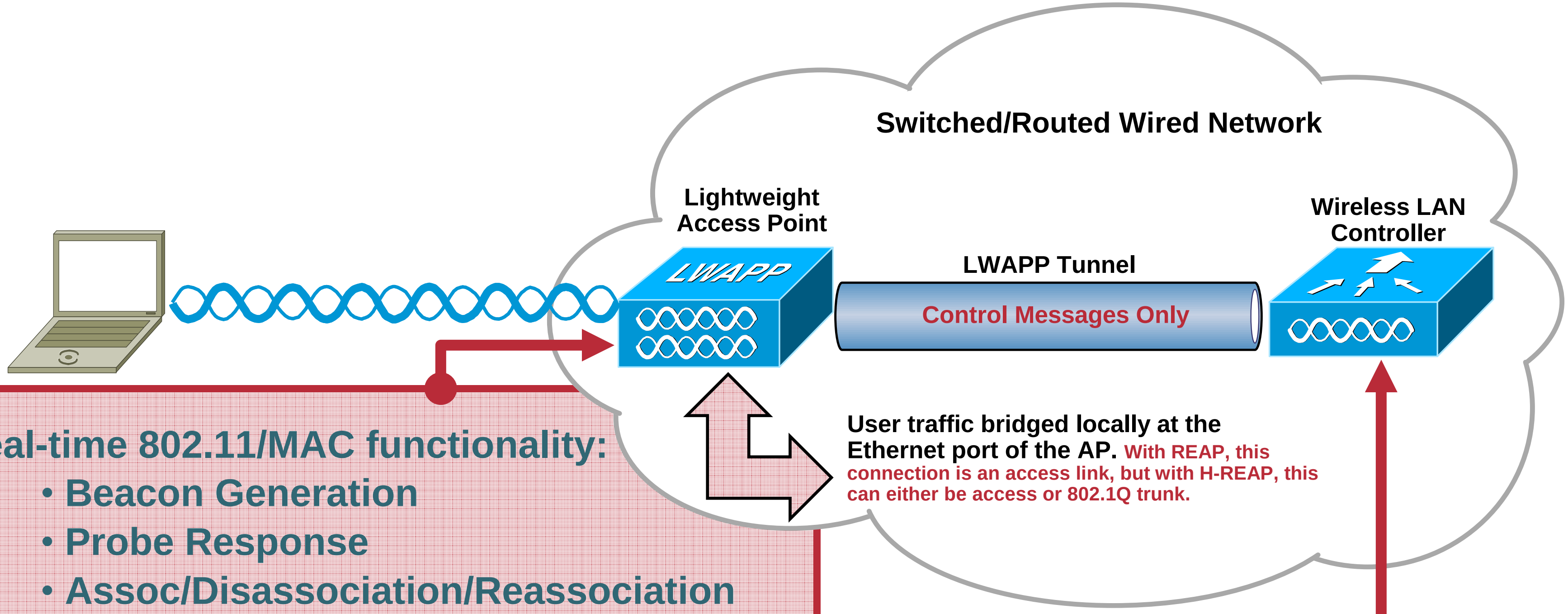
802.11 Distribution services

Wired/Wireless Integration services

Division of Labor—Split MAC Illustrated


LWAPP
LWAPP Tunnel
802.11 Beacon
Probe is Processed by the AP and forwarded to the controller
Probe Request
Probe Response
Load balancing happens here
802.11 Authentication/ Association
Add Mobile (Cleartext, 802.1X Only)
802.1X Authentication & 802.11i Key Exchange
Add Mobile (AES-CCMP, PTK)
802.11 Action Frames
802.11 Data
Encryption/Decryption of RF Packets handled at the AP

Division of Labor—Local MAC



User traffic bridged locally at the Ethernet port of the AP. With REAP, this connection is an access link, but with H-REAP, this can either be access or 802.1Q trunk.

Real-time 802.11/MAC functionality:

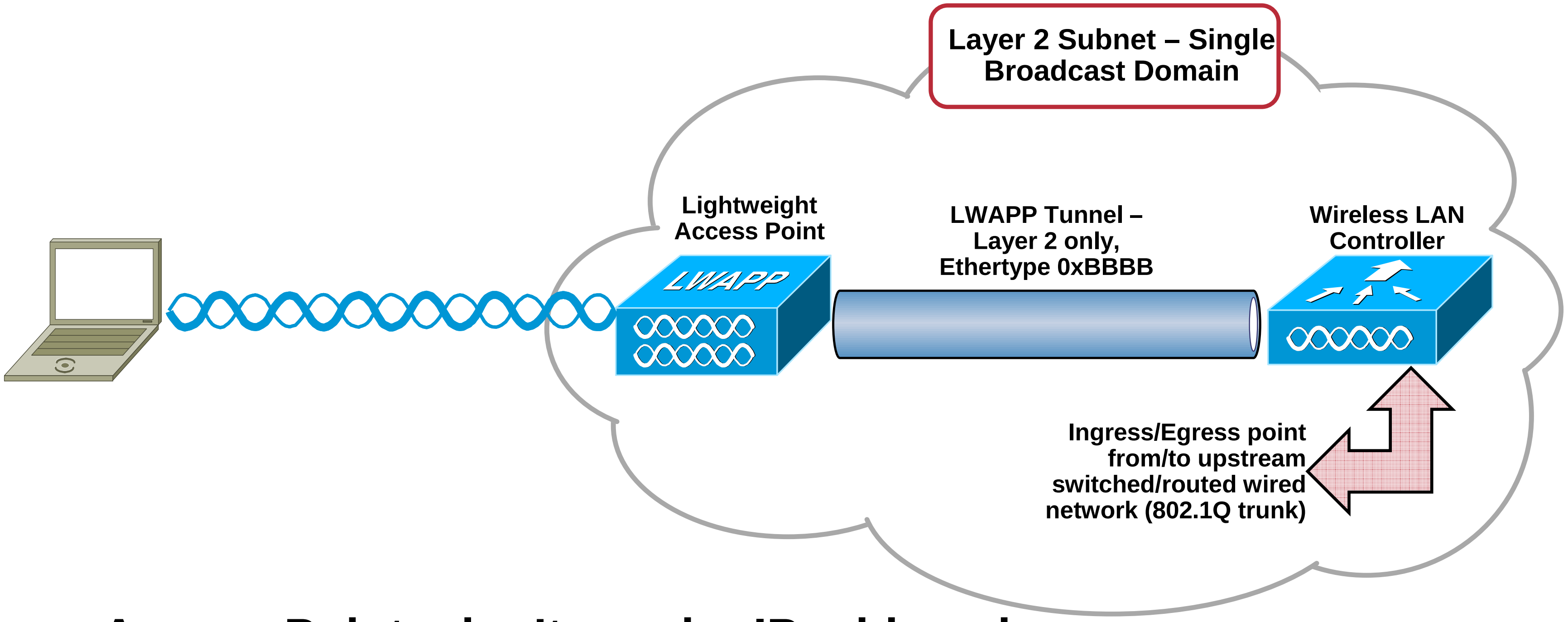
- Beacon Generation
- Probe Response
- Assoc/Disassociation/Reassociation
- Power management/Packet buffering
- 802.11e/WMM scheduling, queueing
- MAC layer data encryption/decryption
- 802.11 control messages

Data encapsulation/de-encapsulation
Fragmentation/De-fragmentation
802.11 Distribution services
Wired/Wireless Integration services

Non real-time 802.11/MAC functionality:

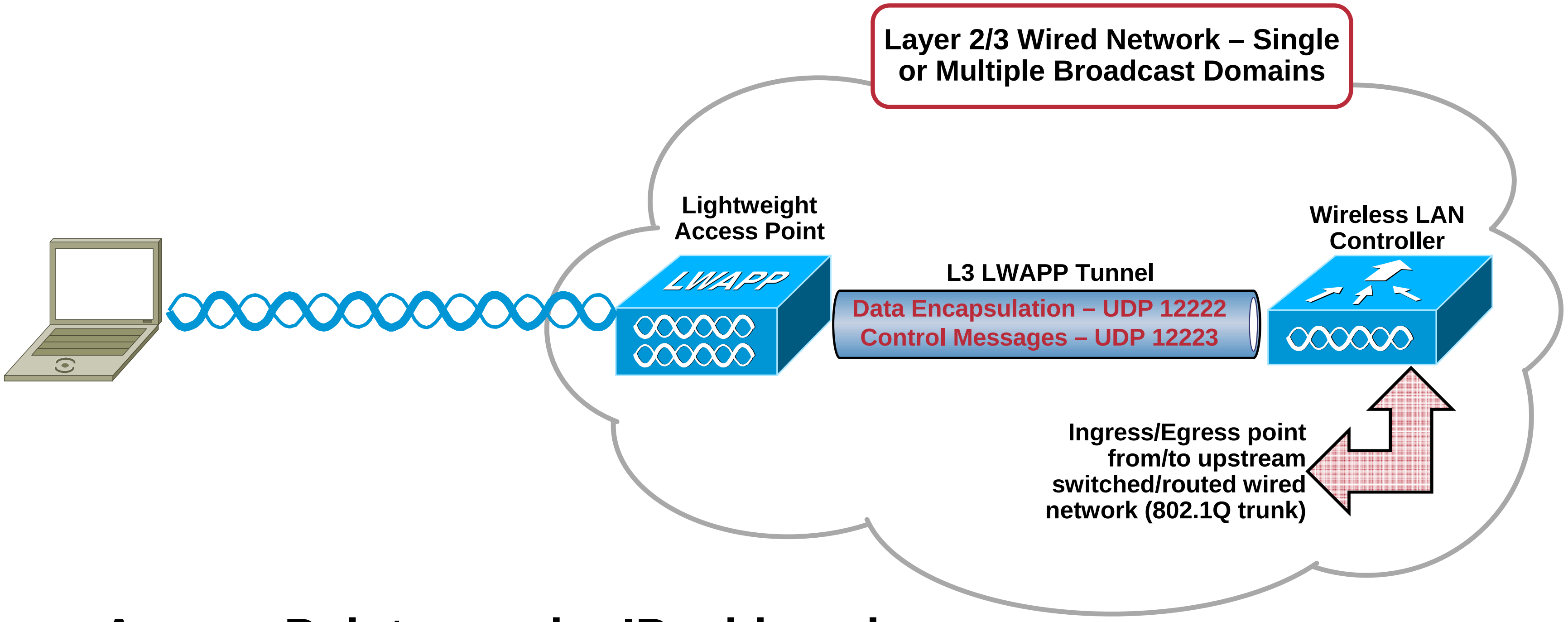
- Proxy Assoc/Disassoc/Reassoc
- 802.11e/WMM resource reservation
- 802.1X/EAP/WPA Key management

Layer-2 LWAPP Architecture


Layer 2 Subnet – Single Broadcast Domain
Lightweight Access Point
LWAPP
LWAPP Tunnel – Layer 2 only, Ethertype 0xBBBB
Wireless LAN Controller
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

- **Access Points don't require IP addressing**
- **Controllers need to be on EVERY subnet on which APs reside**
- **L2 LWAPP was the first step in the evolution of the architecture; many current product do not support this functionality**

Layer-3 LWAPP Architecture


Layer 2/3 Wired Network – Single or Multiple Broadcast Domains
Lightweight Access Point
LWAPP
L3 LWAPP Tunnel
Data Encapsulation – UDP 12222
Control Messages – UDP 12223
Wireless LAN Controller
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

- Access Points require IP addressing
- APs can communicate w/ WLC across routed boundaries
- L3 LWAPP is more flexible than L2 LWAPP and all products support this LWAPP operational 'flavor'

Debugging and Troubleshooting

Troubleshooting 802.11 Wireless LANs Agenda

- Review: Cisco’s Unified Architecture

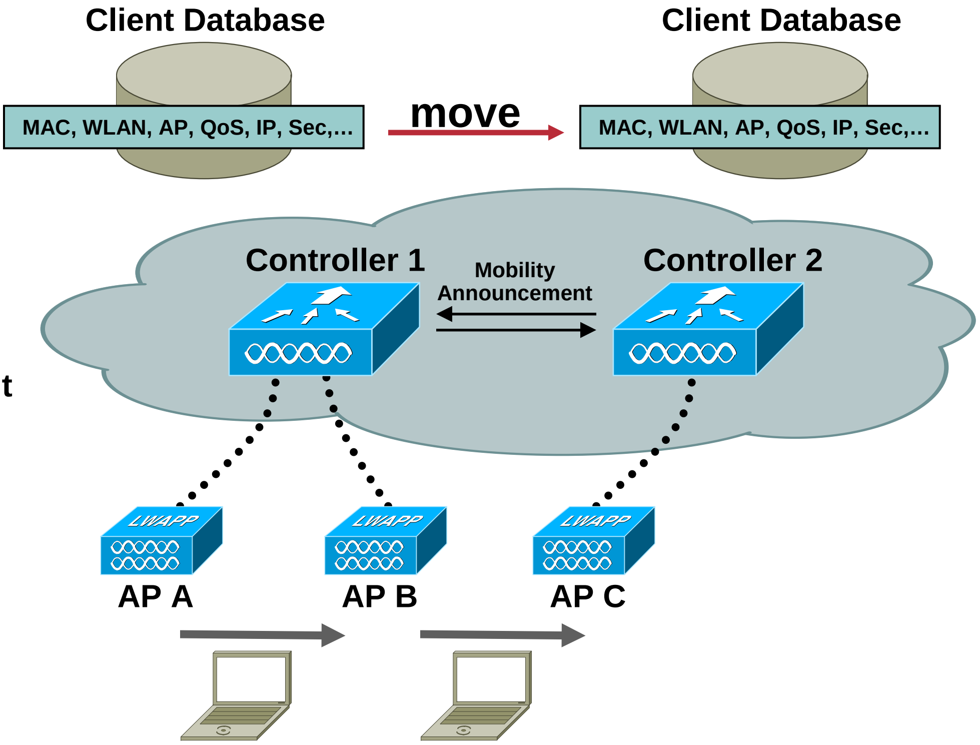
- Debugging and Troubleshooting
  - Wireless LAN Controllers (WLCs)
  - Access Points

Client Mobility

- L2 mobility
- L3 Mobility
    - Fully transparent to clients
    - Conceptually similar to Proxy Mobile IP
        - Foreign and Anchor Controllers
        - Asymmetric traffic flow
- Fast, Secure Roaming
    - PKC – Proactive Key Caching
        - WPA2 / 802.11i Fast Roaming (select supplicants, only)
    - CCKM – Cisco Centralized Key Management (available in 4.0)
        - WPA / WPA2 / 802.11i Fast Roaming (CCX v3 and higher)

Layer 2 Mobility

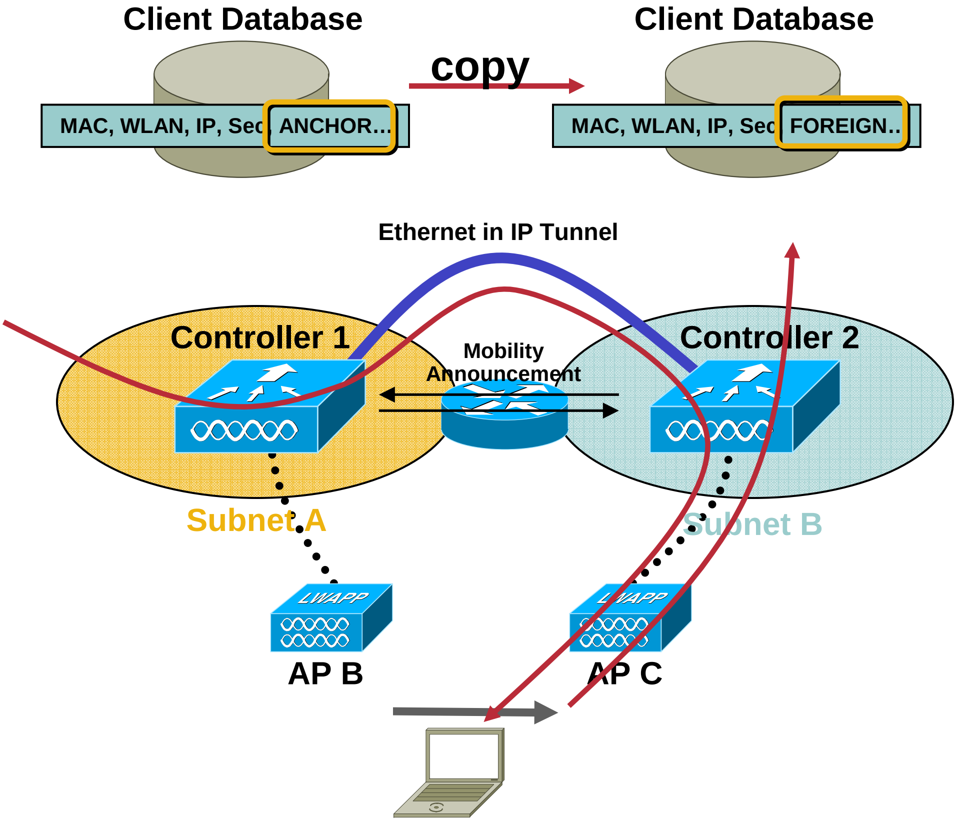
- Client connects to AP A on Controller 1
  - Client database entry created
- Client roams to AP B on Controller 1
  - PKC and CCKM provide fast roam times. Keys are cached, so no need to re-authenticate to Radius server.
- Client roams from AP B (Controller 1) to AP C (Controller 2)
  - Controller 2 makes a Mobility Announcement to peers in Mobility Group looking for Controller with client MAC
  - Controller 1 responds, handshakes, ACKs
  - Client database entry moved to Controller 2
    - PMK data included (master key data from Radius server)
  - PKC and CCKM provide fast roam times. Keys are cached, so no need to re-authenticate to Radius server.



•Roam is transparent to client
•Same DHCP address maintained
•PKC or CCKM provide fast, secure roams

Layer 3 Mobility

- Ethernet in IP Tunnels automatically created between controllers
- Client connects to AP B on Controller 1
  - Client database entry created as ANCHOR
- Client roams to AP C on Controller 2
  - Controller 2 makes a Mobility Announcement to peers in Mobility Group looking for Controller with client MAC
  - Controller 1 responds, handshakes, ACKs
  - Client database entry copied to Controller 2
    - Marked as FOREIGN
    - PMK data included (master key data from Radius server)
  - PKC and CCKM provide fast roam times. Keys are cached, so no need to re-authenticate to Radius server.
- Client roams to AP on 3rd Controller
  - Same as above except FOREIGN client DB entry moved from previous Foreign Controller

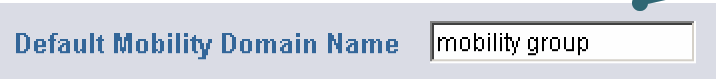


•Roam is transparent to client
•Traffic from client to network exits at Foreign Controller
•Traffic to client tunneled from Anchor to Foreign Controller
•Same DHCP address maintained
•PKC or CCKM provide fast, secure roams

Mobility Configuration

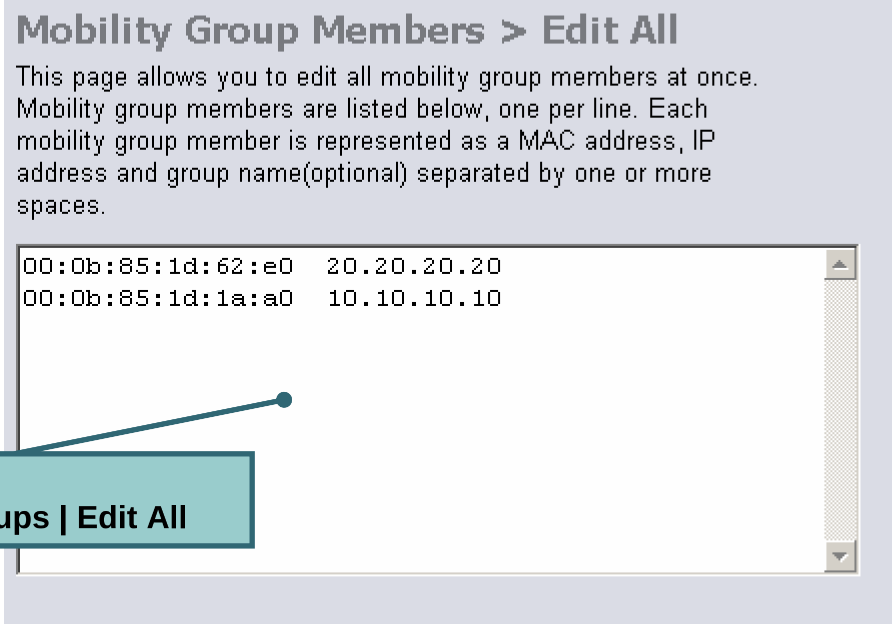
- Make sure that each controller is configured to be in the same Mobility Group

In the controller WebGUI:
Controller | General



Default Mobility Domain Name: mobility group

- Populate each controller with every other controller's MAC and IP address



Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:0b:85:1d:62:e0  20.20.20.20
00:0b:85:1d:1a:a0  10.10.10.10
```

In the controller WebGUI:
Controller | Mobility Management ↳Mobility Groups | Edit All

- Ensure each WLC shares the same Virtual interface IP address

Debugging Mobility: First things first…

- **Can you ping between WLCs in the mobility group?**

  Ping from WLC CLI or GUI

  ```
  (WLC_CLI)>ping [WLC IP Address]
  ```

- **If you can ping, can you ping through both the inter-controller control and data channels?**

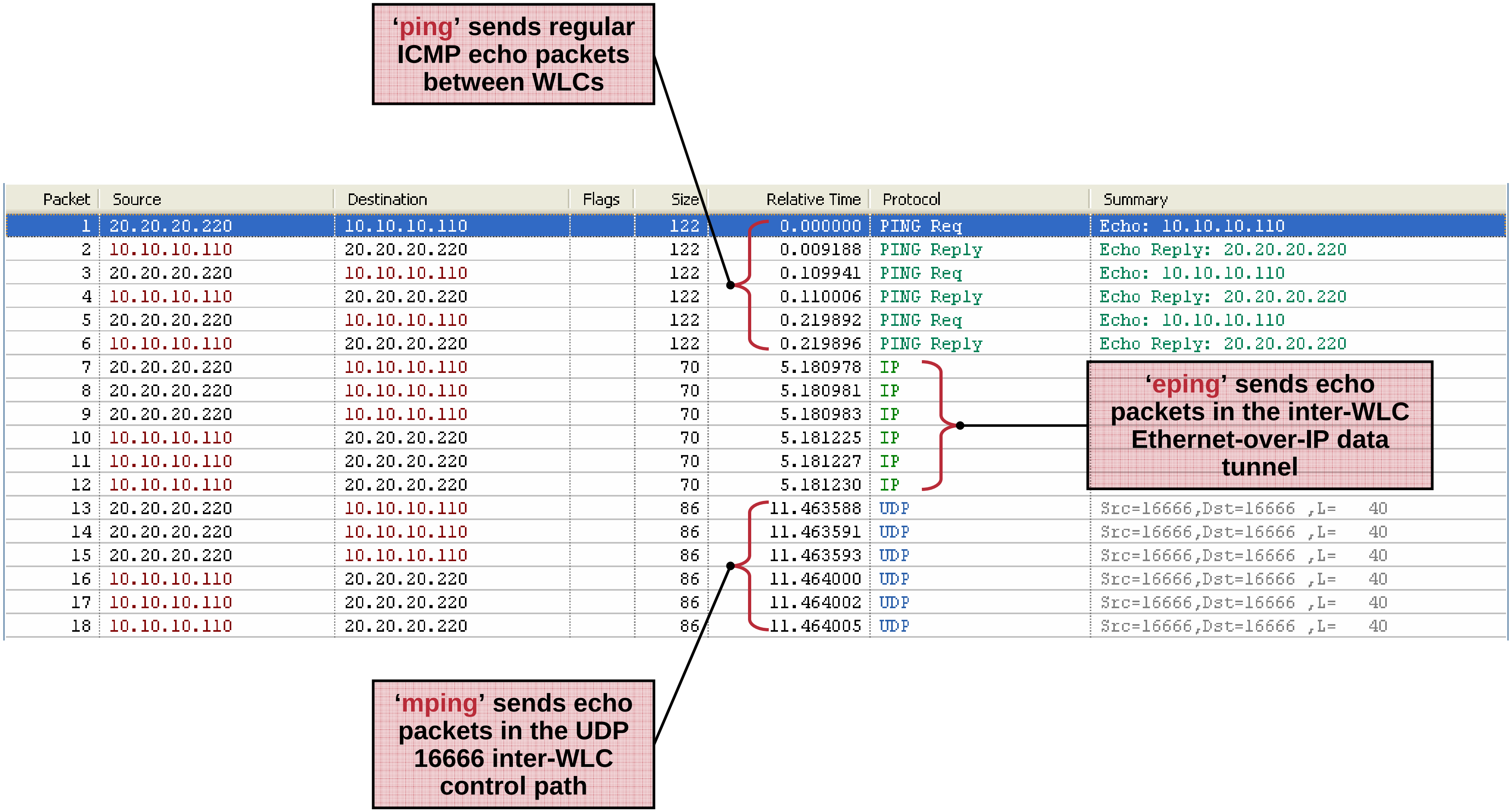
  –CLI-only commands

  eping and mping are new features in the 4.0 controller software release.

  - **Control** `(WLC_CLI)>mping [WLC IP Address]`
  - **Data** `(WLC_CLI)>eping [WLC IP Address]`

•If regular pings are not successful, check WLC IP addressing and network connectivity.
•If pings go through, but mpings do not, ensure each WLC's mobility group name is the same and make sure each WLC's IP, MAC, and mobility group name is entered in every WLC's mobility list.
•If pings and mpings are successful, but epings are not, check the network to make sure that IP protocol 97 (Ethernet-over-IP) is not blocked.

Verifying Connectivity Between WLCs



‘ping’ sends regular ICMP echo packets between WLCs

‘eping’ sends echo packets in the inter-WLC Ethernet-over-IP data tunnel

‘mping’ sends echo packets in the UDP 16666 inter-WLC control path

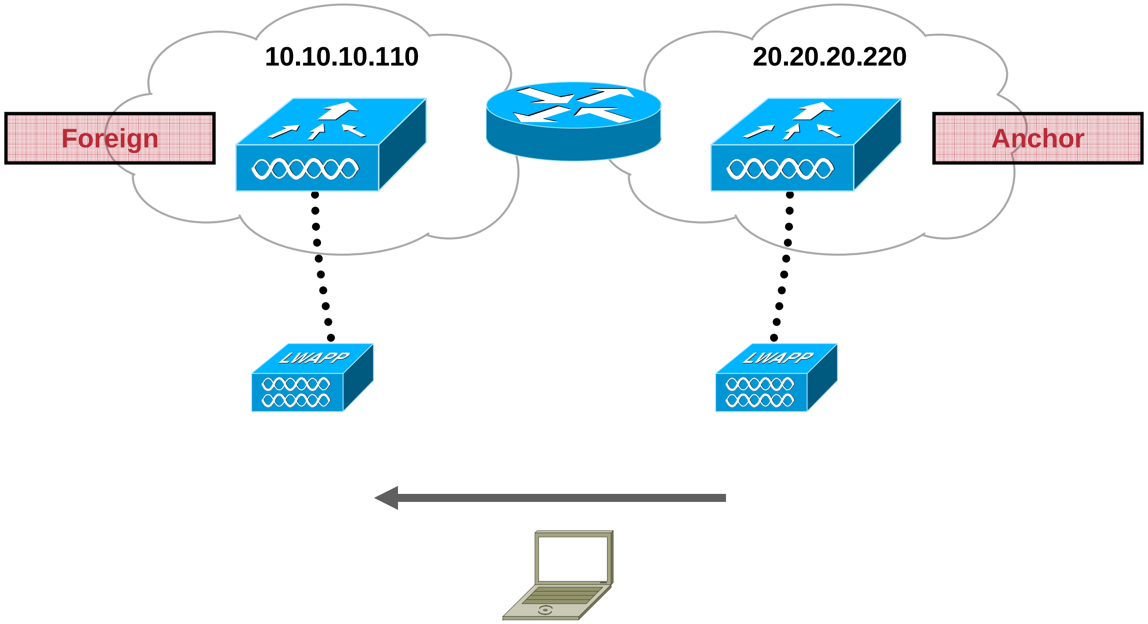
Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1	20.20.20.220	10.10.10.110		122	0.000000	PING Req	Echo: 10.10.10.110
2	10.10.10.110	20.20.20.220		122	0.009188	PING Reply	Echo Reply: 20.20.20.220
3	20.20.20.220	10.10.10.110		122	0.109941	PING Req	Echo: 10.10.10.110
4	10.10.10.110	20.20.20.220		122	0.110006	PING Reply	Echo Reply: 20.20.20.220
5	20.20.20.220	10.10.10.110		122	0.219892	PING Req	Echo: 10.10.10.110
6	10.10.10.110	20.20.20.220		122	0.219896	PING Reply	Echo Reply: 20.20.20.220
7	20.20.20.220	10.10.10.110		70	5.180978	IP	
8	20.20.20.220	10.10.10.110		70	5.180981	IP	
9	20.20.20.220	10.10.10.110		70	5.180983	IP	
10	10.10.10.110	20.20.20.220		70	5.181225	IP	
11	10.10.10.110	20.20.20.220		70	5.181227	IP	
12	10.10.10.110	20.20.20.220		70	5.181230	IP	
13	20.20.20.220	10.10.10.110		86	11.463588	UDP	Src=16666,Dst=16666 ,L= 40
14	20.20.20.220	10.10.10.110		86	11.463591	UDP	Src=16666,Dst=16666 ,L= 40
15	20.20.20.220	10.10.10.110		86	11.463593	UDP	Src=16666,Dst=16666 ,L= 40
16	10.10.10.110	20.20.20.220		86	11.464000	UDP	Src=16666,Dst=16666 ,L= 40
17	10.10.10.110	20.20.20.220		86	11.464002	UDP	Src=16666,Dst=16666 ,L= 40
18	10.10.10.110	20.20.20.220		86	11.464005	UDP	Src=16666,Dst=16666 ,L= 40

Check the Mobility Group

- Make sure every WLC is a part of the same mobility group

```
(WLC_CLI) >show mobility summary
Mobility Protocol Port........................... 16666
Mobility Security Mode........................... Disabled
Default Mobility Domain.......................... cisco_mobility
Mobility Group members configured................ 3

Switches configured in the Mobility Group
   MAC Address          IP Address         Group Name
    00:0b:85:40:7a:00    20.20.20.220       <local>
    00:0b:85:40:81:00    10.10.10.110       cisco_mobility
    00:0b:85:40:a9:00    30.30.30.330       cisco_mobility
```

Mobility Debug Scenario



Dot11 Mobile Debugs

- ## On Foreign Controller

```
(ForeignWLC) >debug mac addr 00:13:ce:57:2b:84

(ForeignWLC) >debug dot11 mobile enable

[TIME]: DEBU STA 00:13:ce:57:2b:84 apfCreateMobileStationEntry:1046 Adding mobile
00:13:ce:57:2b:84 on LWAPP AP 00:13:5f:fa:28:10(0)

[TIME]: DEBU STA 00:13:ce:57:2b:84 apfProcessAssocReq:2170 Association received from mobile
00:13:ce:57:2b:84 on AP 00:13:5f:fa:28:10

[TIME]: DEBU STA 00:13:ce:57:2b:84 apfSendAssocRespMsg:854 Sending Assoc Response to station
00:13:ce:57:2b:84 on BSSID 00:13:5f:fa:28:10 (status 0)
```

- ## On Anchor Controller

```
(AnchorWLC) >debug mac addr 00:13:ce:57:2b:84

(AnchorWLC) >debug dot11 mobile enable

[TIME]: DEBU STA 00:13:ce:57:2b:84 apfUpdateMobileStationLocation:1948 Updated location for station
00:13:ce:57:2b:84 - old AP 00:0b:85:22:95:90-0, new AP 00:00:00:00:00:00-0
```

Mobility Handoff Debugs

- The ‘mobility handoff’ debug shows client handoff between WLCs in a mobility group during inter-WLC roams
- Roaming handoff debug Steps:

  Create a debug filter for the MAC of the client of interest

  Then run the handoff debug on both the anchor and foreign controllers

  Check debug output to verify proper roam operation

‘Mobility Handoff’ Debug on Foreign WLC

```
(ForeignWLC) >debug mac addr 00:13:ce:57:2b:84
(ForeignWLC) >debug mobility handoff enable
<SNIP> Client 802.11 association (roam from anchor WLC) </SNIP>
[TIME]: Mobility packet sent to:
[TIME]:   20.20.20.220, port 16666, Switch IP: 10.10.10.110
[TIME]:   type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 54  seq: 176  len 120
[TIME]:   group id: 369259c9 542c40de 5b412a7f fb59e7c4
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 0.0.0.0, instance: 0
[TIME]:   VLAN IP: 10.10.10.110, netmask: 255.255.255.0
[TIME]: Mobility packet received from:
[TIME]:   20.20.20.220, port 16666, Switch IP: 20.20.20.220
[TIME]:   type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 54  seq: 223  len 554
[TIME]:   group id: 369259c9 542c40de 5b412a7f fb59e7c4
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 20.20.20.124, instance: 0
[TIME]:   VLAN IP: 20.20.20.220, netmask: 255.255.255.0
[TIME]: DEBU CTRLR mmMobileHandoffRcv:3161 Mobility handoff:
  Client: 00:13:ce:57:2b:84, Ip: 20.20.20.124
  Anchor IP: 20.20.20.220, Peer IP: 20.20.20.220
[TIME]: DEBU STA 00:13:ce:57:2b:84 20.20.20.124 RUN (20) pemMscbAddNpu:978 Plumbing simplex mobility tunnel to
      20.20.20.220 as Foreign, (VLAN 0)
[TIME]: DEBU STA 00:13:ce:57:2b:84 apfMmProcessResponse:1282 Mobility Response: mobile 00:13:ce:57:2b:84IP 20.20.20.124
    code 1, reason 0, PEM State RUN, Role Foreign(3)
```

Foreign notifies Anchor of new client

Anchor responds with existing client association information

Anchor Controller’s IP: 20.20.20.220 | Foreign Controller’s IP: 10.10.10.110

‘Mobility Handoff’ Debug on Anchor WLC

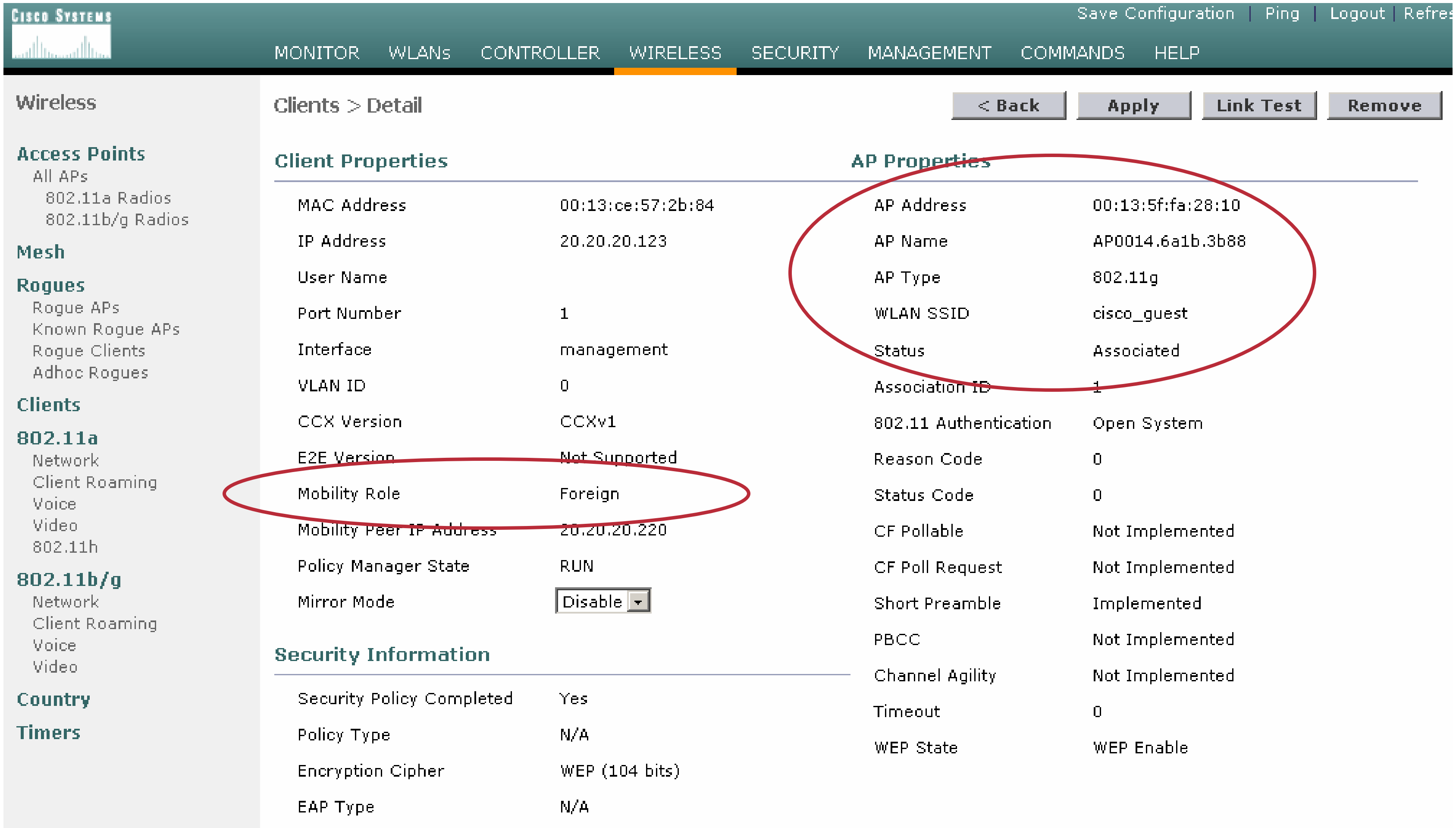
```
(AnchorWLC) >debug mac addr 00:13:ce:57:2b:84
(AnchorWLC) >debug mobility handoff enable
[TIME]: Mobility packet received from:
[TIME]:   10.10.10.110, port 16666, Switch IP: 10.10.10.110
[TIME]:   type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 54  seq: 176  len 120
[TIME]:   group id: 369259c9 542c40de 5b412a7f fb59e7c4
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 0.0.0.0, instance: 0
[TIME]:   VLAN IP: 10.10.10.110, netmask: 255.255.255.0
[TIME]: DEBU CTRLR mmMobileAnnounceRcv:2754 Handoff as Local, Client IP: 20.20.20.124 Anchor IP: 20.20.20.220
[TIME]: Mobility packet sent to:
[TIME]:   10.10.10.110, port 16666, Switch IP: 20.20.20.220
[TIME]:   type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 54  seq: 223  len 554
[TIME]:   group id: 369259c9 542c40de 5b412a7f fb59e7c4
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 20.20.20.124, instance: 0
[TIME]:   VLAN IP: 20.20.20.220, netmask: 255.255.255.0
[TIME]: DEBU STA 00:13:ce:57:2b:84 20.20.20.124 RUN (20) pemUpdateMobilityRole:2443 mobility role update request from Local
    to Anchor Peer = 10.10.10.110, Old Anchor = 20.20.20.220, New Anchor = 20.20.20.220
[TIME]: DEBU STA 00:13:ce:57:2b:84 20.20.20.124 RUN (20) pemMscbAddNpu:962 Plumbing simplex mobility tunnel to
    10.10.10.110 as Anchor (VLAN 0)
[TIME]: DEBU STA 00:13:ce:57:2b:84 apfMmProcessResponse:1282 Mobility Response: mobile 00:13:ce:57:2b:84IP 20.20.20.124
  code 2, reason 1, PEM State RUN, Role Anchor(2)
```

Foreign notifies Anchor of new client

Anchor responds with existing client association information

Anchor Controller’s IP: 20.20.20.220 | Foreign Controller’s IP: 10.10.10.110

Client Record in Foreign WLC



Clients > Detail

Client Properties

MAC Address	00:13:ce:57:2b:84
IP Address	20.20.20.123
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	CCXv1
E2E Version	Not Supported
Mobility Role	Foreign
Mobility Peer IP Address	20.20.20.220
Policy Manager State	RUN
Mirror Mode	Disable

Security Information

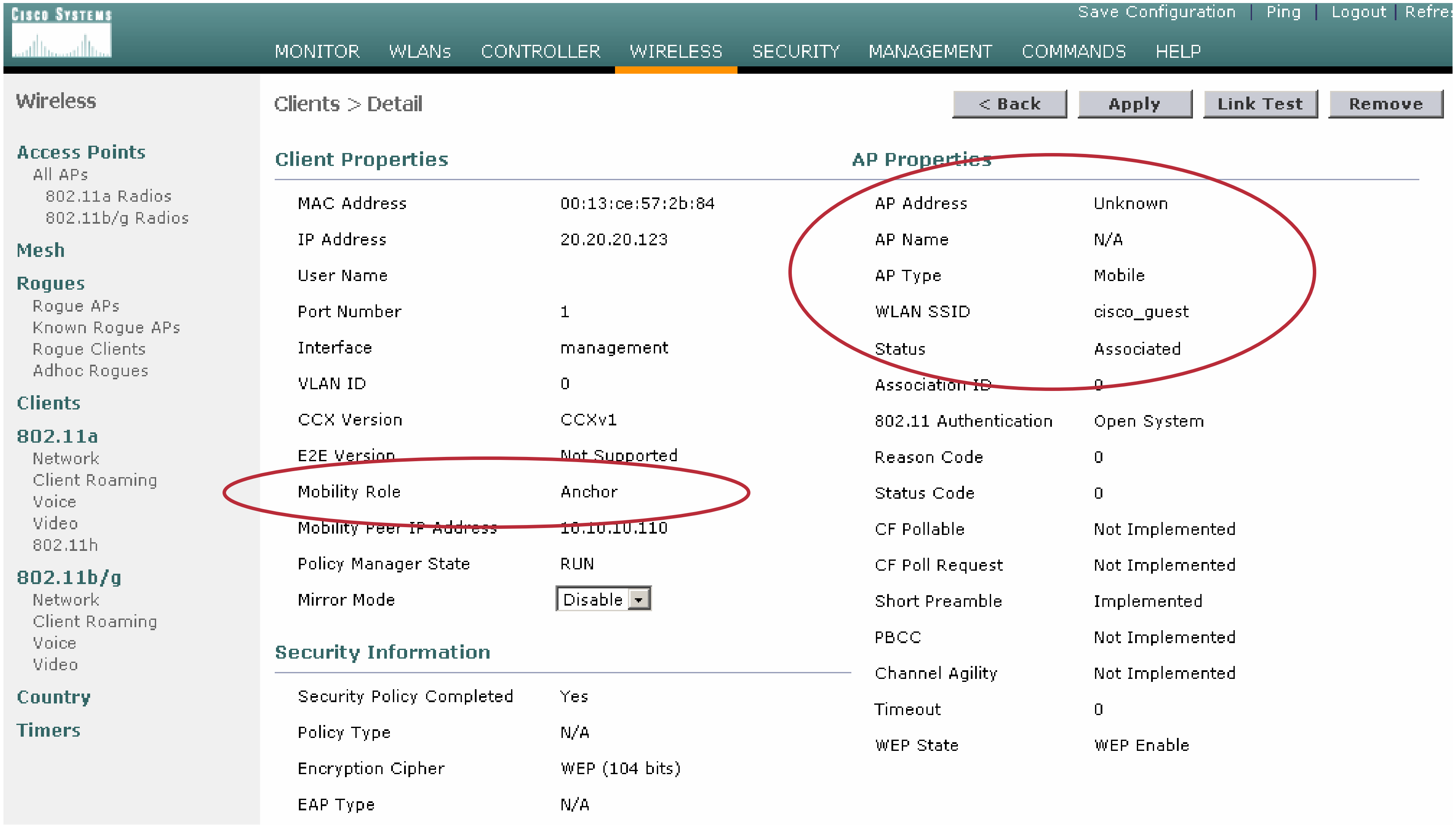
Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	WEP (104 bits)
EAP Type	N/A

AP Properties

AP Address	00:13:5f:fa:28:10
AP Name	AP0014.6a1b.3b88
AP Type	802.11g
WLAN SSID	cisco_guest
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

In the WLC GUI, go to: Wireless | Clients and select Details for the client of choice.

Client Record in Anchor WLC



Clients > Detail

Client Properties

MAC Address	00:13:ce:57:2b:84
IP Address	20.20.20.123
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	CCXv1
E2E Version	Not Supported
Mobility Role	Anchor
Mobility Peer IP Address	10.10.10.110
Policy Manager State	RUN
Mirror Mode	Disable ▾

Security Information

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	WEP (104 bits)
EAP Type	N/A

AP Properties

AP Address	Unknown
AP Name	N/A
AP Type	Mobile
WLAN SSID	cisco_guest
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

In the WLC GUI, go to: Wireless | Clients and select Details for the client of choice.

User Idle Timeout

- **Client sessions will remain for the duration of the User Idle Timeout value**
- **If a client roams from one AP on one controller to another AP on another controller within that window, client state is maintained and a roaming event between controllers results**

NOTE: Depending on application needs, it may be desirable to adjust this parameter to lengthen or shorten the time it will take for client records to be aged out.

User Idle Timeout (seconds) 300

In the WLC GUI, go to: Controller | General and adjust the duration in seconds

Traditional Guest Traffic Termination

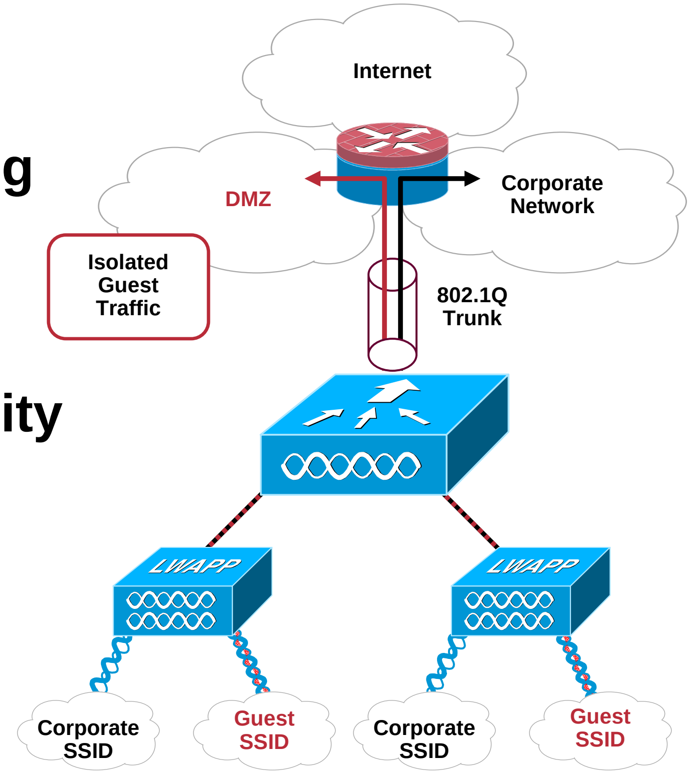
- **The traditional approach to segmenting guest traffic requires ‘pulling’ the guest VLAN through the corporate network**

Many customers:

→ Cannot do this (due to routing to the edge, etc)

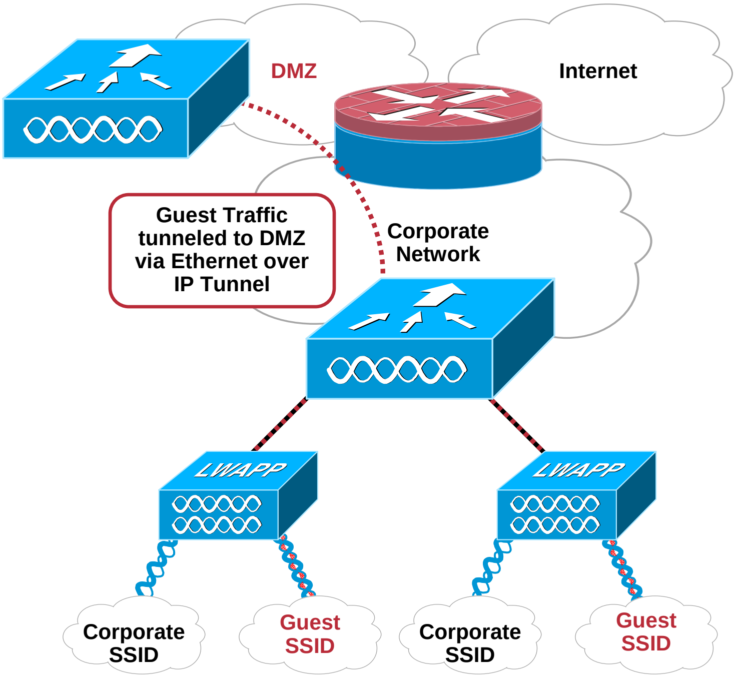
or

→ Will not do this (due to security risks – ARP poisoning, VLAN hopping, etc)

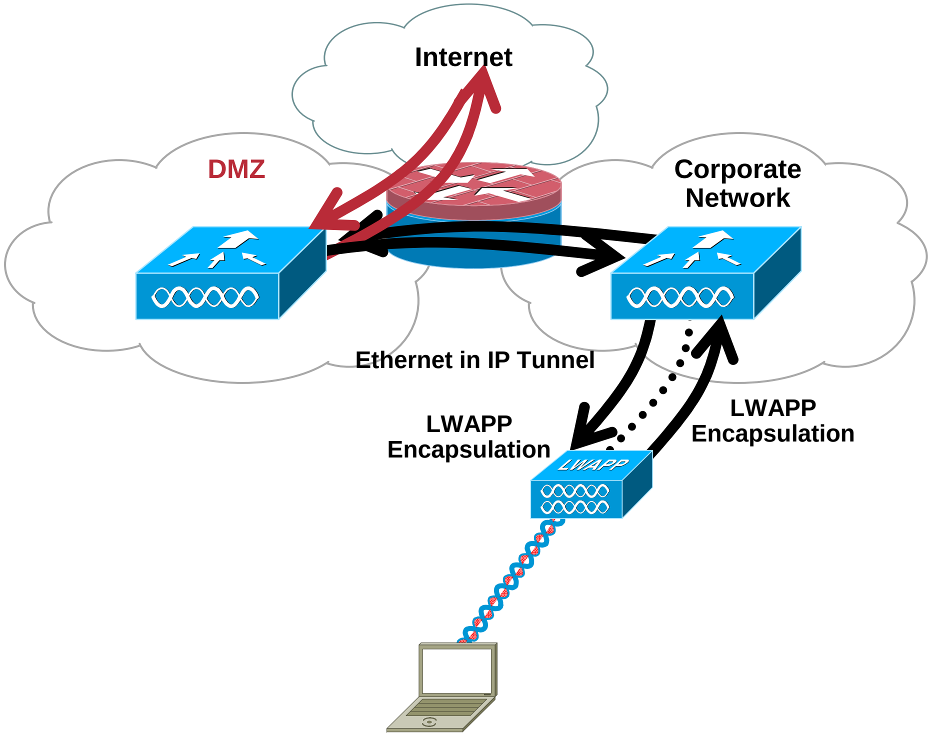


Tunnel Guest Traffic to the DMZ

- By tunneling all guest traffic to a DMZ controller, traffic originates and terminates in the DMZ
- Guest clients logically reside in the DMZ network
- No changes required to existing infrastructure except adding FW rules
- Add additional DMZ controllers for scalability

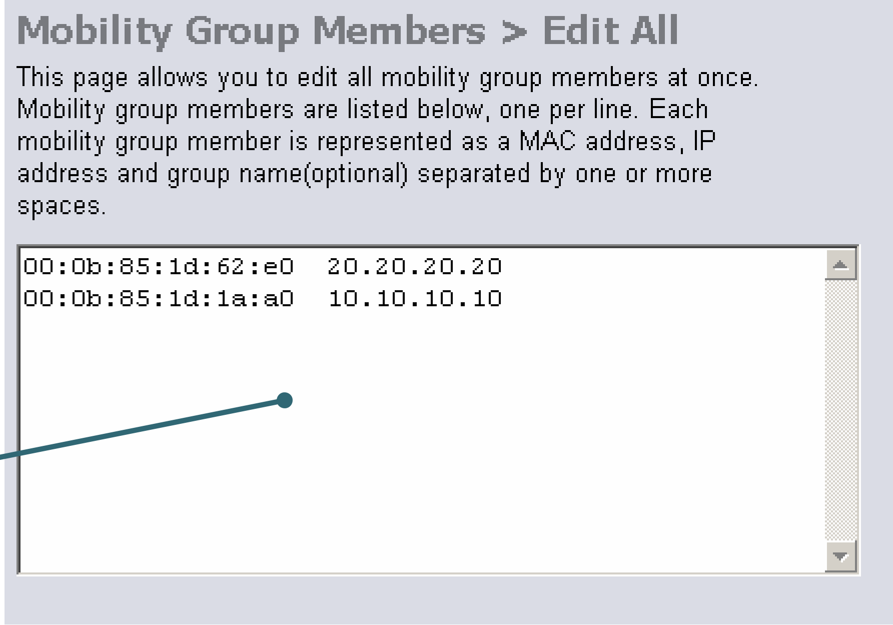


Guest Traffic Flows



Guest Tunneling Configuration

- **Populate each controller with every other controller's MAC and IP address**



Mobility Group Members > Edit All

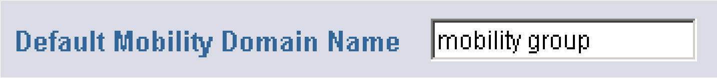
This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:0b:85:1d:62:e0  20.20.20.20
00:0b:85:1d:1a:a0  10.10.10.10
```

In the controller WebGUI:
Controller | Mobility Management | Mobility Groups | Edit All

- **You do <u>not</u> need to have each controller configured to be in the same Mobility Group**

  WLCs on the 'internal' network will only require the same Mobility Group Name if roaming between them is desired; the DMZ controller(s) need not share this name.



Default Mobility Domain Name: mobility group

j7

Slide 37

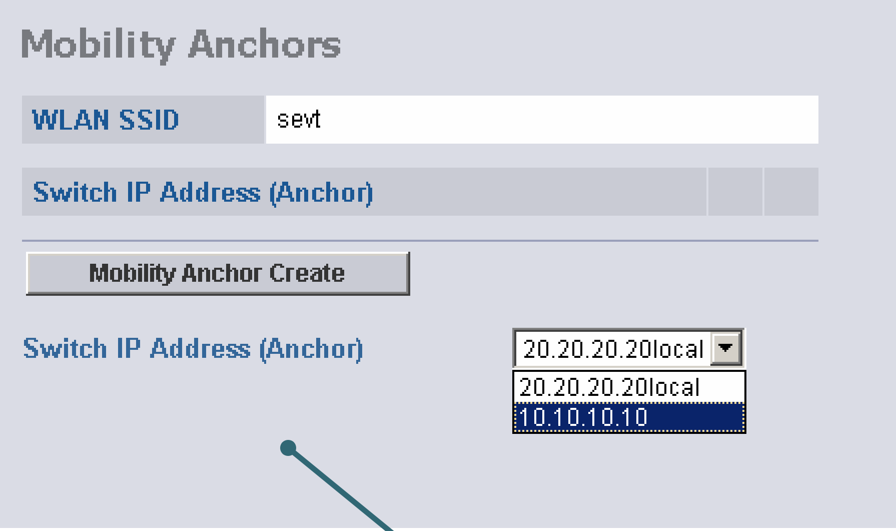
j7 this probably needs a screenshot refresh from the newest WLC code version
jlindema, 3/24/2006

Guest Tunneling Configuration

- **Select a mobility anchor or anchors where traffic will be tunneled**

  This needs to be done for each Guest WLAN on each controller – even the DMZ controller(s)!

- **To configure this, DMZ controller(s) need to be a part of the Mobility List**



Mobility Anchors

WLAN SSID: sevt

Switch IP Address (Anchor)

Switch IP Address (Anchor): 20.20.20.20local

In the controller WebGUI:

- **WLANs | WLANs | [WLAN of Choice] | Mobility Anchors**

In WCS:

- **Configure | Controllers | WLANs | WLANs | [WLAN of Choice] | Mobility Anchors**

In the controller CLI:

```
• > config wlan mobility anchor add [WLAN ID] [Controller Address]

• > config mobility secure-mode enable

     > config certificate compatibility on
```

This is only necessary when backward compatibility with legacy Airespace equipment is required in secure mode

Firewall Entries

Open ports for:

- **Inter-Controller Tunneled Client Data – IP Protocol 97**
- **Inter-Controller Control Traffic – UDP Port 16666 (or 16667, if encrypted)**

These ports MUST be open!.

- **Optional management/operational protocols:**

  SSH/Telnet – TCP Port 22/23

  TFTP – TCP Port 69

  NTP – UDP Port 123

  SNMP – UDP Ports 161 (gets and sets) and 162 (traps)

  HTTPS/HTTP – TCP Port 443/80

  Syslog– TCP Port 514

Design Considerations and Limitations

- Total throughput and client limitations per supported DMZ controller
  - 4100 – 1 Gbps and 1,500 total clients
  - 4402 – 2 Gbps and 2,500 total clients
  - 4404 – 4 Gbps and 5,000 total clients
  - WiSM – 8 Gbps and 10,000 total clients
- Each DMZ controller can handle up to 40 tunnels from internal WLCs
  - Tunnels are counted per WLAN, per WLC
- Firewall limitations
  - Only 1:1 NAT is supported through the firewall
- The 2006 and WLCM module can only originate Guest Tunnels
  - They will not be able to terminate guest traffic in the DMZ

Check Mobility Grouping

- Make sure every internal WLC has its mobility table properly configured

    The DMZ WLC does not need to have the same Mobility Group Name, but make sure it is entered properly into the table

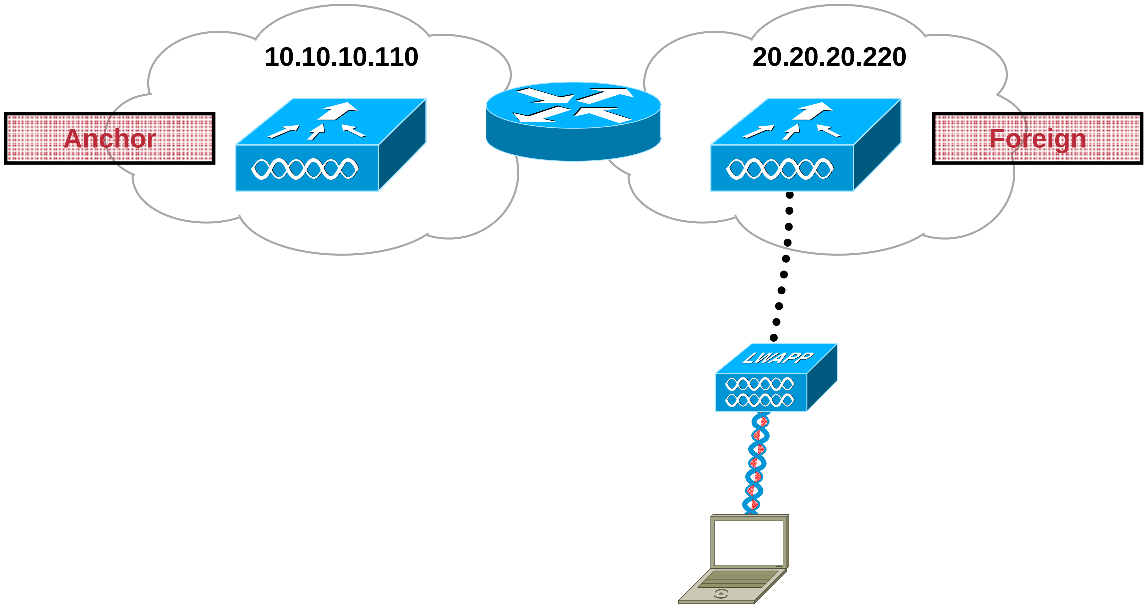
    All internal WLCs between which roaming is desired must have the same Mobility Group Name

```
(WLC_CLI) >show mobility summary
Mobility Protocol Port......................... 16666
Mobility Security Mode......................... Disabled
Default Mobility Domain........................ cisco_mobility_internal
Mobility Group members configured.............. 3

Switches configured in the Mobility Group
   MAC Address              IP Address           Group Name
    00:0b:85:40:7a:00        20.20.20.220          <local>
    00:0b:85:40:81:00        10.10.10.110          cisco_mobility_dmz
    00:0b:85:40:a9:00        30.30.30.330          cisco_mobility_internal
```

Verify WLAN / DMZ Anchor Coupling

```
(WLC_CLI) >show wlan summary
Number of WLANs.................................. 2
WLAN ID  WLAN Name                        Status     Interface Name
-------  ----------------------           ---------  -----------------
1        cisco_internal                   Enabled    internal
2        cisco_guest                      Enabled    management

(WLC_CLI) >show mobility anchor 2
Mobility Anchor Export List
 WLAN ID      IP Address
     2         10.10.10.110
```

Guest Tunnel Debug Scenario



‘Mobility Handoff’ Debug on Foreign/Internal WLC

```
(Internal_WLC) >debug mac addr 00:13:ce:57:2b:84
(Internal_WLC) >debug mobility handoff enable
[TIME]: DEBU STA 00:13:ce:57:2b:84 0.0.0.0 RUN (20) pemMscbAddNpu:1019 Plumbing duplex mobility tunnel to 10.10.10.110
   as Export Foreign (VLAN 0)
[TIME]: Mobility packet sent to:
[TIME]:   10.10.10.110, port 16666, Switch IP: 20.20.20.220
[TIME]:   type: 16(MobileAnchorExport)  subtype: 0  version: 1  xid: 35  seq: 35  len 244
[TIME]:   group id: fdde909c fbe10b7f 157d342a 958ad803
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 0.0.0.0, instance: 0
[TIME]:   VLAN IP: 20.20.20.220, netmask: 255.255.255.0
[TIME]: Mobility packet received from:
[TIME]:   10.10.10.110, port 16666, Switch IP: 10.10.10.110
[TIME]:   type: 17(MobileAnchorExportAck)  subtype: 0  version: 1  xid: 35  seq: 23  len 272
[TIME]:   group id: 413eb1d5 a15f0364 388bea8e b74567c9
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 10.10.10.106, instance: 1
[TIME]:   VLAN IP: 10.10.10.110, netmask: 255.255.255.0
[TIME]: DEBU CTRLR mmAnchorExportAckRcv:2217 Received Anchor Export Ack: 00:13:ce:57:2b:84 from Switch IP: 10.10.10.110
[TIME]: DEBU STA 00:13:ce:57:2b:84 0.0.0.0 RUN (20) pemUpdateMobilityRole:2443 mobility role update request from Export Foreign to
    Export Foreign Peer = 10.10.10.110, Old Anchor = 10.10.10.110, New Anchor = 10.10.10.110
[TIME]: DEBU STA 00:13:ce:57:2b:84 apfMmProcessResponse:1282 Mobility Response: mobile 00:13:ce:57:2b:84IP 0.0.0.0
   code 4, reason 4, PEM State RUN, Role Export Foreign(5)
```

Internal notifies DMZ of new client

DMZ responds with new client association information

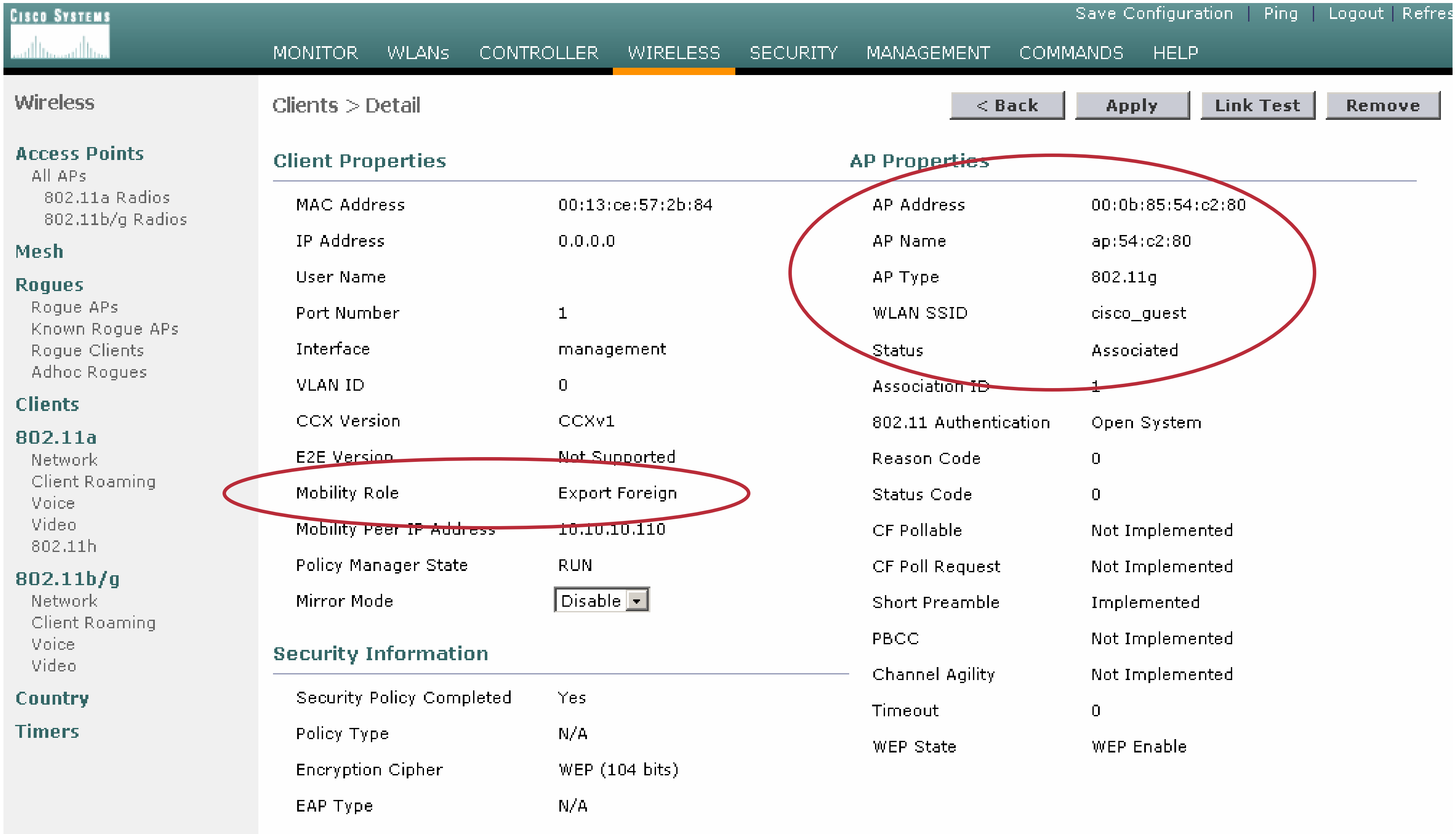
‘Mobility Handoff’ Debug on DMZ WLC

```
(DMZ_WLC) >debug mac addr 00:13:ce:57:2b:84
(DMZ_WLC) >debug mobility handoff enable
[TIME]: Mobility packet received from:
[TIME]:   20.20.20.220, port 16666, Switch IP: 20.20.20.220
[TIME]:   type: 16(MobileAnchorExport)  subtype: 0  version: 1  xid: 34  seq: 34  len 244
[TIME]:   group id: fdde909c fbe10b7f 157d342a 958ad803
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 0.0.0.0, instance: 0
[TIME]:   VLAN IP: 20.20.20.220, netmask: 255.255.255.0
[TIME]: DEBU CTRLR mmAnchorExportRcv:1888 Received Anchor Export request: 00:13:ce:57:2b:84 from Switch IP: 20.20.20.220
[TIME]: DEBU CTRLR mmAnchorExportRcv:2060 Received Anchor Export policy update, valid mask 0x0:
  Qos Level: 0, DSCP: 0, dot1p: 0  Interface Name: , ACL Name:
[TIME]: Mobility packet sent to:
[TIME]:   20.20.20.220, port 16666, Switch IP: 10.10.10.110
[TIME]:   type: 17(MobileAnchorExportAck)  subtype: 0  version: 1  xid: 35  seq: 23  len 272
[TIME]:   group id: 413eb1d5 a15f0364 388bea8e b74567c9
[TIME]:   mobile MAC: 00:13:ce:57:2b:84, IP: 10.10.10.106, instance: 1
[TIME]:   VLAN IP: 10.10.10.110, netmask: 255.255.255.0
[TIME]: DEBU STA 00:13:ce:57:2b:84 0.0.0.0 DHCP_REQD (7) pemMscbAddNpu:995 Plumbing duplex mobility tunnel to 20.20.20.220 as
      Export Anchor (VLAN 0)
[TIME]: DEBU STA 00:13:ce:57:2b:84 10.10.10.106 RUN (20) pemMscbAddNpu:995 Plumbing duplex mobility tunnel to 20.20.20.220 as
      Export Anchor (VLAN 0)
```

Internal notifies DMZ of new client

DMZ responds with new client association information

Client Record in the Internal (Foreign) WLC



Clients > Detail

Client Properties

MAC Address	00:13:ce:57:2b:84
IP Address	0.0.0.0
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	CCXv1
E2E Version	Not Supported
Mobility Role	Export Foreign
Mobility Peer IP Address	10.10.10.110
Policy Manager State	RUN
Mirror Mode	Disable

Security Information

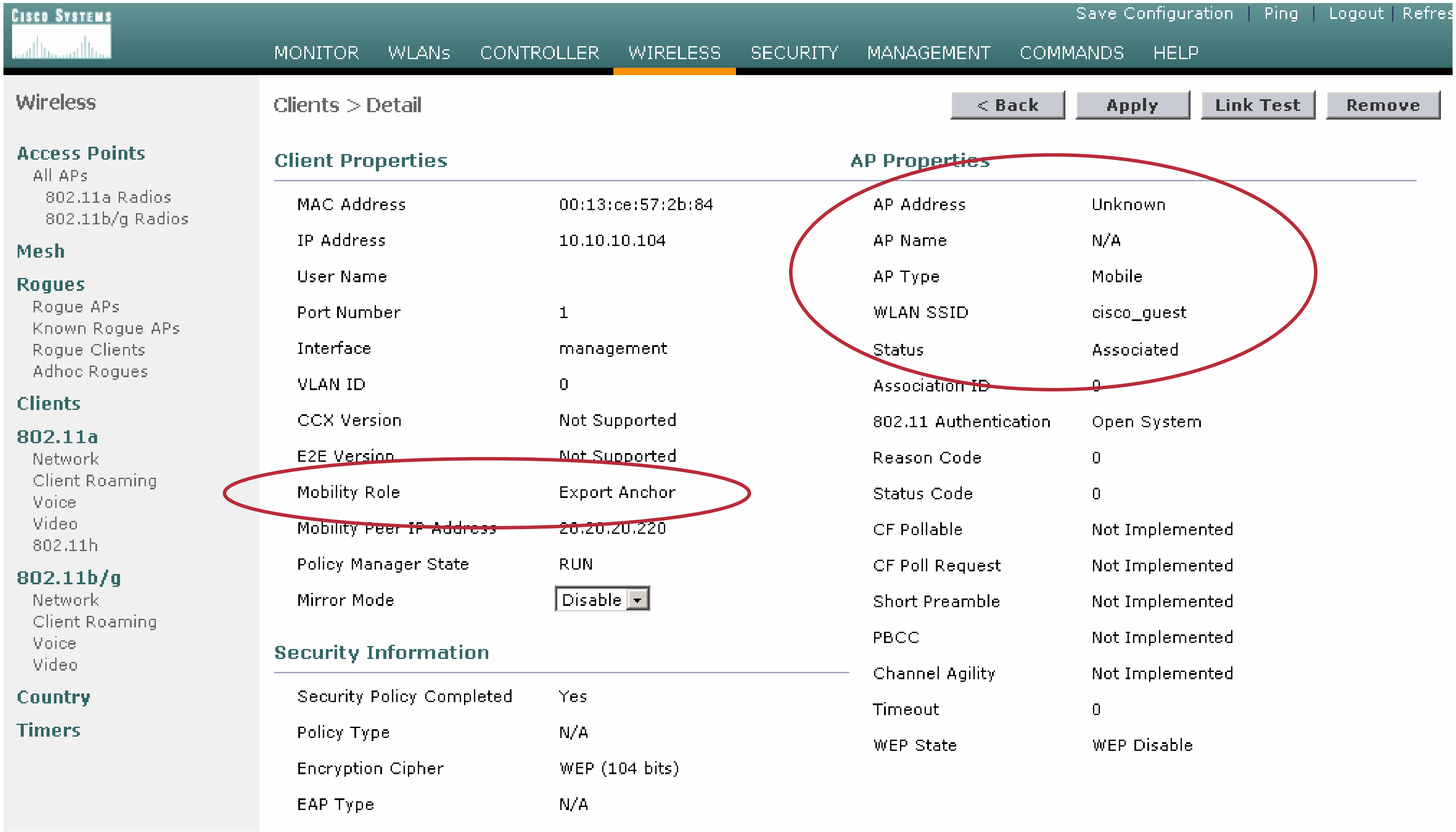
Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	WEP (104 bits)
EAP Type	N/A

AP Properties

AP Address	00:0b:85:54:c2:80
AP Name	ap:54:c2:80
AP Type	802.11g
WLAN SSID	cisco_guest
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

In the WLC GUI, go to: Wireless | Clients and select Details for the client of choice.

Client Record in the DMZ (Anchor) WLC



Clients > Detail

Client Properties

MAC Address	00:13:ce:57:2b:84
IP Address	10.10.10.104
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Export Anchor
Mobility Peer IP Address	20.20.20.220
Policy Manager State	RUN
Mirror Mode	Disable

Security Information

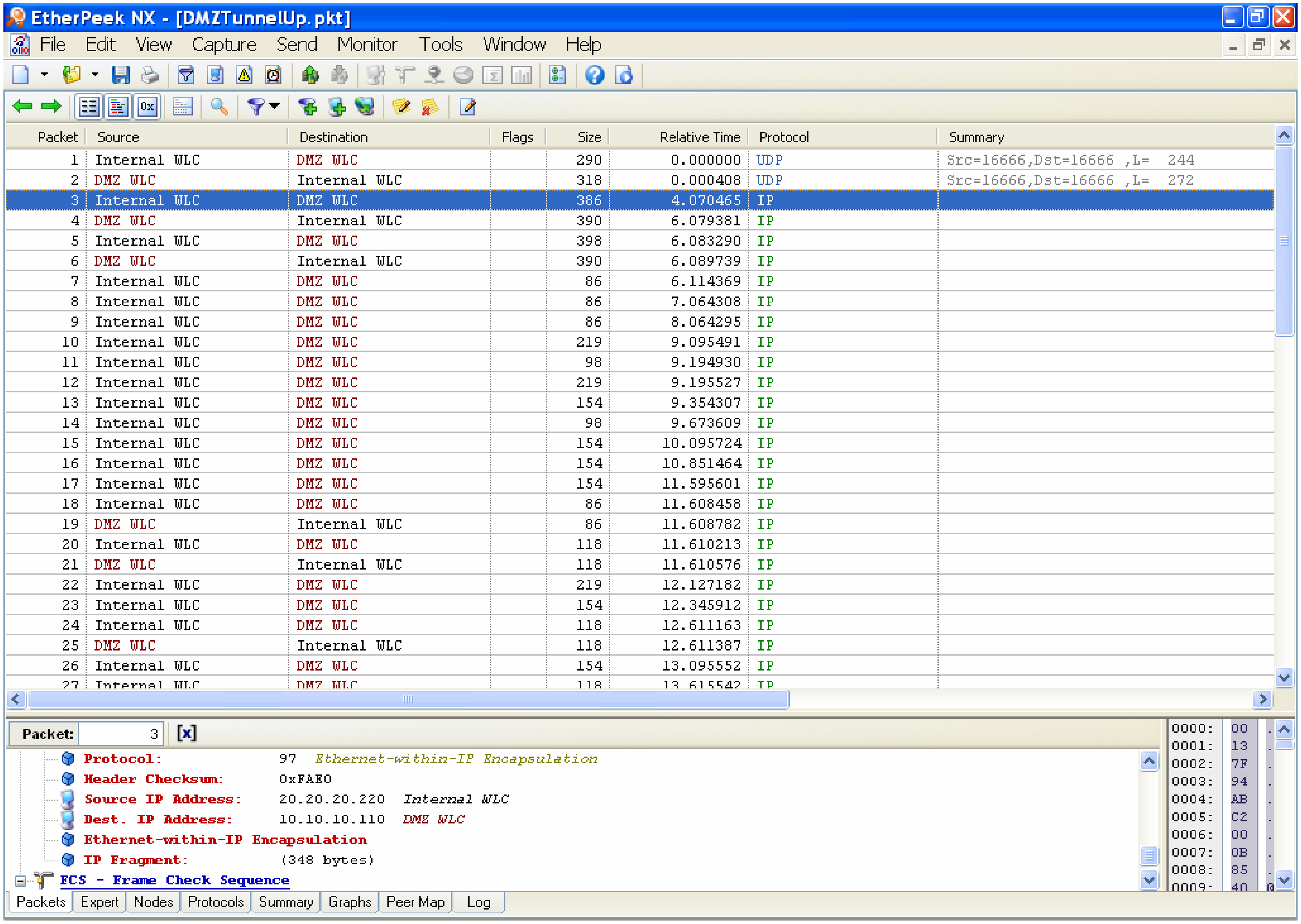
Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	WEP (104 bits)
EAP Type	N/A

AP Properties

AP Address	Unknown
AP Name	N/A
AP Type	Mobile
WLAN SSID	cisco_guest
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

In the WLC GUI, go to: Wireless | Clients and select Details for the client of choice.

Proper Guest Tunnel Operation


EtherPeek NX - [DMZTunnelUp.pkt]
File Edit View Capture Send Monitor Tools Window Help

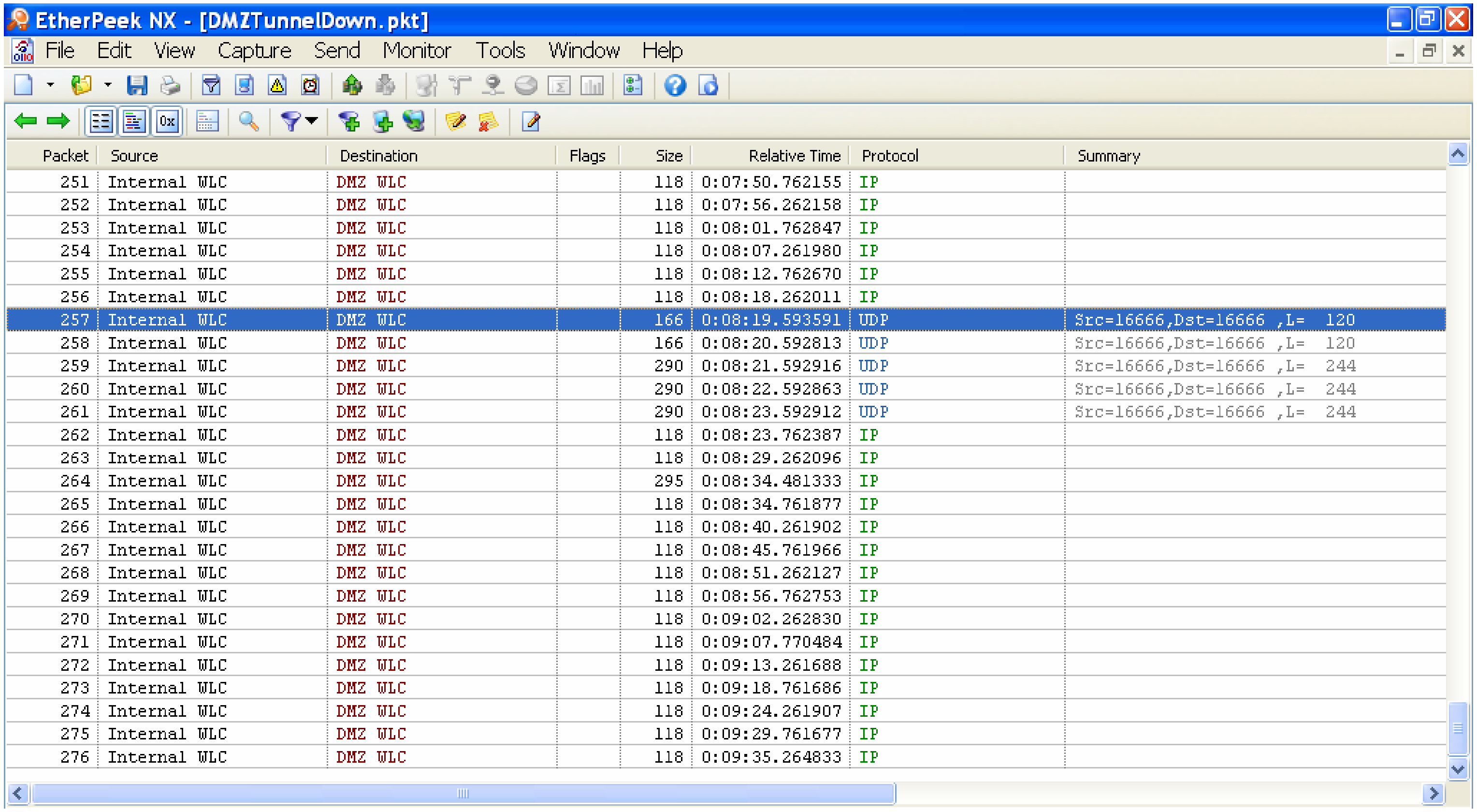
Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1	Internal WLC	DMZ WLC		290	0.000000	UDP	Src=16666,Dst=16666 ,L= 244
2	DMZ WLC	Internal WLC		318	0.000408	UDP	Src=16666,Dst=16666 ,L= 272
3	Internal WLC	DMZ WLC		386	4.070465	IP	
4	DMZ WLC	Internal WLC		390	6.079381	IP	
5	Internal WLC	DMZ WLC		398	6.083290	IP	
6	DMZ WLC	Internal WLC		390	6.089739	IP	
7	Internal WLC	DMZ WLC		86	6.114369	IP	
8	Internal WLC	DMZ WLC		86	7.064308	IP	
9	Internal WLC	DMZ WLC		86	8.064295	IP	
10	Internal WLC	DMZ WLC		219	9.095491	IP	
11	Internal WLC	DMZ WLC		98	9.194930	IP	
12	Internal WLC	DMZ WLC		219	9.195527	IP	
13	Internal WLC	DMZ WLC		154	9.354307	IP	
14	Internal WLC	DMZ WLC		98	9.673609	IP	
15	Internal WLC	DMZ WLC		154	10.095724	IP	
16	Internal WLC	DMZ WLC		154	10.851464	IP	
17	Internal WLC	DMZ WLC		154	11.595601	IP	
18	Internal WLC	DMZ WLC		86	11.608458	IP	
19	DMZ WLC	Internal WLC		86	11.608782	IP	
20	Internal WLC	DMZ WLC		118	11.610213	IP	
21	DMZ WLC	Internal WLC		118	11.610576	IP	
22	Internal WLC	DMZ WLC		219	12.127182	IP	
23	Internal WLC	DMZ WLC		154	12.345912	IP	
24	Internal WLC	DMZ WLC		118	12.611163	IP	
25	DMZ WLC	Internal WLC		118	12.611387	IP	
26	Internal WLC	DMZ WLC		154	13.095552	IP	
27	Internal WLC	DMZ WLC		118	13.615542	IP	

Packet: 3 [x]

```
Protocol:               97  Ethernet-within-IP Encapsulation
Header Checksum:        0xFAE0
Source IP Address:      20.20.20.220  Internal WLC
Dest. IP Address:       10.10.10.110  DMZ WLC
Ethernet-within-IP Encapsulation
IP Fragment:            (348 bytes)
FCS - Frame Check Sequence
```

```
0000:  00
0001:  13
0002:  7F
0003:  94
0004:  AB
0005:  C2
0006:  00
0007:  0B
0008:  85
0009:  40
```

Broken Guest Tunnel



Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
251	Internal WLC	DMZ WLC		118	0:07:50.762155	IP	
252	Internal WLC	DMZ WLC		118	0:07:56.262158	IP	
253	Internal WLC	DMZ WLC		118	0:08:01.762847	IP	
254	Internal WLC	DMZ WLC		118	0:08:07.261980	IP	
255	Internal WLC	DMZ WLC		118	0:08:12.762670	IP	
256	Internal WLC	DMZ WLC		118	0:08:18.262011	IP	
257	Internal WLC	DMZ WLC		166	0:08:19.593591	UDP	Src=16666,Dst=16666 ,L= 120
258	Internal WLC	DMZ WLC		166	0:08:20.592813	UDP	Src=16666,Dst=16666 ,L= 120
259	Internal WLC	DMZ WLC		290	0:08:21.592916	UDP	Src=16666,Dst=16666 ,L= 244
260	Internal WLC	DMZ WLC		290	0:08:22.592863	UDP	Src=16666,Dst=16666 ,L= 244
261	Internal WLC	DMZ WLC		290	0:08:23.592912	UDP	Src=16666,Dst=16666 ,L= 244
262	Internal WLC	DMZ WLC		118	0:08:23.762387	IP	
263	Internal WLC	DMZ WLC		118	0:08:29.262096	IP	
264	Internal WLC	DMZ WLC		295	0:08:34.481333	IP	
265	Internal WLC	DMZ WLC		118	0:08:34.761877	IP	
266	Internal WLC	DMZ WLC		118	0:08:40.261902	IP	
267	Internal WLC	DMZ WLC		118	0:08:45.761966	IP	
268	Internal WLC	DMZ WLC		118	0:08:51.262127	IP	
269	Internal WLC	DMZ WLC		118	0:08:56.762753	IP	
270	Internal WLC	DMZ WLC		118	0:09:02.262830	IP	
271	Internal WLC	DMZ WLC		118	0:09:07.770484	IP	
272	Internal WLC	DMZ WLC		118	0:09:13.261688	IP	
273	Internal WLC	DMZ WLC		118	0:09:18.761686	IP	
274	Internal WLC	DMZ WLC		118	0:09:24.261907	IP	
275	Internal WLC	DMZ WLC		118	0:09:29.761677	IP	
276	Internal WLC	DMZ WLC		118	0:09:35.264833	IP	

- **The inter-WLC control and data planes will look identical for both Mobility and Guest Tunneling functions, except with Mobility, the Ethernet-over-IP data tunnel is asymmetric and will only flow from Anchor controller to Foreign controller**

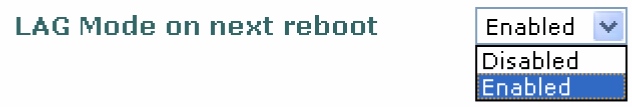
Link Aggregation

- LAG binds all WLC ports into one logical interface
- No need for additional AP Managers
- If WLC ports or switch ports fail, the remaining working ports will continue to operate in the LAG group
- Both the WLC and the upstream switch need to be configured to operate using Link Aggregation

Link Aggregation

- In the WLC

```
(WLC_CLI) >config lag enable
```



LAG Mode on next reboot

In the WLC GUI, go to: Controller | General and select 'enable'. A WLC reboot is required to enact changes.

- In the upstream Cisco L2/L3 switch

```
Configure terminal
interface port-channel <id>
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk native vlan <native vlan id>
   switchport trunk allowed vlan <allowed vlans>
   switchport mode trunk
   no shutdown
interface GigabitEthernet <interface id>
   switchport
   Channel-group <id> mode on
   No shutdown
```

NOTE: Individual interfaces' 'channel-group' IDs needs to match the desired 'port-channel' ID number.

Do this for each interface that connects to the WLC

Troubleshooting 802.11 Wireless LANs Agenda

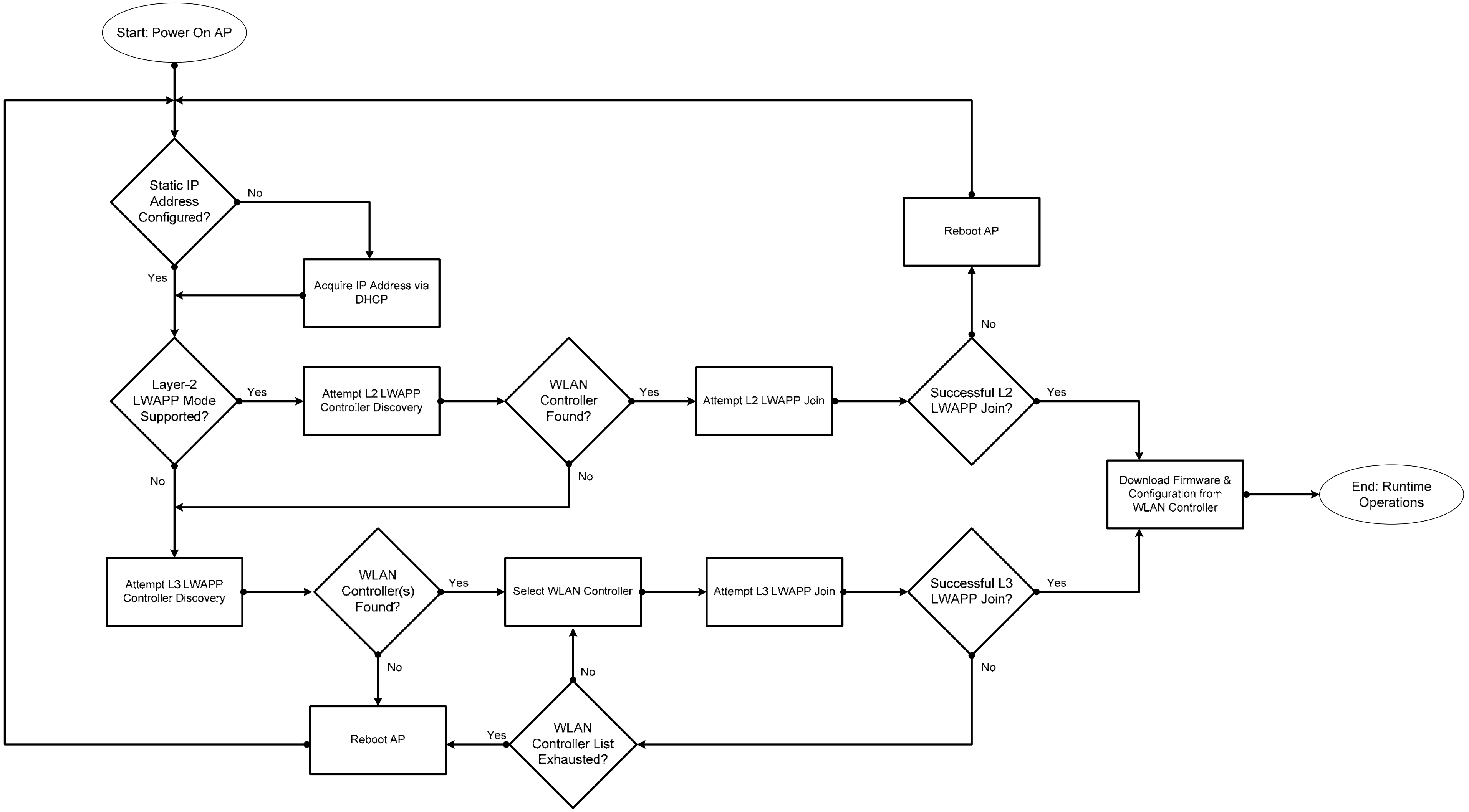
- Review: Cisco’s Unified Architecture

- Debugging and Troubleshooting
  - Wireless LAN Controllers (WLCs)
  - Access Points

LWAPP AP/WLC Discovery Process

- **Every LWAPP AP requires connectivity with a controller to provide wireless service and allow for configuration**
- **LWAPP specifies a process by which this AP / WLC Discovery process occurs**
    - **Hunting Algorithm**
    - **Discovery Algorithm**
    - **Join Process**

WLAN Controller Hunt, Discovery, Join Flowchart


Start: Power On AP
Static IP Address Configured?
No
Yes
Acquire IP Address via DHCP
Layer-2 LWAPP Mode Supported?
Yes
No
Attempt L2 LWAPP Controller Discovery
WLAN Controller Found?
Yes
No
Attempt L2 LWAPP Join
Successful L2 LWAPP Join?
Yes
No
Reboot AP
Download Firmware & Configuration from WLAN Controller
End: Runtime Operations
Attempt L3 LWAPP Controller Discovery
WLAN Controller(s) Found?
Yes
No
Select WLAN Controller
Attempt L3 LWAPP Join
Successful L3 LWAPP Join?
Yes
No
WLAN Controller List Exhausted?
Yes
No
Reboot AP

WLAN Controller Hunting Algorithm

1. Power on the AP
2. If a static IP address has not been previously configured, the AP issues a DHCP DISCOVER to get an IP address
3. If L2 mode is supported, attempt an L2 LWAPP WLAN Controller Discovery (Ethernet broadcast)
4. If L2 mode is not supported or step 3 fails to find a WLAN controller, attempt an L3 LWAPP WLAN Controller Discovery
5. If step 4 fails, reboot and return to step 1

LWAPP L3 WLAN Controller Discovery Algorithm

AP goes through the following steps to compile a single **LIST OF WLAN CONTROLLERS**

1. LWAPP Discovery broadcast on local subnet
2. Over-the-Air Provisioning (OTAP)
3. Locally stored controller IP addresses
4. DHCP vendor specific option 43 (IP Address should be "Management Interface" IP)
5. DNS resolution of "CISCO-LWAPP-CONTROLLER.localdomain"(should resolve to the "Management Interface" IP)
6. If no controller found, start over…

L3 LWAPP WLAN Controller Discovery Algorithm

- Once a list of WLAN Controllers is compiled, the AP sends a unicast LWAPP Discovery Request message to EACH OF THE CONTROLLERS IN THE LIST
- WLAN Controllers receiving the LWAPP discovery messages respond with an LWAPP Discovery Response
- LWAPP Discovery Response contains important information:

  Controller name, controller type, AP capacity, current AP load, “Master Controller” status, AP-Manager IP address

- AP waits for its “Discovery Interval” to expire, then selects a controller and sends an LWAPP 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 (specified in the Controller “name” field in the LWAPP Discovery Response)**
  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.**

     This last step provides the whole system with automatic AP/WLC load-balancing functionality.

WLAN Controller Join Process—Mutual Authentication

- **AP LWAPP Join Request contains AP's signed X.509 certificate**
- **WLAN Controller validates the certificate before sending an LWAPP Join Response**
  - **Manufacture Installed Certificate (MIC)—Cisco 1000 Series, all Cisco Aironet APs manufactured after July 18, 2005**
  - **Self-Signed Certificate (SSC)—LWAPP Upgraded Cisco Aironet APs manufactured prior to July 18, 2005**
  - **SSC APs must be "authorized" on the WLAN Controller**
- **If AP is validated, the WLAN Controller sends the LWAPP 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 LWAPP-based APs

- Converting Aironet APs to support LWAPP
  - Supported APs:
    - All 1131 and 1242
    - 1200-series APs with 802.11g or new 802.11a
    - 1100-series APs with 802.11g
    - 1300-series Outdoor AP (AP mode only)
- Certificate Types
  - Self-signed Certificate (SSC)
  - Manufacturer-installed Certificate (MIC)
    - Note the 'AP' vs 'LAP' in Access Point part numbers

NOTE: 1000-Series APs will only ever 'speak' LWAPP, requiring a controller

Troubleshooting LWAPP-based APs

- **Check the basics first**

  Can the AP and the WLC communicate?

  Make sure the AP is getting an address from DHCP (check the DHCP server leases for the AP’s MAC address)

  If the AP’s address is statically set, ensure it is correctly configured

  Try pinging from controller to AP and from AP to 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

NOTE: **APs with serial ports can have a WLC IP address input manually (this is particularly useful for H-REAPs and other APs where discovery mechanisms might not be available.**

```
(AP_CLI)#debug lwapp console client
```
(this prevents the AP from rebooting)

```
(AP_CLI)#lwapp ap controller ip <controller ip address>
```
(new in 4.0)

Successful LWAPP AP Join

```
(WLC_CLI) >debug mac addr 00:0b:85:54:ce:00
(WLC_CLI) >debug lwapp events enable
[TIME]: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:54:ce:00 to 00:0b:85:40:4a:c0 on port '29'
[TIME]: Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:54:ce:00 on Port 29
[TIME]: Received LWAPP JOIN REQUEST from AP 00:0b:85:54:ce:00 to 06:0a:20:20:00:00 on port '29'
[TIME]: LWAPP Join-Request MTU path from AP 00:0b:85:54:ce:00 is 1500, remote debug mode is 0
[TIME]: Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:54:ce:00
[TIME]: Register LWAPP event for AP 00:0b:85:54:ce:00 slot 0
[TIME]: Register LWAPP event for AP 00:0b:85:54:ce:00 slot 1
[TIME]: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:54:ce:00 to  00:0b:85:40:4a:cb
[TIME]: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -A
[TIME]: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -A
[TIME]: Successfully transmission of LWAPP Config-Message to AP 00:0b:85:54:ce:00
[TIME]: Running spamEncodeCreateVapPayload for SSID ‘cisco-guest‘
[TIME]: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:54:ce:00
[TIME]: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:54:ce:00
[TIME]: Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:54:ce:00
[TIME]: Received LWAPP Up event for AP 00:0b:85:54:ce:00 slot 0!
[TIME]: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:54:ce:00
[TIME]: Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:54:ce:00
[TIME]: Received LWAPP Up event for AP 00:0b:85:54:ce:00 slot 1!
```

Failed LWAPP AP Authentication

```
(WLC_CLI)>debug mac addr 00:12:80:ad:7a:9c
(WLC_CLI)>debug lwapp events enable
[TIME]: Received LWAPP DISCOVERY REQUEST from AP 00:12:80:ad:7a:9c to ff:ff:ff:ff:ff:ff on port '1'
[TIME]: Successful transmission of LWAPP Discovery-Response to AP 00:12:80:ad:7a:9c on Port 1
[TIME]: Received LWAPP JOIN REQUEST from AP 00:12:80:ad:7a:9c to 06:0a:10:10:00:00 on port '1'
[TIME]: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP
    00:12:80:ad:7a:9c.
[TIME]: Unable to free public key for AP  00:12:80:AD:7A:9C
[TIME]: DEBU CTRLR spamProcessJoinRequest:1574 spamProcessJoinRequest : spamDecodeJoinReq failed
```

Set the WLC's time!

- **The #1 reason APs fail to join is inaccurate controller 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!

NOTE: In the US, your APs' regulatory coding is '– A', NOT '– N'!!!

```
(WLC_CLI) >debug mac addr 00:12:80:ad:7a:9c
(WLC_CLI) >debug lwapp events enable
<SNIP> LWAPP Discovery Request/Reply and Join Request/Reply </SNIP>
[TIME]: * apfSpamProcessStateChange:1522 Register LWAPP event for AP 00:12:80:ad:7a:9c slot 0
[TIME]: * apfSpamProcessStateChange:1522 Register LWAPP event for AP 00:12:80:ad:7a:9c slot 1
[TIME]: * spamHandleLradMsg:599 Received LWAPP CONFIGURE REQUEST from AP 00:12:80:ad:7a:9c to  00:0b:85:40:7a:03
[TIME]: * spamProcessApIpAddrPayload:16133 Updating IP info for AP 00:12:80:ad:7a:9c -- static 0, 20.20.20.135/255.255.255.0, gtw 20.20.20.1
[TIME]: * spamUpdateRcbLradIp:334 Updating IP 20.20.20.135 ===> 20.20.20.135 for AP 00:12:80:ad:7a:9c
[TIME]: DEBU CTRLR spamVerifyRegDomain:6167 spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -JP
[TIME]: * spamVerifyRegDomain:6202 AP 00:12:80:ad:7a:9c 80211bg Regulatory Domain (-A) does not match with country (JP)  reg. domain -JP for slot 0
[TIME]: DEBU CTRLR spamVerifyRegDomain:6167 spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -J
[TIME]: * spamVerifyRegDomain:6202 AP 00:12:80:ad:7a:9c 80211a Regulatory Domain (-A) does not match with country (JP)  reg. domain -JP for slot 1
[TIME]: DEBU CTRLR spamVerifyRegDomain:6210 spamVerifyRegDomain AP RegDomain check for the country JP  failed
[TIME]: * spamProcessConfigRequest:1730 AP 00:12:80:ad:7a:9c: Regulatory Domain check Completely FAILED. The AP will not be allowed to join.
[TIME]: * apfSpamProcessStateChangeInSpamContext:1556 apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP
      00:12:80:ad:7a:9c slot 0
[TIME]: * apfSpamProcessStateChangeInSpamContext:1556 apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP
      00:12:80:ad:7a:9c slot 1
[TIME]: * apfSpamProcessStateChange:1530 Deregister LWAPP event for AP 00:12:80:ad:7a:9c slot 0
[TIME]: * apfSpamProcessStateChange:1530 Deregister LWAPP event for AP 00:12:80:ad:7a:9c slot 1
* <SNIP> DEBU STA 00:12:80:ad:7a:9c</SNIP>
```

- The Fix?
  - Make sure you match your APs' regulatory domain with your WLCs'.
- How do you know how to make sure you do?
  - Go to: www.cisco.com/warp/public/779/smbiz/wireless/approvals.html

Authorizing Bridge and Mesh APs

```
(WLC_CLI) >debug mac addr 00:0b:85:54:dc:e0
(WLC_CLI) >debug lwapp events enable
[TIME]: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:54:dc:e0 to ff:ff:ff:ff:ff:ff on port '1'
[TIME]: Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:54:dc:e0 on Port 1
[TIME]: Received LWAPP JOIN REQUEST from AP 00:0b:85:54:dc:e0 to 00:0b:85:33:18:40 on port '1'
[TIME]: LWAPP Join-Request AUTH_STRING_PAYLOAD, invalid BRIDGE key hash AP 00:0b:85:54:dc:e0
[TIME]: LWAPP Join-Request Bridge Authentication Failed for AP 00:0b:85:54:dc:e0
[TIME]: Unable to free public key for AP  00:0B:85:54:DC:E0
[TIME]: spamDeleteLCB: stats timer not initialized for AP 00:0b:85:54:dc:e0
[TIME]: spamProcessJoinRequest : spamDecode JoinReq failed
```

The Fix?

- `(WLC_CLI) >config auth-list add mic 00:0b:85:54:dc:e0`

Remember: All Bridge and Mesh APs need to have their MAC addresses entered in all controllers to be allowed to join the network.

AP CLI Commands

- **New CLI commands have been added to APs in the 4.0 release to add deployment flexibility (available only on APs with console ports)**

  Set the AP's IP address

  ```
  (AP_CLI)#lwapp ap ip address <IP Address> <Subnet Mask>
  (AP_CLI)#lwapp ap ip default-gateway <IP Address>
  ```

  Set the AP's hostname

  ```
  (AP_CLI)#lwapp ap hostname <WORD>
  ```

  Set the controller to which the AP will connect (this can be used when no other controller discovery method is available)

  ```
  (AP_CLI)#lwapp ap controller ip address <IP Address>
  ```

AP/WLC Failover

- APs will failover to other WLCs if the LWAPP control plane is interrupted

  After either:

  A missed heartbeat to WLC (sent every 30 seconds)

  or

  A Non-ACK'd LWAPP control packet

  Then:

  The AP will send 5 successive heartbeats (each a second apart)

  If no reply is received, the AP/WLC path is assumed down and the AP will attempt to join another controller

- So, make sure ALL WLCs in the cluster will properly allow all APs to join

  Make sure all WLCs are set to the correct time

  Make sure all WLCs have all upgraded APs' SSC hashes

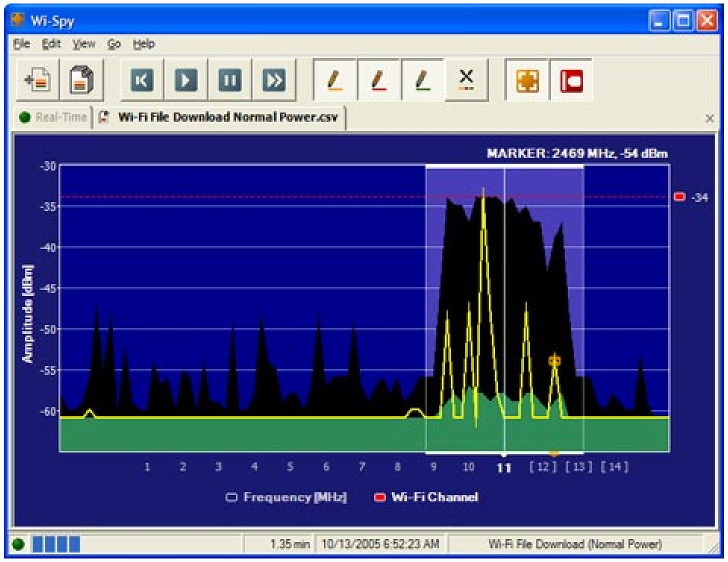
Troubleshooting 802.11 Wireless LANs Agenda

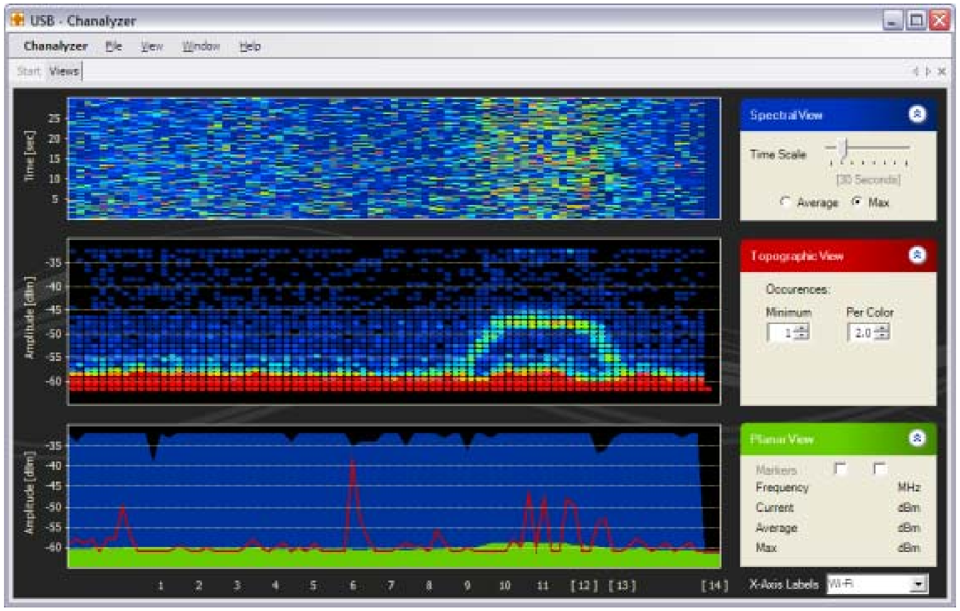
- **Review: Cisco's Unified Architecture**
- **Review: Basic System Configuration**
- **Debugging and Troubleshooting**
  - **Wireless LAN Controllers (WLCs)**
  - **Access Points**

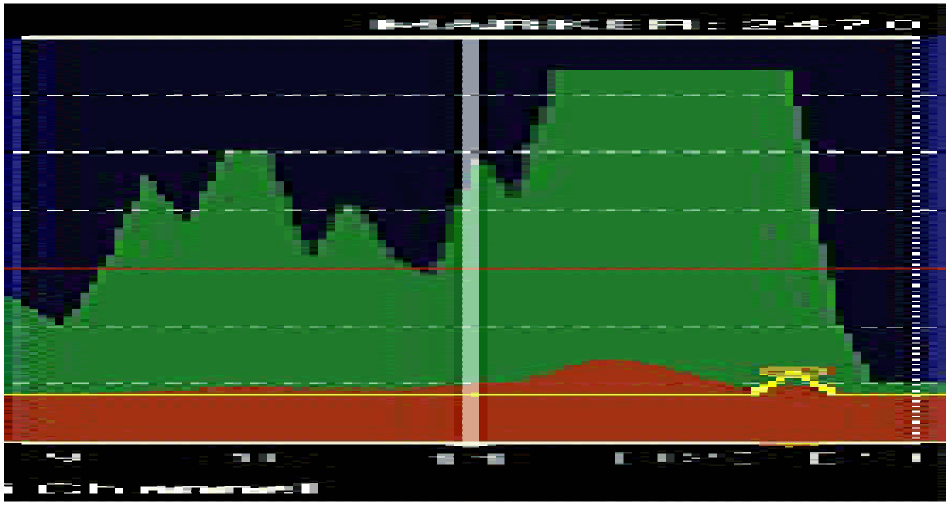
Tools of the trade…

www.Thinkgeek.com

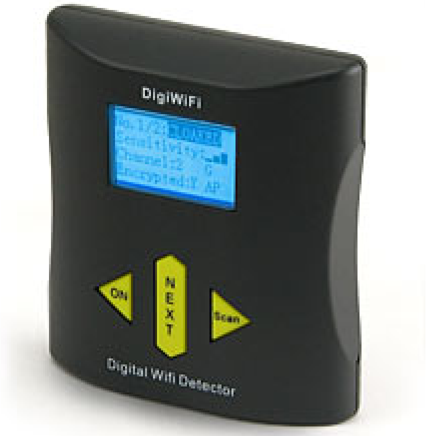
Wi-Spy Spectrum Analyzer

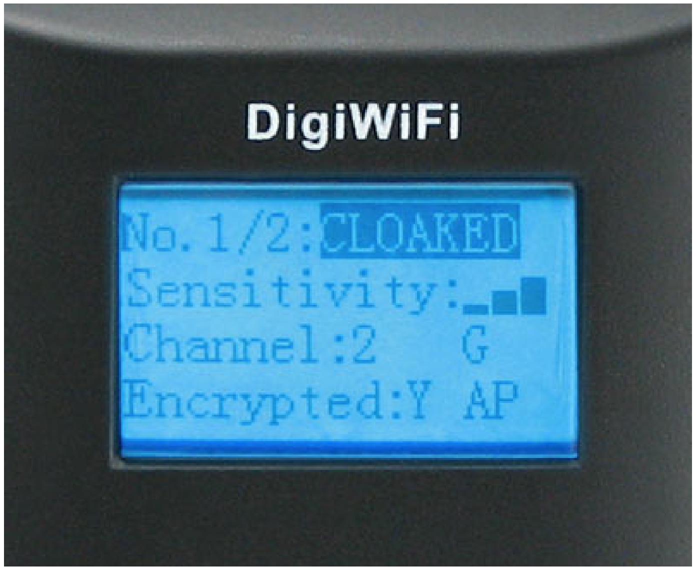






WiFi Finders

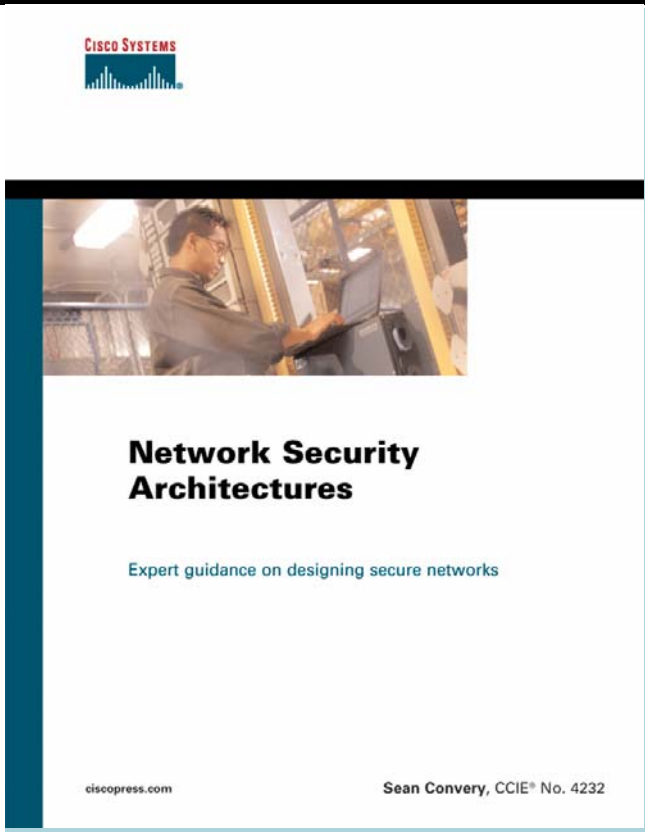




Q and A

Recommended Reading

- Continue your Networkers learning experience with further reading for this session from Cisco Press
- Check the Recommended Reading flyer for suggested books



Cisco Systems

Network Security Architectures

Expert guidance on designing secure networks

ciscopress.com

Sean Convery, CCIE® No. 4232

Available Onsite at the Cisco Company Store

Complete Your Online Session Evaluation!

- Win fabulous prizes! Give us your feedback!
- Receive 10 Passport Points for each session evaluation you fill out
- Go to the Internet stations located throughout the Convention Center
- Winners will be posted on the Internet stations and digital plasma screens
- Drawings will be held in the World of Solutions

  Monday, June 20 at 8:45 p.m.

  Tuesday, June 21 at 8:15 p.m.

  Wednesday, June 22 at 8:15 p.m.

  Thursday, June 23 at 1:30 p.m.