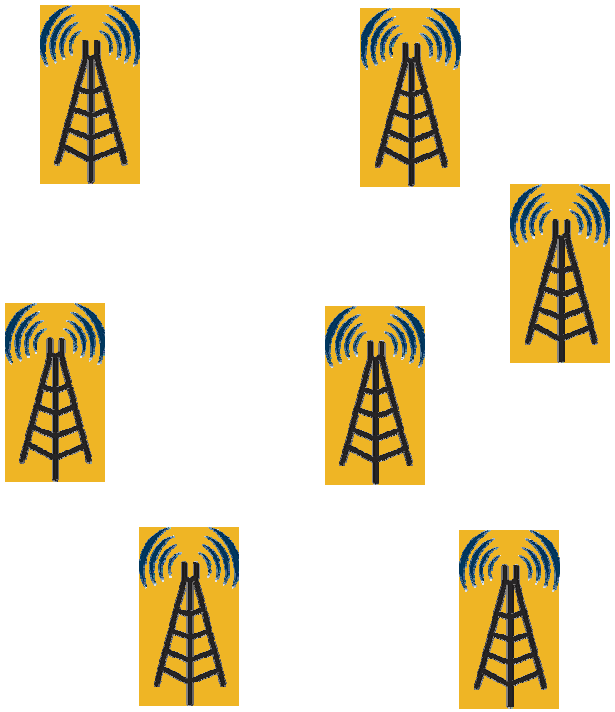
Tech Update
December 2006

Hans Donnerborg, hans@cisco.com

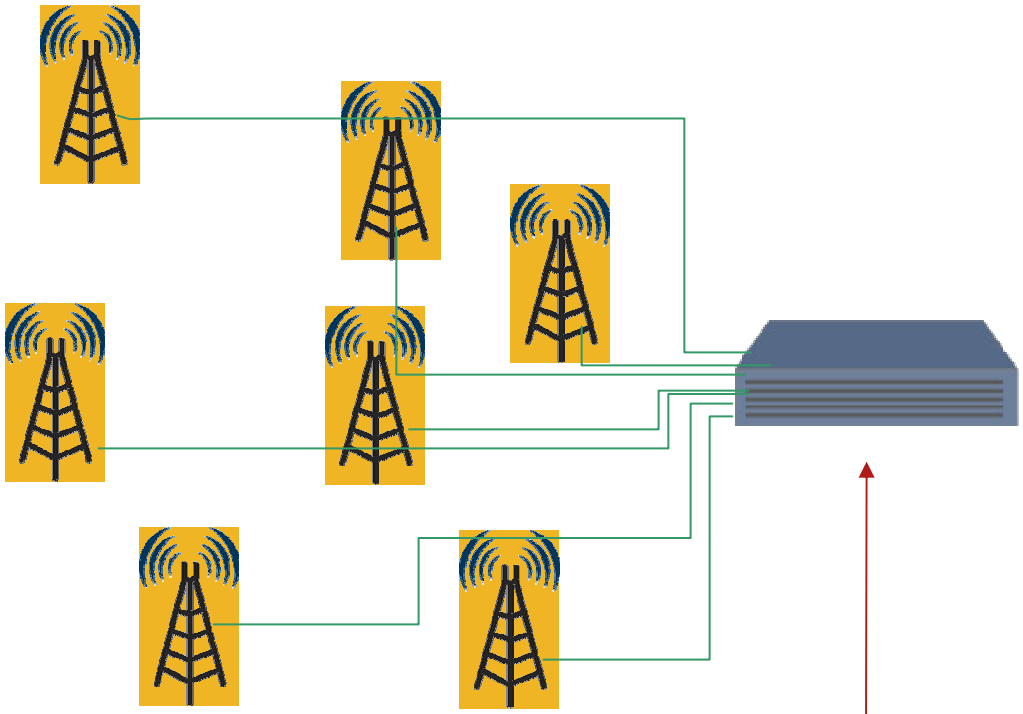
Cisco Unified Wireless Network Overview

Centralization – not a new idea



- Original cellular networks were nodal.
- Lots of call drops
- Lots of administration
- Roaming wasn't very good
- Not capable of providing advanced services

Enter the Base Station Controller

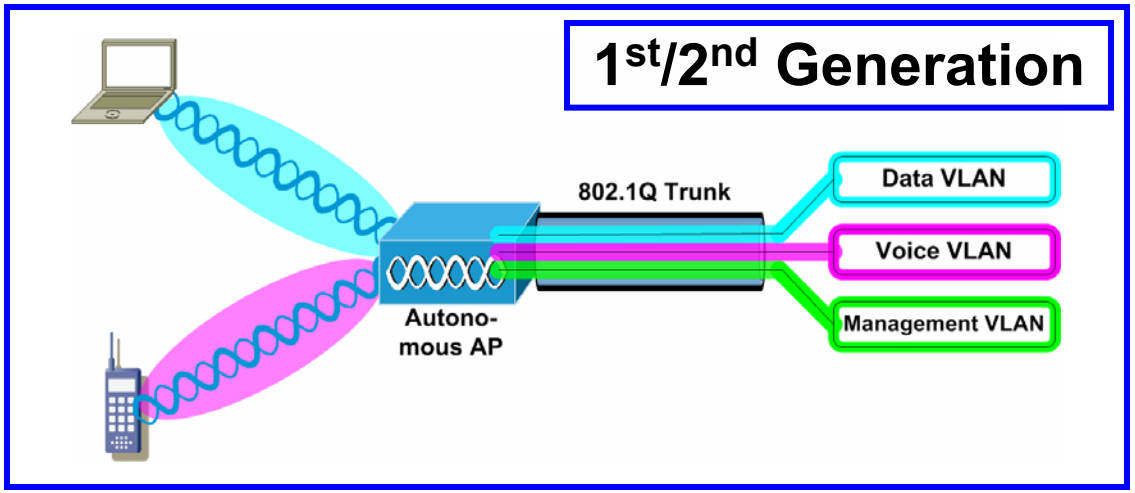


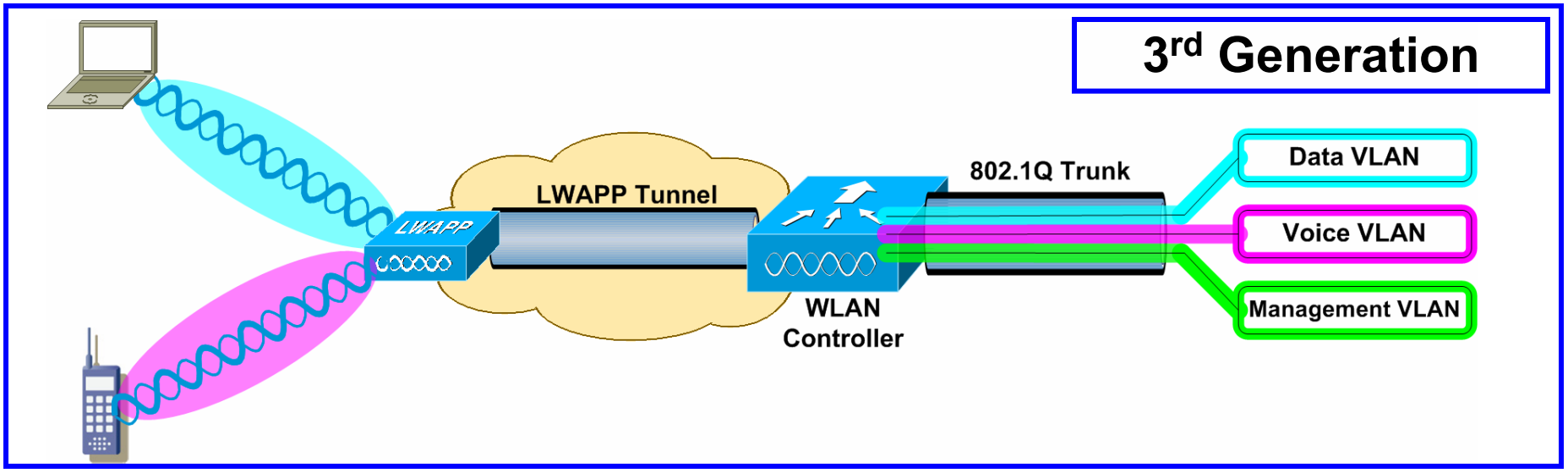
- Complete view of the network
- Improved roaming
- One point of administration
- Enabled provisioning of advanced services

Management/Control
Base stations are used to handle call setup, handovers, and other functions across an entire cellular network.

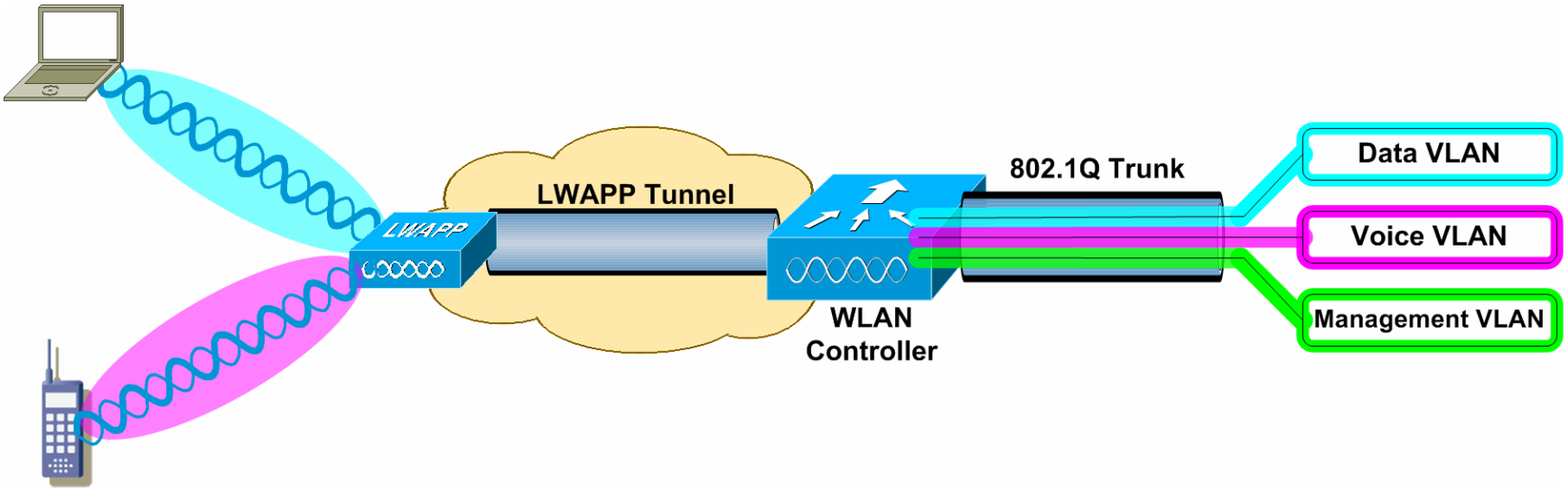
Understanding WLAN Controllers—1st/2nd Generation vs. 3rd Generation Approach

- 1st/2nd generation—APs act as 802.1Q translational bridge, putting client traffic on local VLANs
- 3rd generation—Controller bridges client traffic centrally





Understanding WLAN Controllers—The WLAN Controller as a Network Device



- WLAN Controller

  For wireless end-user devices, the controller is a 802.1Q bridge that takes traffic of the air and puts it on a VLAN

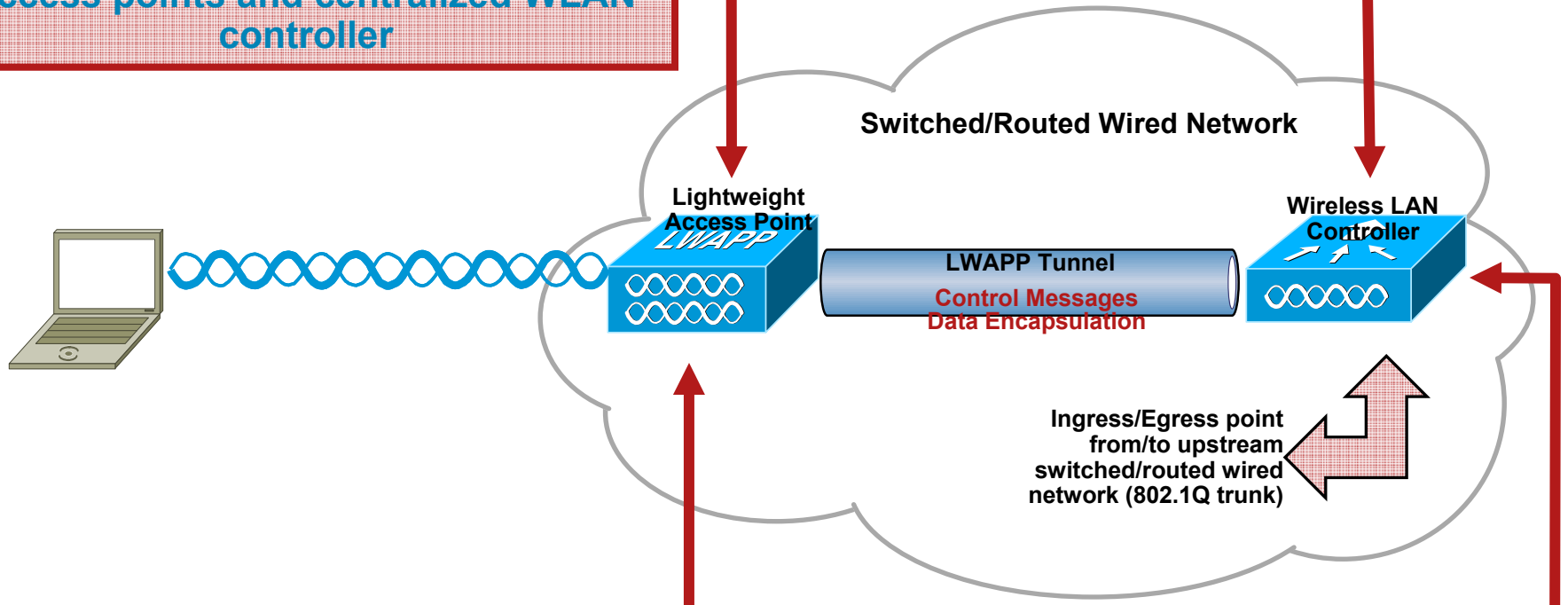
  From the perspective of the AP, the controller is an LWAPP Tunnel end-point with an IP address

  From the perspective of the network, it's a Layer-2 device connected via one or more 802.1Q trunk interfaces

- The AP connects to an access port—no concept of VLANs at the AP

Cisco Centralized WLAN Model

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



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

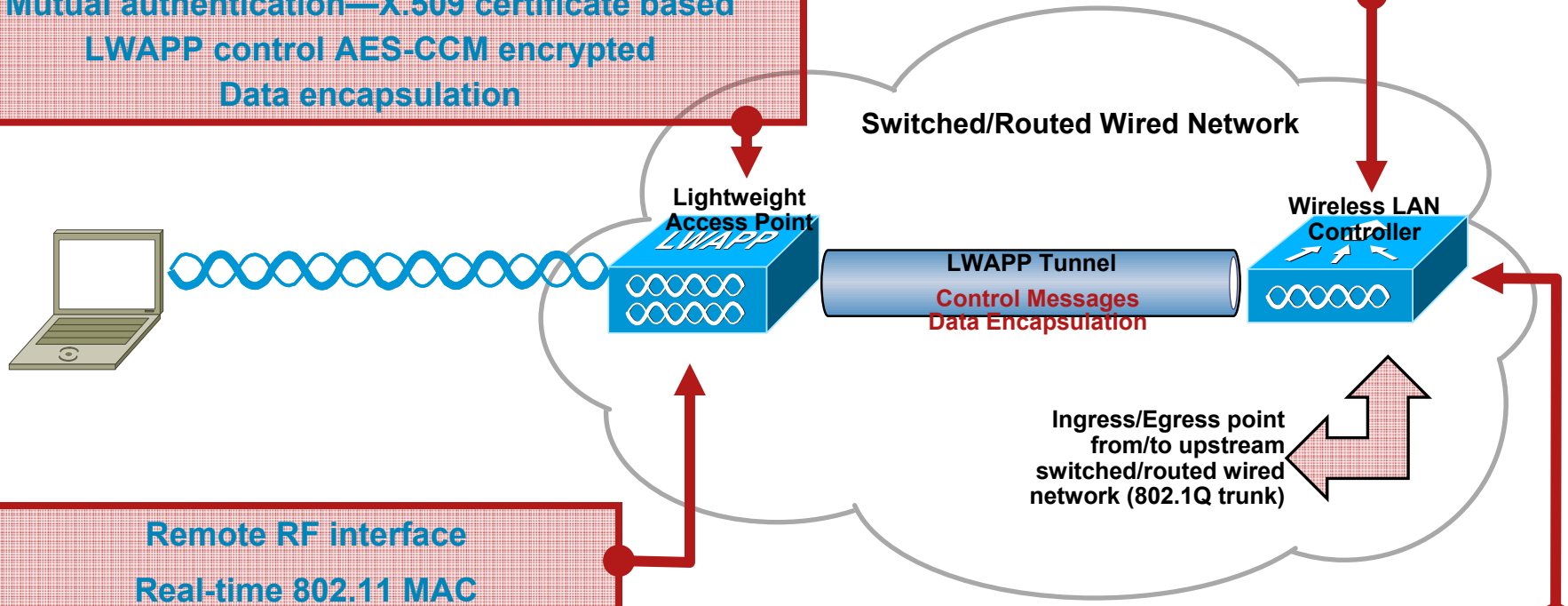
Mutual authentication—X.509 certificate based

LWAPP control AES-CCM encrypted

Data encapsulation

Radio resource management

Mobility management



Remote RF interface

Real-time 802.11 MAC

RF spectral analysis

WLAN IDS Signature analysis

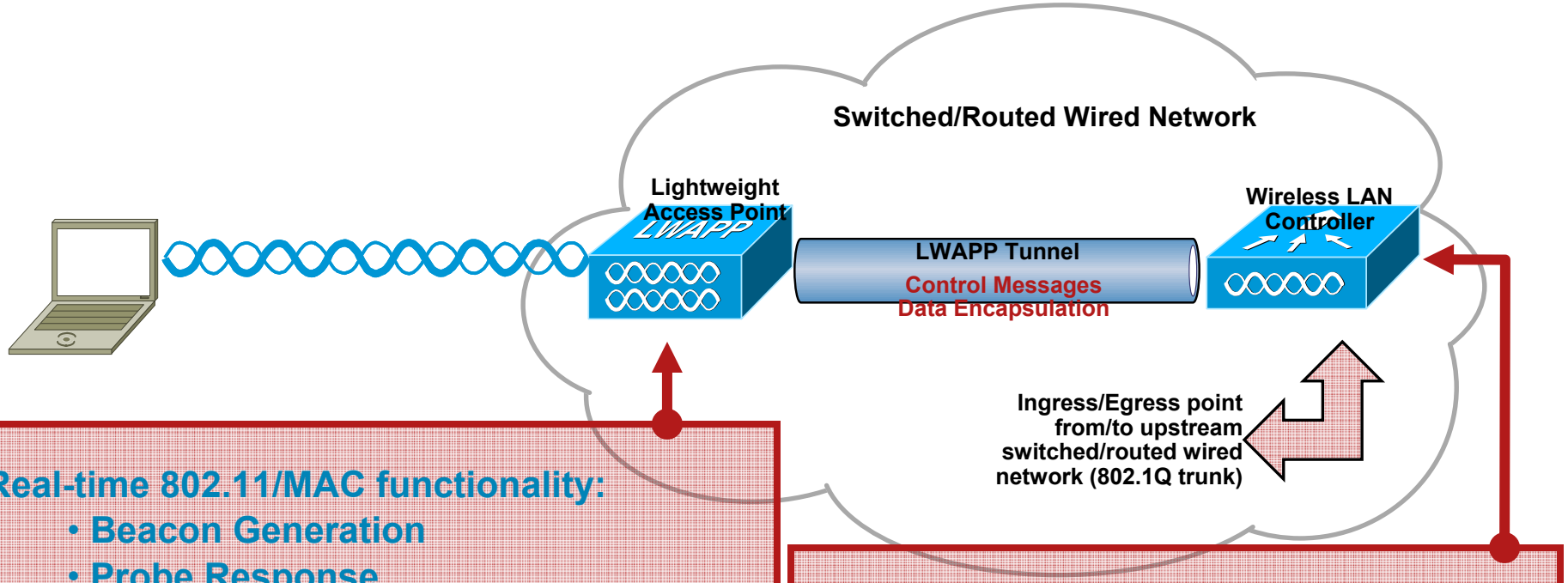
Security management

QoS policies enforcement

Centralized configuration, firmware management

Northbound management interfaces

Division of Labor—Split MAC



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

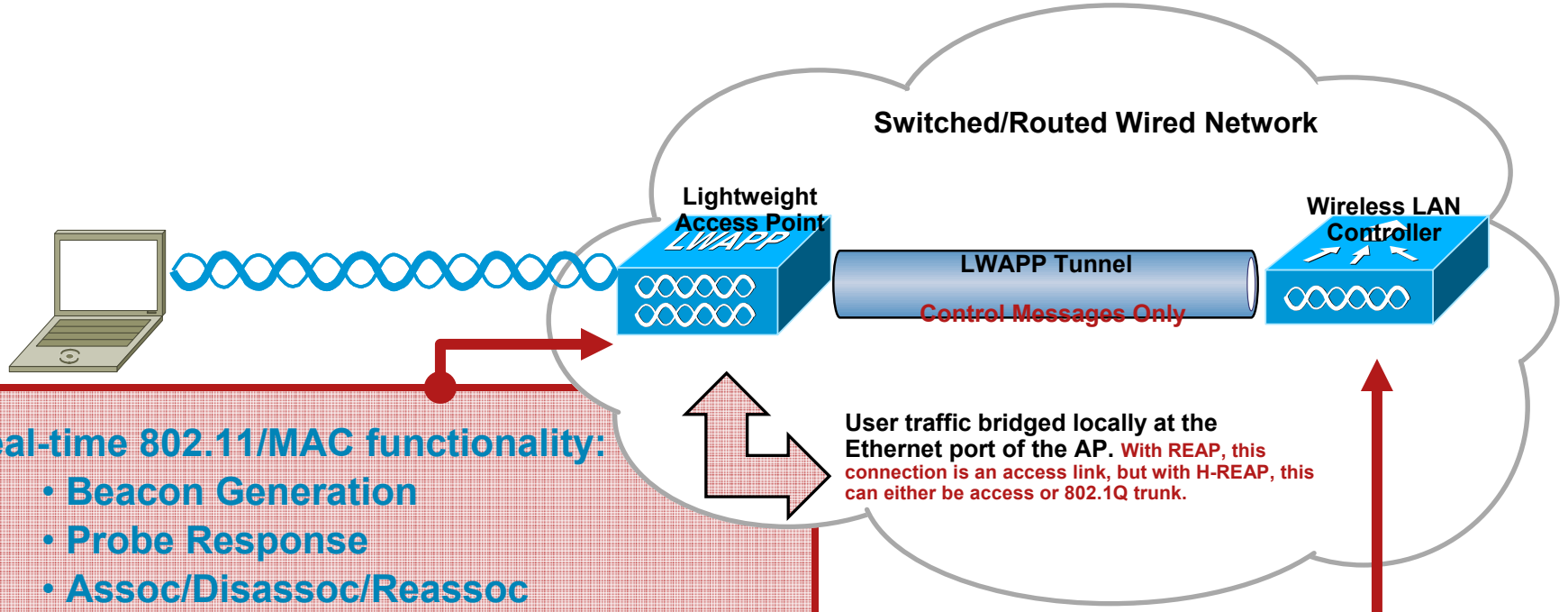
Data encapsulation/de-encapsulation
Fragmentation/De-fragmentation

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—Local MAC



Real-time 802.11/MAC functionality:

- Beacon Generation
- Probe Response
- Assoc/Disassoc/Reassoc
- 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

LWAPP State Machine (Simplified)

- LWAPP defines a state machine that governs the AP and controller behavior
- Major states:

  Discovery—AP looks for a controller

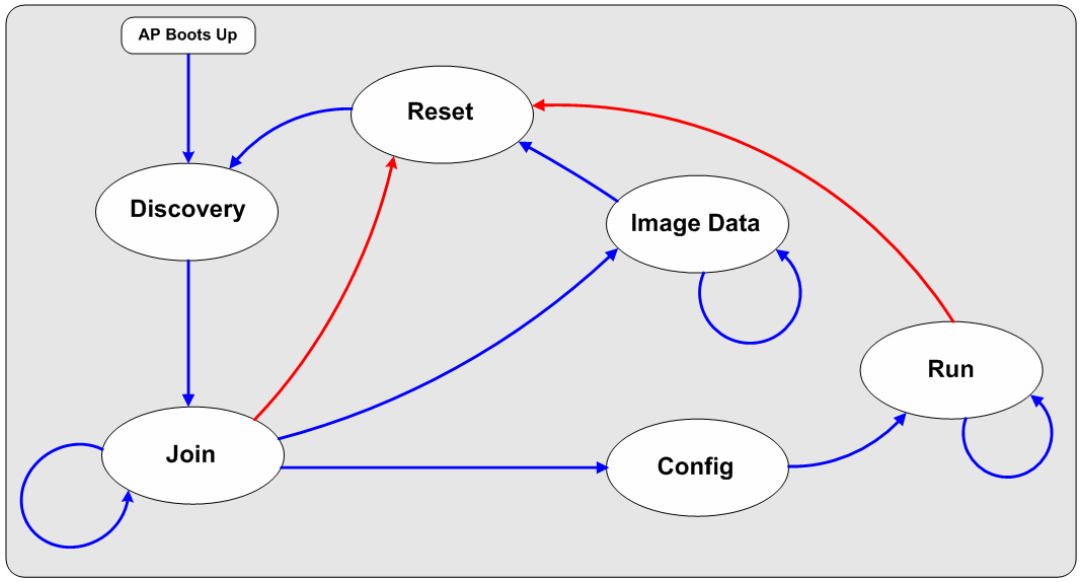
  Join—AP attempts to establish a secured relationship with a controller

  Image Data—AP downloads code from controller

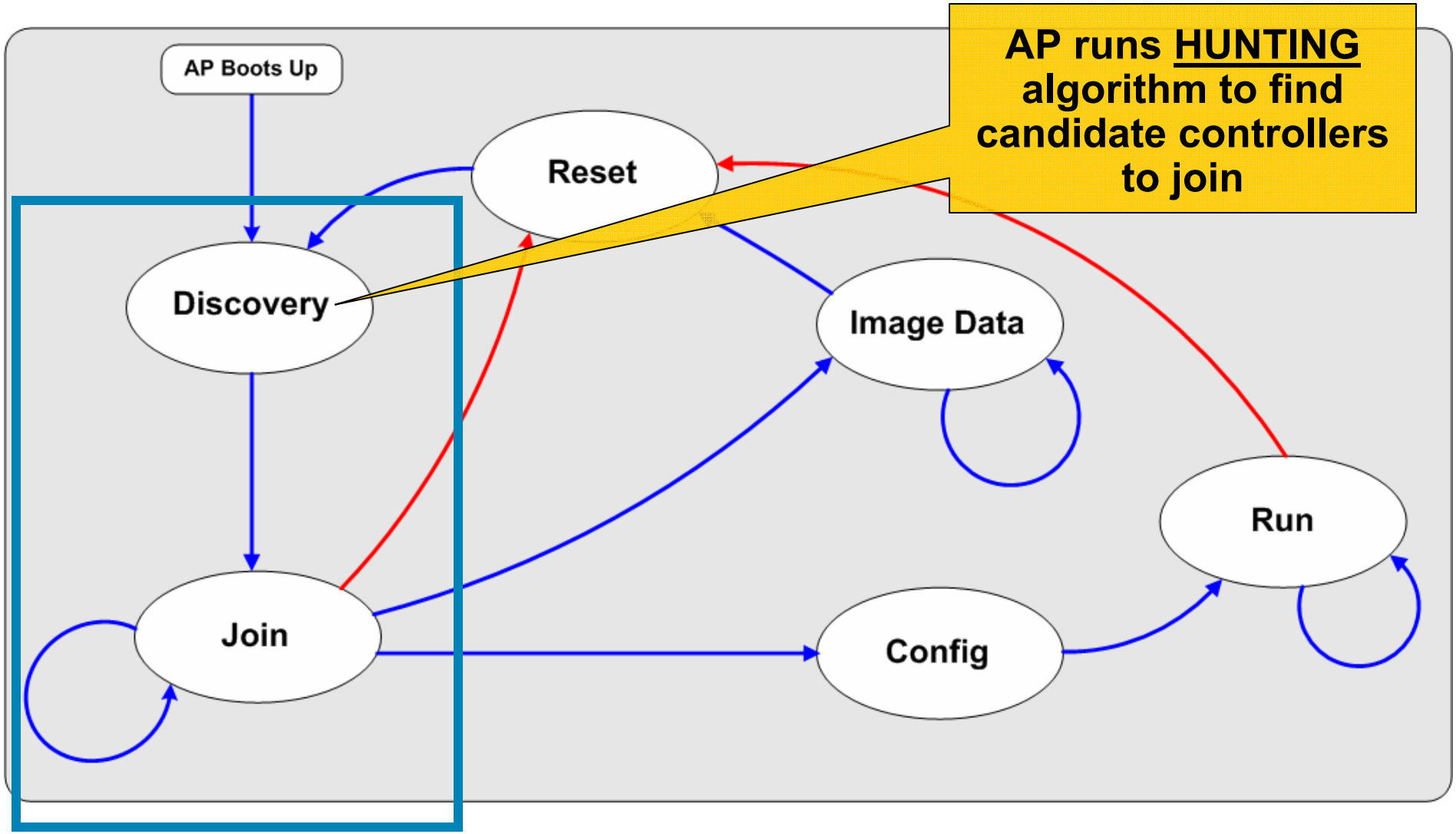
  Config—AP receives configuration from controller

  Run—AP and controller operate normally and service data

  Reset—AP clears state and starts over
- Note: LWAPP/CAPWAP RFC defines other states

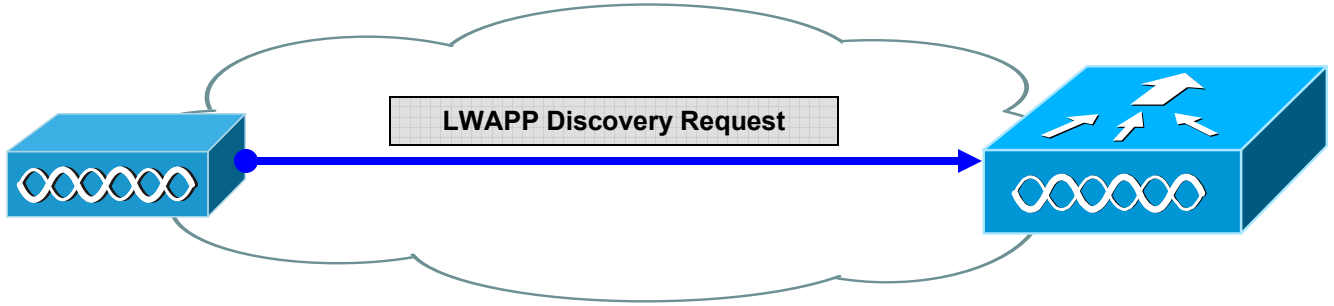


LWAPP Discovery State

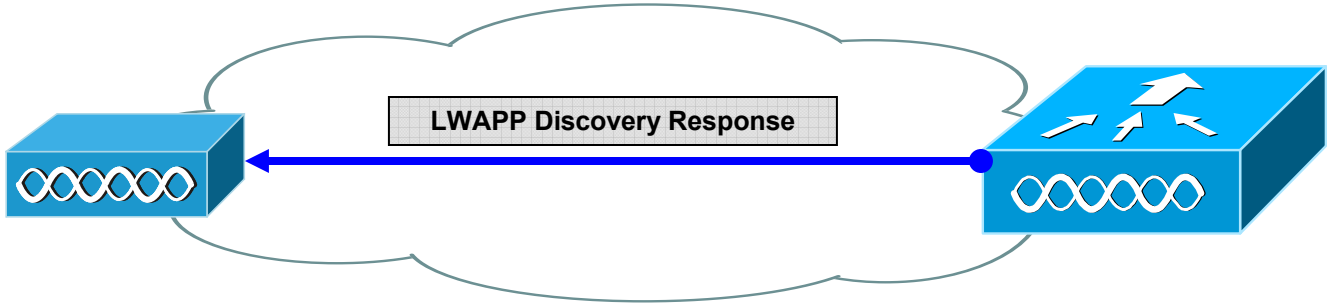


LWAPP Control Messages for Controller Hunting/Discovery

- LWAPP Discovery Request – AP issues 1 or more of these messages to find controllers (sent to Management Interface IP Address)



- LWAPP Discovery Response – Any controller receiving an LWAPP Discovery Request responds with this message to the requesting AP



WLAN Controller Hunting Algorithm

1. AP issues a DHCP DISCOVER to get an IP address (unless it has a previously configured static IP address)

2. If L2-LWAPP Mode is supported send an LWAPP Discovery Request in an Ethernet broadcast

   If a WLAN Controller in L2 LWAPP Mode responds with an LWAPP Discovery Response, the AP moves to the LWAPP Join phase

3. If L2-LWAPP Mode is not supported or step 2 fails to find a WLAN controller, attempt an L3-LWAPP WLAN Controller Discovery*

4. If step 3 fails to find a valid candidate controller, reboot and return to step 1

Layer-3 LWAPP WLAN Controller Discovery

- The AP goes through the following discovery steps:

1. LWAPP Discovery Request broadcast on local subnet (IP broadcast)

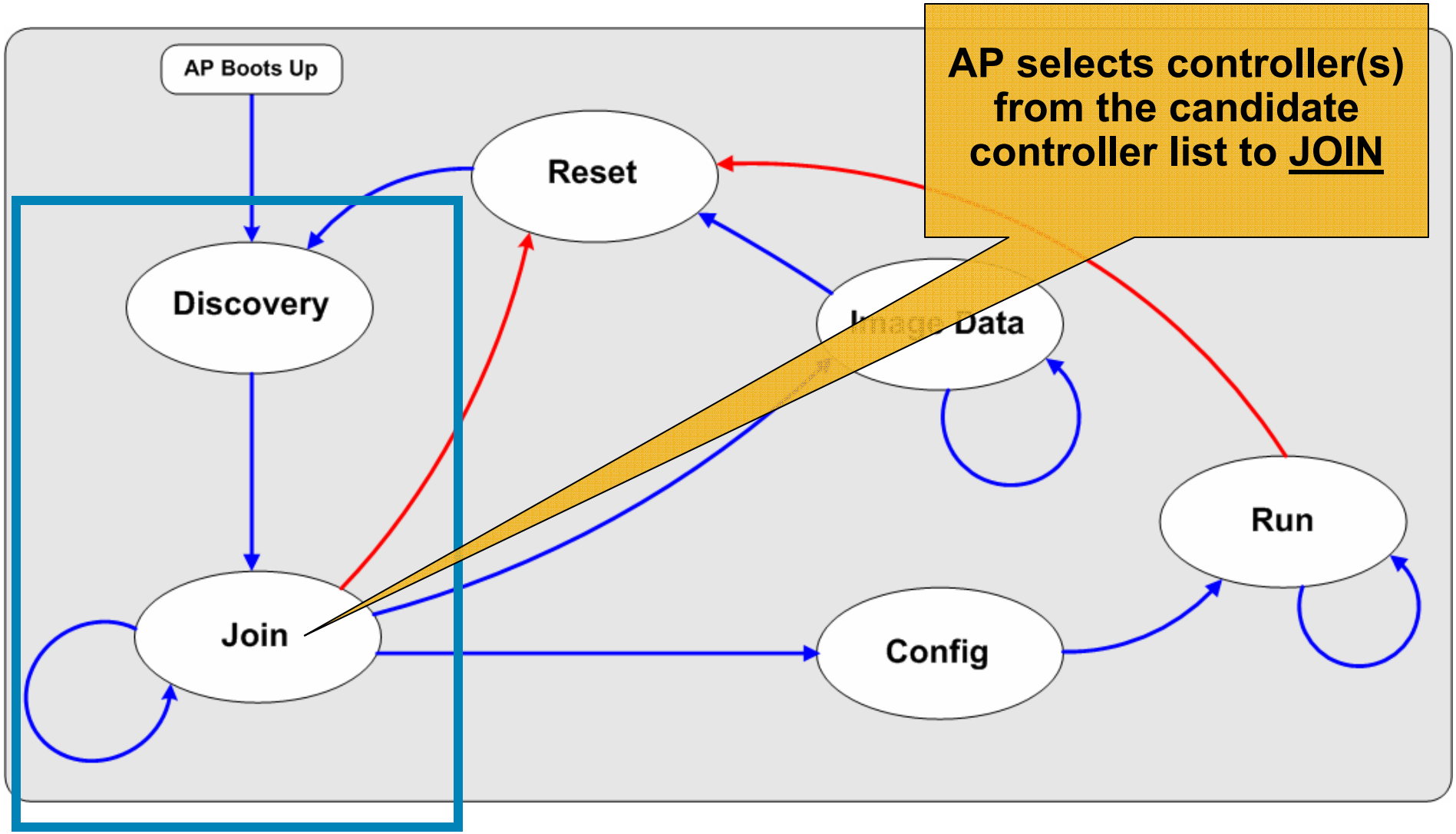
   WLAN Controller on same subnet as AP will respond with LWAPP Discovery Request
2. LWAPP Discovery Request sent to controller IP addresses learned via Over-the-Air Provisioning (OTAP)

   OTAP—Already joined APs advertise WLAN Controller in Over-the-Air neighbor messages
3. LWAPP Discovery Request sent to ALL locally stored controller IP address(es)

   AP stores controller IP address of previously joined controller plus the controller's "Mobility Group" members in NVRAM
4. LWAPP Discovery Request sent to IP Address(es) learned in vendor specific DHCP Option 43
5. LWAPP Discovery Request sent to IP Address(es) learned through DNS resolution of "CISCO-LWAPP-CONTROLLER.localdomain"
6. If no controller found, start hunting algorithm over

- AP compiles a LIST of candidate controllers from the received LWAPP Discovery Responses

LWAPP Join State



WLAN Controller Selection Algorithm

- LWAPP Discovery Response contains important information from the WLAN Controller:

  Controller sysName, controller type, controller AP capacity, current AP load, “Master Controller” status, AP Manager IP address(es) and number of APs joined to the AP Manager

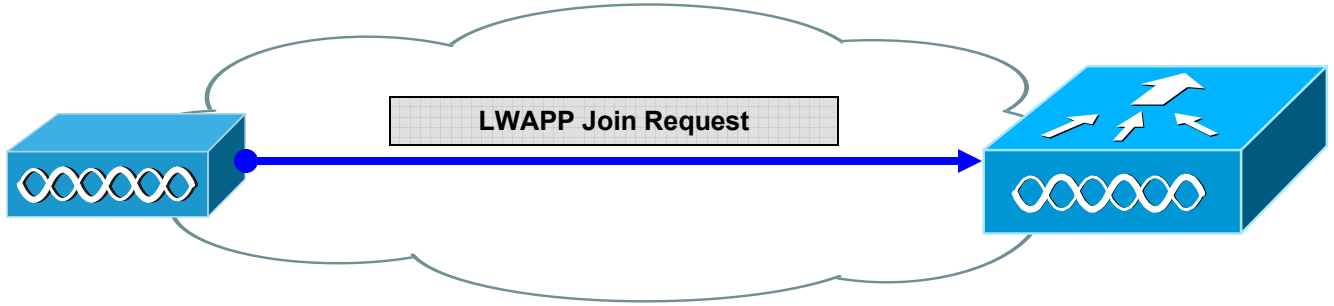
- After an “LWAPP Discovery Interval” timer expires, the AP selects a controller to join using the following decision criteria:

  1. If AP has been previously configured with a primary, secondary, and/or tertiary controller, the AP will attempt to join these first (specified in the Controller sysName)
  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.

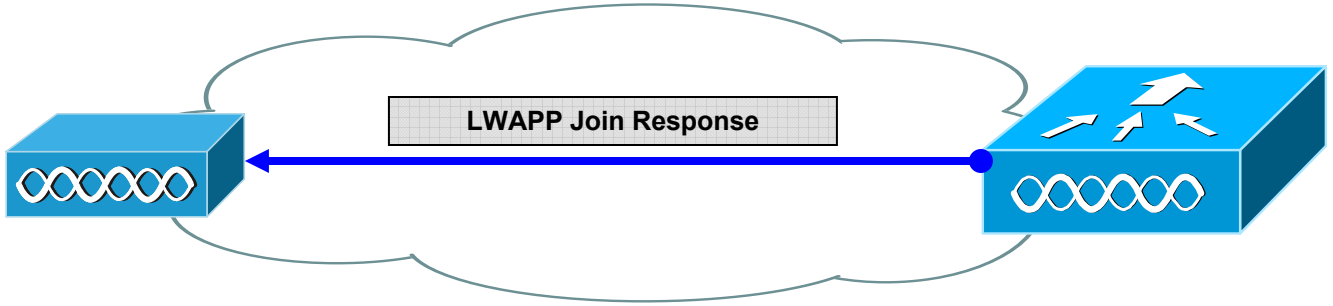
     This last step provides the whole system with dynamic AP load-balancing

LWAPP Control Messages for Join Process

- LWAPP Join Request – AP sends this messages to selected controller (sent to AP Manager Interface IP Address)

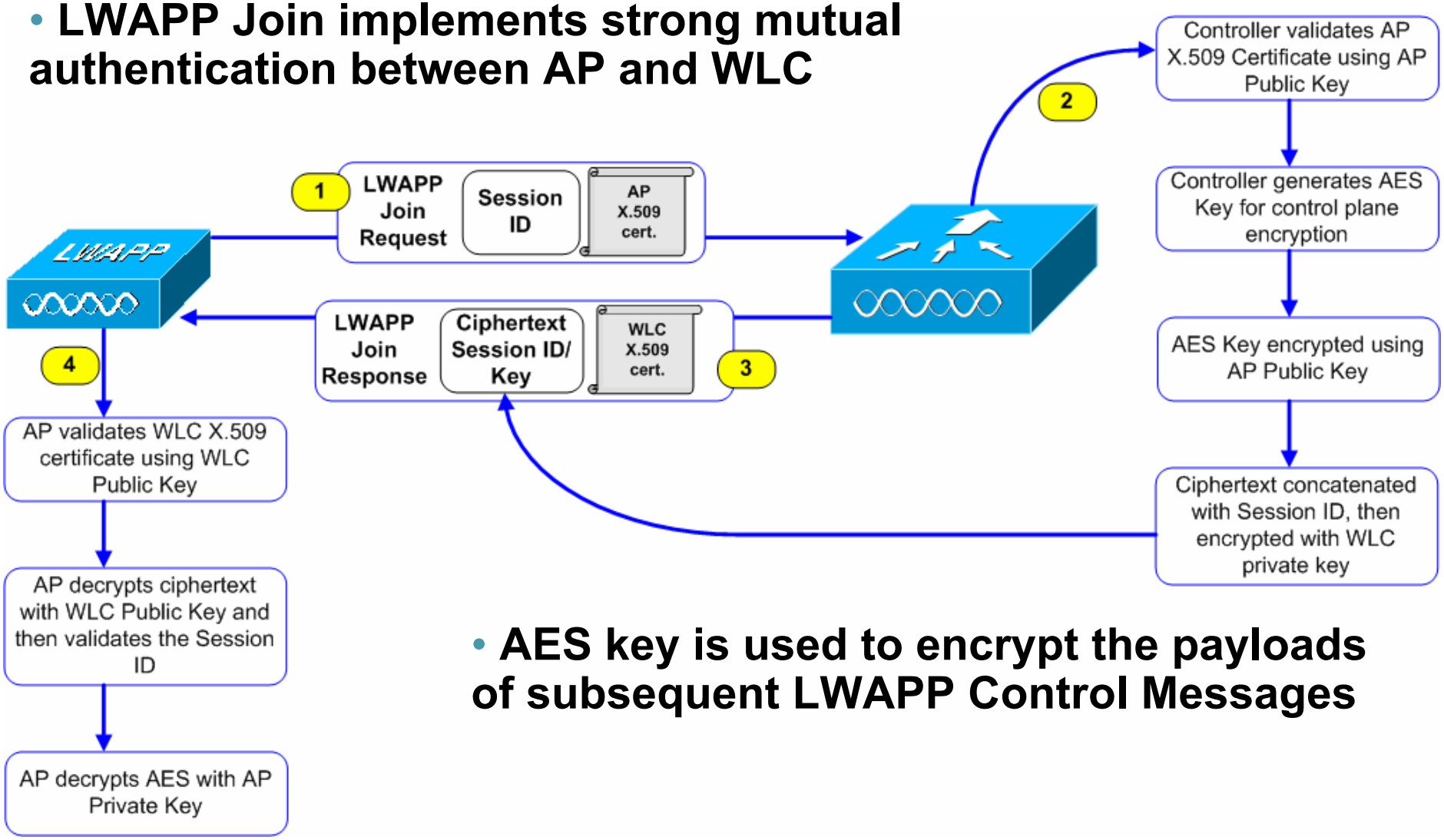


- LWAPP Join Response – If controller validates AP request, it sends the LWAPP Join Response indicating that the AP is now registered with that controller



Securing the LWAPP Join Process

- **LWAPP Join implements strong mutual authentication between AP and WLC**

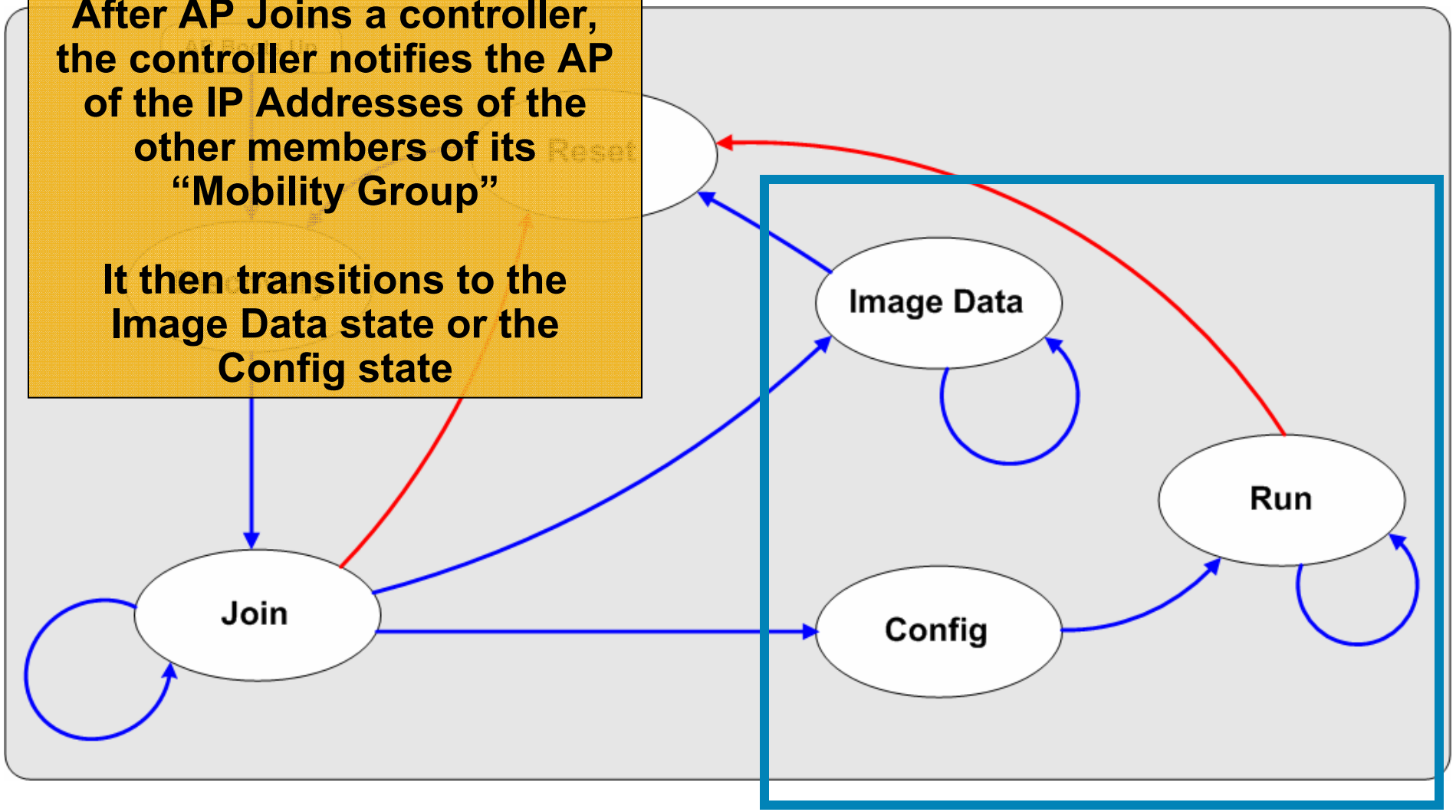


- **AES key is used to encrypt the payloads of subsequent LWAPP Control Messages**

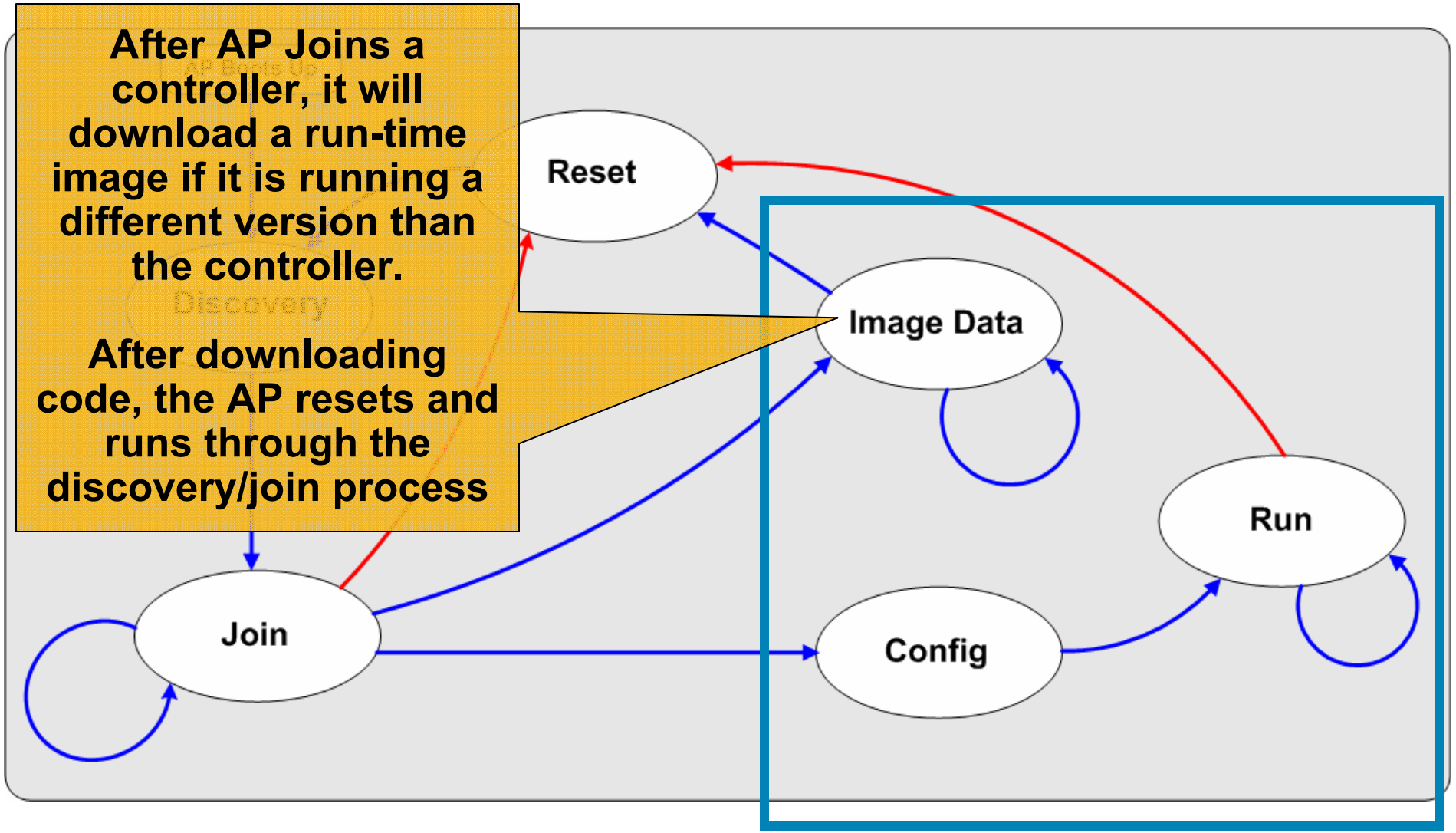
LWAPP Image Data State

After AP Joins a controller, the controller notifies the AP of the IP Addresses of the other members of its "Mobility Group"

It then transitions to the Image Data state or the Config state



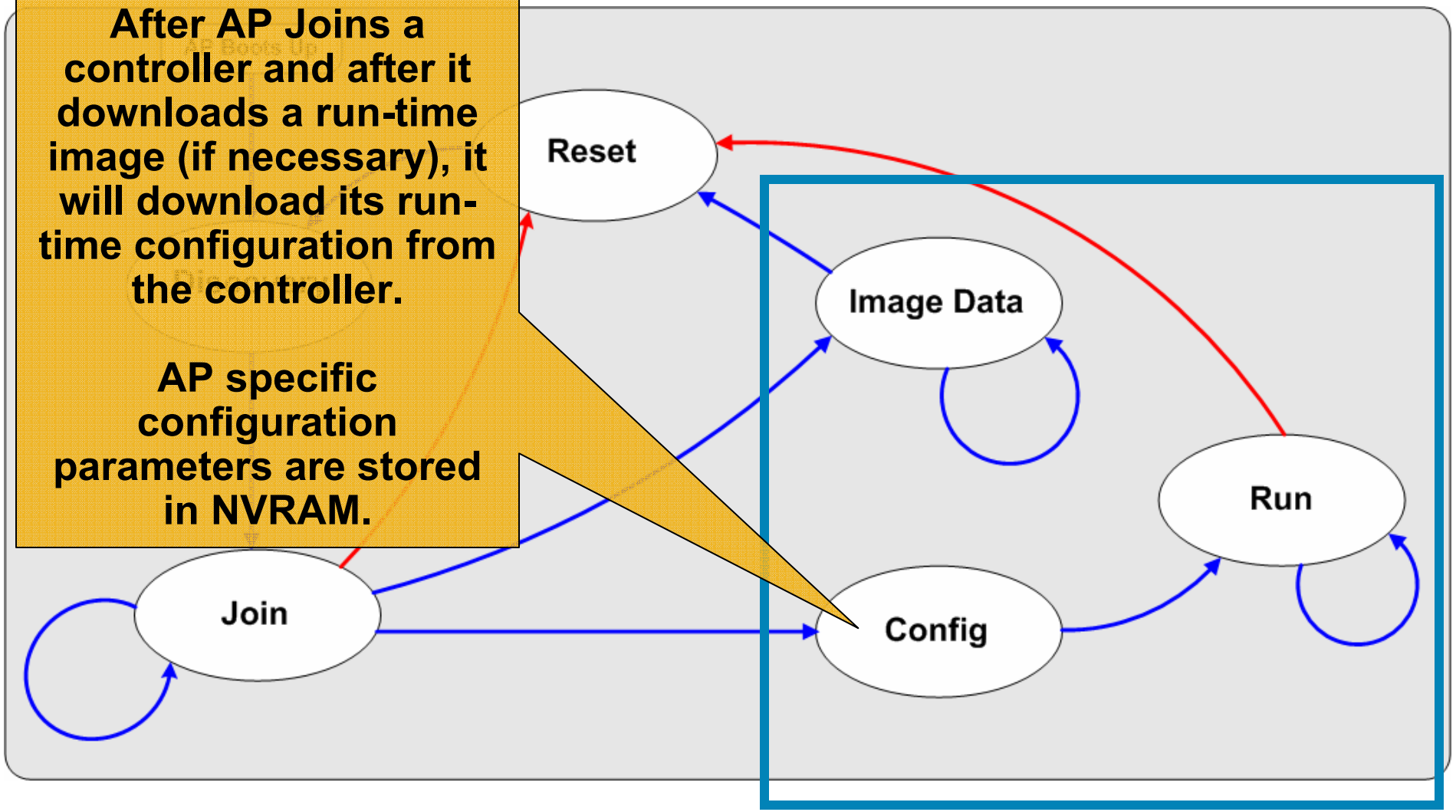
LWAPP Image Data State



LWAPP Config State

After AP Joins a controller and after it downloads a run-time image (if necessary), it will download its run-time configuration from the controller.

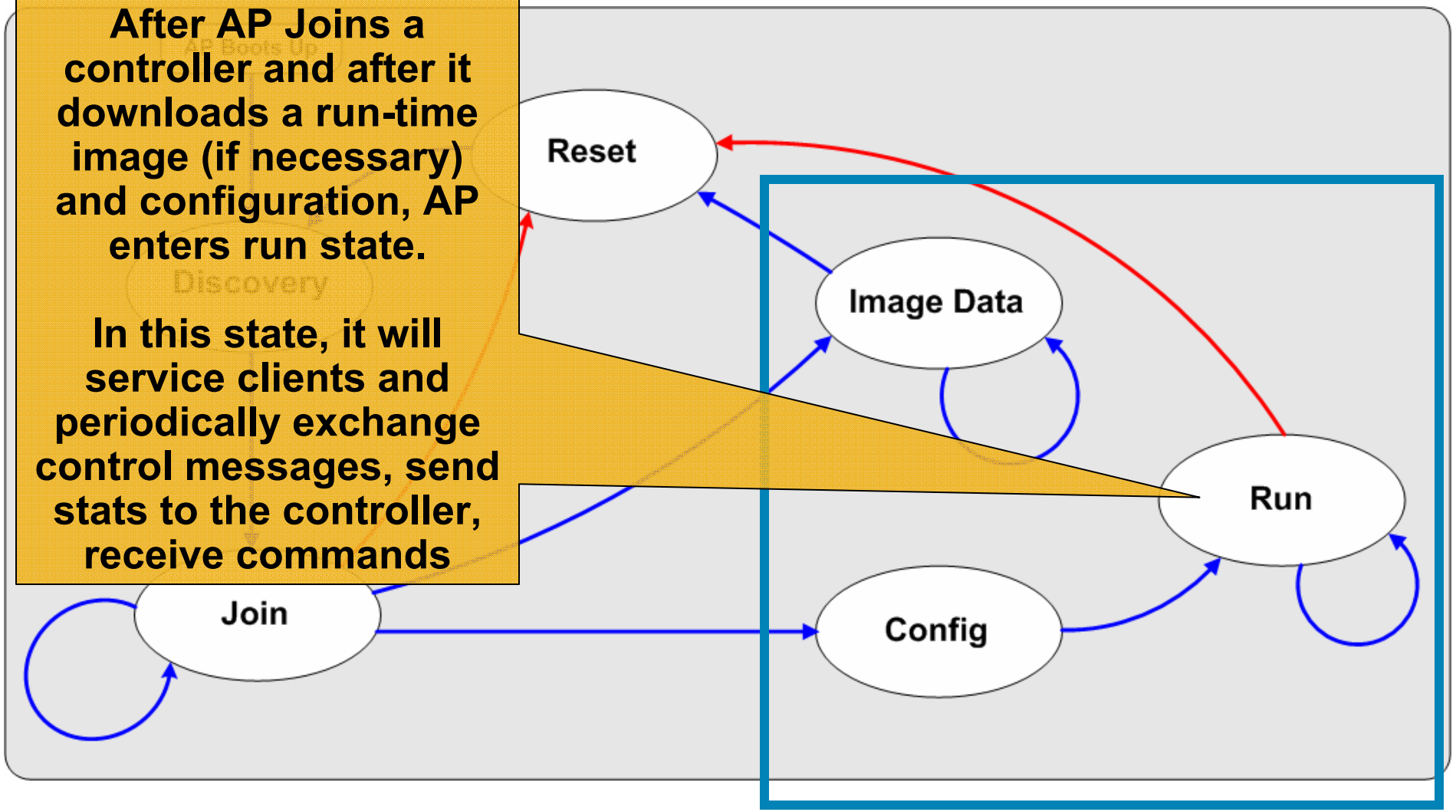
AP specific configuration parameters are stored in NVRAM.



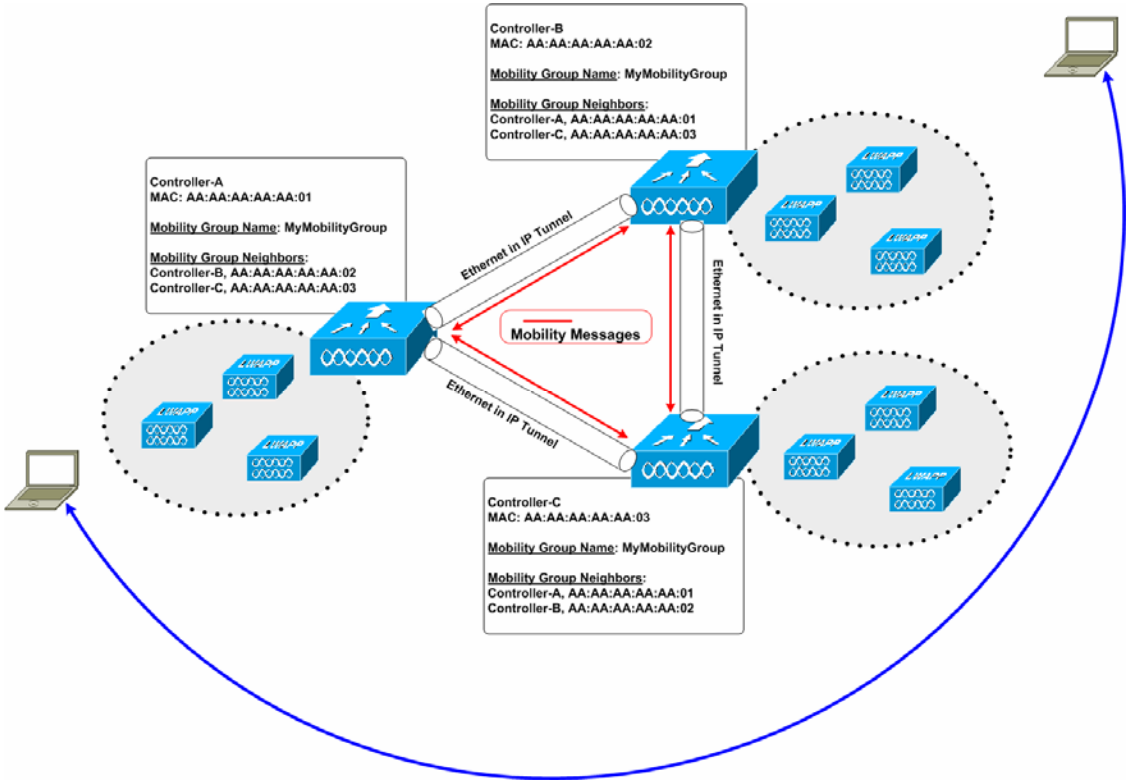
LWAPP Run State

After AP Joins a controller and after it downloads a run-time image (if necessary) and configuration, AP enters run state.

In this state, it will service clients and periodically exchange control messages, send stats to the controller, receive commands



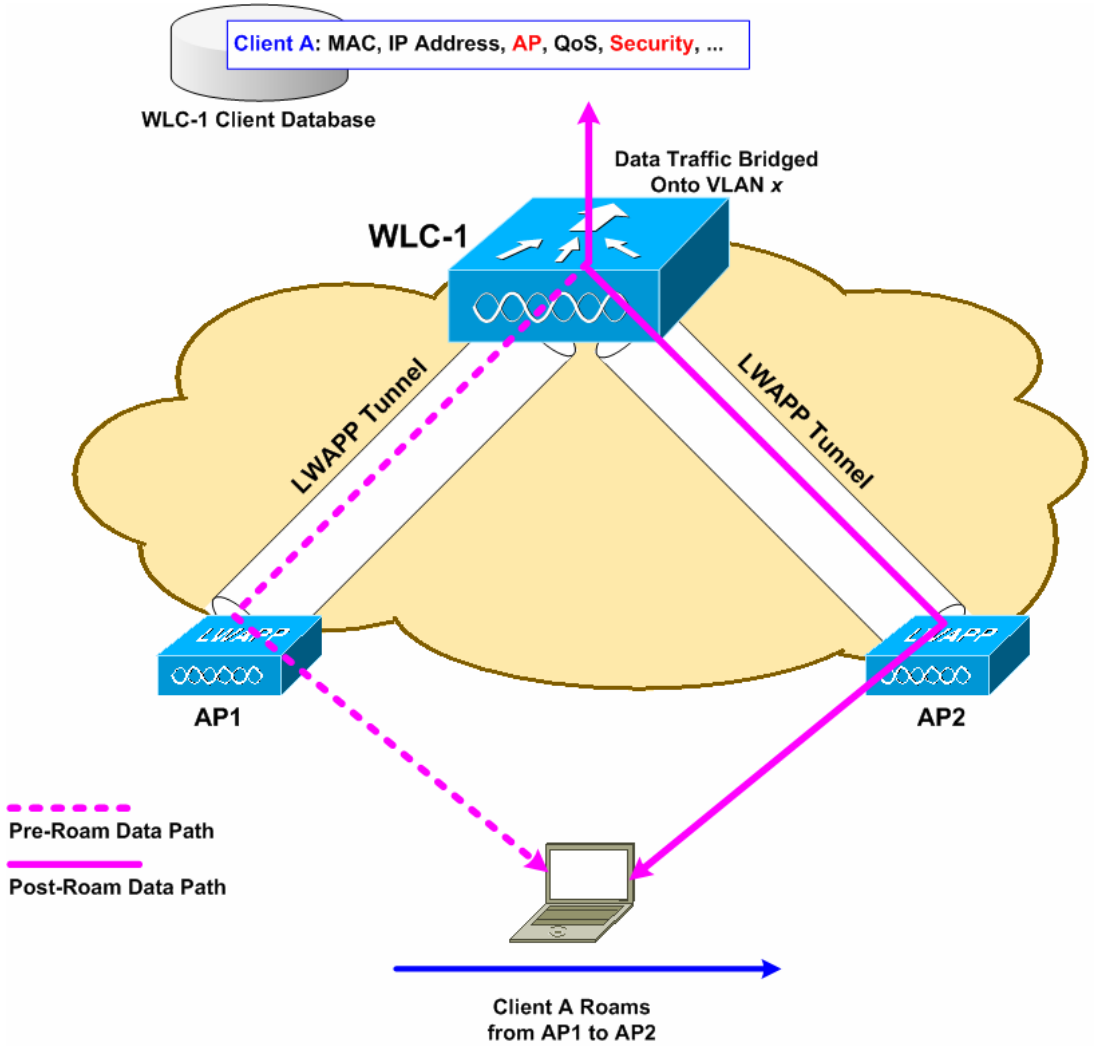
Scaling the Architecture with Mobility Groups



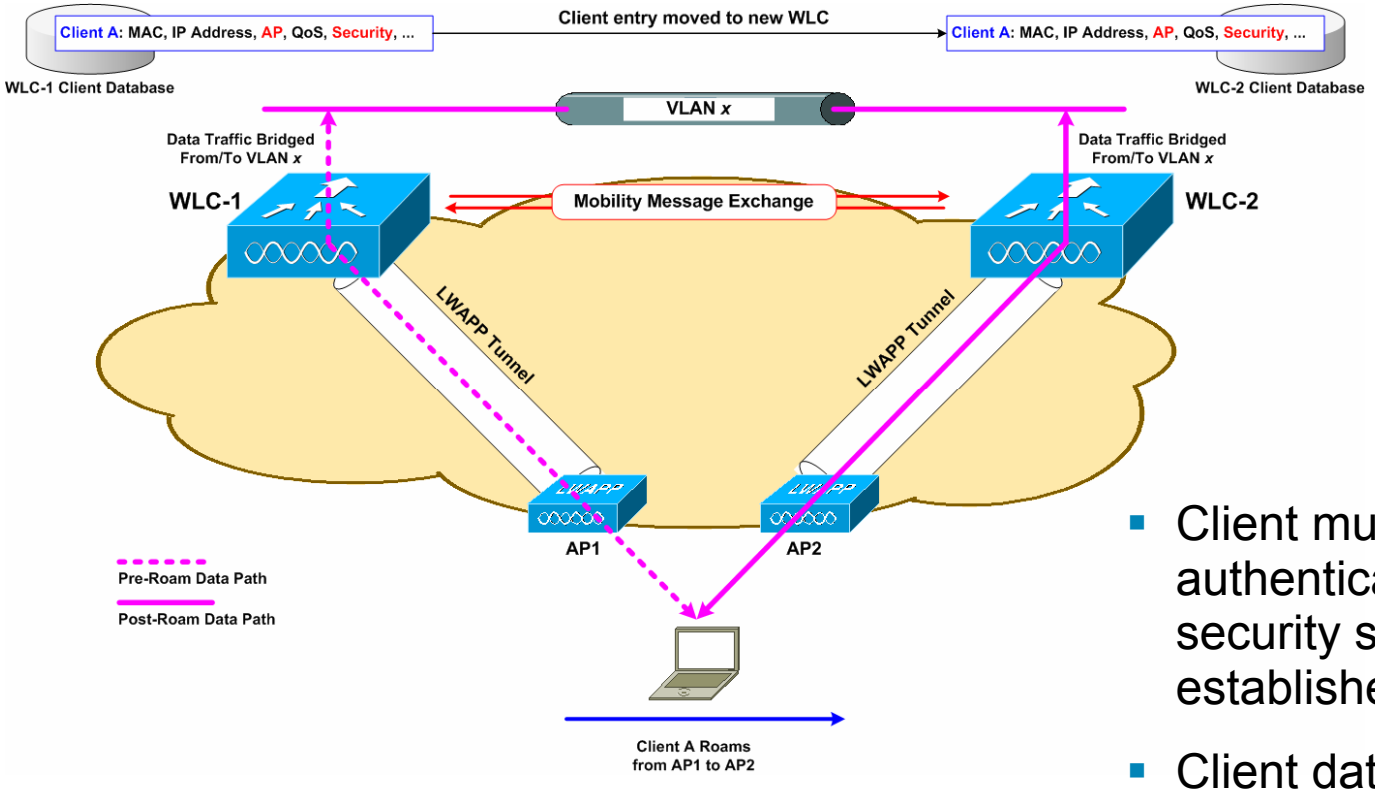
- Mobility Group allows controllers to peer with each-other to support seamless roaming across controller boundaries
- APs learn the IPs of the other members of the mobility group after the LWAPP Join process
- Support for up to 24 controllers, 3600 APs per mobility group
- Mobility messages exchanged between controllers
- Data tunneled between controllers in EtherIP (RFC 3378)

Intra-Controller Roaming

- Intra-Controller roam happens when an AP moves association between APs joined to the same controller
- Client must be re-authenticated and new security session established
- Controller updates client database entry with new AP and appropriate security context
- No IP address refresh needed



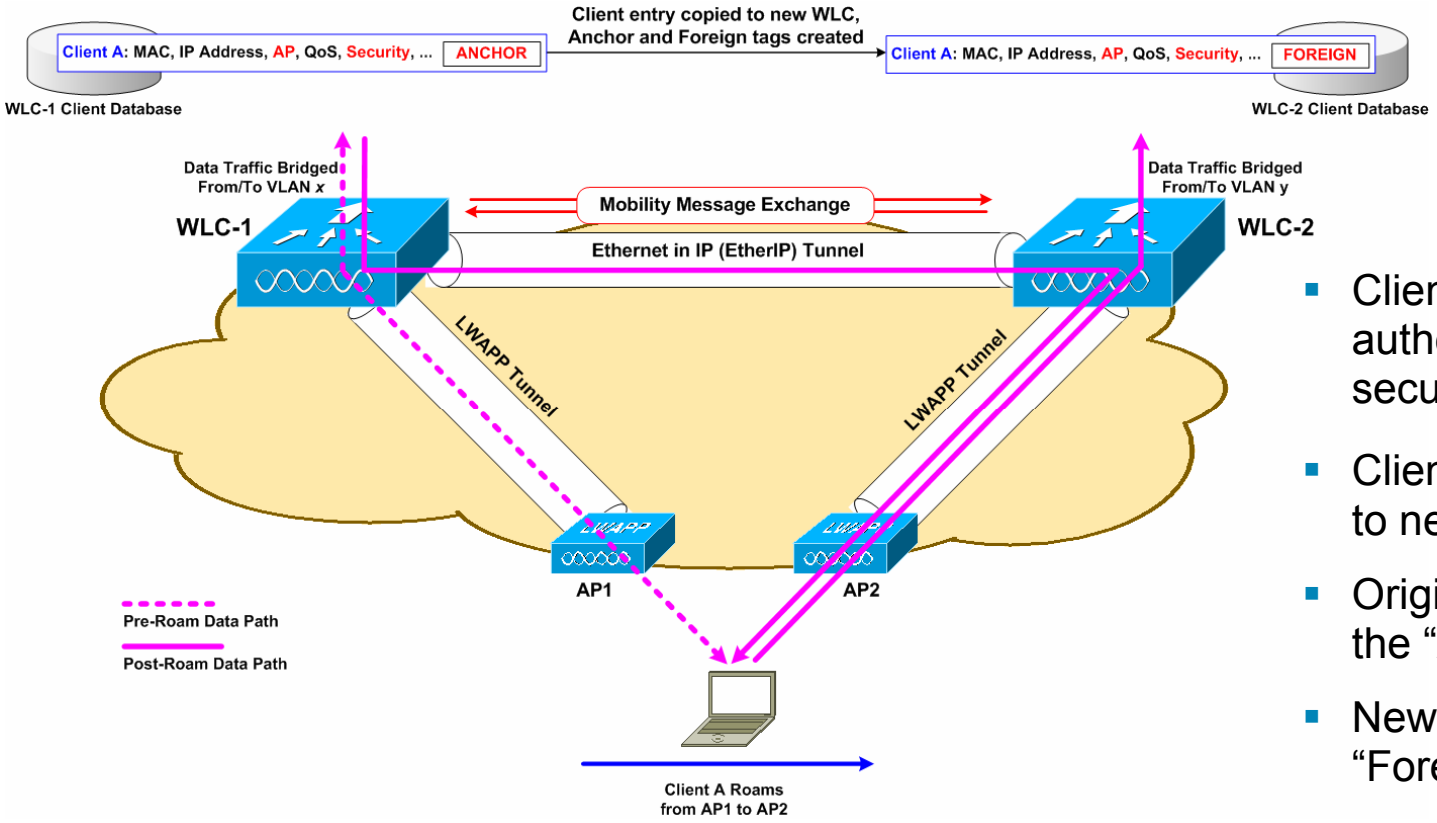
Layer-2 Roaming—Inter-Controller



- L2 Inter-Controller roam happens when an AP moves association between APs joined to the different controllers but client traffic bridged onto the same subnet

- Client must be re-authenticated and new security session established
- Client database entry moved to new controller
- No IP address refresh needed

Layer-3 Roaming—Inter-controller



- L3 Inter-Controller roam happens when an AP moves association between APs joined to the different controllers but client traffic bridged onto different subnet

- Client must be re-authenticated and new security session established
- Client database entry copied to new controller
- Original controller tagged as the “Anchor”
- New controller tagged as the “Foreign”
- No IP address refresh needed
- Asymmetric traffic path established

Roaming Requirements

- Roaming must be fast… Latency can be introduced by:
  - Client channel scanning and AP selection algorithms
  - Re-authentication of client device and re-keying
  - Refreshing of IP address
- Roaming must maintain security
  - Open auth, static WEP – session continues on new AP
  - WPA/WPAv2 Personal – New session key for encryption derived via standard handshakes
  - 802.1x, 802.11i, WPA/WPAv2 Enterprise – Client must be re-authenticated and new session key derived for encryption

Fast Secure Roaming

- Client channel scanning and AP selection algorithms—Improved via CCX features
- Refreshing of IP address—Irrelevant in controller-based architecture!
- Re-authentication of client device and re-keying

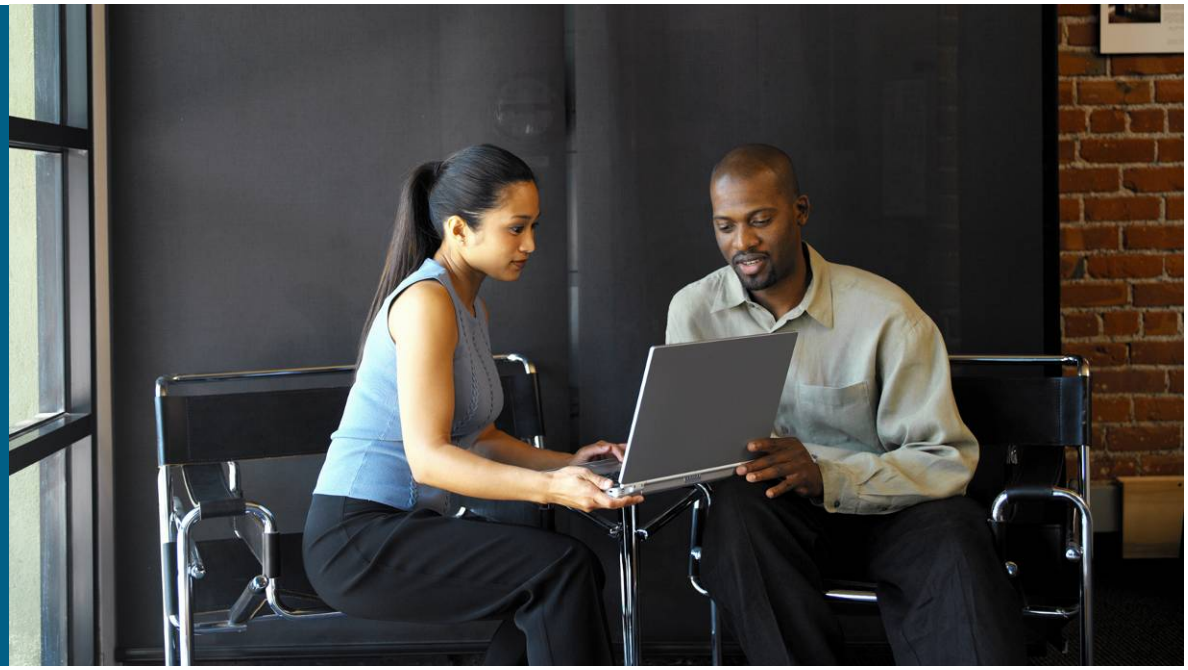
  Cisco Centralized Key Management (CCKM)

  Proactive Key Caching (PKC)

Supporting Roaming—Design Best Practices and Caveats

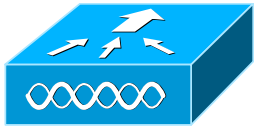
- Minimize inter-controller roaming in your designs
- Design the network for <= 10msec RTT latency between controllers
- Inter-controller layer-2 roaming is more efficient than layer-3 roaming
- Layer-3 roaming—consider the effects of things like uRPF and stateful security features in your designs
- Use PKC and/or CCKM to speed up and secure roaming
- Client roaming behavior—mileage varies by vendor, driver, supplicant. Look for CCXv4 feature-set

Controller design



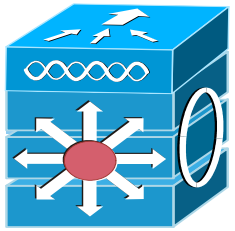
Campus WLAN Controller Options

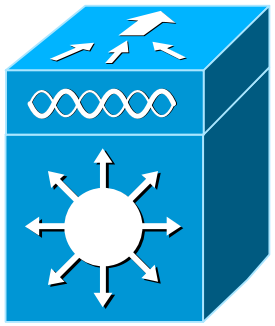
- Standalone Appliance Controller
  - Routed Network exists on another platform
  - Dot1Q trunk to switched/routed network
- Integrated Controller
  - Routed network can exist on the same platform
  - Layer 2 connection is internal
  - Layer 2 or 3 Connection to network routed network



440x

Appliance





Cisco 3750G Integrated WLAN Controller

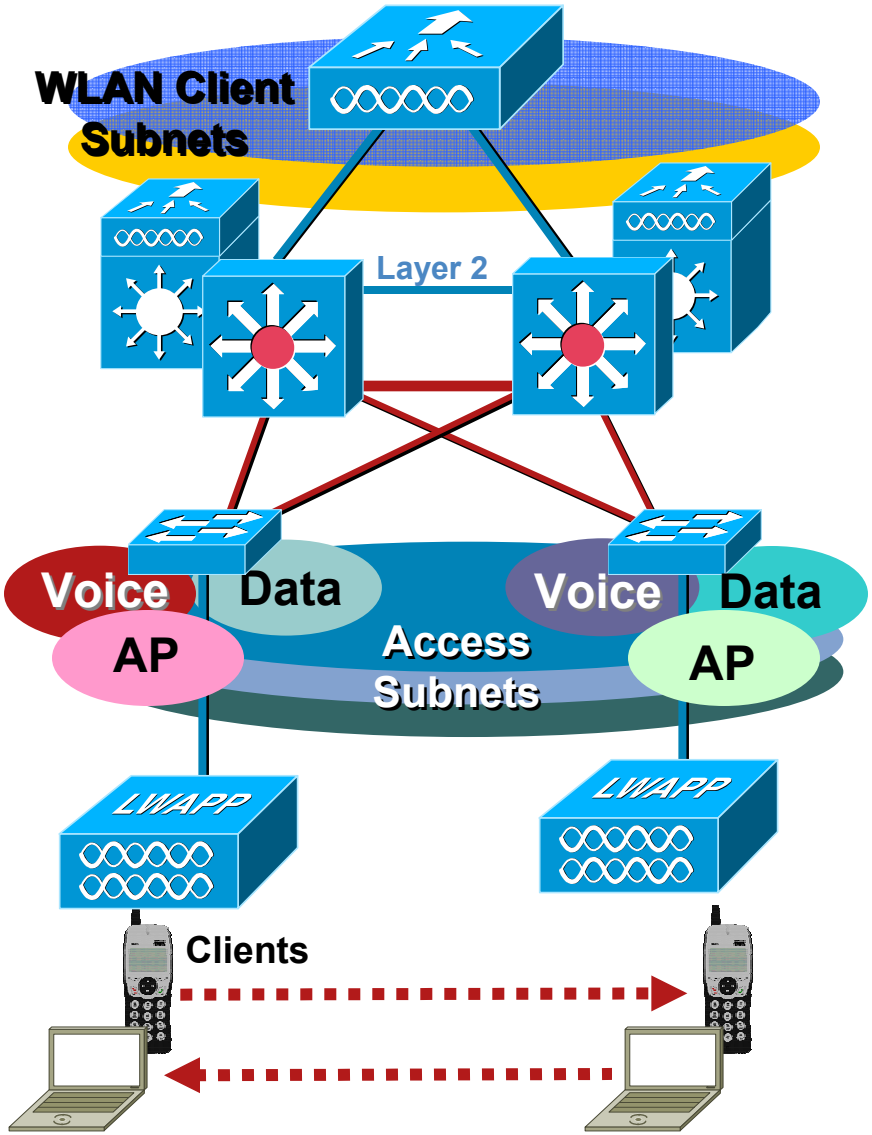
WiSM

Integrated

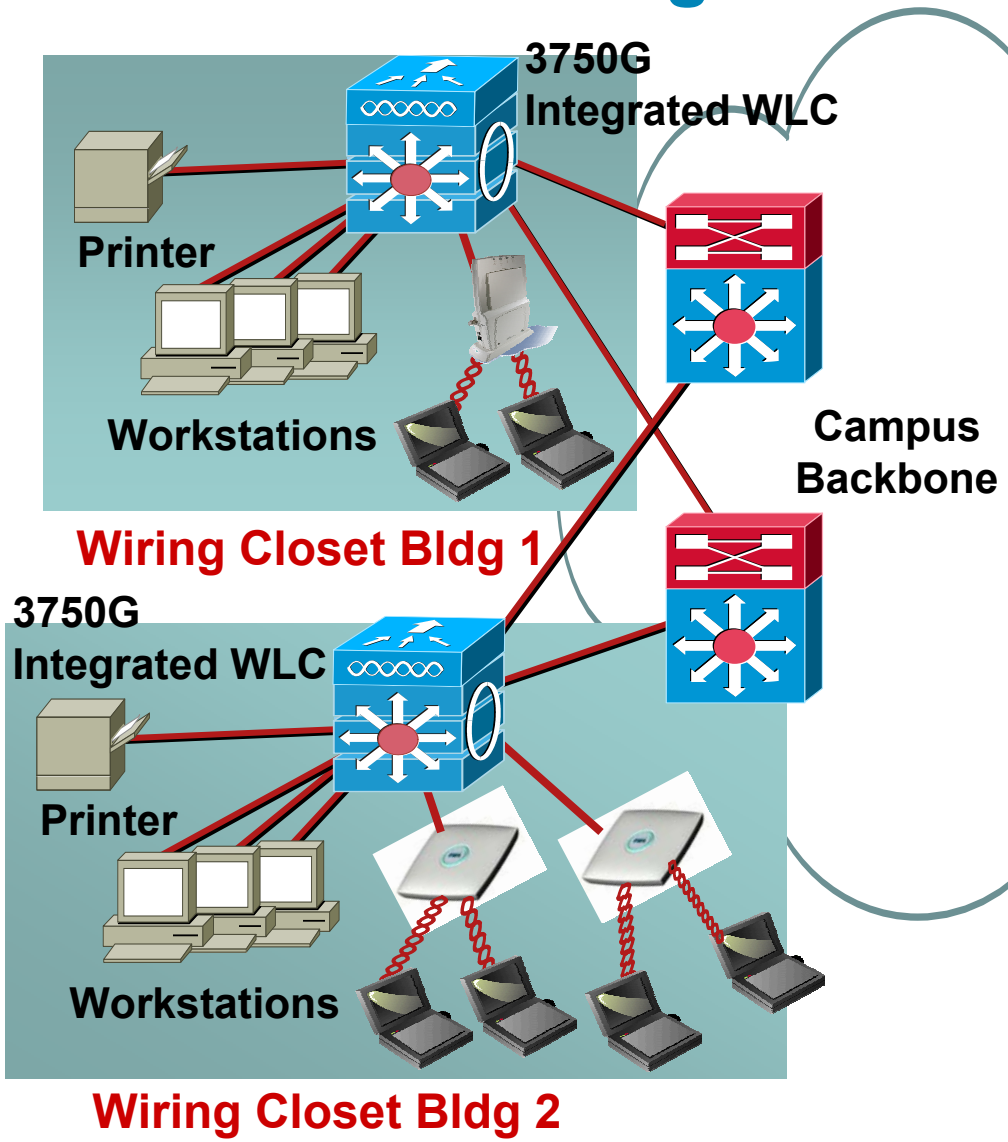
Where to Place a WLAN Controller? Distributed Designs

- WiSM(s) or 440x WLAN Controller(s) connected at Distribution Layer
- Controller Redundancy
- Key Design Considerations:
  - Spanning tree
  - HSRP/GLBP
  - Traffic flow
    - Load balancing
    - Resiliency
  - Access layer “collapsed” into distribution layer
    - Access Layer IP Addressing
    - Access layer features need to be implemented in the distribution layer

Mobility!

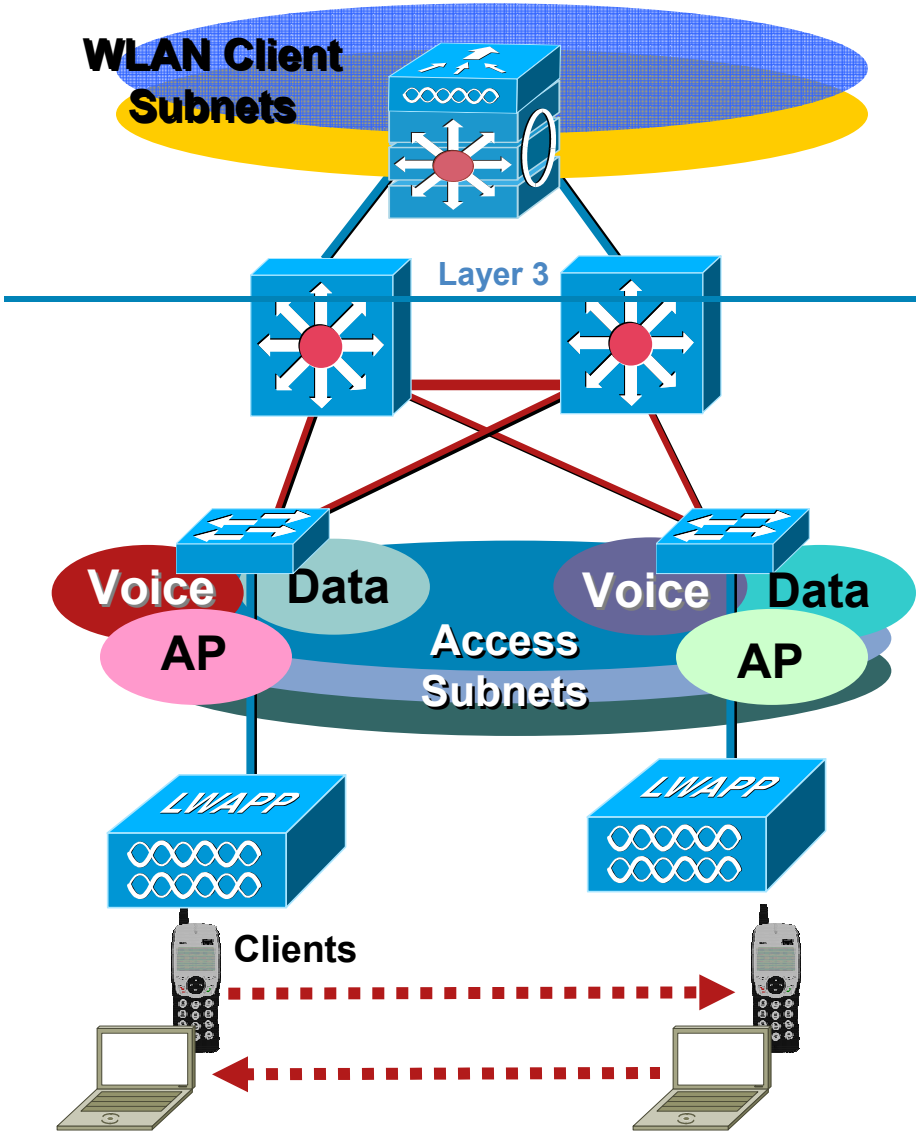


Where to Place a WLAN Controller? Distributed Designs—Enterprise Wiring Closet



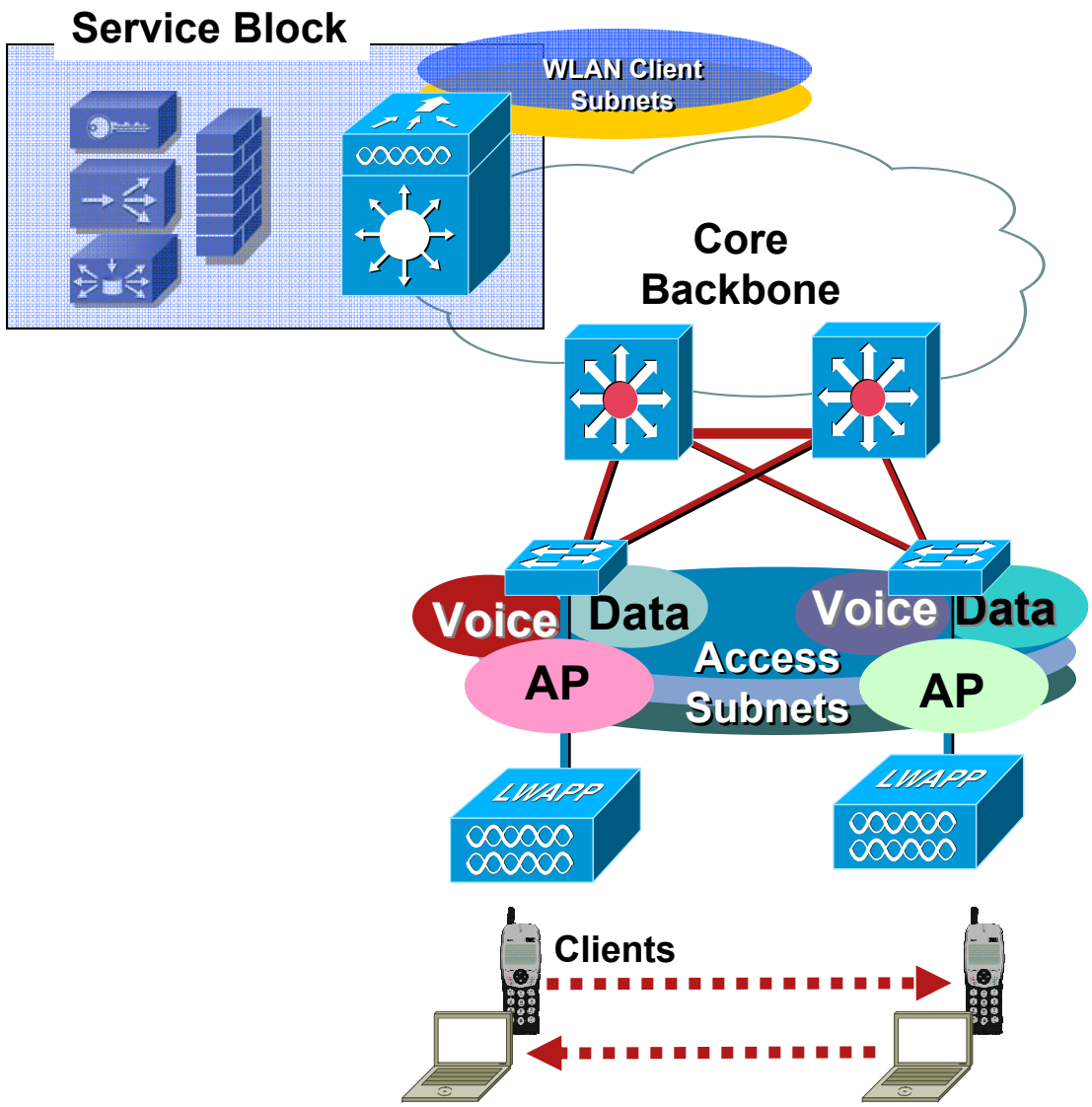
- Cisco 3750G Integrated WLAN Controllers deployed in wiring closets
- Controller redundancy can be achieved within the switch stack
- Access layer kept at the access layer—leverage 3750G features
- Cost-effective uplink redundancy via SFP ports
- Inter-wiring closet mobility needs to be considered

Where to Place a WLAN Controller? Distributed Designs—Cisco 3750G Unified WLC



- Logical placement of access layer technology at “Top-of-stack”
- Leverage 3750 access layer features
- Cisco 3750 Integrated WLAN Controllers deployed at the distribution block
- Cost-effective L3 uplink redundancy via SFP ports
- Switched/Routed network load-balances traffic to the switch
- Switch stacking capabilities:
  - Controller redundancy within the stack
  - Increased AP capacity
- Inter-distribution block mobility needs to be considered

Where to Place a WLAN Controller? Centralized Design—WiSM



- Economy of scale
  - Vertical/Horizontal scalability
    - "Big Box" with 5 WiSMs
    - Easy to add more capacity
  - Incremental improvement in cost-per-AP (CAPEX)
- Lower OPEX
  - Simplified management
    - Fewer end-points
    - Aggregation of traffic
  - HA routing/switching/power
  - Skilled operational staff
- Efficient mobility
- Simplified services integration
- Key campus design concepts
  - < 10 msecs latency recommended
  - Stub network connection
  - Assumes plenty-of-bandwidth
- Could be done with stacks of 440x
  - Less economy of scale
  - Not as integrated
  - Routing/switching design challenges

AP Deployment Strategies

- Problem: How to Deploy Lightweight APs and have them join the (right) WLAN controller?
- Solution 1: LWAPP Discovery Algorithm
- Solution 2: Prime the APs
- Solution 3: Have APs join statically defined “master controller” (AKA “NOC” controller), then assign them to the right controller(s)
- Solution 4: AP CLI commands

AP Deployment—CLI Commands

- New CLI commands available for deploying LAPs:

  # lwapp ap ip address <ip addr> <netmask> ! Optional

  # lwapp ap default-gateway <gateway ip addr>

  # lwapp ap controller ip address <wlc management ip>

  # lwapp ap controller primary <p-sysname> secondary <s-sysname> tertiary <t-sysname>

- CLI commands can be used only until the AP joins a WLC!
- After an AP joins the WLC, commands are cleared:

  # clear lwapp private-config

- But… commands cannot be cleared until administrator sets the username/password from the WLC

  > config ap username <uname> password <pword> [all | Cisco AP]

Redundancy

- AP Redundancy

  RF “Self-Healing” allows system to compensate dynamically for lost APs

  System must be designed to support self-healing

  Self-Healing across controllers requires controllers be in the same RF Group

- Controller Port Redundancy

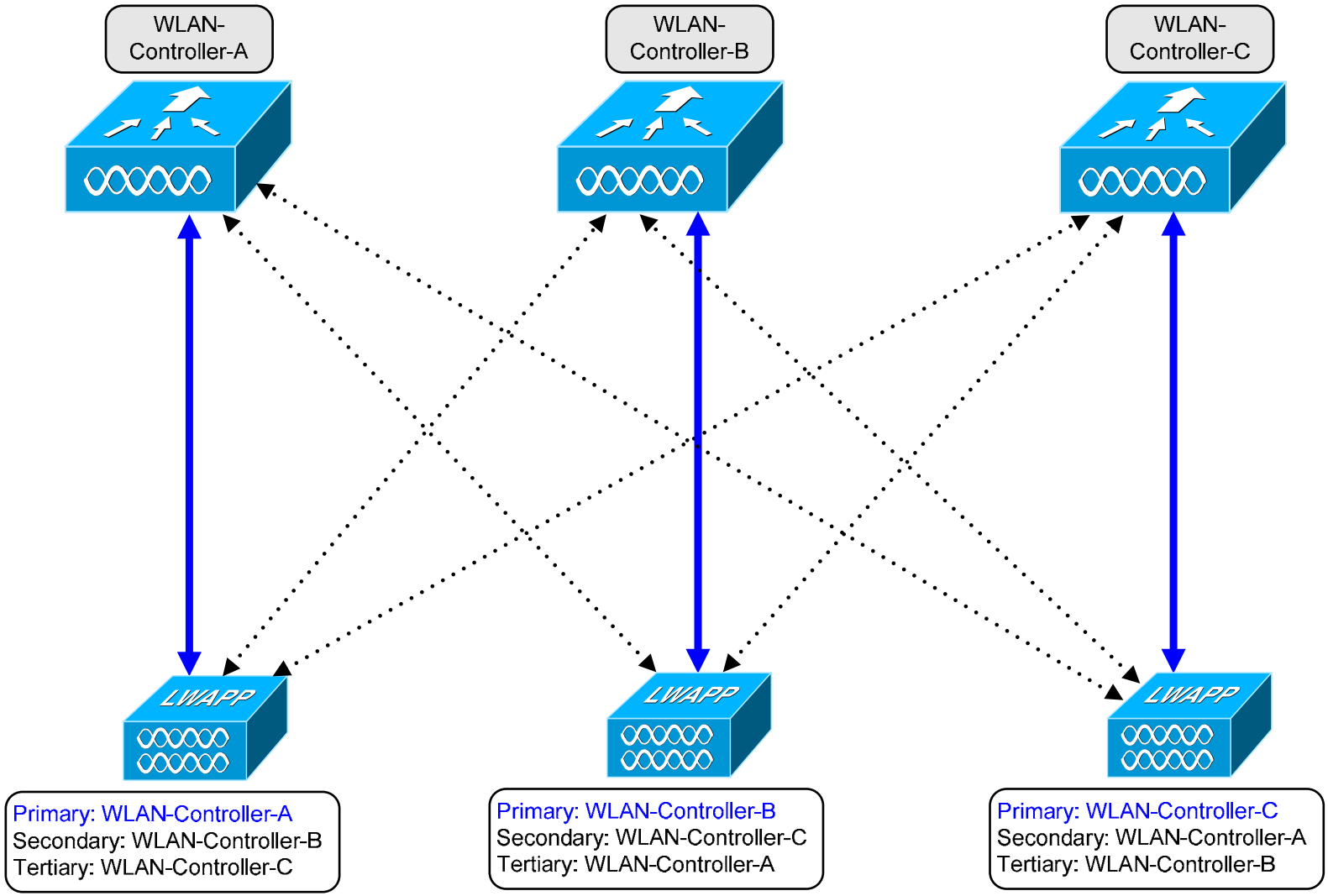
  Map interfaces to primary and a secondary physical port

  LAG handles this dynamically

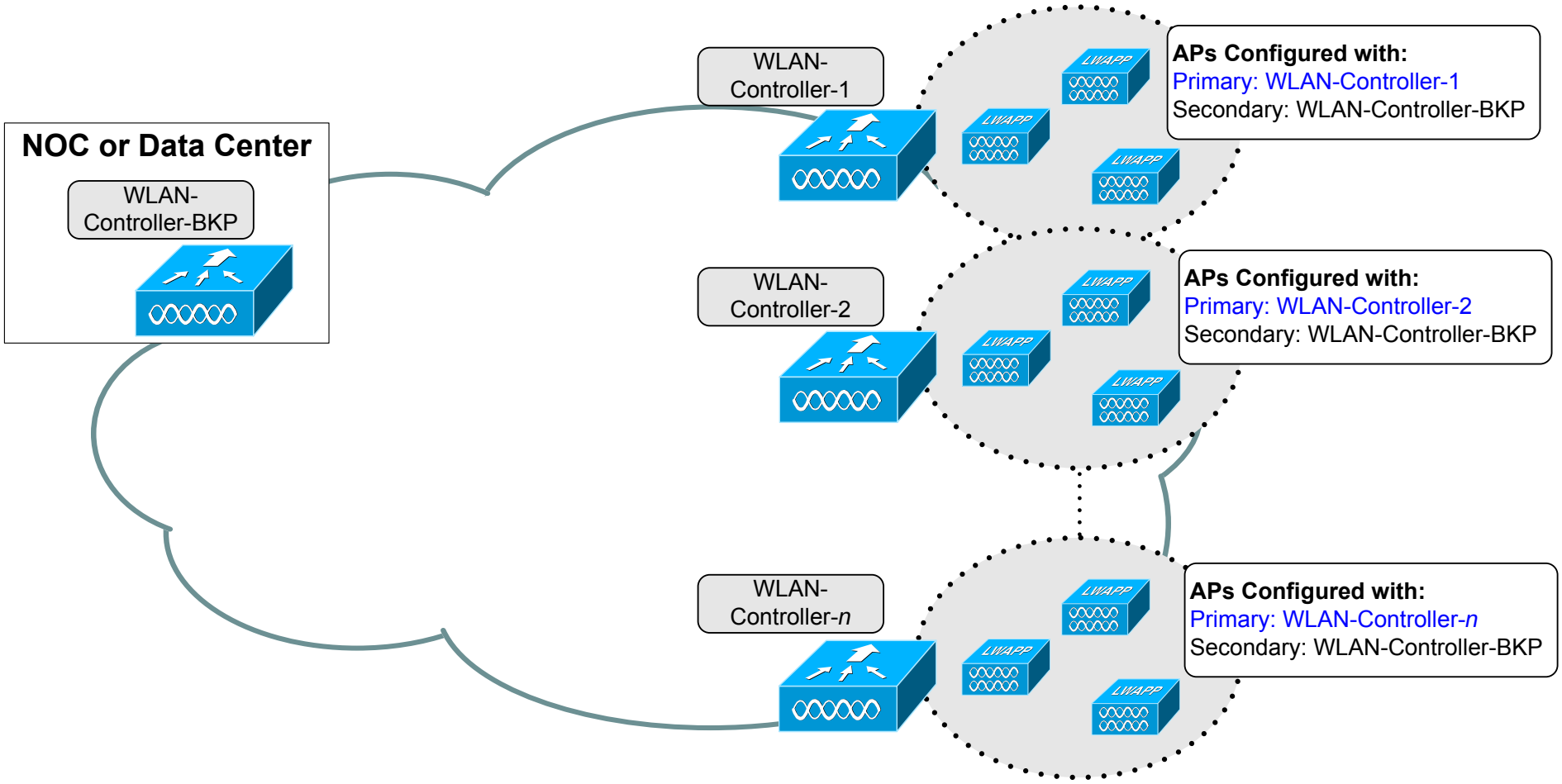
- Controller Redundancy

  Dynamic vs. Deterministic

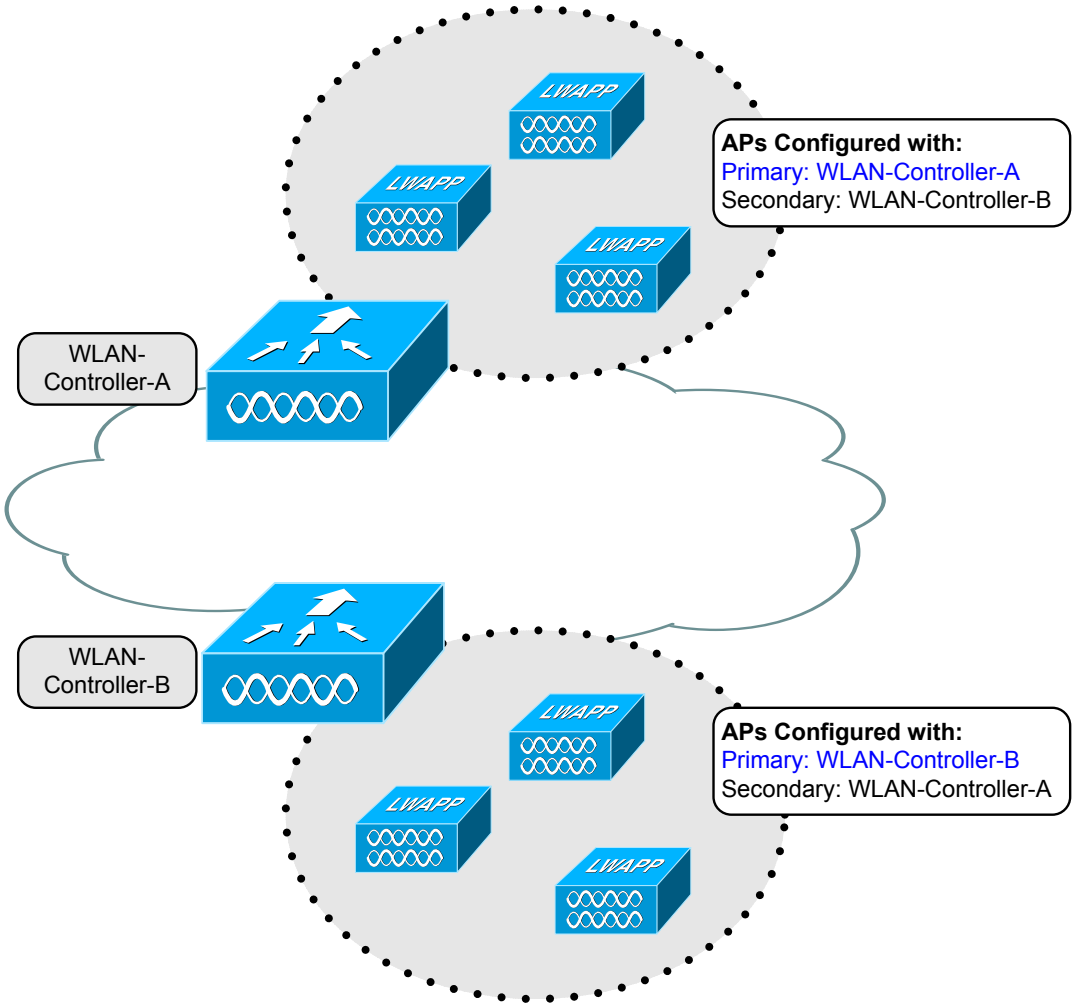
Controller Redundancy



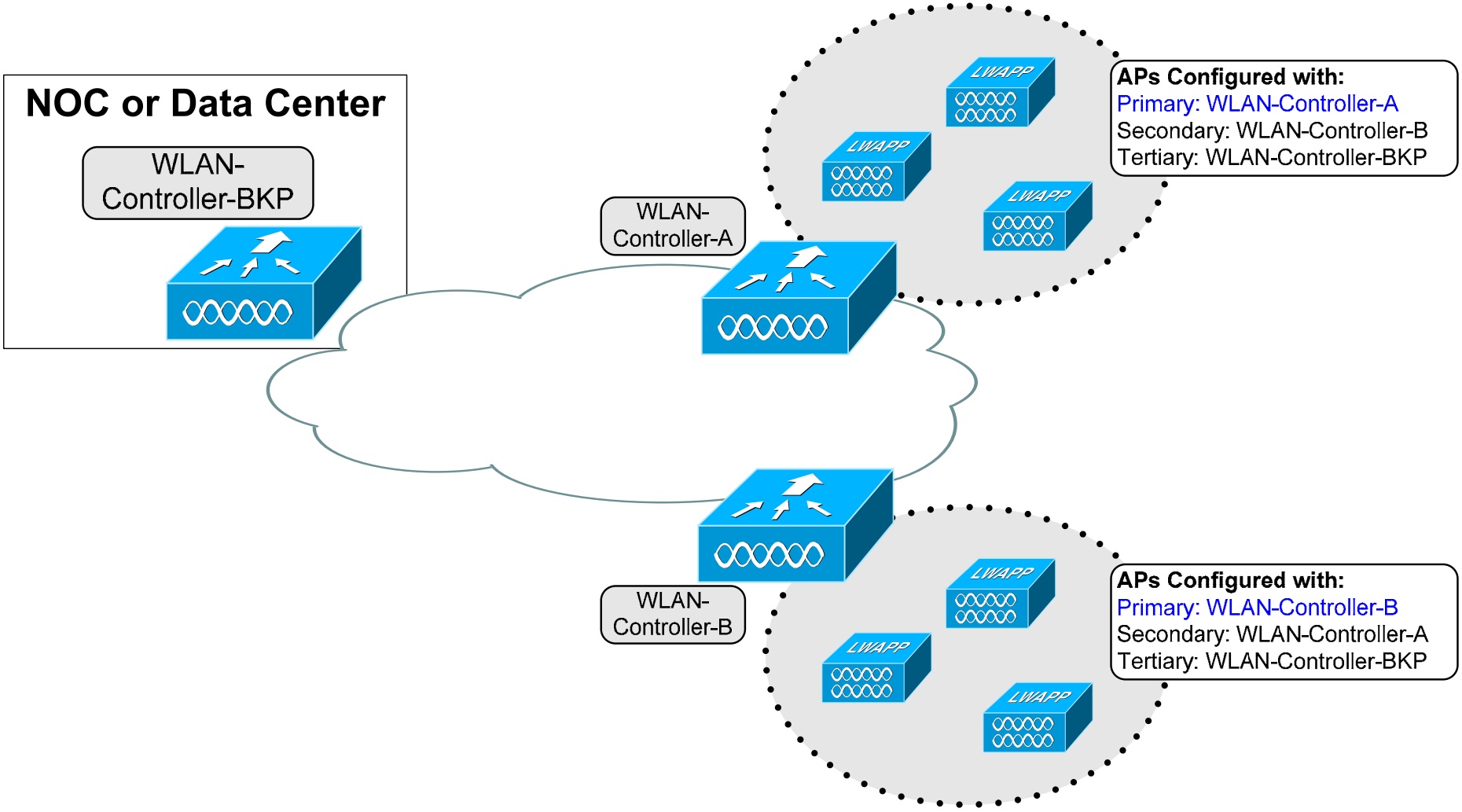
Controller Redundancy Designs—N+1



Controller Redundancy Designs—N+N

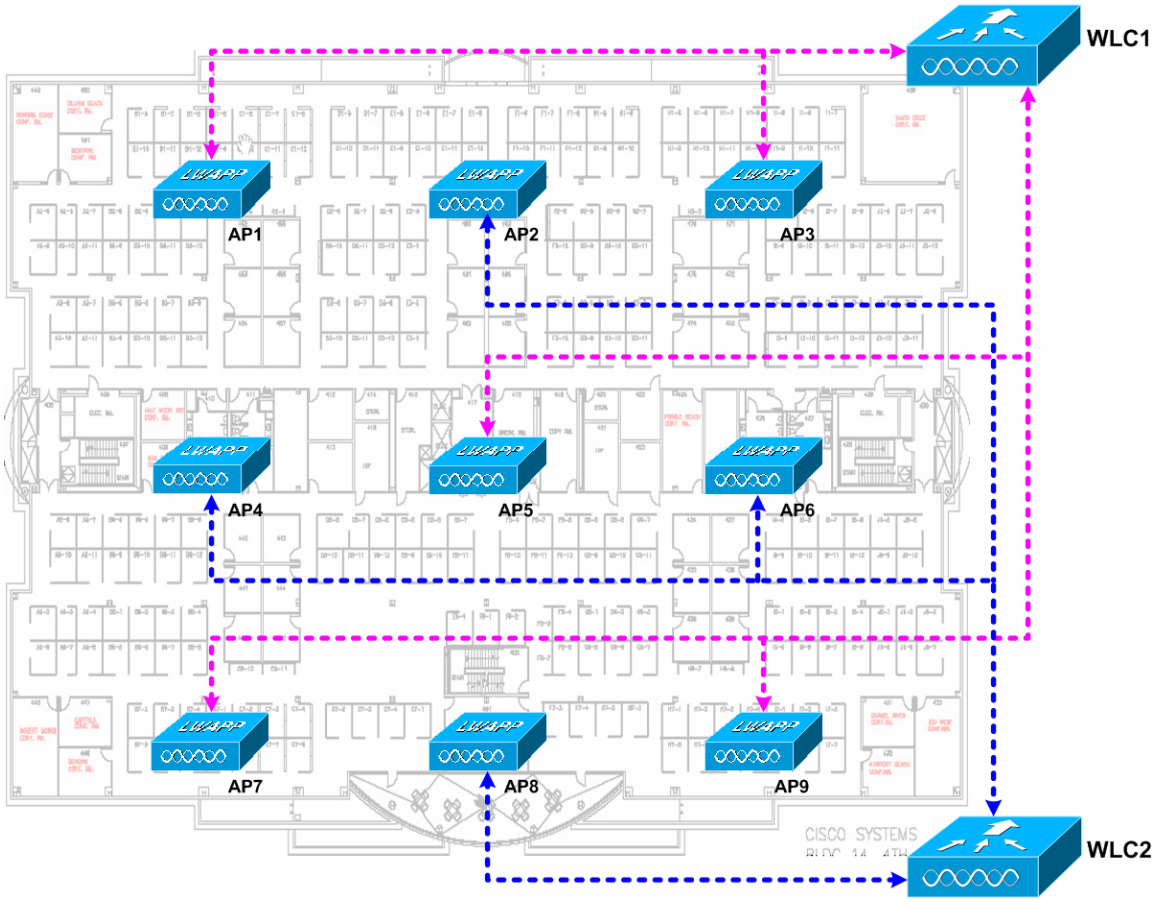


Controller Redundancy Designs—N+N+1

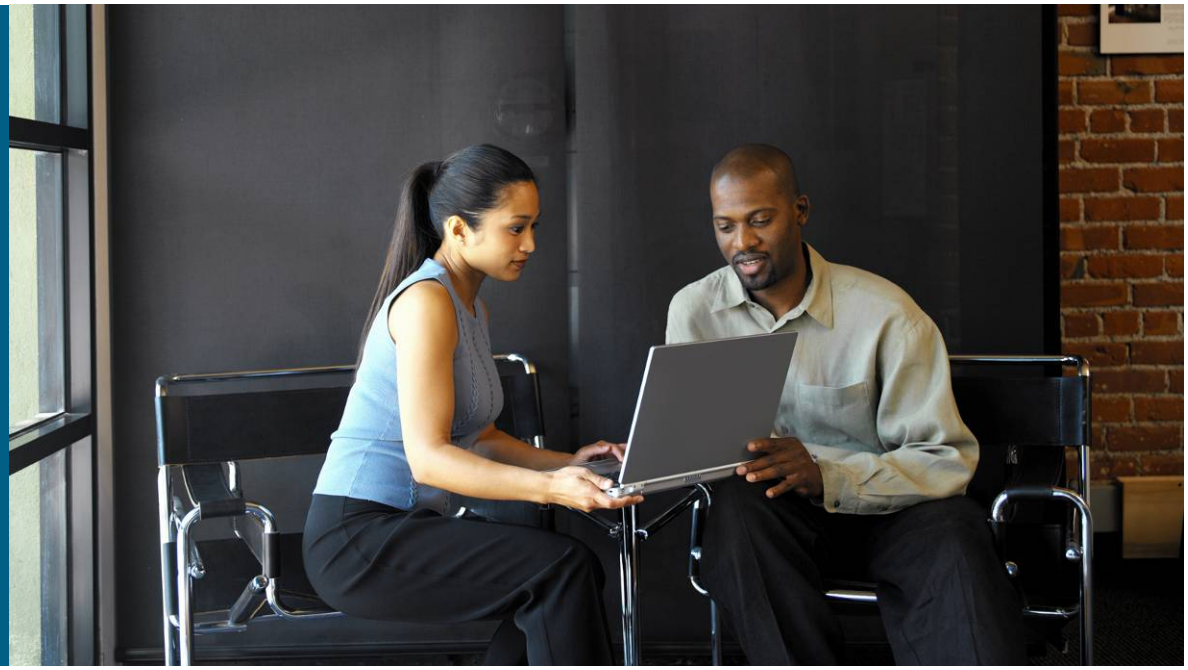


Access Point Layout—"Checker Board" Designs

- APs alternate join relationships between controllers
- Can be done dynamically or deterministically
- Results in more inter-controller roaming even in common settings
- Lose client load-balancing feature
- Clients still get disconnected in the event of controller failure
- Cisco recommends limiting use of these designs
- Cisco DOES NOT recommend this design for general use



Guest Access



Traditional Guest Traffic Termination

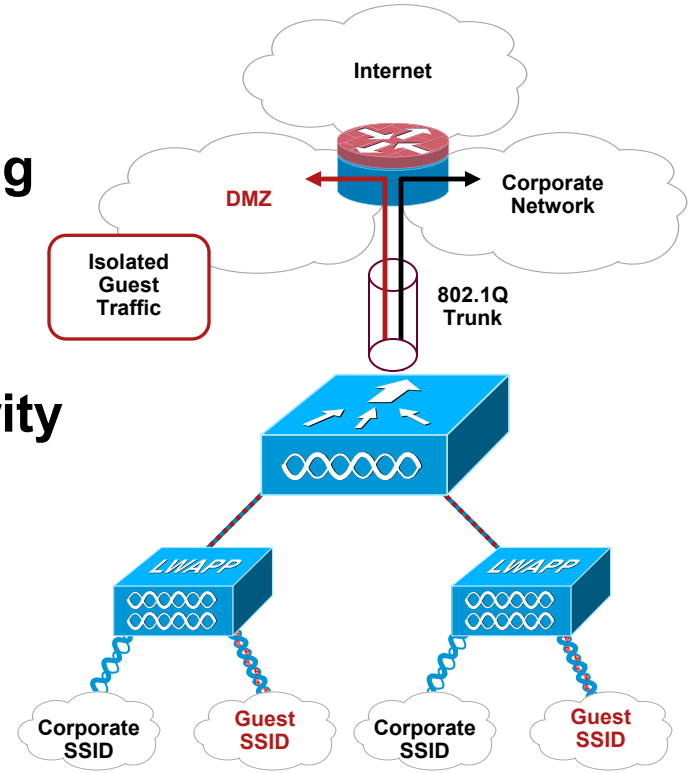
- **The traditional approach to segmenting guest traffic requires 'pulling' the guest VLAN through the corporate network**

Many customers:

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

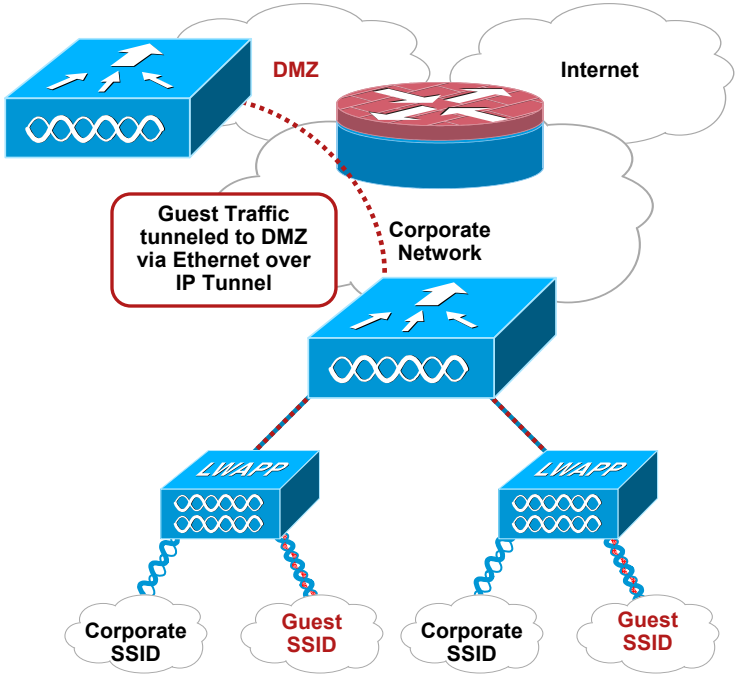
or

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

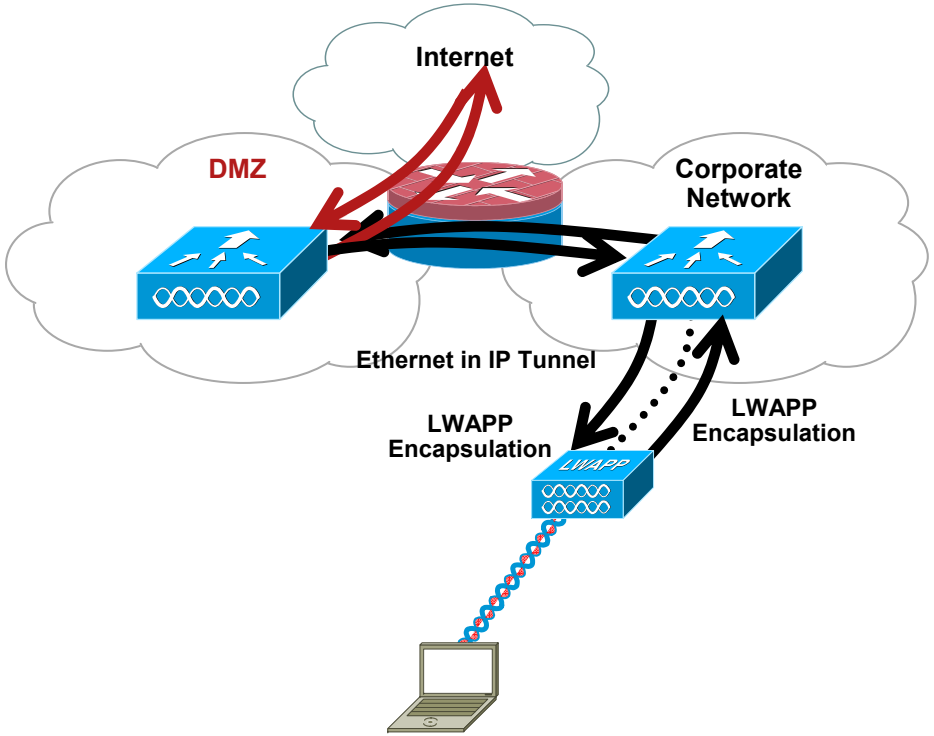


Tunnel Guest Traffic to the DMZ

- 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

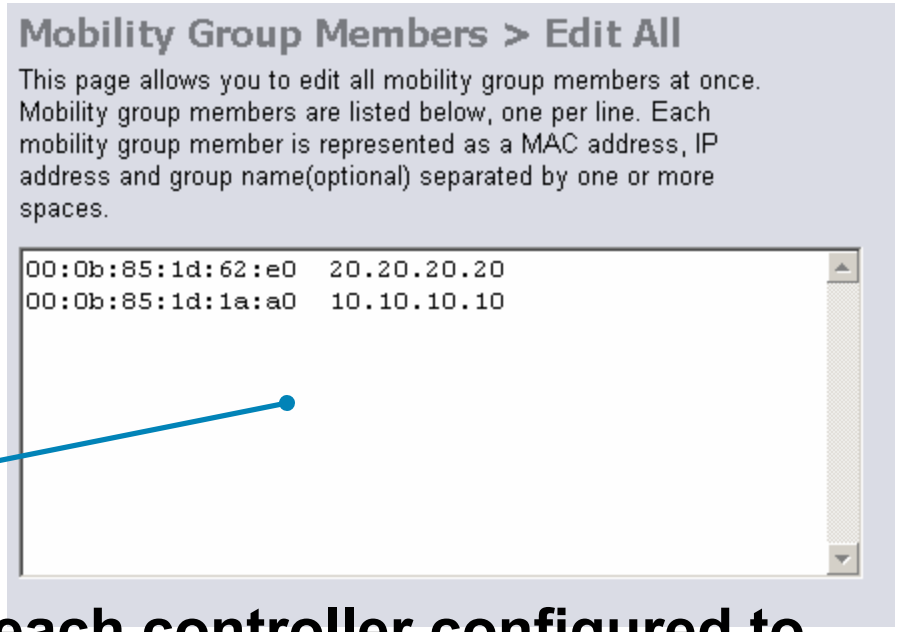


Guest Traffic Flows



Guest Tunneling Configuration

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



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

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

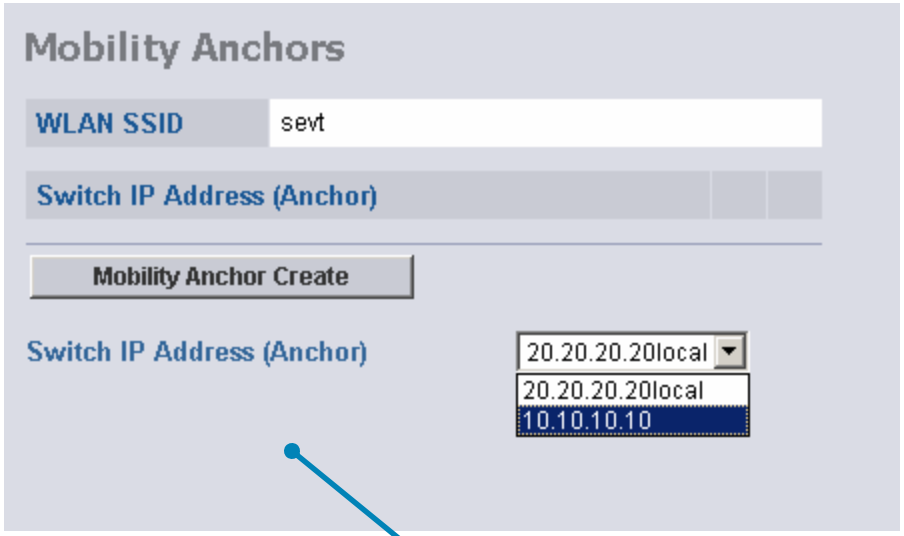
  WLCs on the 'internal' network will only require the same Mobility Group Name if roaming between them is desired; the DMZ controller(s) need not share this name.

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**



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 enables encryption for inter-WLC communications

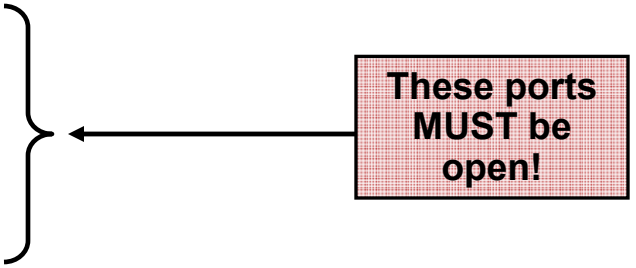
This is only necessary when backward compatibility with legacy Airespace equipment is required in secure mode

Firewall Entries

- **Open ports for:**

  Inter-Controller Tunneled Client Data – IP Protocol 97

  Inter-Controller Control Traffic – UDP Port 16666 (or 16667, if encrypted)



- **Optional management/operational protocols:**

  SSH/Telnet – TCP Port 22/23

  TFTP – UDP 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

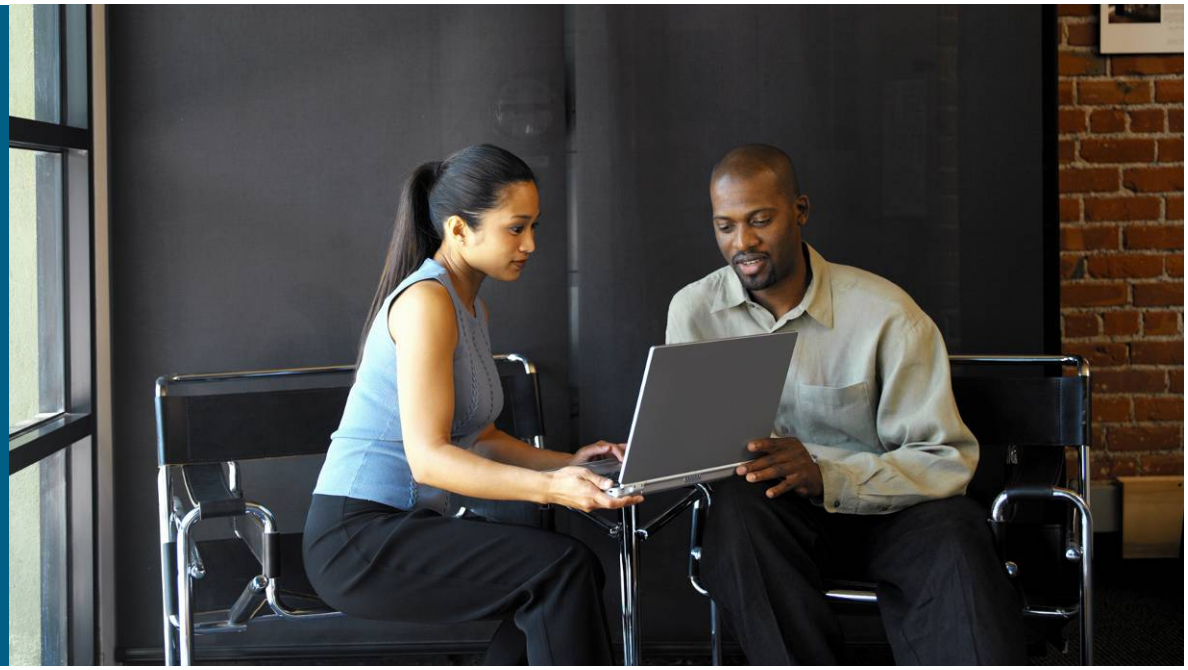
- **Total throughput and client limitations per supported DMZ controller**
  - **4100 – 1 Gbps and 1,500 total clients**
  - **4402 – 2 Gbps and 2,500 total clients**
  - **4404 – 4 Gbps and 5,000 total clients**
  - **WiSM – 8 Gbps and 10,000 total clients**
- **Each DMZ controller can handle up to 40 tunnels from internal WLCs**
  - **Tunnels are counted per WLC, irrespective of the number of tunneled WLANs**
- **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**

Design Considerations and Limitations (continued)

- You can load up the DMZ with multiple controllers for added capacity
- As each new client connects, the internal controllers will selectively load balance across the DMZ controllers
- There is a heartbeat between internal and DMZ controllers, so if a DMZ controller fails, alarms are generated

  Though that's all well and good, there's no failover mechanism today – wait for Concannon

Location Design



Cisco 2710 Location-Based Services

Cisco 2710 Location Appliance

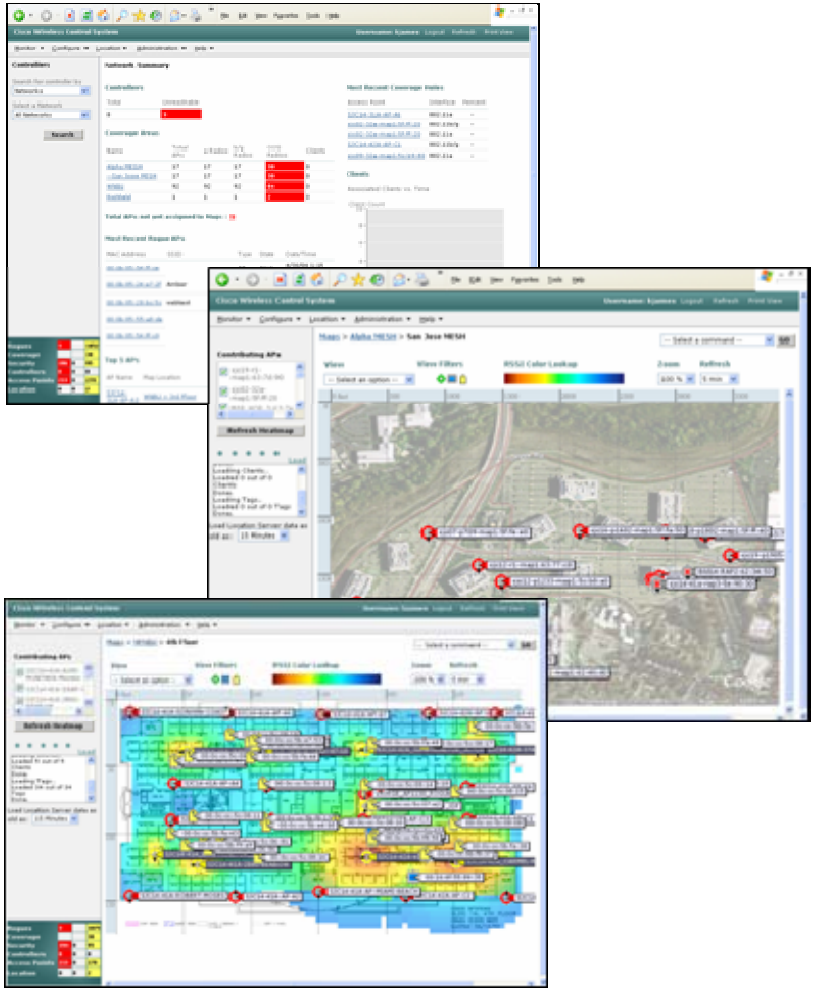
- Cisco 2700-Series Wireless Location Appliance—AIR-LOC2710-L-K9
- Advanced RF fingerprinting utilized for high accuracy location tracking within a few meters
- Real-time location tracking
  - Wi-Fi client devices
  - Wi-Fi active RFID tags
  - Rogue clients and APs
- Industry's 1st location solution integrated into a WLAN infrastructure
  - No client software required
  - No proprietary RF readers—leverages the existing Cisco WLAN infrastructure

WCS, Controllers, and the Location Appliance

- WCS is the single “front end” for location
- All configuration and management of the Location Appliance is done through WCS
- Visual representation, as well as historical replay of location data is performed by WCS
- Network designs kept in both WCS and the 2700
- Device information is forwarded from controllers up to the Location Appliance where it is stored

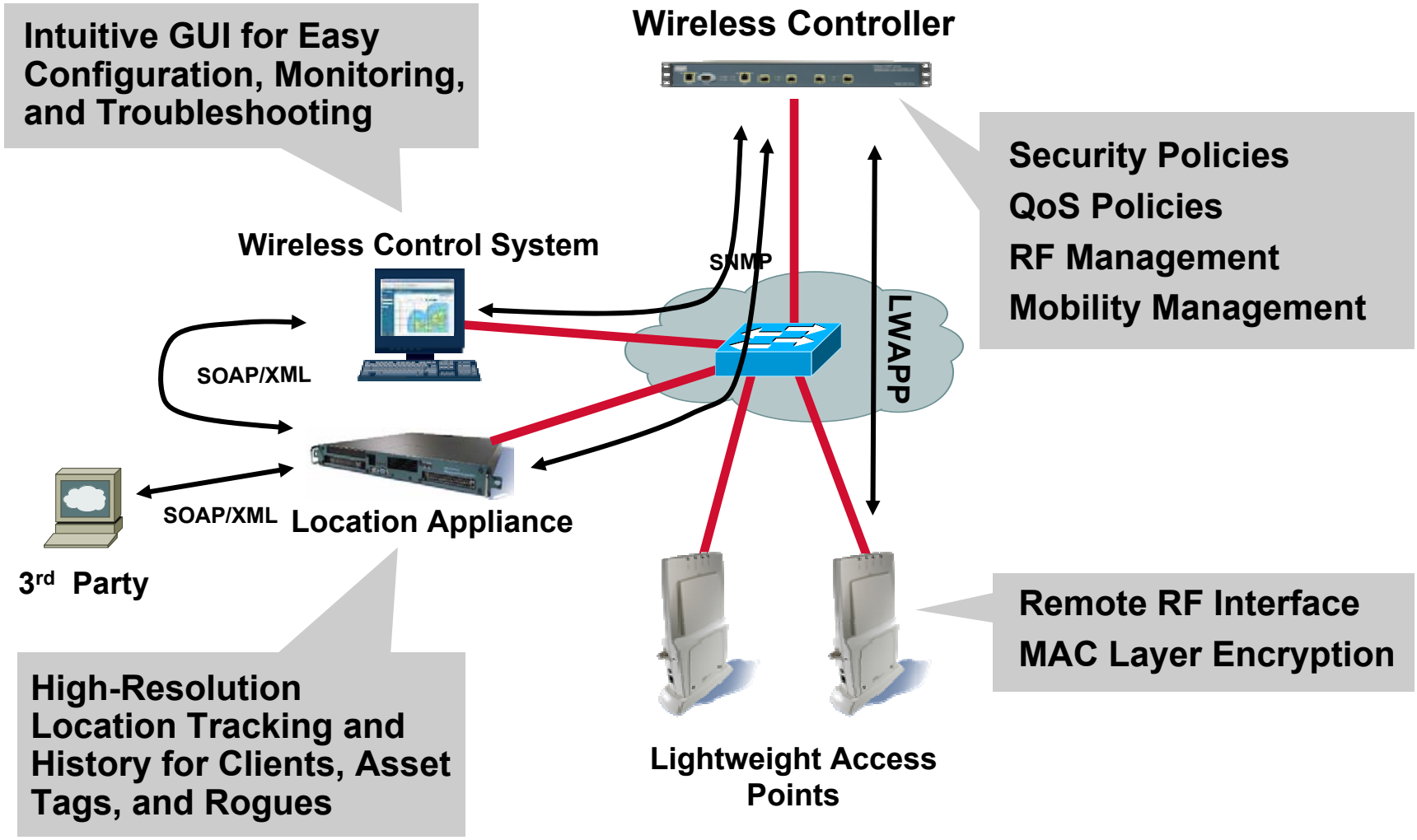
Cisco Wireless Control System (WCS)

- WCS is the management platform for Cisco's controller-based solution
- WCS is used for:
  - Network planning and ongoing monitoring
  - Real-time visibility and control of the air space
  - Unified policies that are centrally managed and enforced
  - Management of Cisco controllers and lightweight APs
- WCS is optional, but highly recommended when:
  - Multiple controllers are deployed, supporting numerous APs
  - Advanced WLAN services are deployed (IDS, location, voice, etc.)



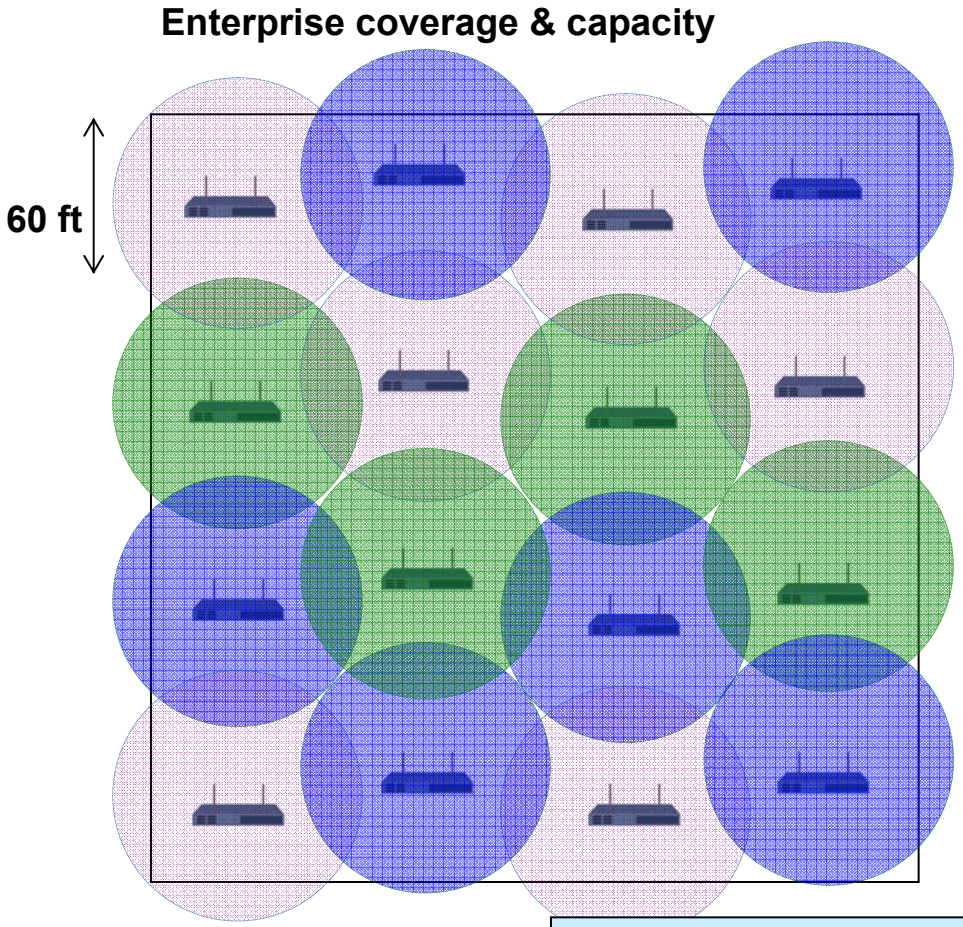
Location General Architecture

Centralized WLAN Solution Overview



Enterprise WLAN Strategy

- Smaller, overlapping cells
- Increased average capacity
  - 802.11a can provide more channels to reduce interference
- Provides higher availability in the event of an AP failure
- APs should not be placed too close together since clients will still transmit at normal power output
  - Clients can cause interference issues with other APS and clients



Graphic is using only 3 channels to show option to avoid interference

802.11a:	11-14 Mbps
802.11g:	11-14 Mbps
802.11b/g:	2 / 2-4 Mbps
802.11b:	2 Mbps

Location Appliance Highlights

- Ability to track up to 2500 devices (hard limit)
- Track all active 802.11 RF devices
  - Clients
  - Rogues (APs and clients)
  - Asset tags
- Display of multiple devices on network floor plan
- Playback of device location (history)
- Provides a “northbound” API for third party application integration (to select partners only)
- Scalable—just add additional 2700s and manage everything through WCS

Location Appliance Deployment Considerations

- Location appliance accuracy
  - 10 meters 90% and 5 meters 50% (new accuracy considerations)
- Higher density AP deployment (Enterprise WLAN)
  - Supports enterprise WLAN
  - Higher location tracking accuracy
- RF coverage provided outside of building perimeter
  - Higher location tracking along building edges
- Location appliance only functions with active 802.11 RFID tags
  - Passive 802.11 RF ID tags will not work
  - Cisco working with many vendors towards passive-active RF ID convergence
- Location appliance only functions with AP with supported fingerprint
  - RF pattern key to RF fingerprinting algorithm

WCS OS/Client Support Version 4.0

- OS Support
  - Windows 2003 (all editions)
  - RedHat Enterprise Linux - RHEL4-AS & RHEL4-ES
- Hardware Requirements

	AP	WLC	CPU	CPU Speed	RAM	HD
High End	3,000	250	Xenon Quad	3.2 GHz	8 GB	200 GB
Standard	2,000	150	Dual Core	3.2 GHz	4 GB	80 GB
Low End	500	50	Single	3 GHz	2 GB	60 GB
WLSE	1,500	100	Supports 1130 “Non Dell” hardware			

- Client Browser Support

  IE 6.0/SP1 on Windows

CiscoWorks WLSE converted to WCS

High End system requires tuning to perform adequately

Architecture Considerations Location

Architecture Questions

- How many Assets?

  Assets include anything you need to track i.e. beds, computers, tags, infusion pumps, employees, high risk patients, expensive equipment.

- How many buildings?

- Growth Potential?

Deploying with Location in Mind

- AP placement and density are crucial
- General guidelines:

  Each device needs to be heard at better than -75 dBm by no fewer than 3 APs/Monitors

  The more APs/Monitors that hear a device, the better

  Optimal AP/Monitor density is approximately one every 50 to 70 linear feet, depending on the environment and WLAN requirements

  Place APs/Monitors toward the perimeter of coverage areas

Architecture limitations

- Network design is many to one Location Appliance

  meaning you can have many network designs all tracked by a single location appliance
- Controller to Location appliance is one to one mapping
- WCS knows about all elements in design

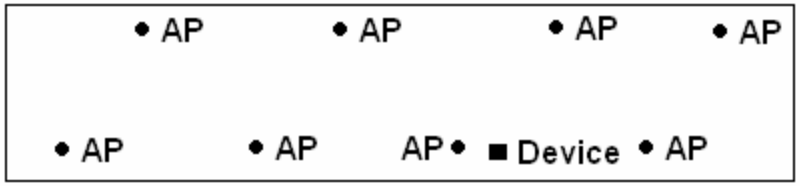
Location Planning for AP Placement

Location AP Deployment Considerations Manual Configuration

- While AP density is met with the example to the left, both density and location requirements are met in the example to the right

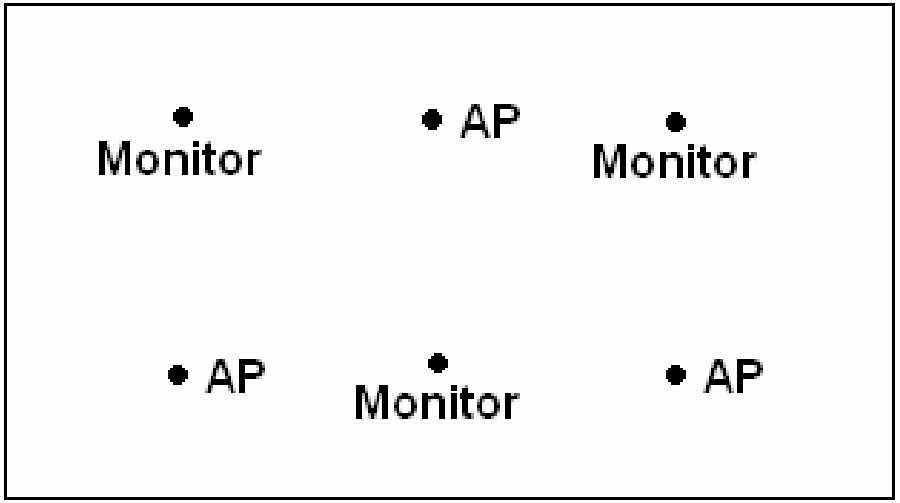
Though the above design may provide enough AP density for high bandwidth applications, location will suffer because each AP's view of a single device isn't varied enough and thus, location will be difficult to determine

By moving the APs to the perimeter of the coverage area and staggering them, each will have a higher likelihood of offering a distinctly different view of the device, resulting in higher location fidelity



Location AP Deployment Considerations (Cont.)

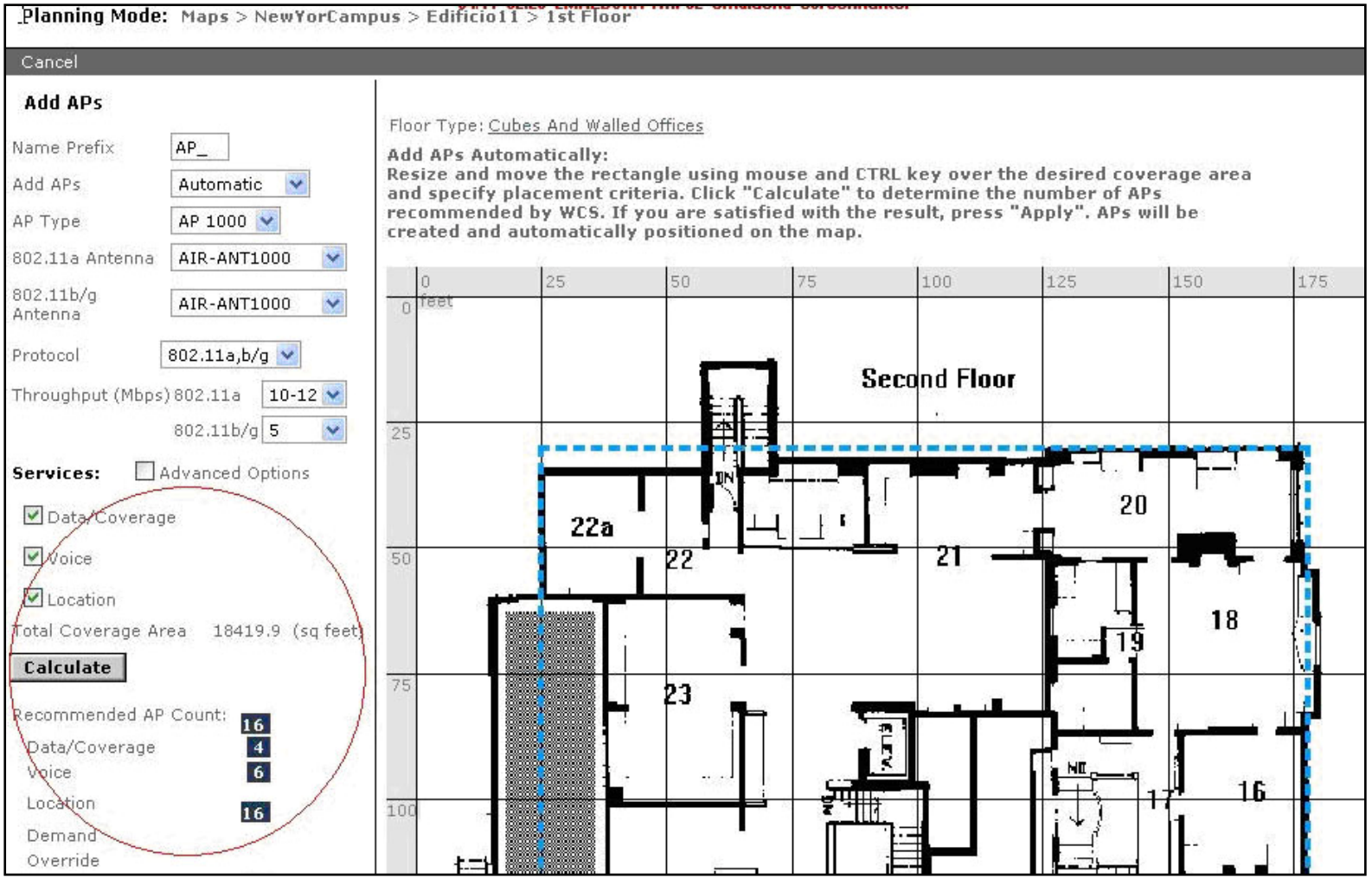
- Utilization of Monitor APs can help location in some cases, especially 802.11b-only implementations



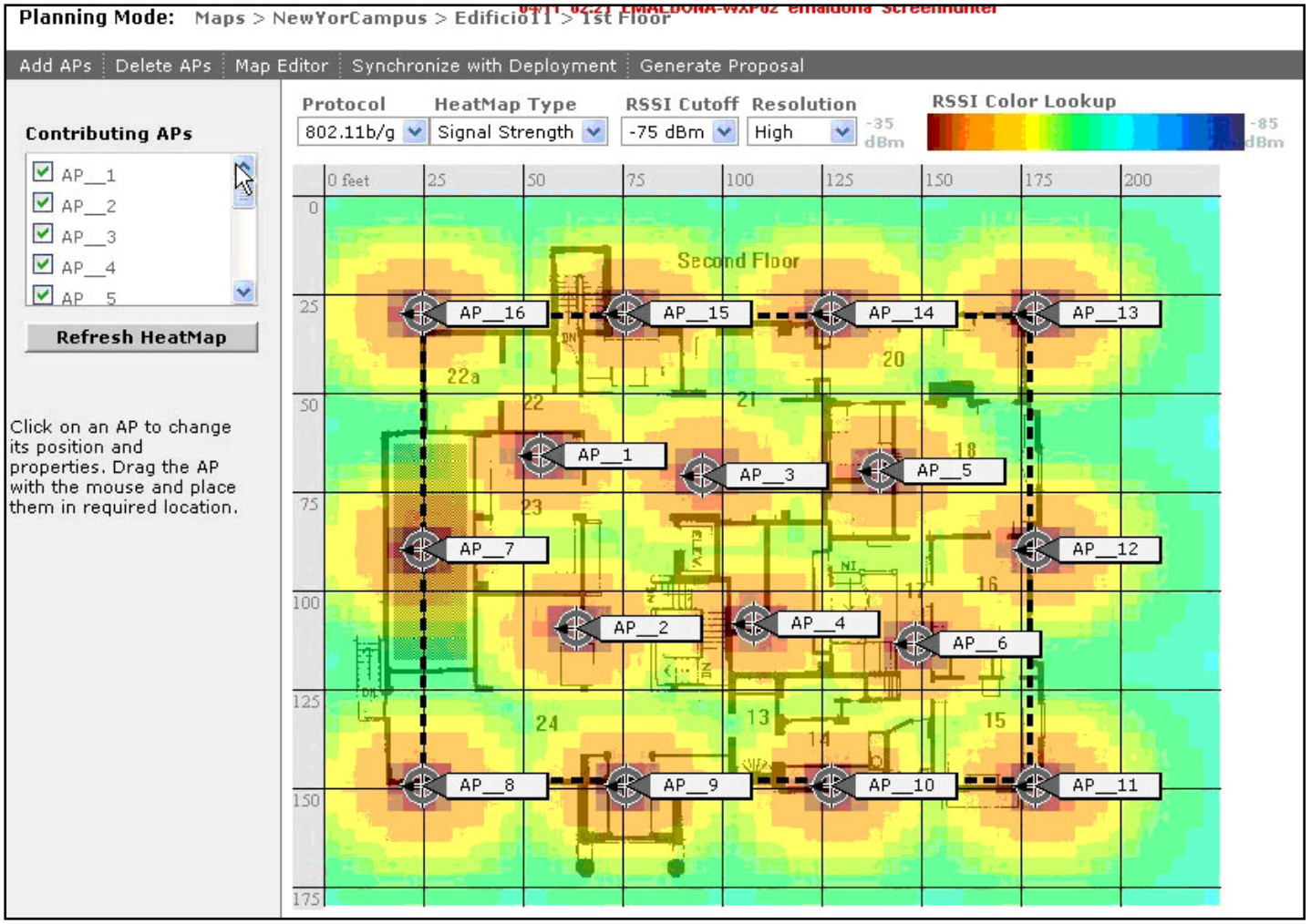
Less dense WLAN installations, such as those of voice networks, will find their location fidelity greatly increased by the addition and proper placement of Monitor APs

- Monitor APs are listen only devices

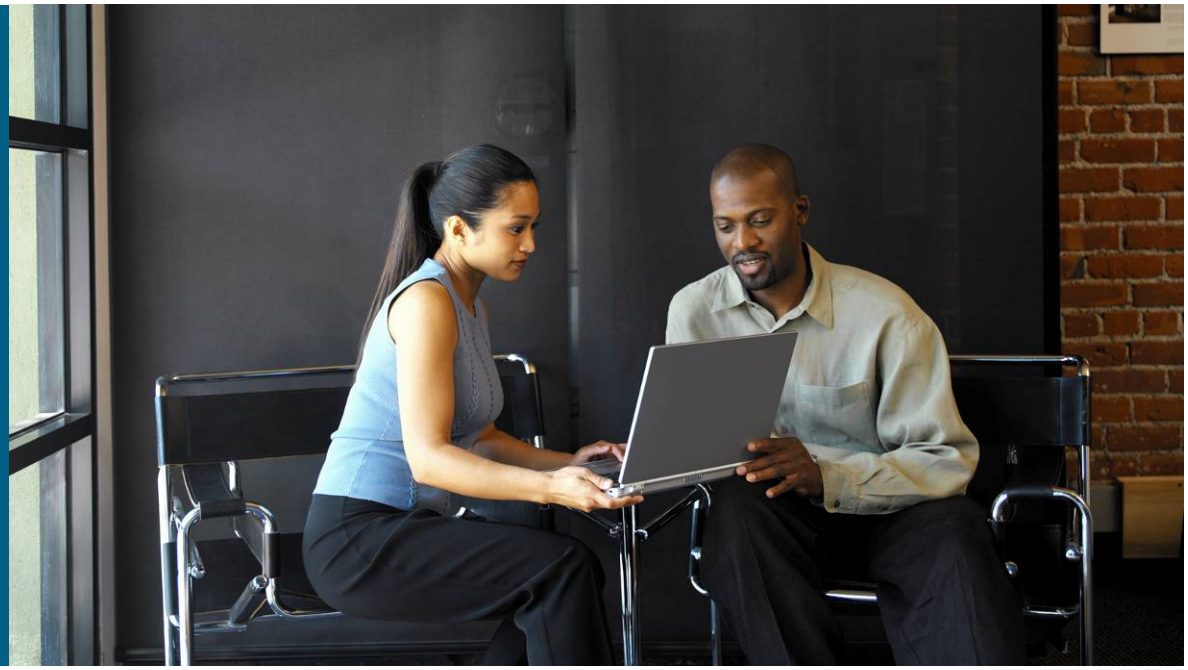
Location Planning



Planning Mode (Cont.)



RRM



Radio Resource Management

- Key RF challenges with 802.11's unlicensed bands:
  - Limited non-overlapping channels
  - Physical characteristics of RF propagation
  - Contention for the medium
  - Transient nature of RF environments
- RRM addresses these challenges:
  - Continuous assessment of RF environment
  - Dynamic channel and power management
  - Coverage holes: Detection and Correction
  - Coverage resiliency and co-channel issues mitigation
- Can tweak and/or override for non-standard deployments

RRM - What happens where, and when?

Functionality	Performed at/by:	When
RF Grouping	WLCs elect the Group Leader	WLC Boot-up or reboot*
Dynamic Channel Assignment	Group Leader	Every 600 seconds
Transmit Power Control	Group Leader	Every 600 seconds
Coverage Hole Detection and Correction	Local WLC	Every 180 seconds**

*The RF Grouping algorithm then runs at 600 second intervals

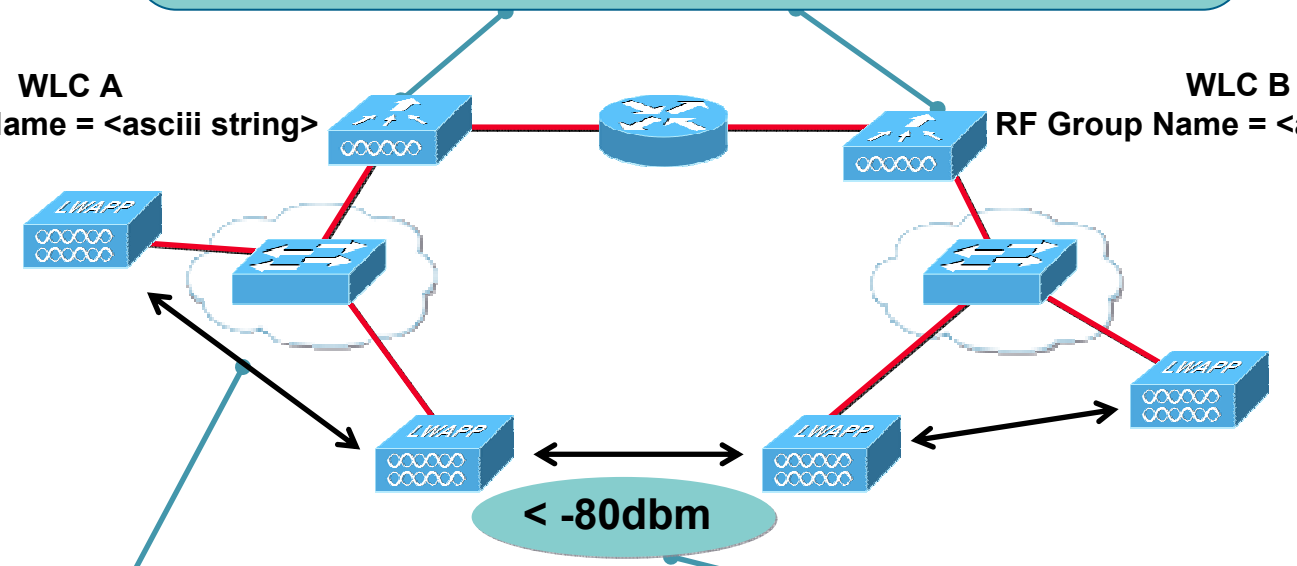
**This value (defaulting to 180 seconds) is modifiable by changing the “Coverage Measurement” parameter from the “Monitor Intervals” section.

RF Grouping

RF GROUPING: Controllers elect an RF Group Leader that analyzes RF data and neighbor relationships to make optimized decisions about the RF environment for the entire system

WLC A
RF Group Name = <asciii string>

WLC B
RF Group Name = <ascii string>

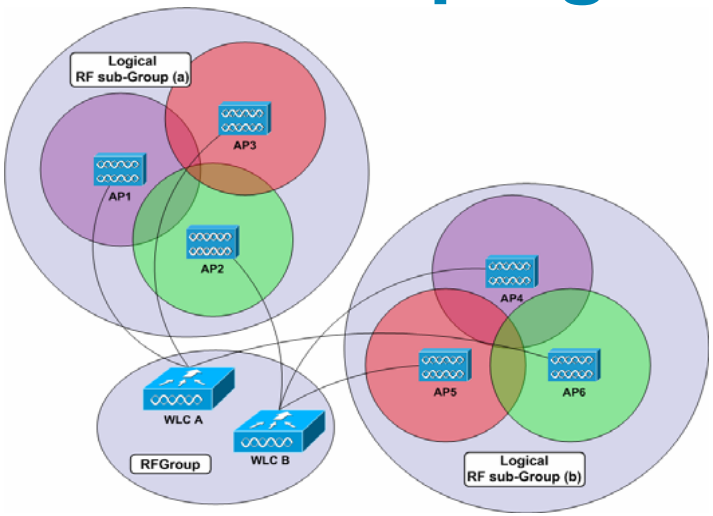


NEIGHBOR MESSAGES:

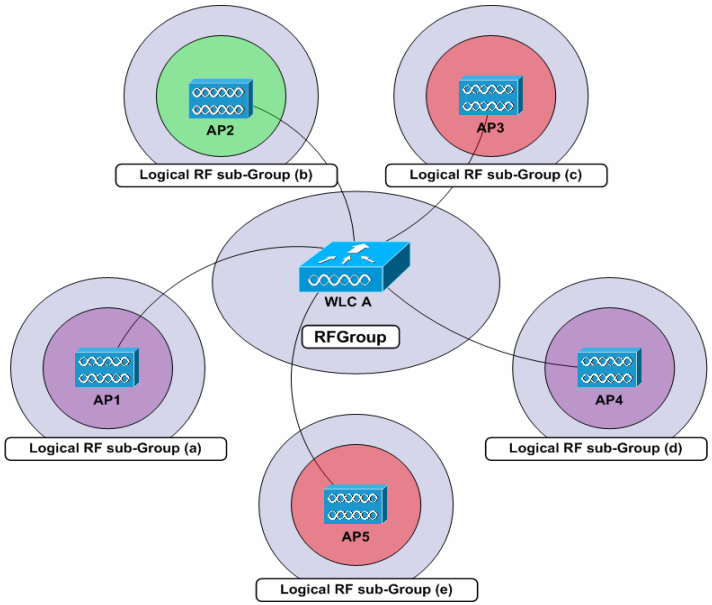
- Sent at full power and lowest supported datarate
- Sent every 60 seconds
- Contain information about the AP
- Authenticated via a MIC based on RF Group Name

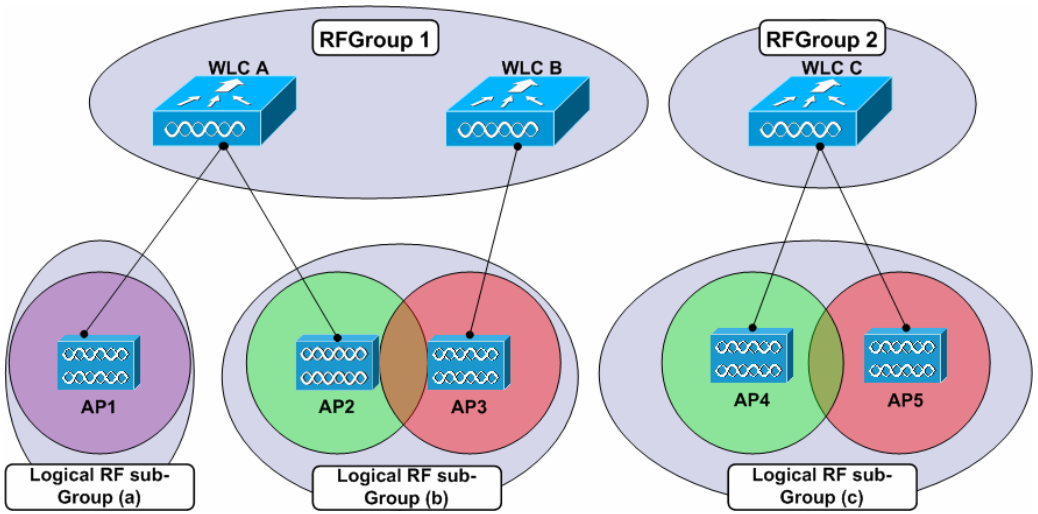
- If APs on different controllers hear neighbor messages from APs in the same RF Group at -80 dBm or stronger, they group their RF domains
- Channel and power settings then computed by the Group Leader
- RF Grouping happens at the WLC level. APs do not form groups

RF Grouping



- Multiple “RF sub-Groups” can exist within a single RF Group
- RRM is calculated on a per RF sub-Group basis
- RF Domains can be inter or intra-controller
- Multiple RF sub-Groups may be formed even when controllers share an RF Group name
- RF Groups/Domains apply per PHY type
- Group leader need not be the same for both PHY types





Verifying AP Neighbors

- Can the AP see others?

  Monitor ↳Wireless ↳ [802.11a|802.11b/g Radios] ↳Radio Detail

- How many?
- How well?

  show ap auto-rf [802.11a/802.11b] <Cisco AP>

- Are other APs on the same WLC or different WLC?

  This affects grouping at the WLC level

Dynamic Channel Assignment (DCA)

- Out-of-the box APs begin transmitting on channels 1 (2.4 GHz), 36 (5 GHz)—RRM will make changes to the channel-plan subsequently, if necessary
- Running APs will resume service on their previously assigned channel-plan across reboots
- Metrics reported by each AP to controller:

  Load: % total time transmitting/receiving 802.11 frames

  Noise: AP calculated noise values on each serviced channel

  Interference: % of the medium taken up by contending 802.11 transmissions

  Signal Strength: RSSI values of the AP's neighbors
- RF Group Leader analyzes AP-specific metrics to determine near-optimal channel plan and make changes as necessary
- Special weighting and dampening logic is applied as part of the DCA algorithm to minimize channel plan alterations and prevent system-wide changes

Transmit Power Control (TPC)

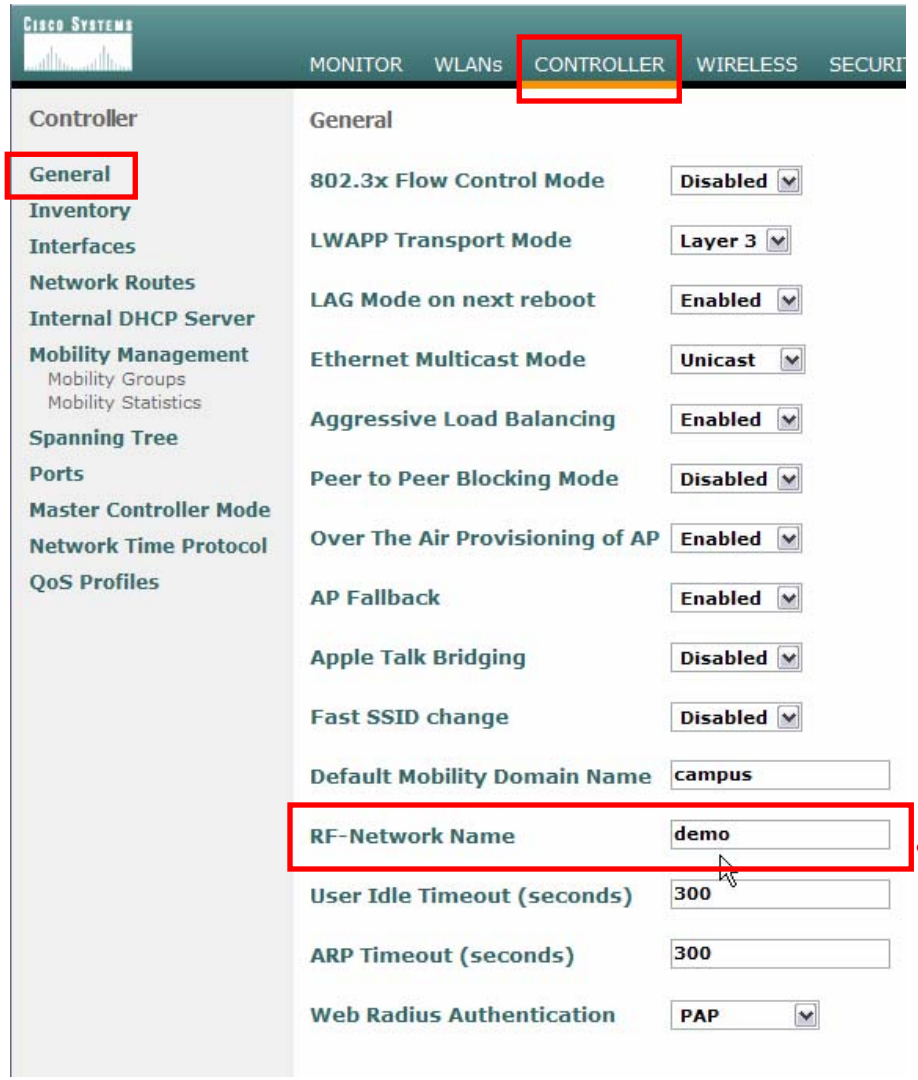
- Out-of-the-box APs transmit at the highest power setting
- Running APs will resume service at their previous transmit power settings across reboots
- RF Group leader applies TPC algorithm per-AP, per-band
- RF Group leader adjusts the AP transmit power so that the 3rd “loudest” neighbor will be heard at -65dBm or lower
- TPC algorithm will only adjust transmit power down
- Transmit power increase is a function of Coverage Hole Detection and Correction algorithm

Coverage Hole Detection and Correction (CHA)

- Coverage Hole Detection and Correction algorithm adjusts transmit power up, compensates for “dead” APs
- Coverage Hole Detection and Correction is run per controller, every 180 seconds
- “Coverage Hole” – client SNR level crosses SNR threshold for a minimum of 60 seconds
- Controller adjusts transmit power up in the event of a coverage hole
- SNR threshold varies based on AP transmit power and controller coverage profile value (configurable)

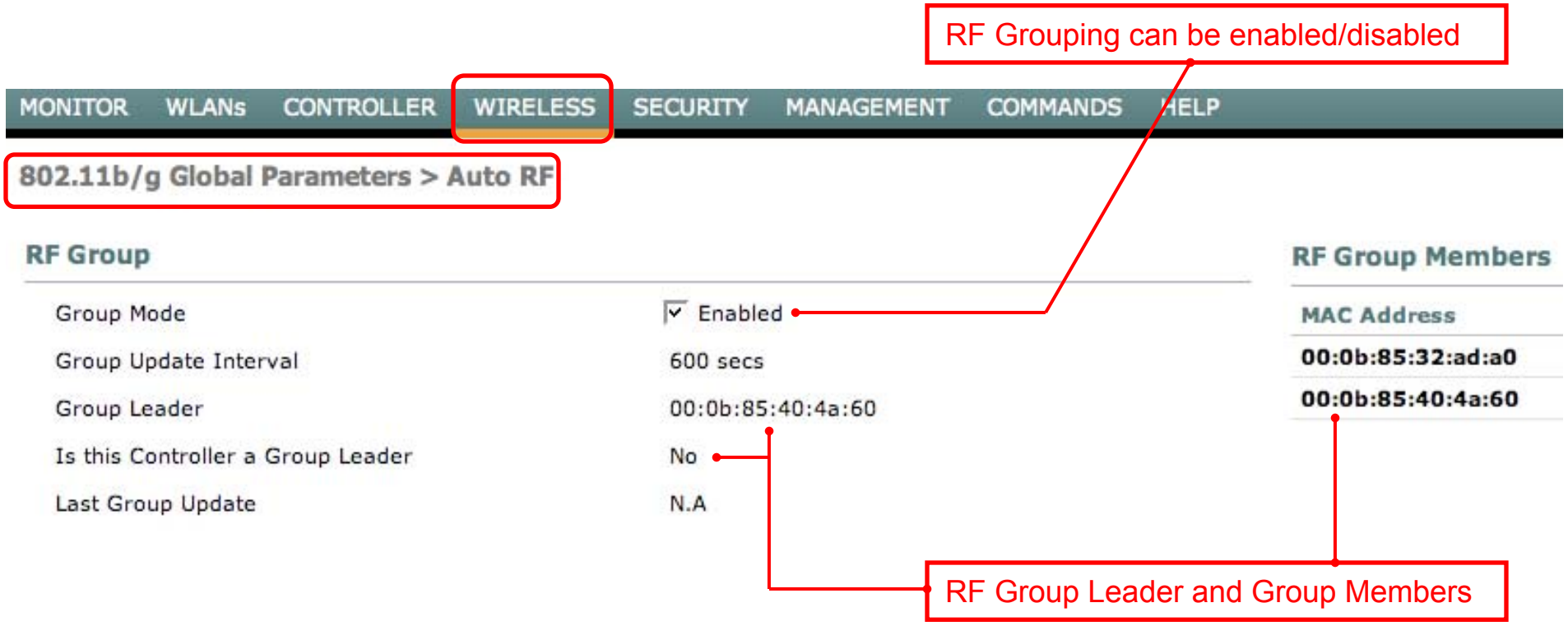
Client SNR Threshold = AP Transmit Power – Constant Value – Coverage Profile Value

RRM Configurable Parameters - RF Grouping

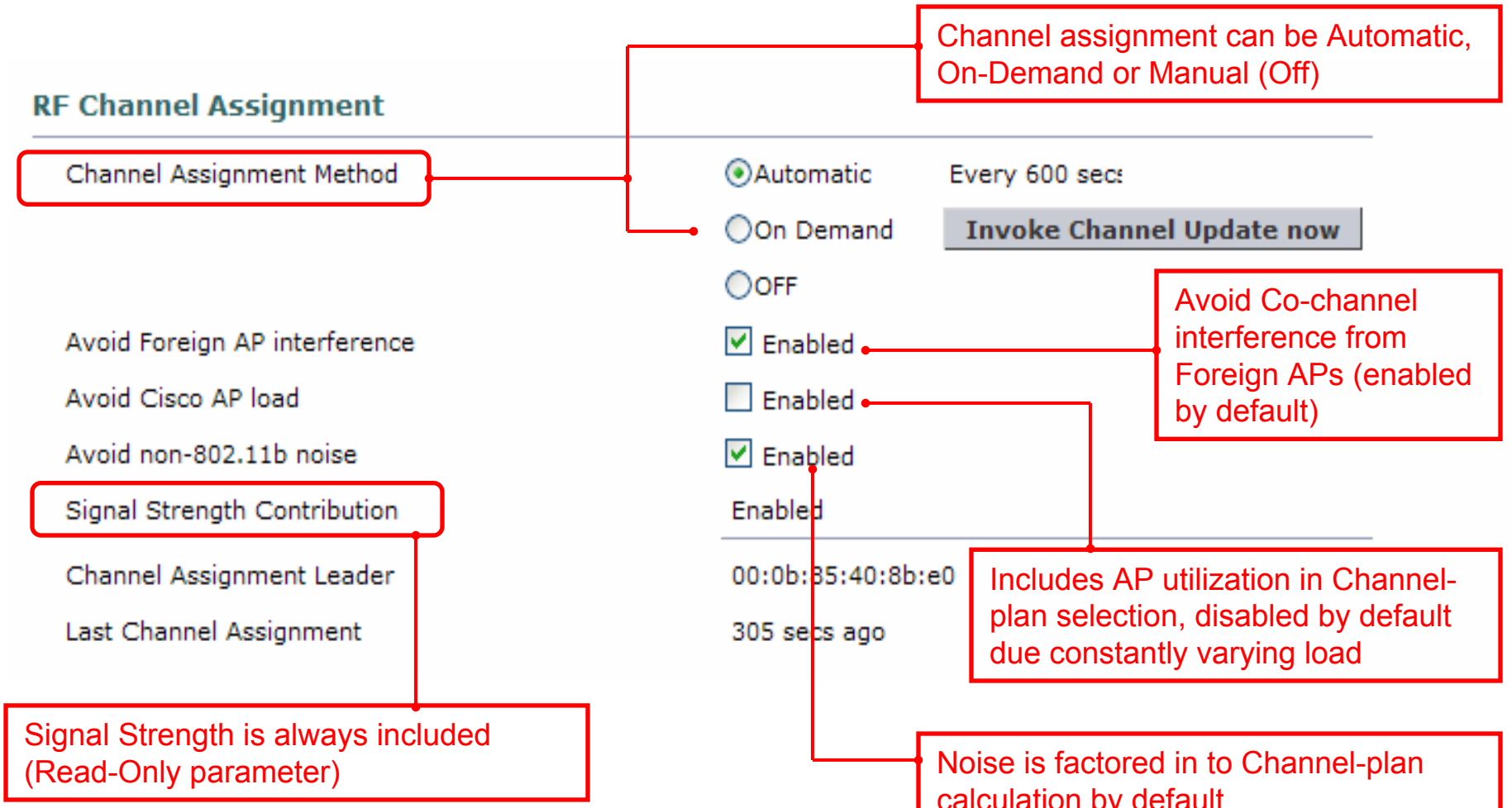


RF Group Name != Mobility Domain Name

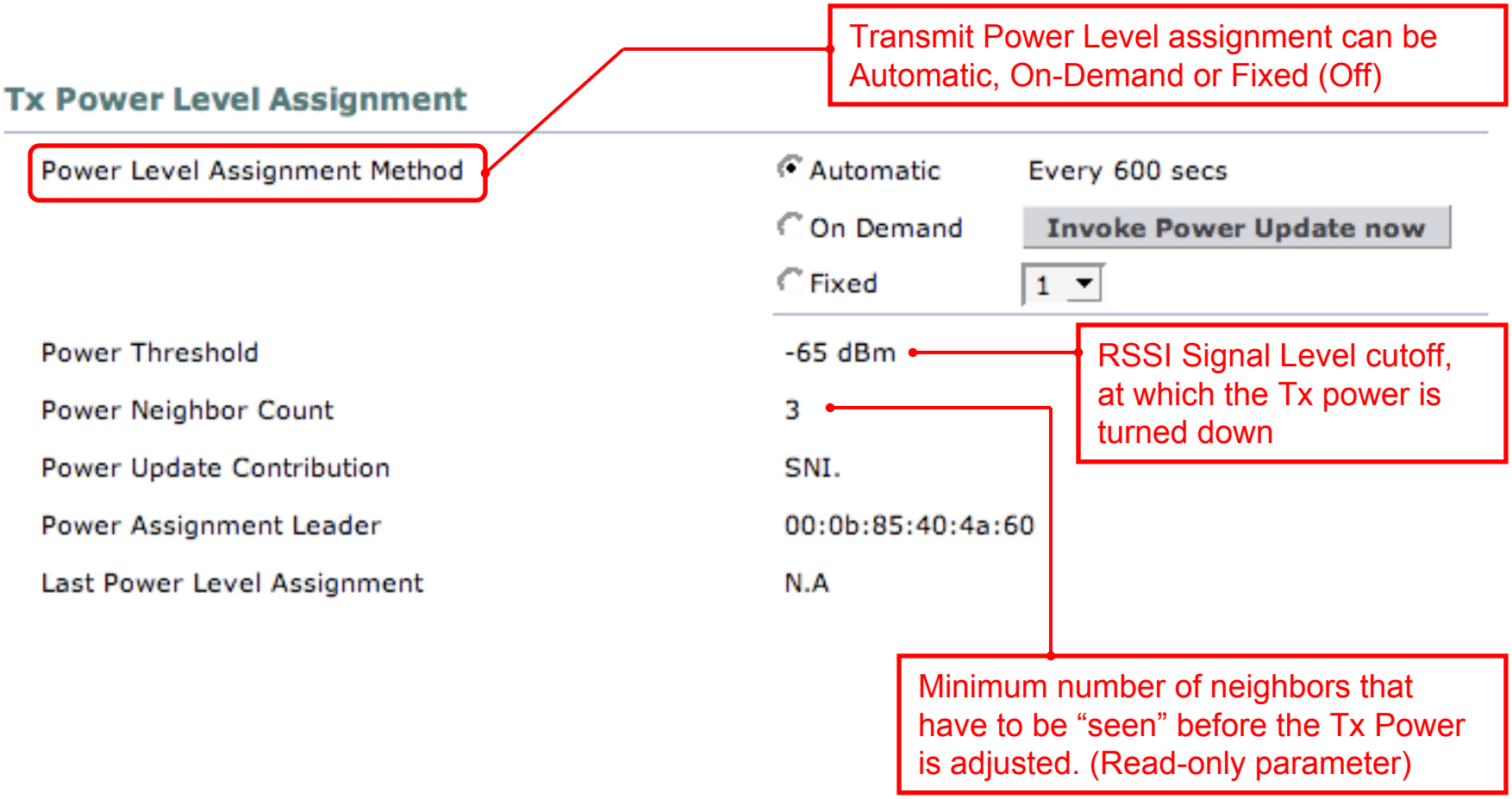
RRM Configurable Parameters - RF Grouping



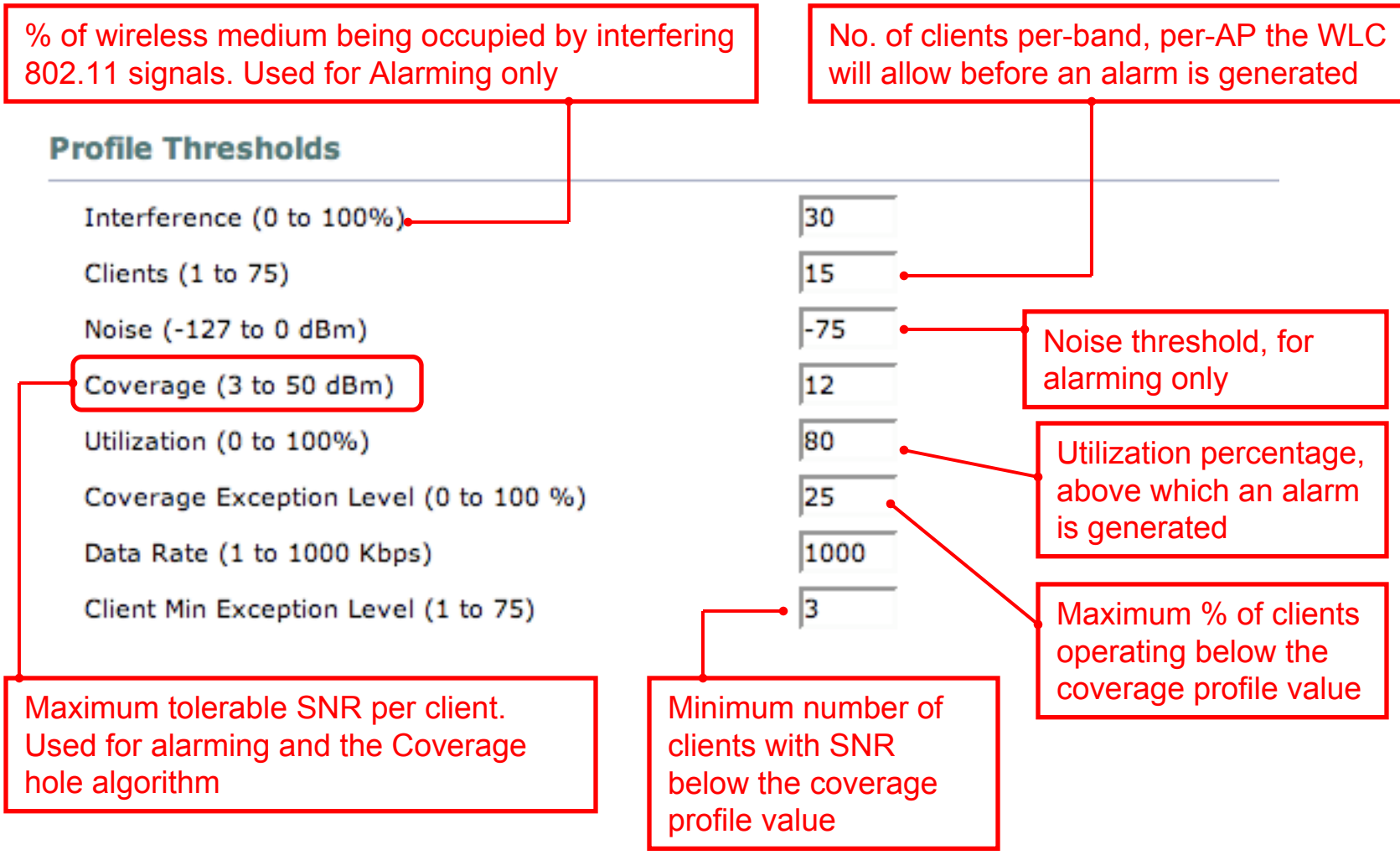
RRM Configurable Parameters - DCA



RRM Configurable Parameters - TPC

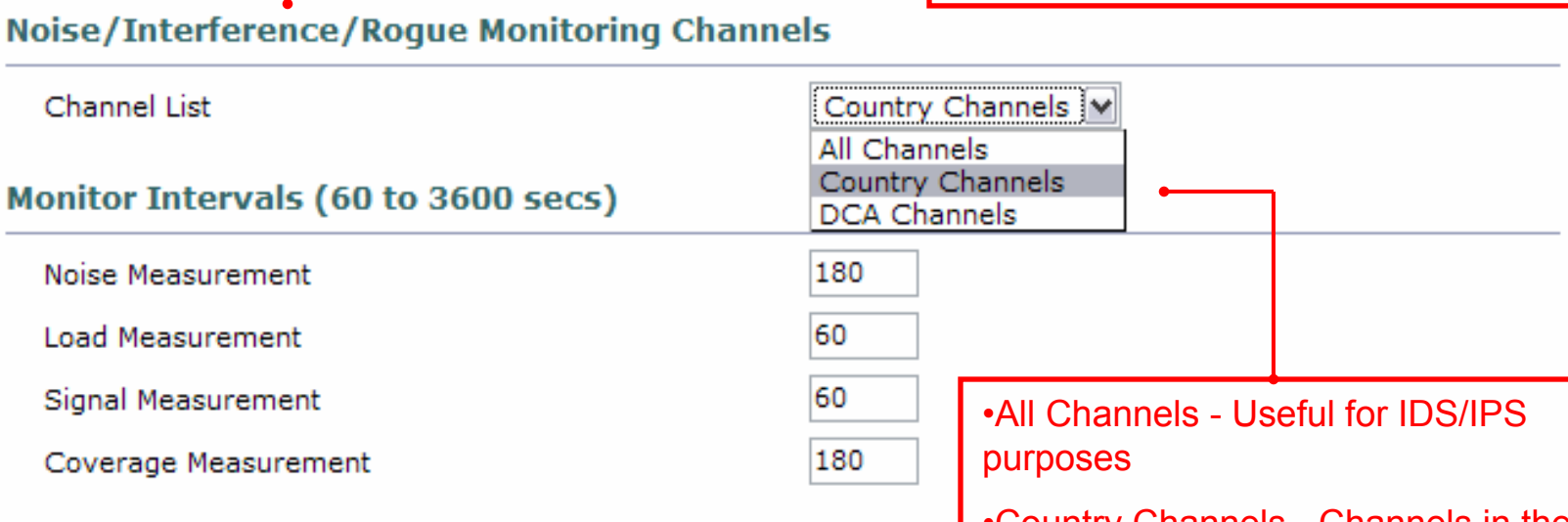


RRM Configurable Parameters - Profile Thresholds



RRM Configurable Parameters - Monitoring Parameters

APs gather RRM data for each channel in the configured channel list



Adjusting monitoring intervals changes the frequency at which the APs perform RRM measurements

- All Channels - Useful for IDS/IPS purposes
- Country Channels - Channels in the configured regulatory domain
- DCA Channels - Channels only in the Dynamic Channel assignment list. Can be configured to add/remove channels from this list

Advance Commands and Tweaks

- Adjusting TPC
  - To reduce cell-sizes in “hot” environments to reduce overlap
  - To reduce collision and retry rates
  - To reduce high co-channel interference in dense deployments
  - config advanved 802.11b tx-power-thresh
- Changing Profile Thresholds
  - Everything used for reporting only (except “Coverage Profile”)
- Adding/Deleting channels from DCA channels list
  - config advanced 802.11b channel [add|delete] <channel #>
- Changing Monitor Intervals
  - Impacts
  - Why change?

TPC - Before and After

AP 1	AP 2	AP 3	AP 4
AP 2 at -46dBm	AP 3 at -47dBm	AP 2 at -43dBm	AP 2 at -48dBm
AP 3 at -53dBm	AP 4 at -52dBm	AP 4 at -57dBm	AP 3 at -51dBm
AP 4 at -71dBm	AP 1 at -49dBm	AP 1 at -59dBm	AP 1 at -58dBm

AP 1	AP 2	AP 3	AP 4
AP 2 at -46dBm	AP 3 at -47dBm	AP 2 at -43dBm	AP 2 at -48dBm
AP 3 at -53dBm	AP 4 at -52dBm	AP 4 at -57dBm	AP 3 at -51dBm
AP 4 at -71dBm	**AP 1 at -69dBm**	**AP 1 at -65dBm**	**AP 1 at -68dBm**

Remember: Only the 3rd Loudest neighbor's power is adjusted downward

CHA - Before and After

- First - the equation:

Client SNR Threshold = AP Transmit Power – Constant Value – Coverage Profile Value

- Consider:

  Client SNR = 13dB

  AP's Tx Power = 11 dBm (power level 4)

  WLC's Coverage profile threshold = 12 dB (default)

- Algorithm applied:

  Client SNR cutoff = 11dBm – 17dBm – 12dB = |-18dB|

  Client's SNR of 13dB is in violation of the present SNR cutoff of 18dB; the Coverage Hole Detection and Correction algorithm increases the AP's transmit power to 17dBm

  Result = Client SNR cutoff = 17dBm – 17dBm – 12dB = |-12dB|

Client Load Balancing*

- Performed across APs per-controller, controller-level function
- Clients are **never** disassociated/de-authenticated
- So, how does it work?

  Reason Code 17 is sent to the client in response to association request

  Clients that honor the association response code 17 “move on” to look for better APs.

  Lot of ‘not-so-smart’ clients, a.k.a sticky clients do no honor reason code 17 and are let on at the **2nd** attempt.

  AP Selection for client is based on AP utilization and best client SNR to AP

- Improve roaming and differentiate from competition:

  S51 (CCXv4 - example: CB21AG) - Directed roaming, L2 Roam enhancements

  CCKM (LEAP support in CCXv2, all other types in CCXv4)

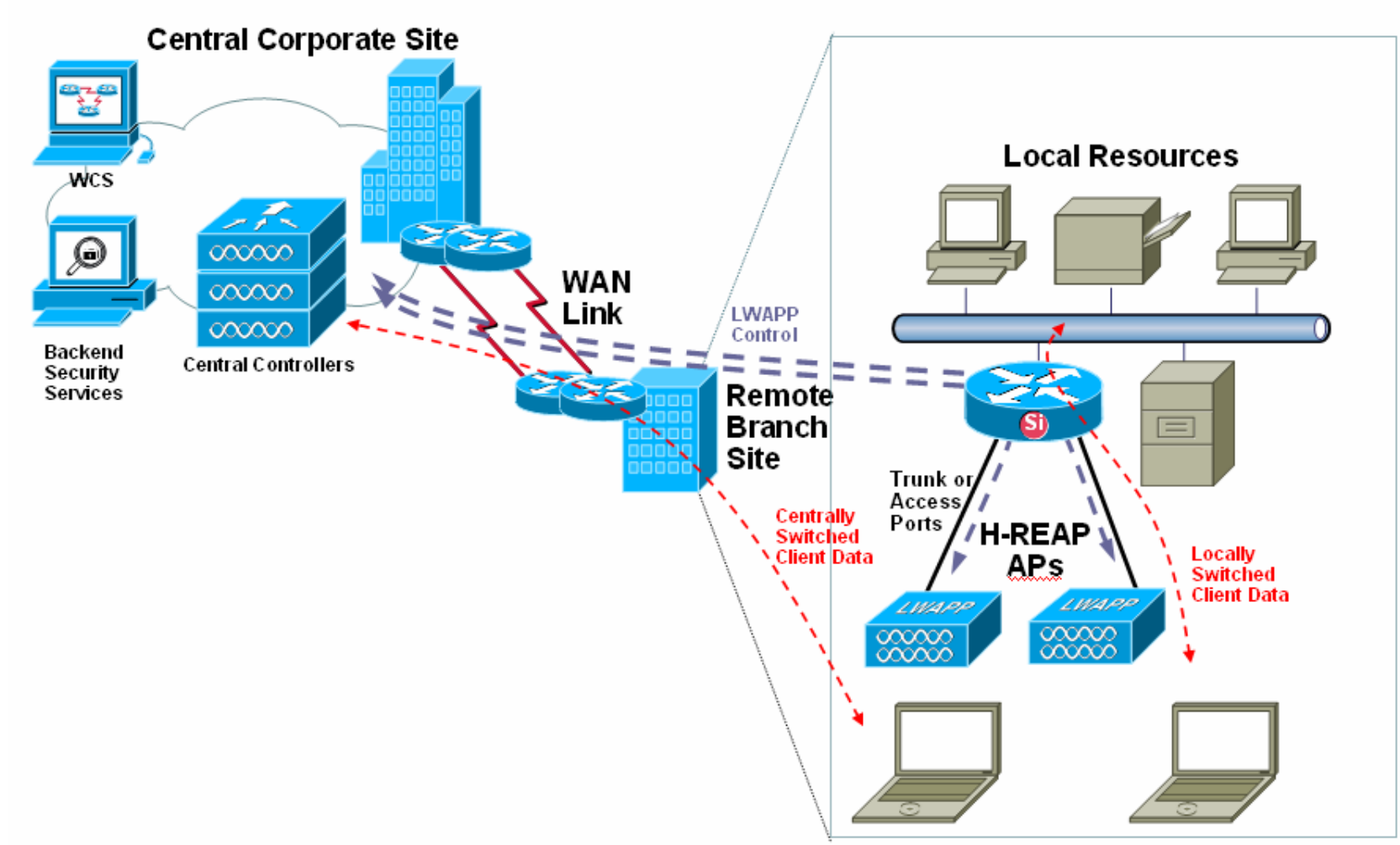
*Not related to RRM in any way

H-REAP

Hybrid REAP

- HREAP solution for small/branch offices and retail on the LWAPP IOS platforms
- WAN outage survivability
- Support for bridging traffic onto local VLANs—"Local Switching"
- Support for tunneling traffic to controller—"Central Switching"
- New AP CLI commands added to LWAPP IOS APs for initial provisioning

Sample HREAP Network



Supported Platforms

- **Access Points:**
  Cisco Aironet 1130, Cisco Aironet 1240
- **Controllers:**
  Cisco 2000 Wireless LAN Controller,
  Cisco 4400 Series Wireless LAN Controller,
  Cisco Catalyst 6500 Series Wireless Services Module (WiSM),
  Cisco Wireless LAN Controller Module,
  Cisco Catalyst 3750G Series Unified Access Switch

Connected Mode vs. Standalone Mode

- **Connected mode—When H-REAP can reach Controller (connected state), the controller is responsible for all (non-802.11) client authentications**

- **Standalone mode—When controller is not reachable by the H-REAP AP (WAN link is down), it goes into the standalone state and does client authentications by itself**

Authentication Supported

Standalone mode

- Open
- Shared
- WPA-PSK
- WPA2-PSK

Connected mode

- Open
- Shared
- WPA-PSK
- WPA2-PSK
- Dynamic WEP / dot1X
- WPA-dot1X
- WPA2-dot1X
- Onboard VPN
- L2TP / IPsec (pass-through)
- Web Auth (onboard / pass-through)

Security Functionality

Security Type	Connected Mode (Centrally Switched)	Connected Mode (Locally Switched)	Standalone Mode (Locally Switched)
Open	Yes	Yes	Yes
Shared	Yes	Yes	Yes
WPA-PSK	Yes	Yes	Yes
WPA2-PSK	Yes	Yes	Yes
Client Exclusion/Blacklisting	Yes	Yes	No *
MAC Address Authentication (onboard or upstream)	Yes	Yes	No new auths.
Dynamic WEP (802.1X)	Yes	Yes	No new auths.
WPA (802.1X)	Yes	Yes	No new auths.
WPA2 (802.1X)	Yes	Yes	No new auths.
Identity-based Networking Services (IBNS)	Yes	Not Supported	Not Supported
NAC	Yes	Yes	No new auths.
WebAuth (onboard or upstream)	Yes	Yes	No new auths.
VPN (onboard or upstream)	Yes	Not Supported	Not Supported †
Cranite	Yes	Not Supported †	Not Supported †
AirFortress	Yes	Not Supported †	Not Supported †

Feature Support

Feature	Connected Mode (Centrally Switched)	Connected Mode (Locally Switched)	Standalone Mode (Locally Switched)
CCKM/PKC Fast, Secure Roaming	Not Supported	Not Supported	Not Supported
CAC and TSPEC	Yes*	Yes*	Not Supported*
RFID / Location-Based Services	Yes	Yes	Not Supported
Client Load-balancing	Not Supported	Not Supported	Not Supported
Peer-to-Peer Blocking	Yes	Not Supported	Not Supported
WIDS	Yes	Yes	Not Supported
RLDP	Yes	Yes	Not Supported
RADIUS/TACACS+ Authentication	Yes	Yes	Not Supported
RADIUS/TACACS+ Accounting	Yes	Yes	Not Supported

Sample H-REAP Configuration

WLAN SSID	Security	Switching
Corporate	WPA2 (802.1X)	Local – VLAN 11
RemoteSite	WPA2 - PSK	Local – VLAN 12
Guest	WebAuth	Central (Tunneled to DMZ Controller)

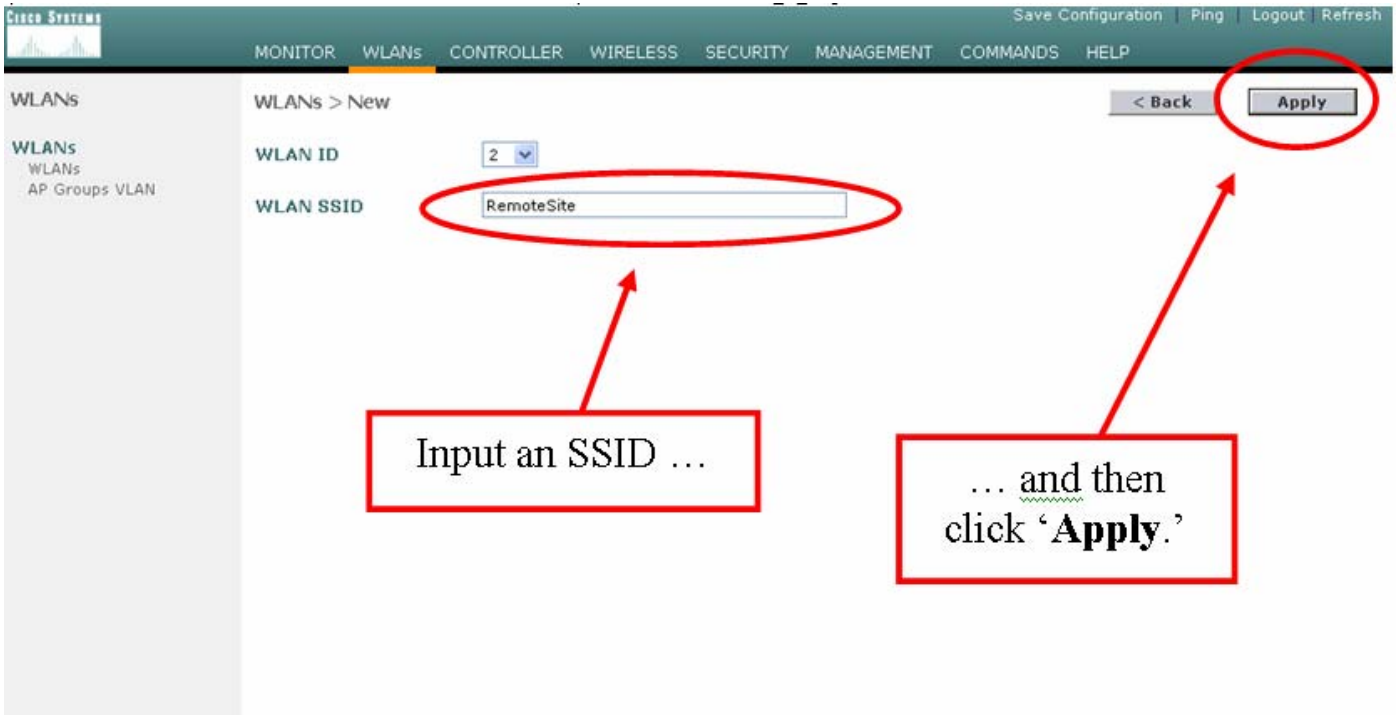
Configuring the AP's Upstream Switch

- AP will get an IP address on the native VLAN
- Sample local switch configuration:

```
ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H-REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
```

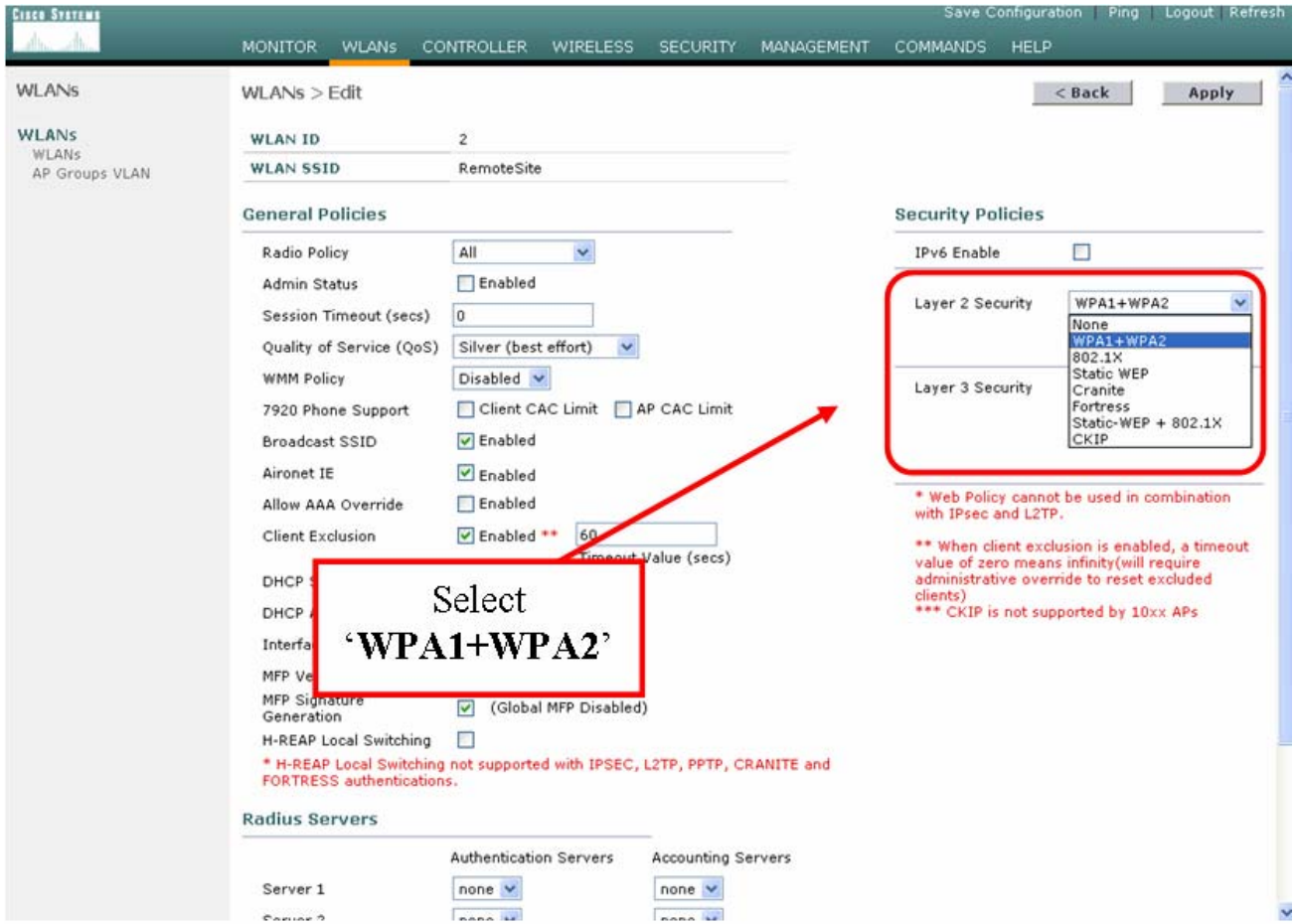
H-REAP WLAN Configuration

- **Create a WLAN**



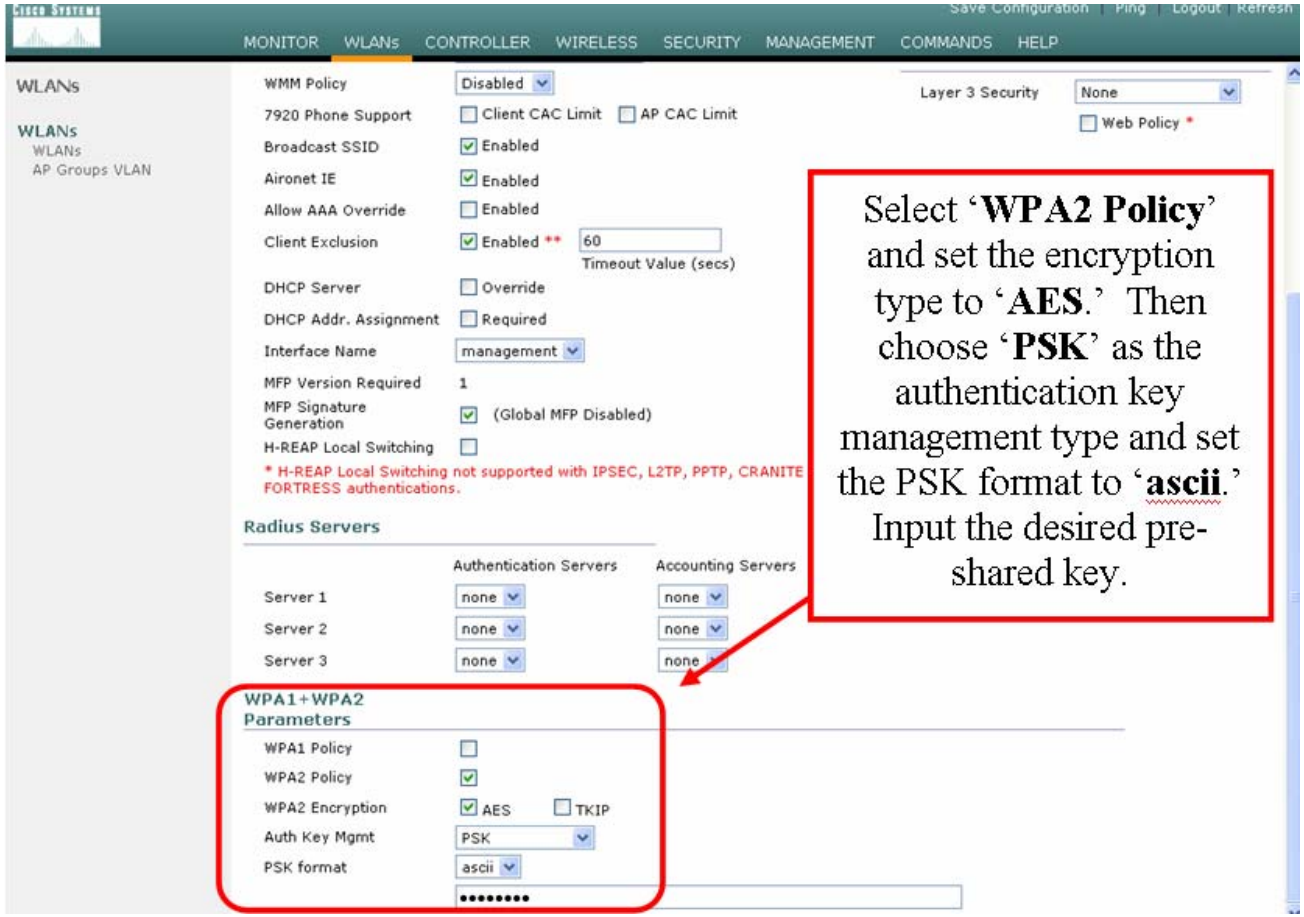
H-REAP WLAN Configuration (continued)

- **Add the appropriate security configuration**



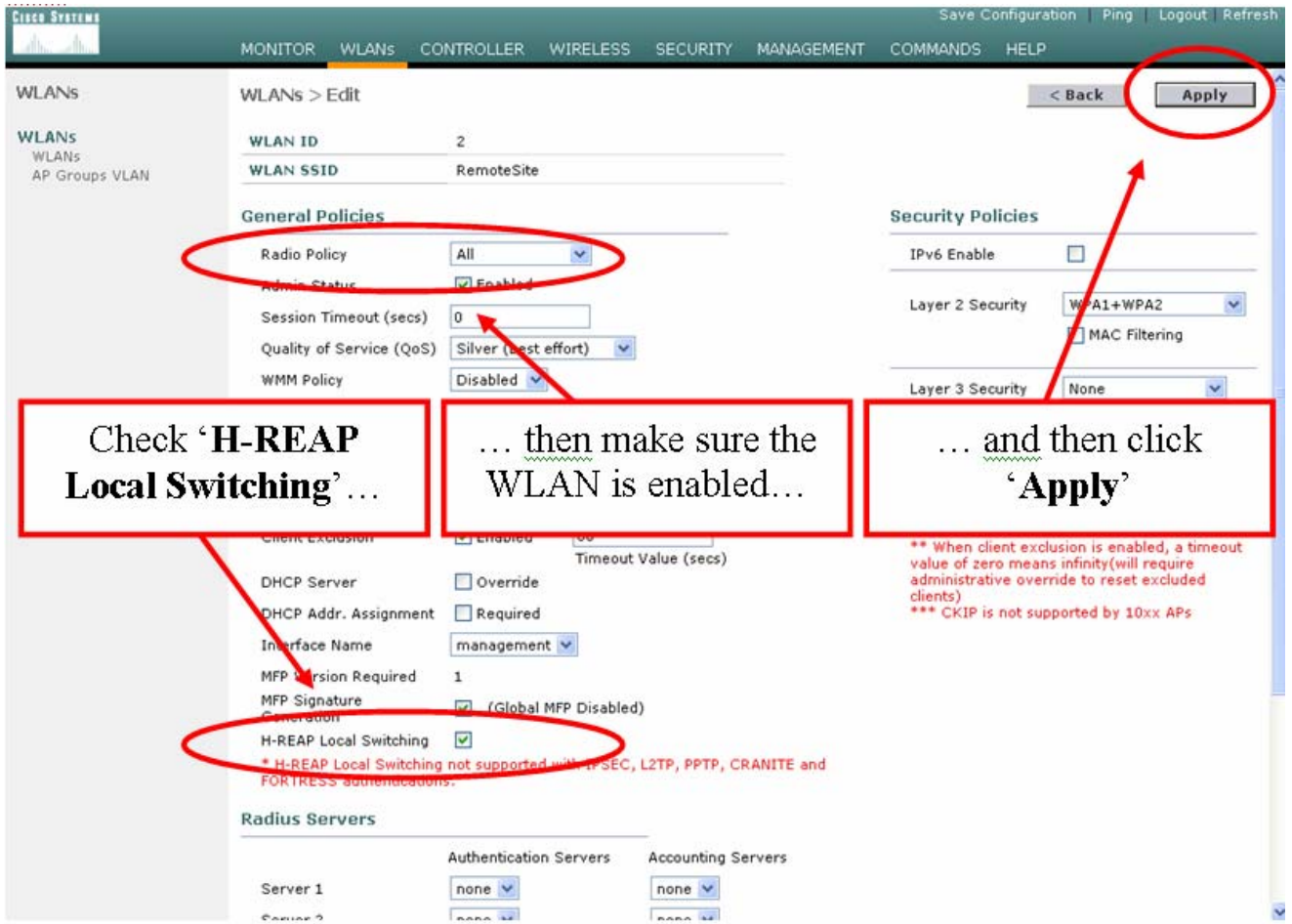
H-REAP WLAN Configuration (continued)

- **Configure the security policy**



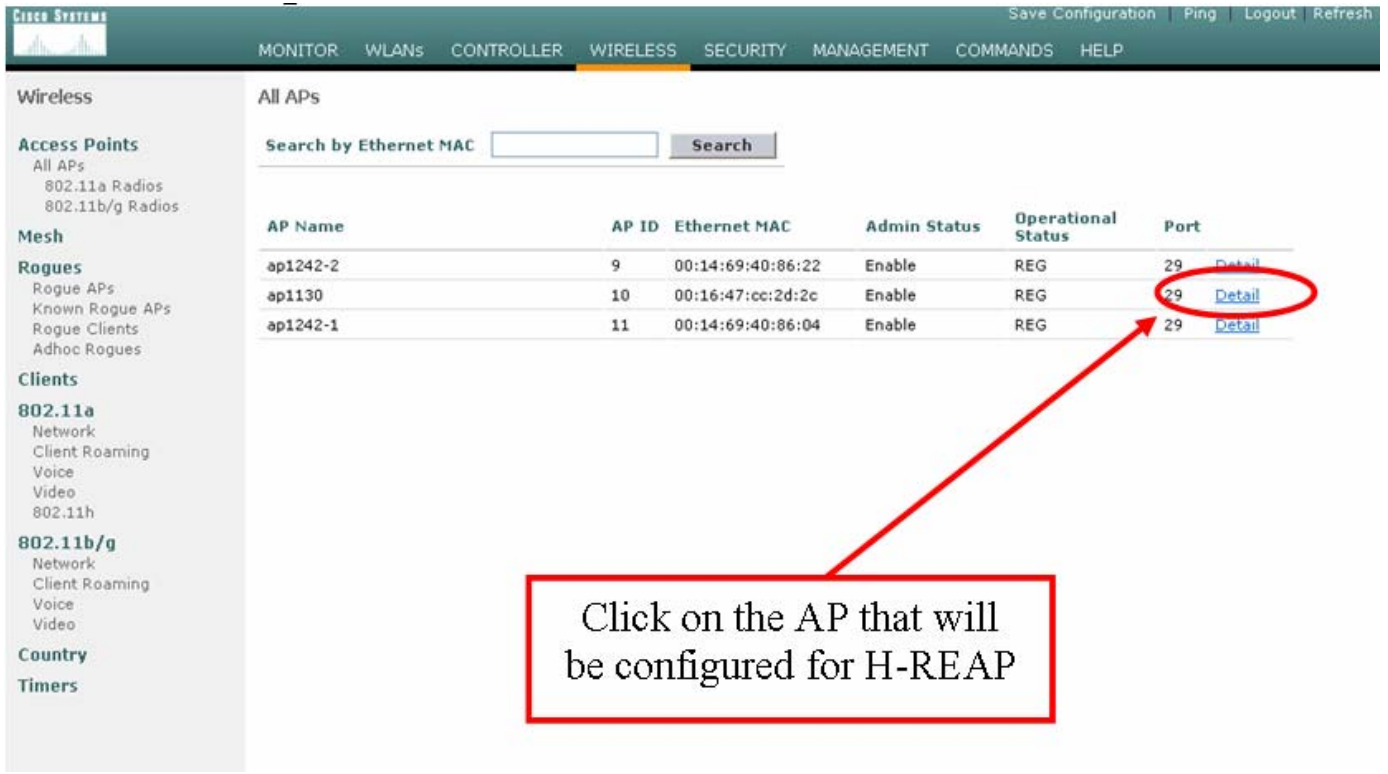
H-REAP WLAN Configuration (continued)

- **Configure the WLAN for H-REAP operation**



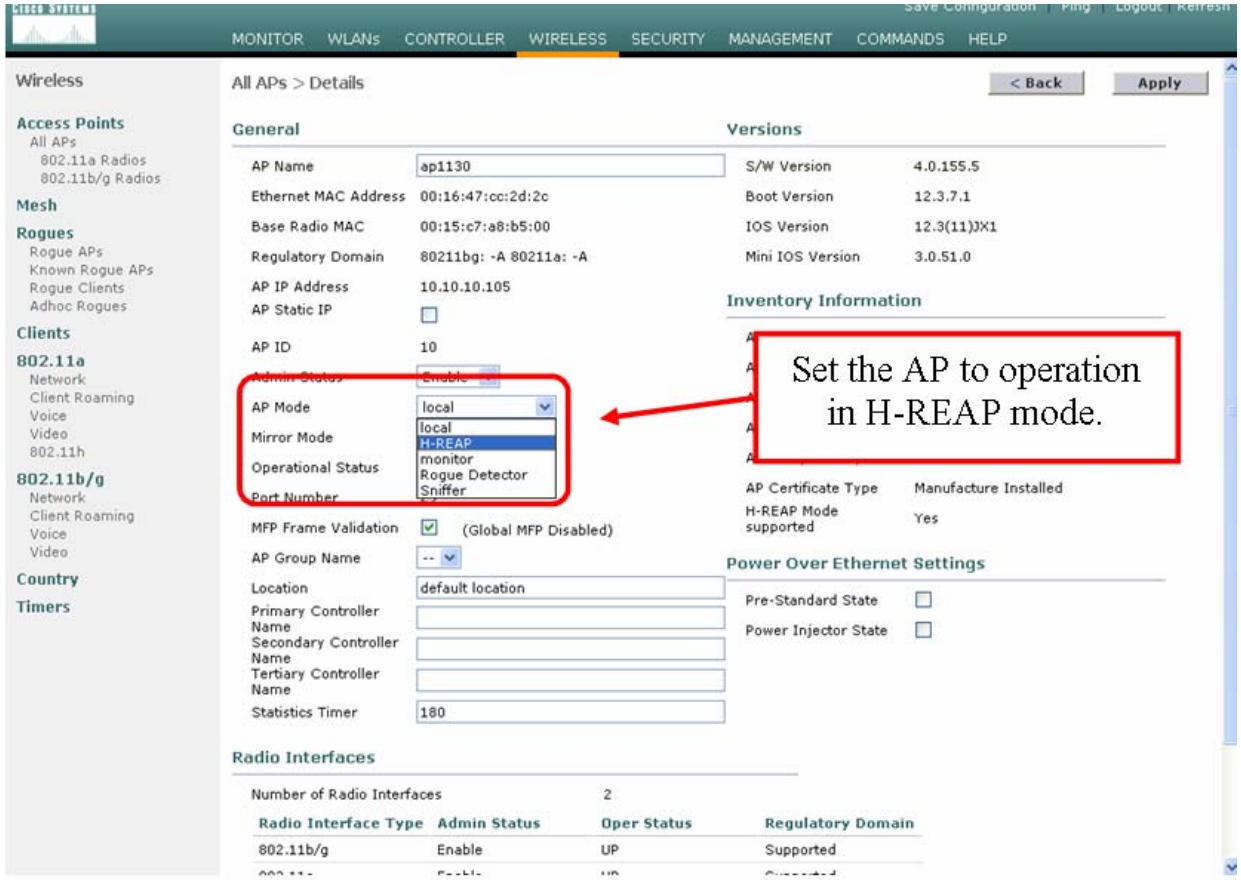
H-REAP AP Configuration

- **Select desired AP...**



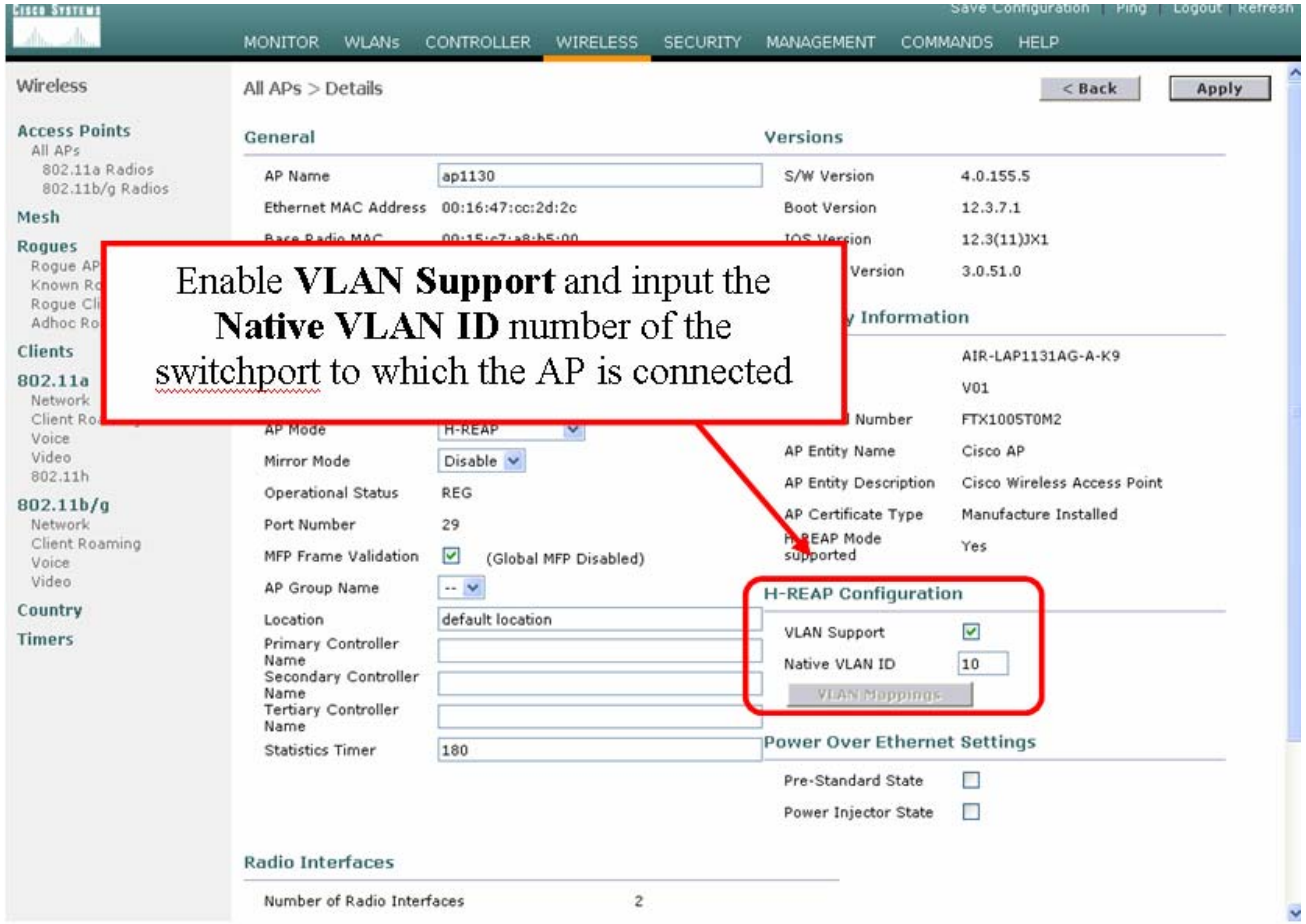
H-REAP AP Configuration (continued)

- **... and set it to H-REAP mode**



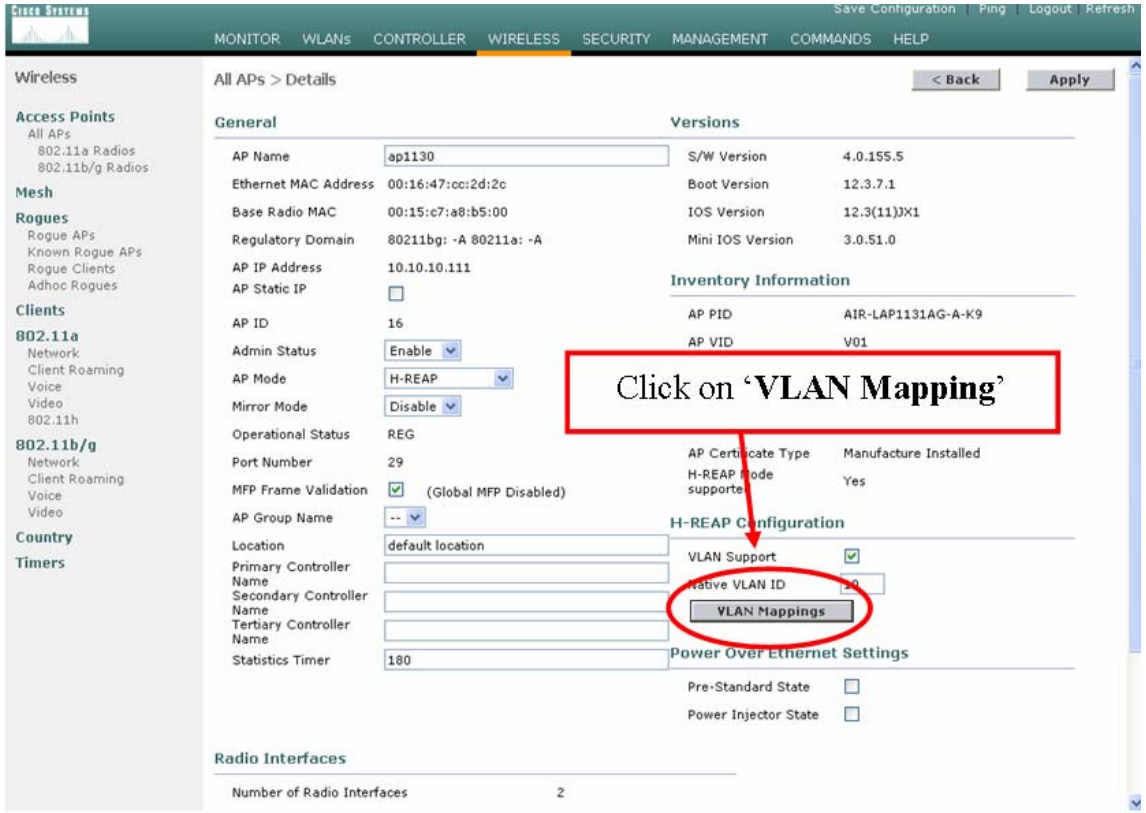
H-REAP AP Configuration (continued)

- **Configure H-REAP switchport operation**



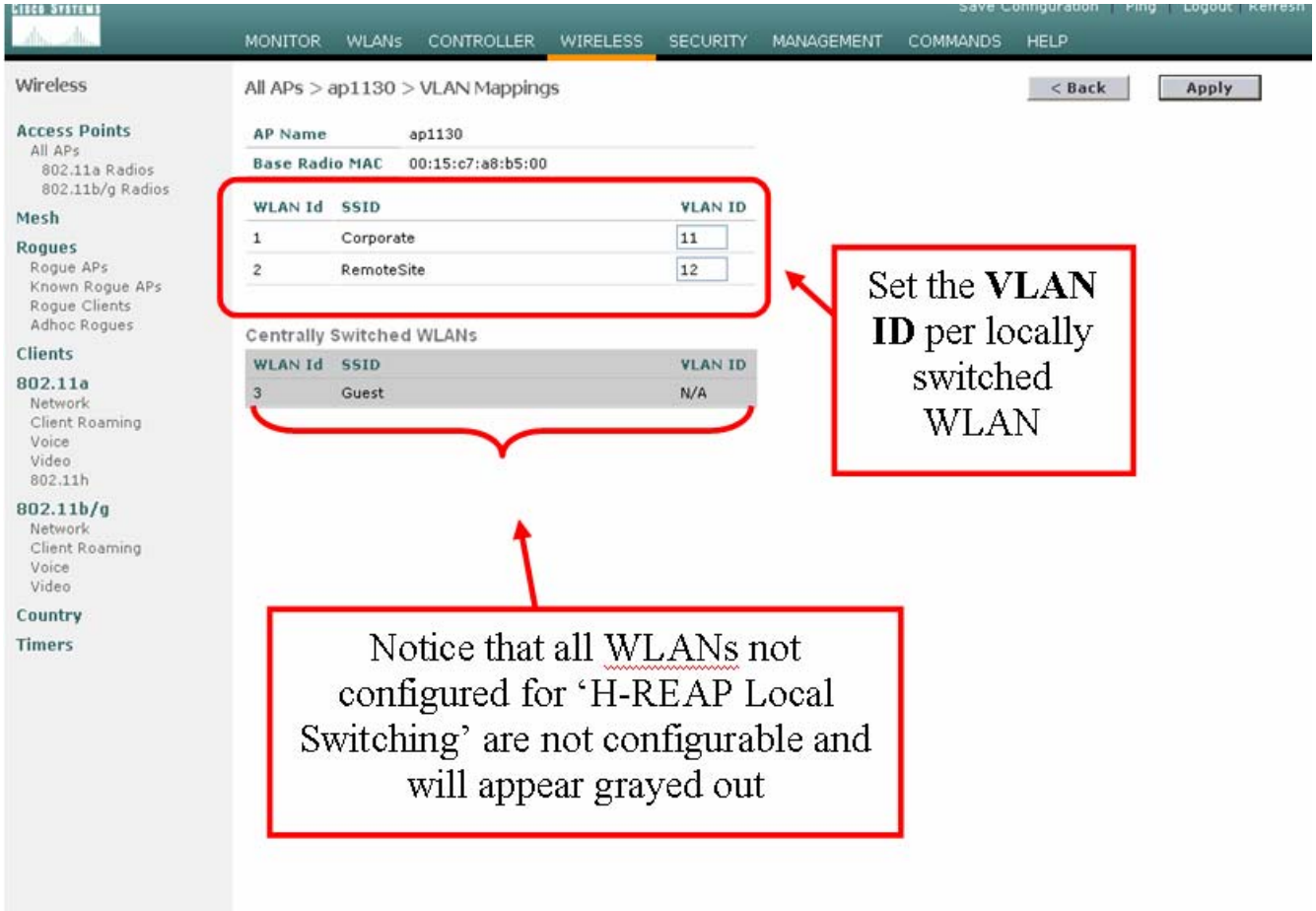
H-REAP AP Configuration (continued)

- **Select ‘VLAN Mapping’...**



H-REAP AP Configuration (continued)

- ... and configure local VLAN tagging



H-REAP Design Considerations

- **Designed solely for remote and branch office settings with no more than 3 H-REAPs per site**

  “Things are gonna change... I can feel it.”

- **Technical H-REAP Requirements:**

  No more than 100ms roundtrip latency

  500 byte MTU minimum

  ≥ 128 kbps WAN link

- **No optimization for:**

  Fast, secure roaming (CCKM, PKC)

  Voice (no CAC or TSPEC support in standalone mode)

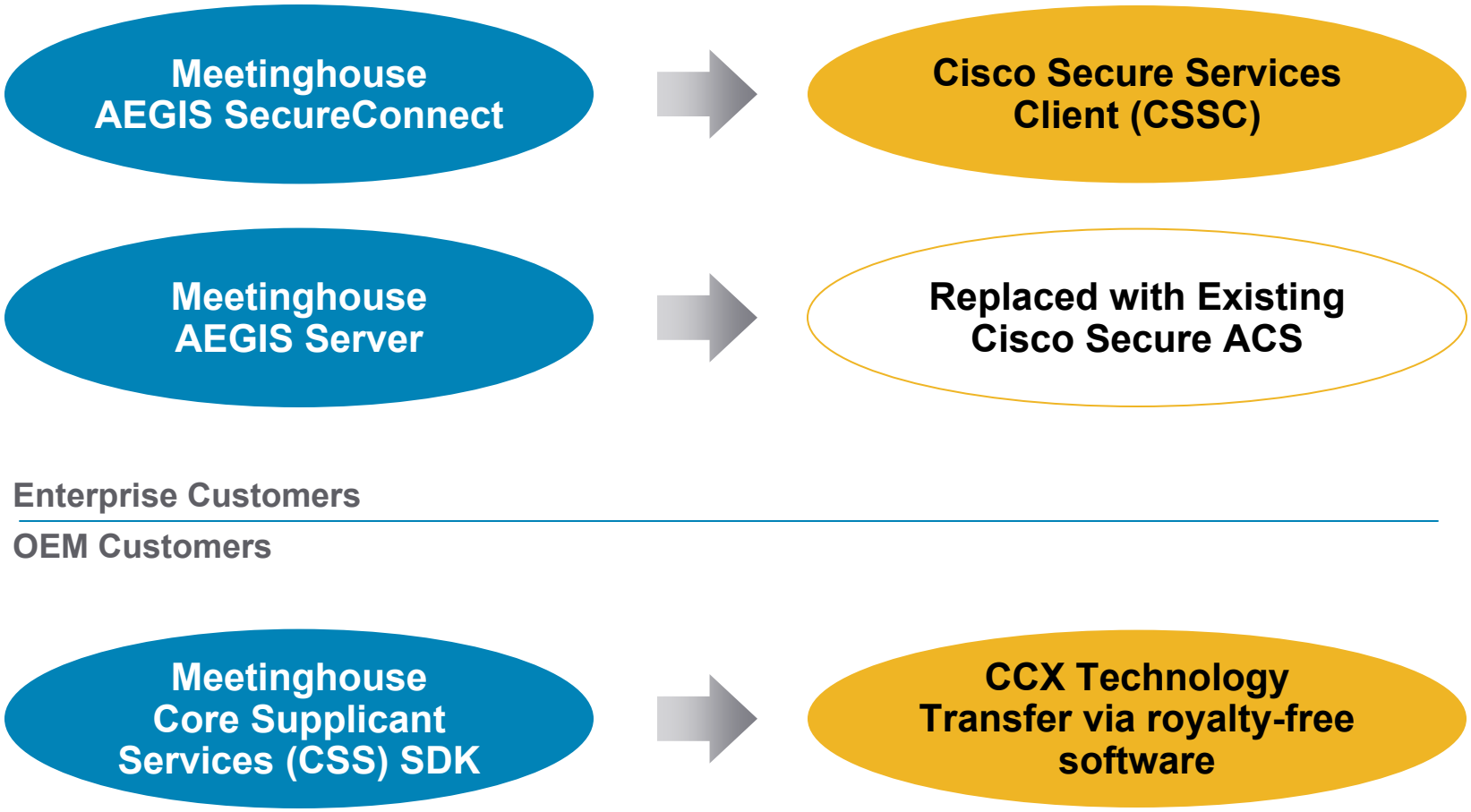
  Location (it ‘works’ but isn’t supported today)

CSSC

Meetinghouse Acquisition Drivers

- Cisco was already distributing private-label Meetinghouse AEGIS technology for CTA
  - 801.X wired-only, FAST-only operation
- Full Meetinghouse AEGIS provided extended capabilities
  - Support wired and wireless clients
  - Full suite of EAP methods
  - Support for other OS
- Client software essential for end-to-end Cisco solutions
  - Required component for IBNS and NAC
- Provides a foundation for a future unified Cisco client

Product Transition to Cisco



Retired Meetinghouse Products

- Retired products are dated, older generation technology

  Too expensive to support under Cisco quality standards

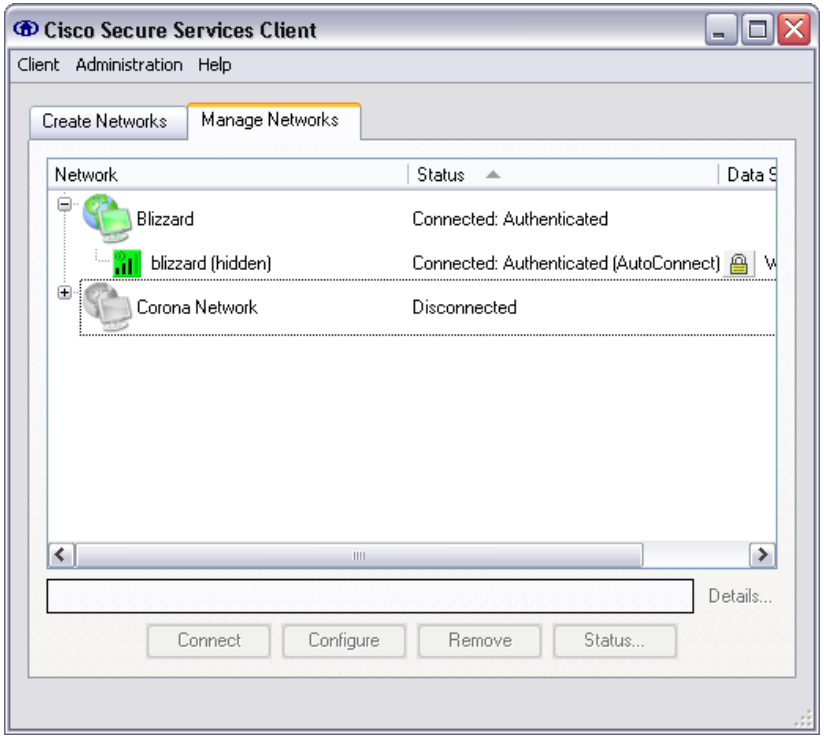
- EOS status declared pre-acquisition to limit support obligations

Product Name	Version	OS Supported	EOS	EOL
AEGIS Client	1.x	MAC OS	2/10/2007	2/10/2008
AEGIS Client	1.x	Palm OS		
AEGIS Client	1.x	Solaris		
AEGIS Client	1.x	Linux		
AEGIS Client	2.1.x	Win98/NT		
AEGIS Client	2.1.x	Win PPC 2002, Win Mobile 2003, WinCE 4.1/4.2		
AEGIS Client	2.2.x	WinXP/2000		
AEGIS SecureConnect	4.0.0	WinXP/2000	2/10/2007	2/10/2008
AEGIS SecureConnect	4.0.1	WinXP/2000		
AEGIS SecureConnect	4.0.2	WinXP/2000		
AEGIS SecureConnect	4.0.3	WinXP/2000		
AEGIS Server	1.1.x	Solaris	2/10/2007	2/10/2008
AEGIS Server	1.1.x	Linux		

CSSC Product Overview

CSSC 4.0.5 Product Highlights

- Wired & wireless LAN ports
  - Open or secure (802.1X)
  - Broadcast or hidden SSIDs
- Profiles for managing different networks
  - (Not for wired until network identity for wired LANs)
- Full suite of EAP methods
- Wide range of user credentials
- CTA support
- SSO, GPO, PAC, login scripts



CSSC Applications

- IBNS

  All switches and APs support 802.1X

  802.1X port control requires use of client

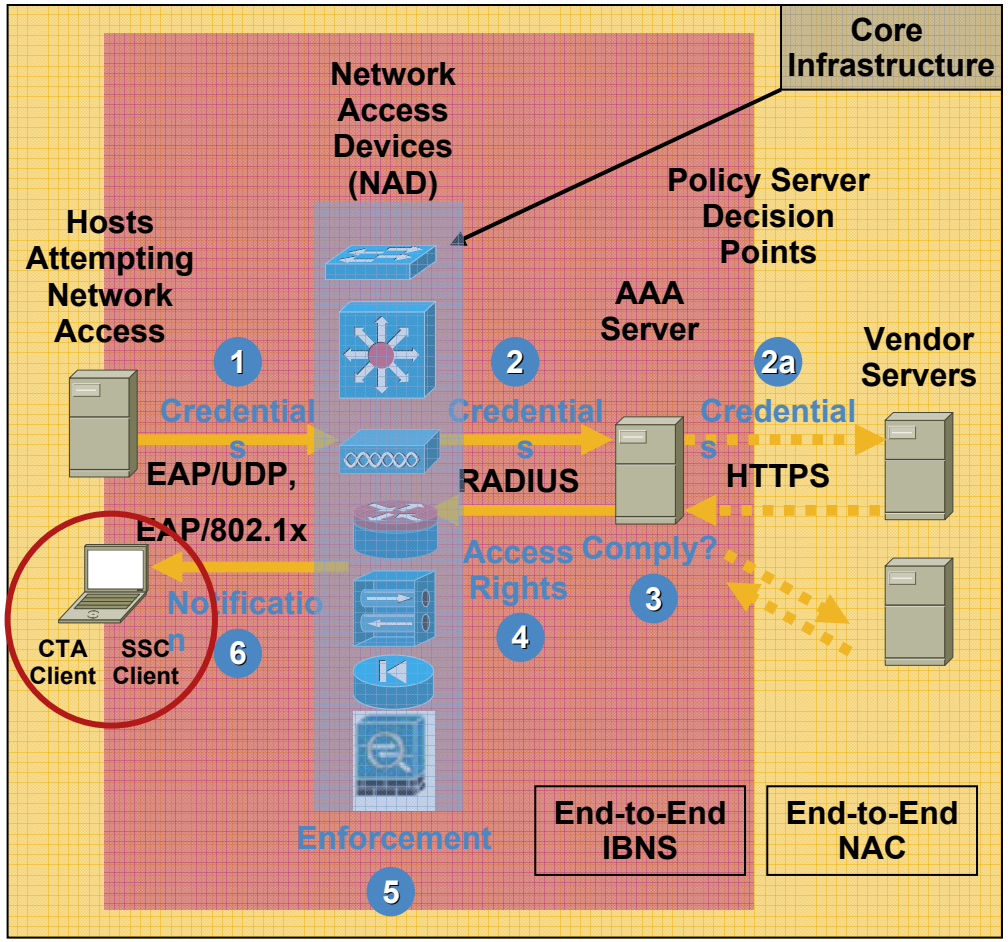
- NAC

  Builds on IBNS

- 802.1af/AE (future)

  Builds on IBNS

  Extends CSSC wired LAN port control with new technology



Deployment Issues

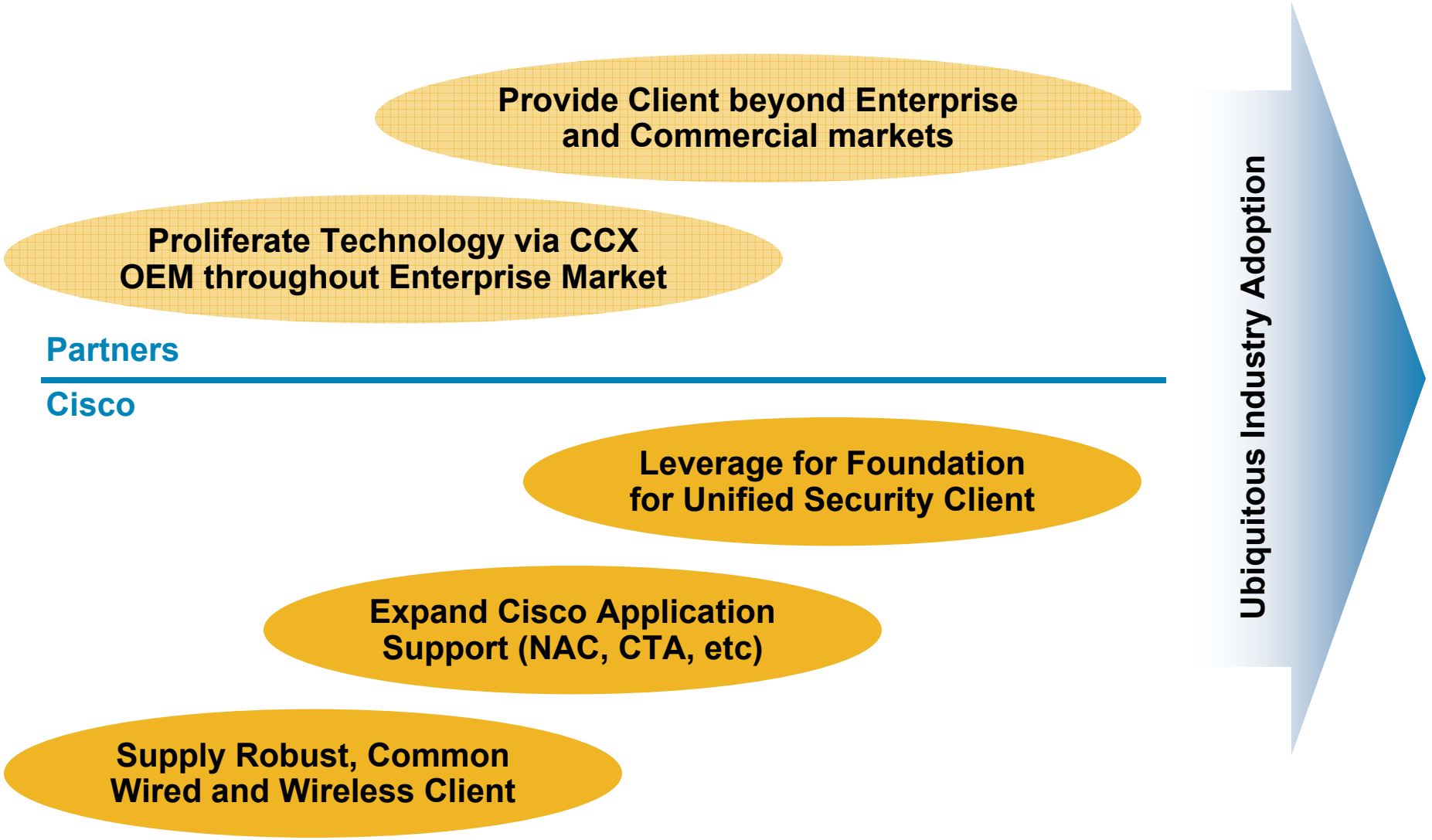
- Machine login
  - Emulating traditional LAN
  - Drivers largely unaware of 802.1X timing issues
- Single Sign On
  - Credential handling
  - GINA chaining previously out of vogue
    - Essential if multiple vendors involved (directory, smart cards)
- CCX essentials – authentication
  - EAP type support and database compatibility
  - Server Trust
  - EAP-FAST auto or authenticated provisioning
  - CCX-completion to come

Deployment Issues, continued

- Wireless NIC considerations
  - WPA handshake
  - Roaming/802.11 association persistence setting
- Hidden/Non-broadcast SSID
  - “Actively search for this access device”

Secure Services Client Strategy and Roadmap

Cisco Secure Services Client Strategy



Key Roadmap Features

- CSSC 4.0.6

  XML Provisioning

  Multiple XML files currently used for profile, policy, networks

  Completely provision all data elements in client

  Transport-agnostic – deliver XML Provisioning via .msi, SMS, email, URL, CSA, etc.

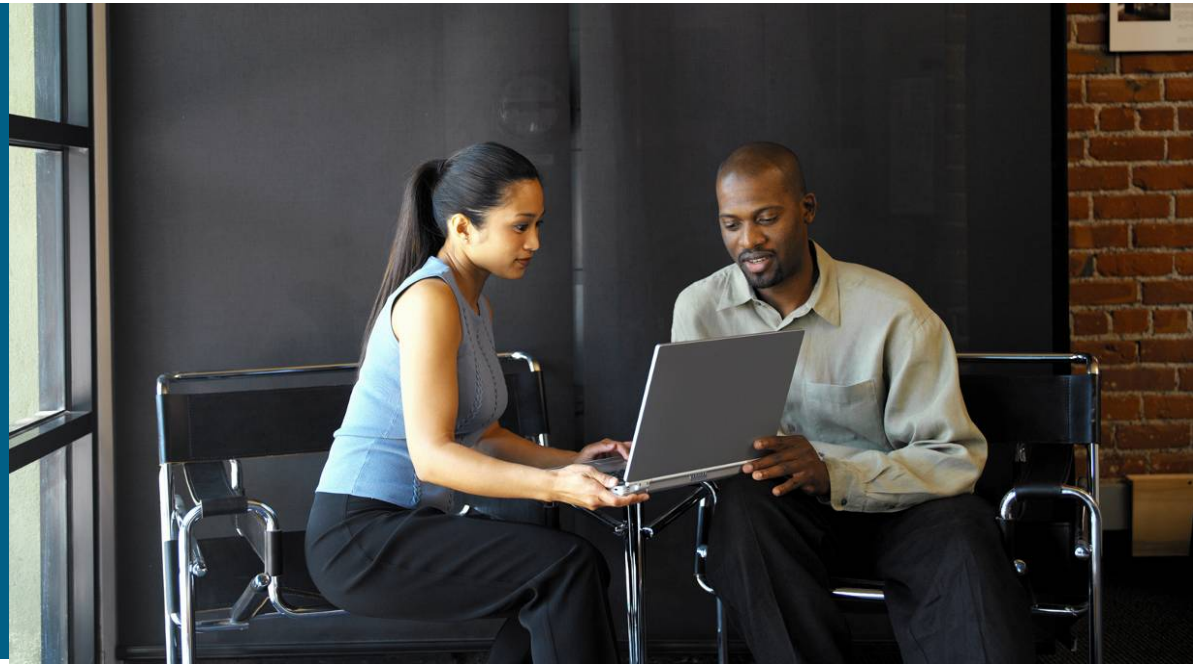
- CSSC 5.0

  New User Interface

  New, more intuitive GUI

  Consolidates usability requests from multiple users

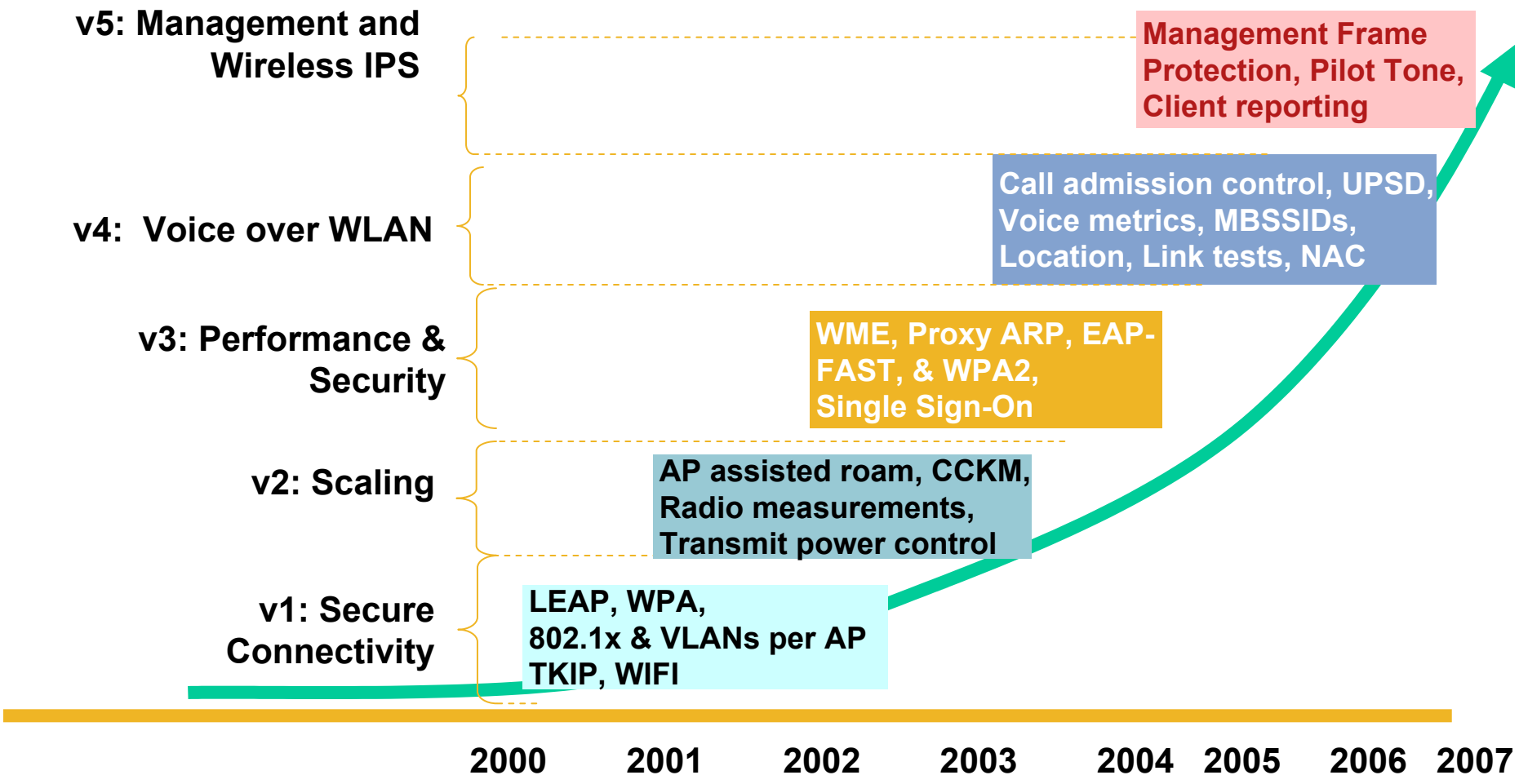
Cisco Compatible Extensions (CCX) Program



CCX Program Objectives

- Standards represent a technology baseline for interoperability
- Cisco has a history of innovation and extensions for better networks
- A program for delivering new technology early to market with other product developers
- A track record for sharing innovative technology through standards

CCX Releases 1-5



CCX Enables Innovative Solutions

Successful Solutions Taken To 802.11 Standards Body		
Radio measurements	→	802.11h and 802.11k
Fast roaming	→	802.11r
Expedited bandwidth request	→	802.11u
Client Diagnostics	→	802.11v
Real-time reporting	→	802.11v
Management frame protection	→	802.11w

CCX Established and New Components

- Established components
  - Royalty free **technology** license
  - CCX Specifications
  - Certification Program (Keylabs)
- New components
  - Royalty free **software** license
  - CCX Rapid Adoption Kit (SDK and more)
  - Technology transfer for wireless device
    - Vista, WinXP/2K, WinCE, Windows Mobile, Linux
  - Ecosystem of support to enable delivery of CCX to all devices
    - Overcome barrier of any OS

Q and A