Introduction to 802.11 Technology

Suebpong Nitichai
Email: sniticha@cisco.com

IEEE 802.11 Family
Technology Overview

IEEE 802.11 Standard define :

- A **Physical layer**
  Radio Frequencies, Data Modulation, …
  (802.11, 802.11b, 802.11g, 802.11a, 802.11n, …)

- A **MAC layer**
  How to access the medium, how to manage the collisions, …

IEEE 802.11b

- Ratified as standard in Sept, 1999
- Uses 2.4 GHz unlicensed spectrum
- Different physical access defined (PHY)

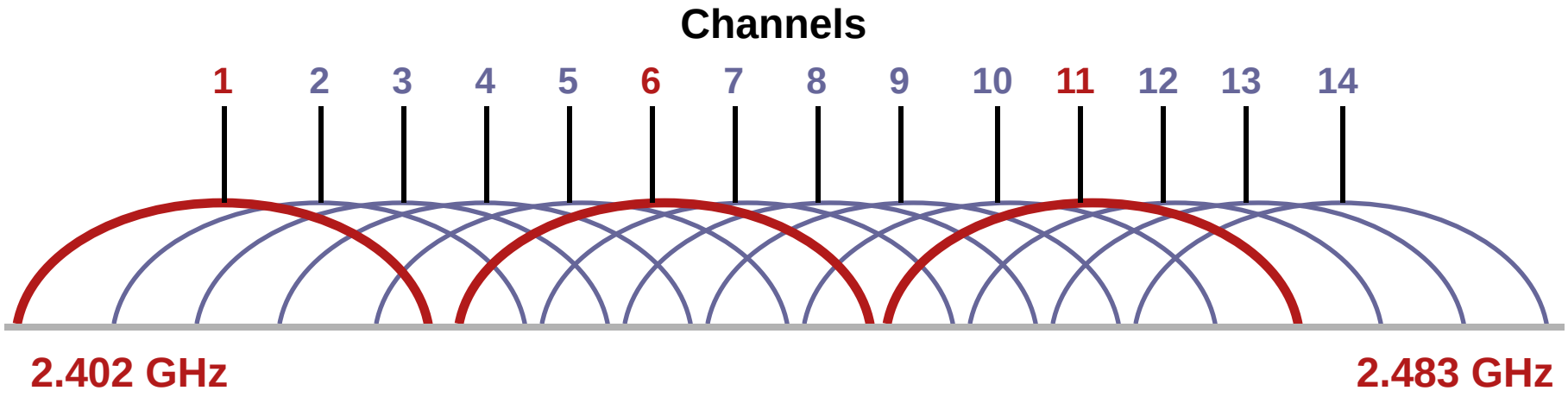
  Direct sequence at 1, 2, 5.5, and 11 Mbps,
  Can “downshift” to lower data rates for longer range

  Frequency hopping at 1 and 2 Mbps for 2.4 Ghz (legacy)

  Infrared (obsolete)

- 11 US channels, 13 ETSI channels, 14 Japan channels
- Generally approved for worldwide use in many countries

IEEE 802.11b
Direct Sequence @ 2.4 GHz



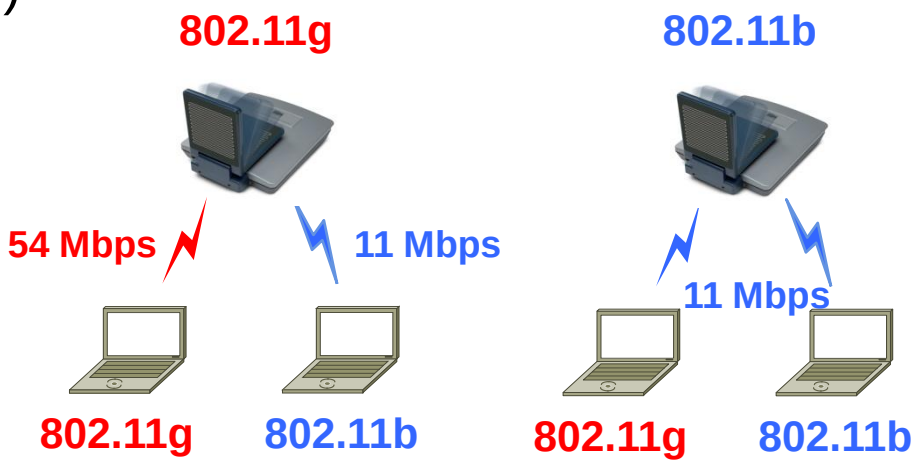
- Up to (14) 22 MHz wide channels
- 3 non-overlapping channels (1, 6, 11)
- Up to 11 Mbps data rate
- 3 access points can occupy the same space for a total of 33 Mbps aggregate throughput, but not on same radio card

IEEE 802.11g

- Ratified as standard in June, 2003
- Same frequencies as IEEE 802.11b (2.4 GHz)
- Backward compatible with 802.11b
- Orthogonal Frequency Division Multiplexing (OFDM)

  Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps
- Direct sequence (802.11b backwards compatible)

  Data rates: 1, 2, 5.5, and 11 Mbps



IEEE 802.11a

- Ratified as standard in Sept, 1999
- Orthogonal Frequency Division Multiplexing (OFDM)

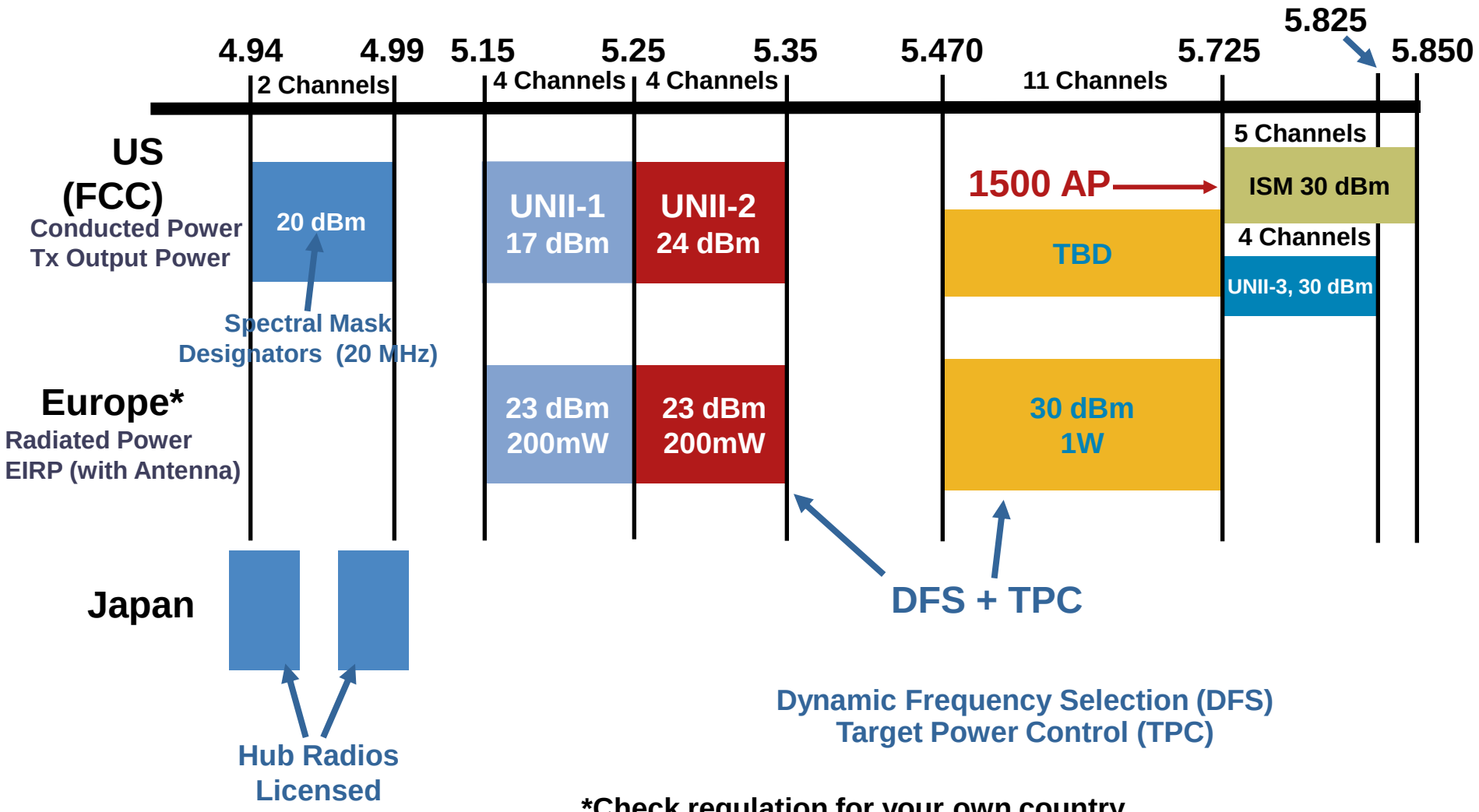
  Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps

  Can “downshift” to lower data rates for longer range
- Compliant in some countries
- 5 GHz band has more channels than 2.4 GHz band

  19 non-overlapping channels in ETSI Regulation Area

  (vs. 3 channels for 2.4 GHz) for greater scalability

Current State of 5 GHz Bridging Spectrum



*Check regulation for your own country

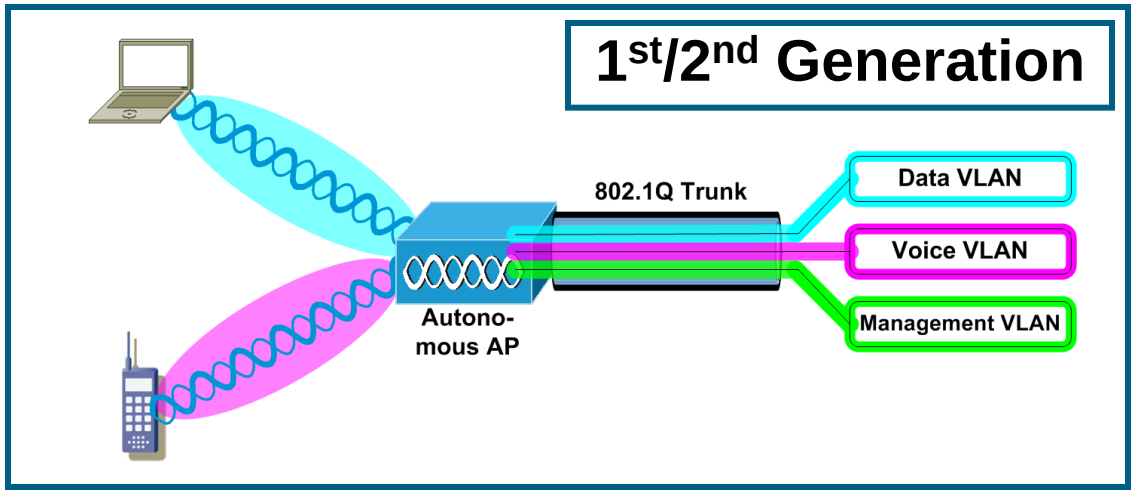
IEEE 802.11 Radio Summary
Properties

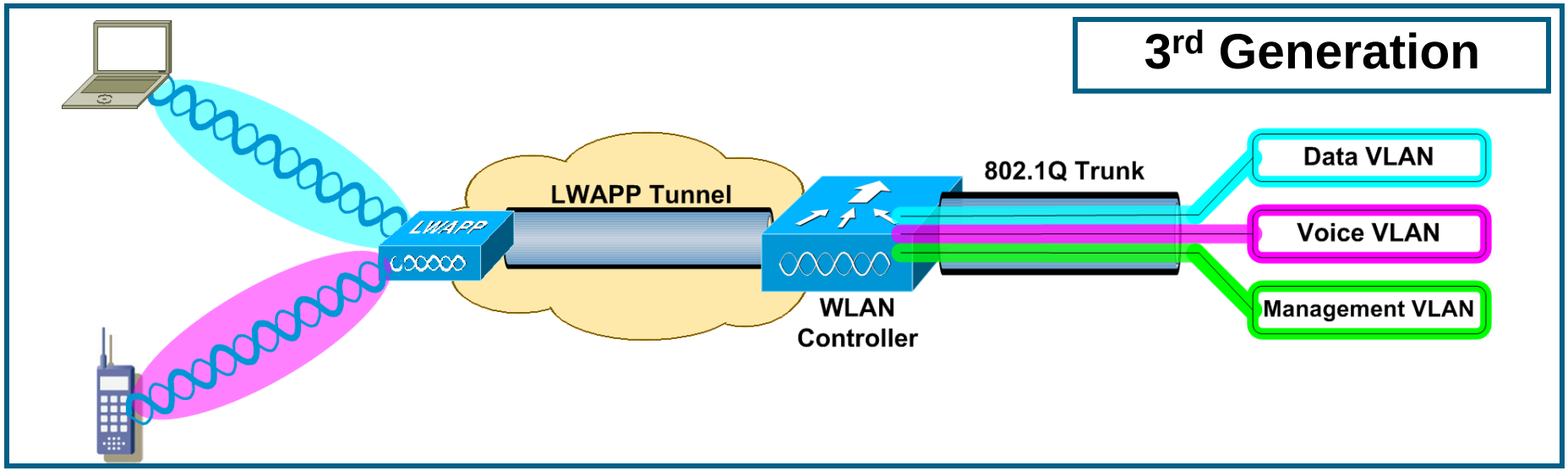
	802.11	802.11b	802.11g	802.11a
Ratified	1999	1999	2003	1999
Data Rates (Mbps)	1,2	1,2,5.5,11	1,2,5.5,11 and 6,9,12,18,24, 36,48,54	6,9,12,18,24, 36,48,54
Number of Non-Overlapping Channels	Frequency Hopping	3	3	8 Indoors/ 11 Outdoors
Frequency Range (GHz)	2.402–2.483			5.15–5.35, 5.47–5.725*
Status	Obsolete	Worldwide Available		Limited Worldwide Availability

Introduction to the Cisco Unified Wireless Network

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

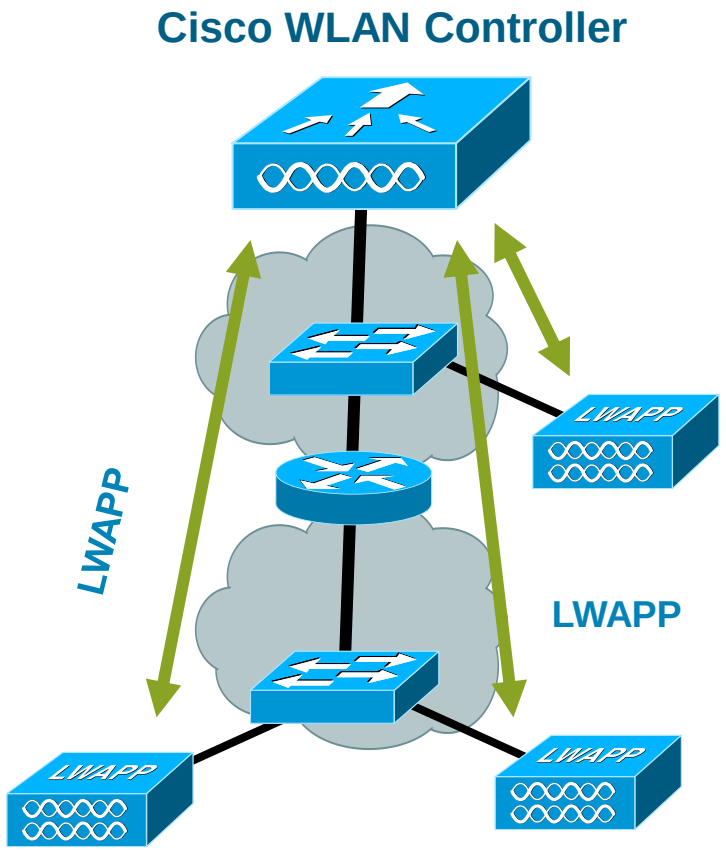
- 1st/2nd generation—APs act as 802.1Q translational bridge, putting client traffic on local VLANs
- 3rd generation—Controller bridges client traffic centrally





Centralized Wireless LAN Architecture
Overview

- Processing split between APs and controllers
  - 802.11 functionality shared
- Central management—AP is essentially a remote RF interface
- Based on LWAPP protocol
- APs hold no security credentials
- APs unusable without a controller—Just expensive paperweights!
- Data traffic can be bridged locally or at controller



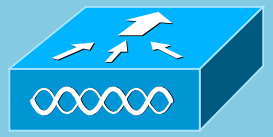
Centralized Wireless LAN Architecture

AP/Controller: Division of Labor

Controller

- 802.11 MAC Mgmt – (re)association requests & action frames
- 802.11 data – encapsulate and sent to AP
- 802.11e resource reservation – control protocol carried to AP in 802.11 mgmt frames – signaling done in the controller.
- 802.11i authentication & key exchange

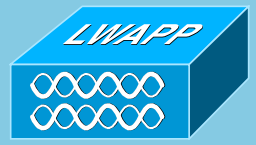
Cisco WLAN Controller



LWAPP

AP

- 802.11 – beacons, probe response, auth (if open)
- 802.11 control – packet ack & retransmission (latency)
- 802.11e – frame queuing & packet prioritization (real-time access)
- 802.11i – Layer 2 encryption

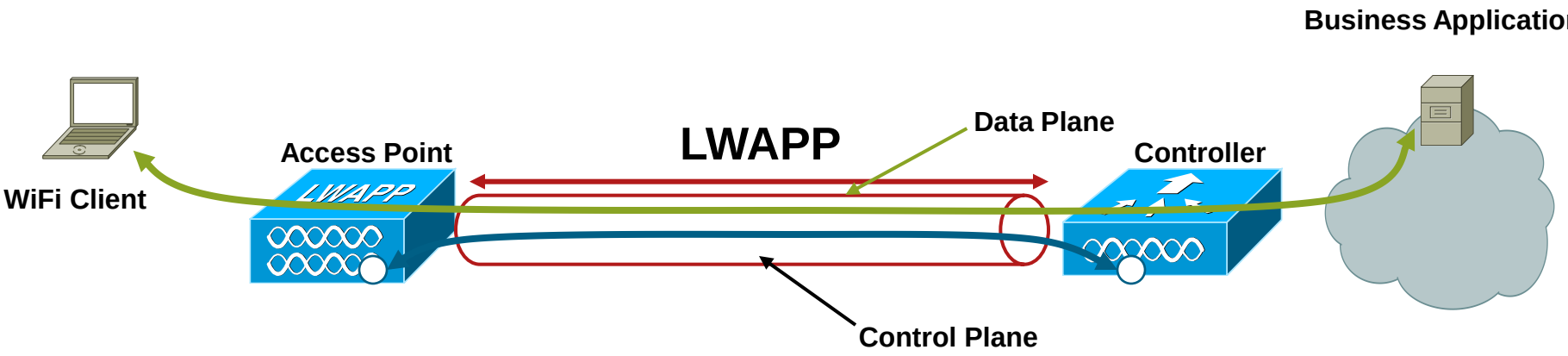


Lightweight Access Points

Centralized Wireless LAN Architecture

What Is LWAPP?

- LWAPP—Light weight access point protocol is used between APs and WLAN controller
- LWAPP carries control and data traffic between the two
  - Control plane is AES-CCM encrypted
  - Data plane is not encrypted
- It facilitates centralized management and automated configuration
- Open, standards-based protocol (submitted to IETF CAPWAP WG)



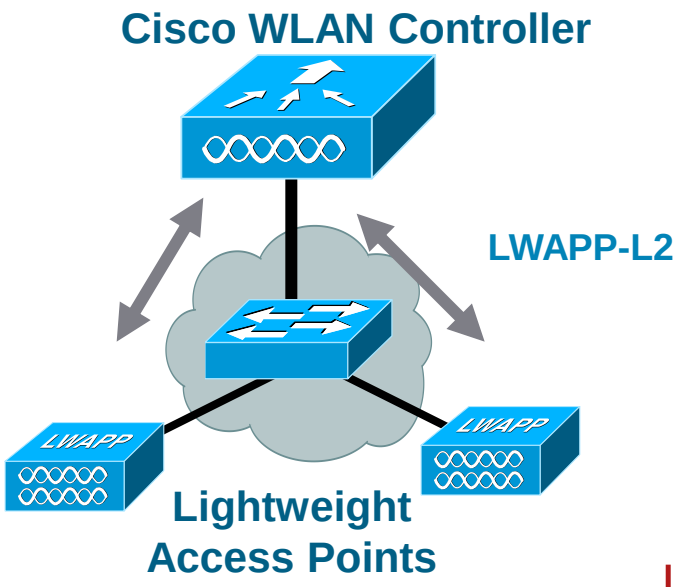
Difference between LWAPP and CAPWAP

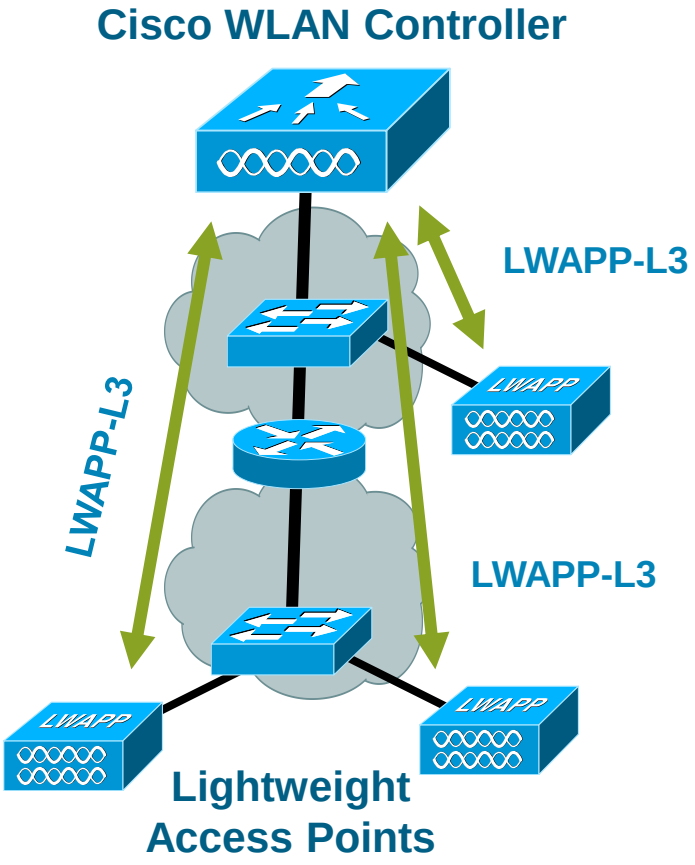
Description	LWAPP	CAPWAP
Fragmentation/Re-assembly	Relies on IpV4	CAPWAP itself does both
Path-MTU Discovery	Not supported	Has a robust P-MTU discovery mechanism, can also detect dynamic MTU changes
Control Channel Encryption between AP and WLC	Yes (using AES)	Yes (Using DTLS)
Data Channel Encryption between AP and WLC	No	**Yes (using DTLS)**
UDP Ports	12222, 12223	**5246 (ctrl) 5247 (data)**

LWAPP Modes

Layer 2 and Layer 3 LWAPP

- Layer 2 LWAPP is in an Ethernet frame
  - AP and WLC in same L2 domain
- Layer 3 LWAPP is in a UDP/IP frame
  - AP need IP address
  - Support routing between AP and WLC



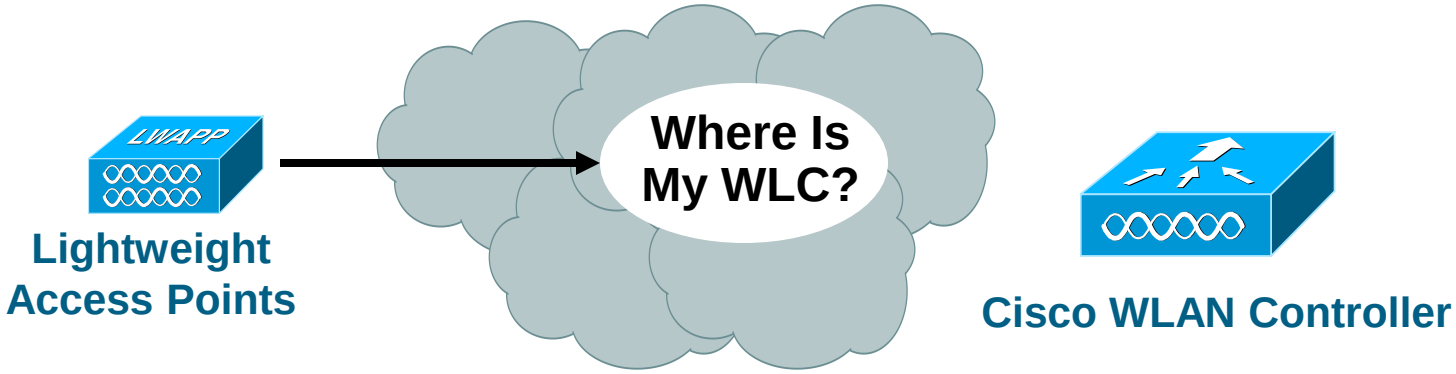


LWAPP-L3 Is Now the Preferred Solution

Architecture Deployment

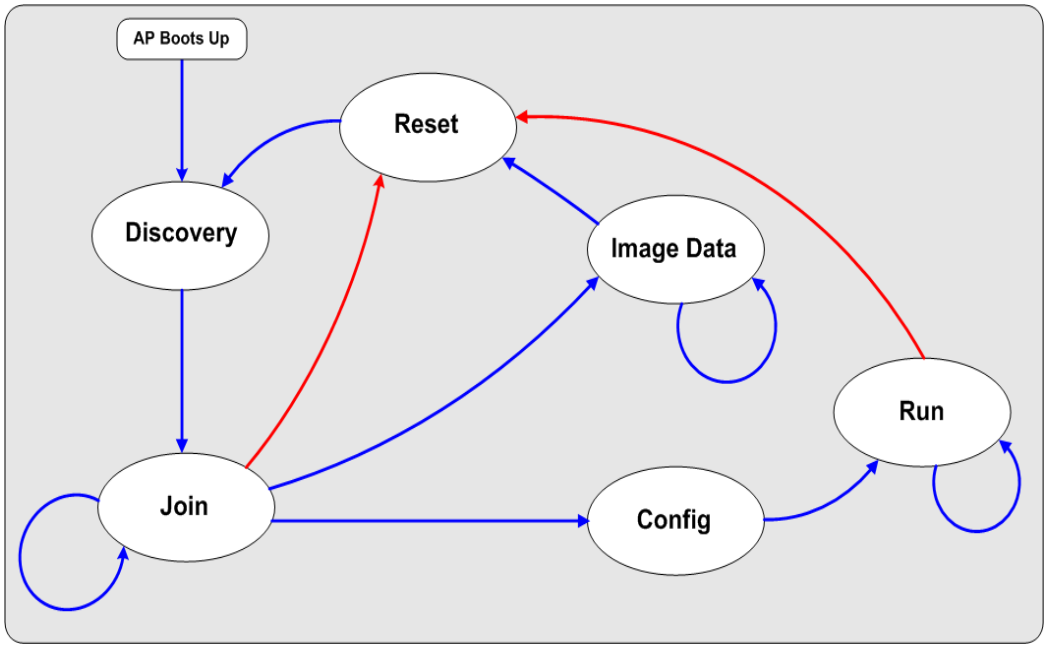
Access Points Need to Be Associated with WLAN Controller

- Hunting phase: AP needs to find WLC
- Join phase: AP associates securely with WLC
- Authorization phase: WLC accept or not AP
- Configuration phase: WLC upload firmware (if needed), WLC upload AP configuration

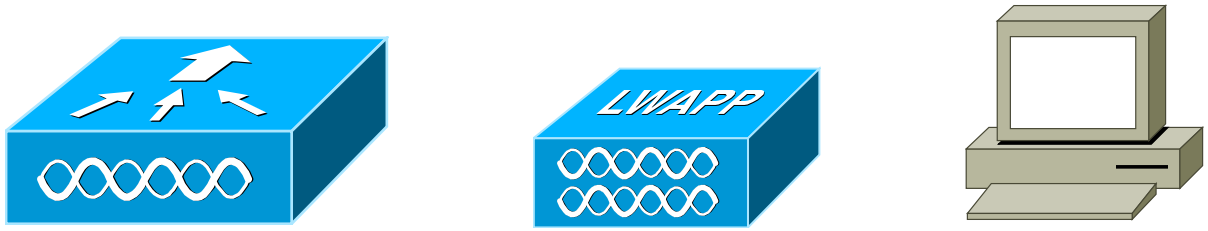


LWAPP State Machine (Simplified)

- 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



Components of Centralized Architecture



- **WLC**

  Cisco Unified Wireless LAN controllers aggregrate WLAN client traffic and control the Wireless network

- **APs**

  Lightweight access points are used in all unified wireless architectures and provides client wireless access, and tunneling to the WLC.

- **WCS**

  Cisco Wireless Control System provides centralized management, RF planning and visualization tools, and location services

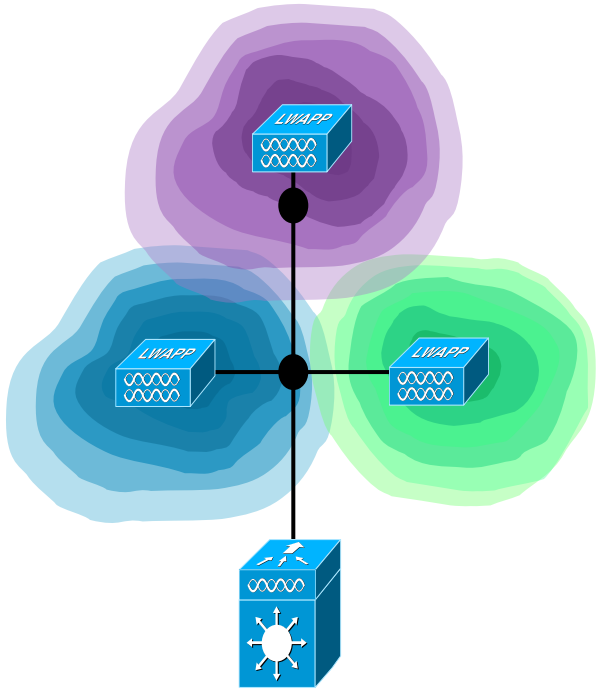
Deploying with RRM in Mind

RRM—Radio Resource Management

- What are RRM's objectives?
  - –To dynamically balance the infrastructure and mitigate changes
  - –Monitor and maintain coverage for all clients
  - –Manage Spectrum Efficiency so as to provide the optimal throughput under changing conditions
- What RRM does not do
  - –Substitute for a site survey
  - –Correct an incorrectly architected network
  - –Manufacture spectrum

How Does RRM Do This?

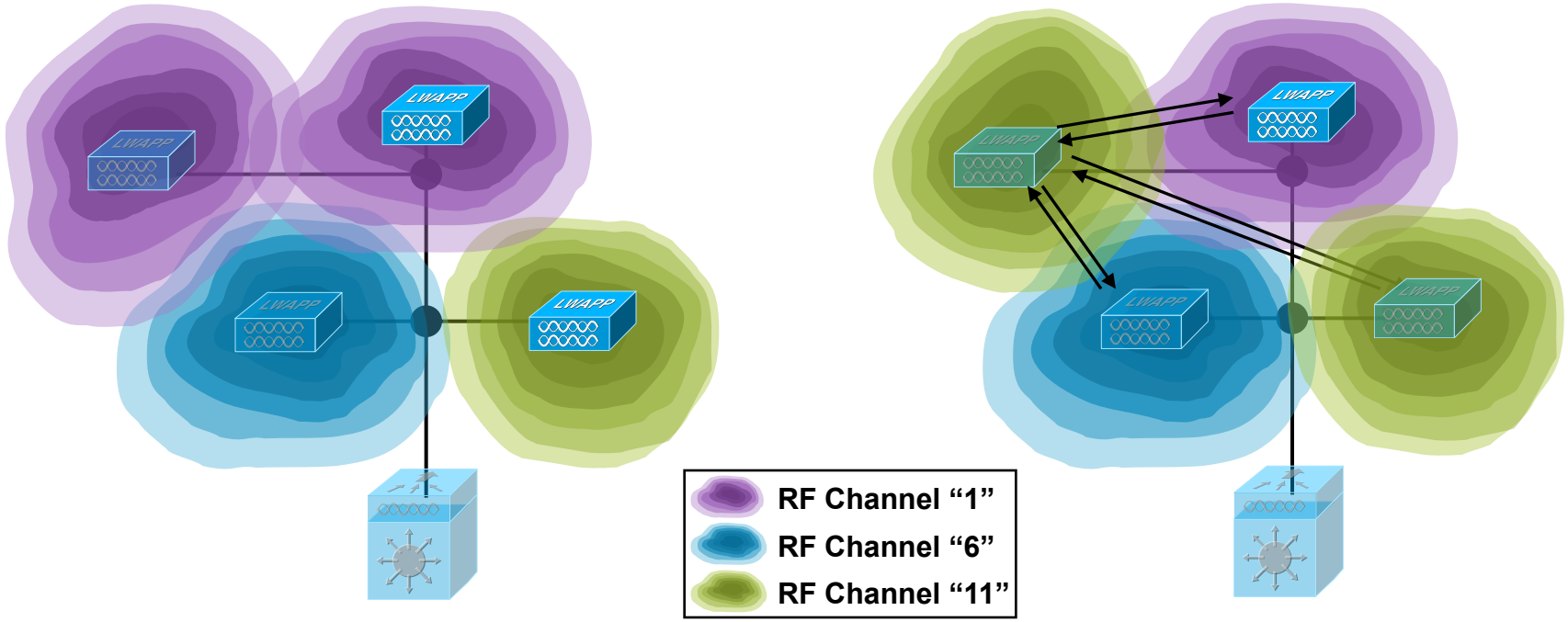
- **DCA**—Dynamic Channel Assignment
  - –Each AP radio gets a transmit channel assigned to it
  - –Changes in “air quality” are monitored, AP channel assignment changed when deemed appropriate (based on DCA cost function)
- **DPC**—Dynamic Power Control
  - –Tx Power assignment based on radio to radio pathloss
  - –DPC is in charge of reducing Tx on some APs—but may also increase Tx by defaulting back to power level higher than the current Tx level
- **CHDM**—Coverage Hole Detection and Mitigation
  - –Detecting clients in coverage holes
  - –Deciding on Tx adjustment (typically Tx increase) on certain APs based on (in)adequacy of estimated downlink client coverage



RRM —DCA— Dynamic Channel Assignment

New Access Point Causes Co-Channel Interference

System Optimizes Channel Assignments to Decrease Interference



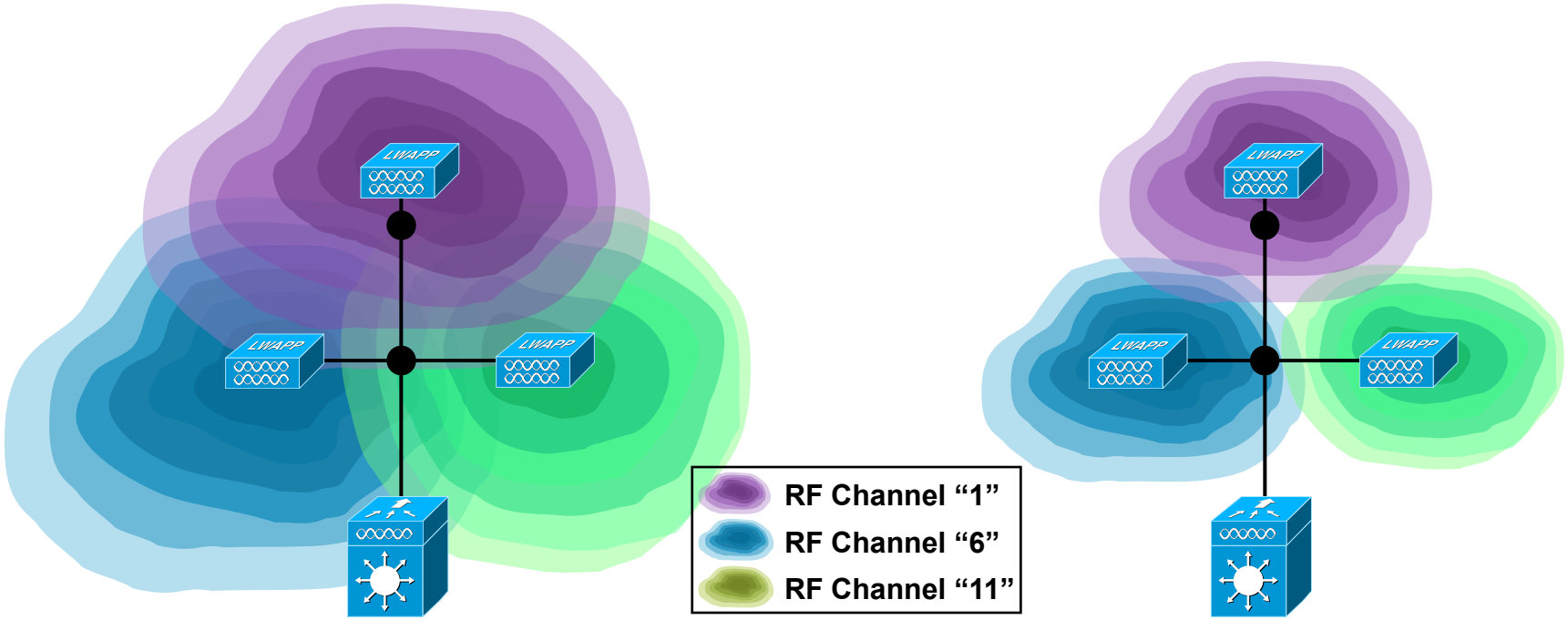
What It Does

- Ensures that available RF spectrum is utilized well across frequencies/channels
  - –Best network throughput is achieved without sacrificing stability or AP availability to clients

RRM —DPC— Dynamic Power Control

Power Not Optimized—RF Signal Bleeds—Causes Interference

Decreased Power Limits Interference and Improves Application Performance

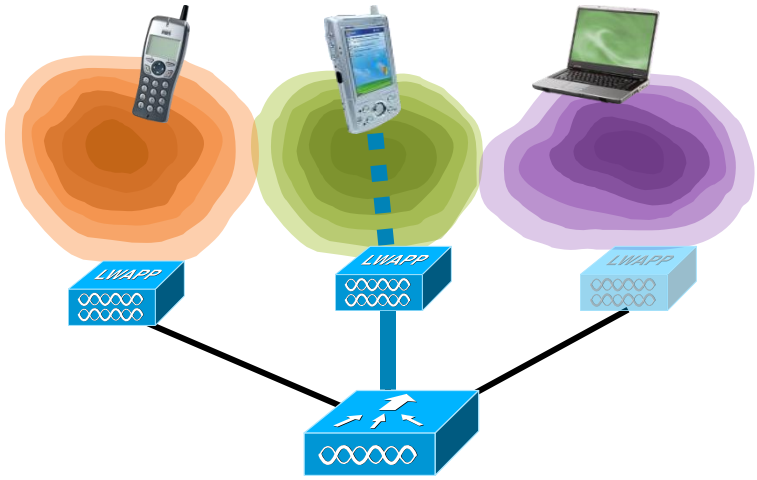


What It Does

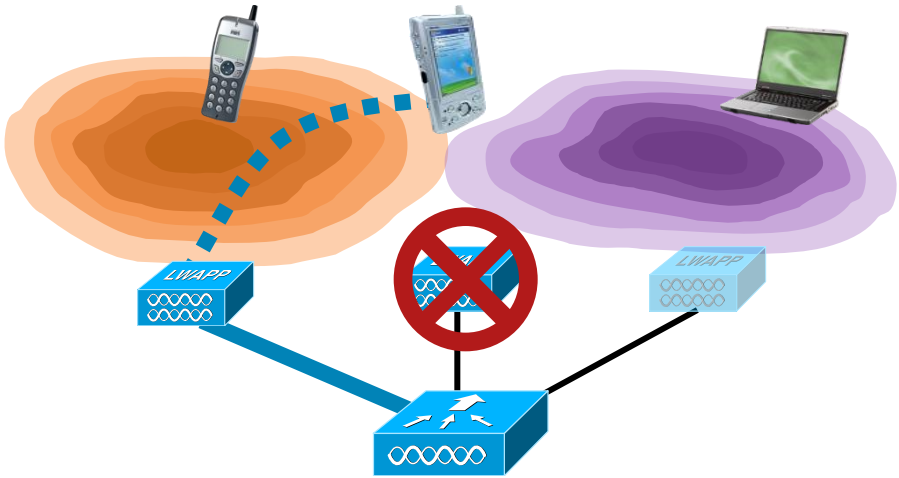
- TX power assignment based on radio to radio pathloss
- DPC cf. in charge of reducing Tx on some APs—but it can also increase Tx by defaulting back to power level higher than the current Tx level (under appropriate circumstances)

Radio Resource Management
Coverage Hole Detection and Mitigation

Normal Operation



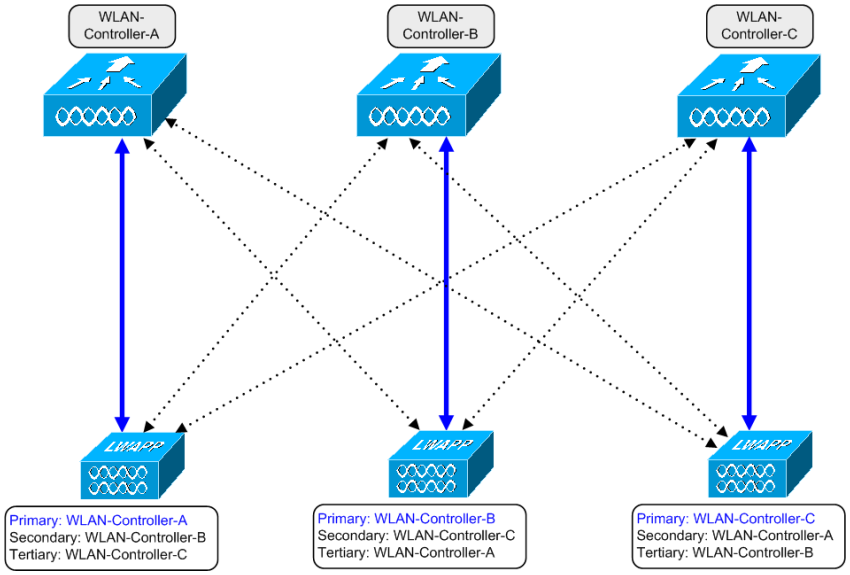
Access Point Failure
Coverage Hole Detected and Filled



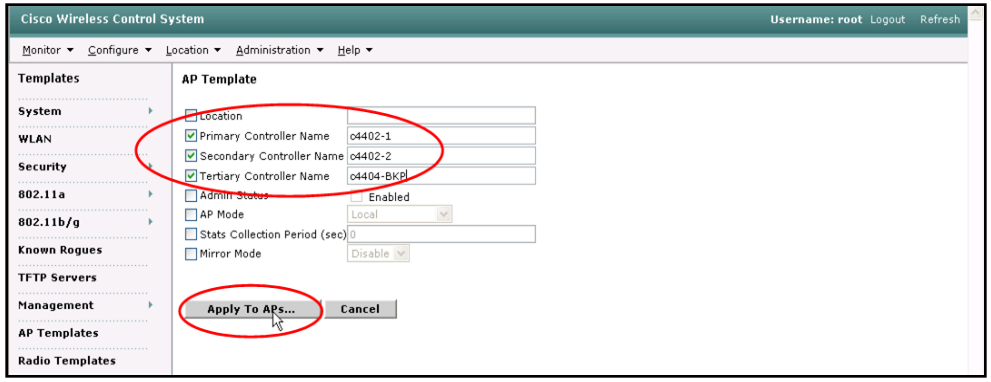
What It Does

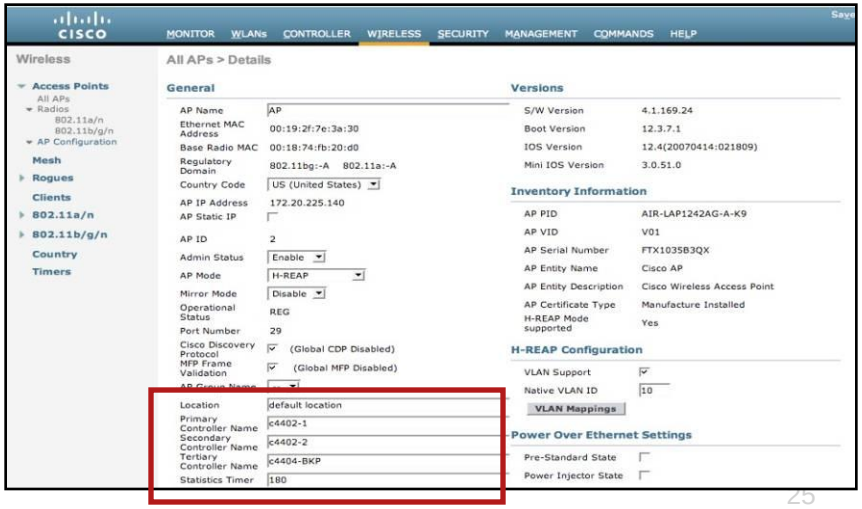
- No single point of failure
- Automated network failover decreases support and downtime costs
- Wireless network reliability approaches wired

Deterministic Redundancy

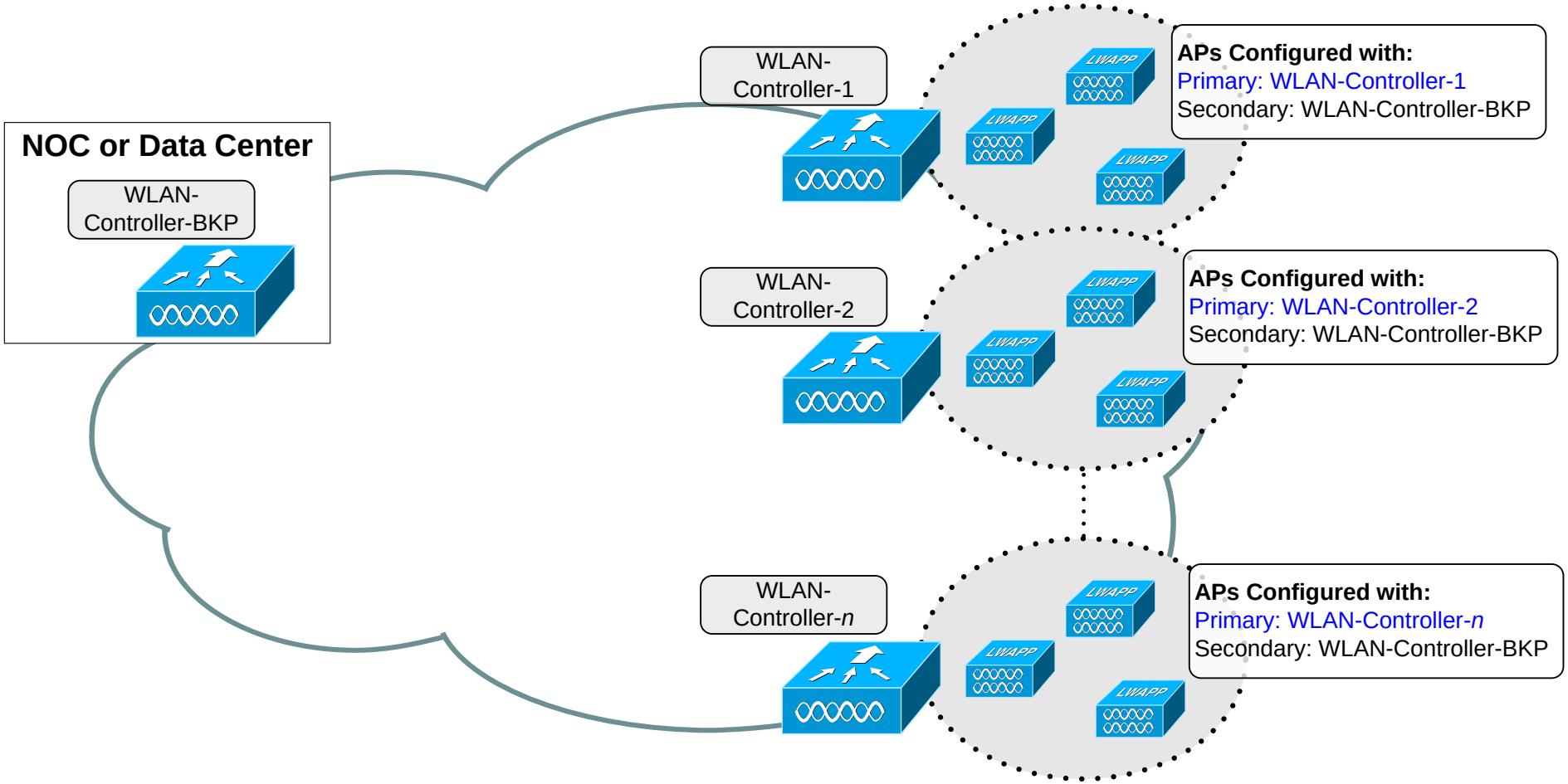


- Administrator statically assigns APs a primary, secondary, and/or tertiary controller
  - Assigned from controller interface (per AP) or WCS (template-based)
- Pro
  - Predictability—Easier operational management
  - More network stability
  - More flexible and powerful redundancy design options
  - Faster failover times
  - "Fallback" option in the case of failover
- Con
  - More upfront planning and configuration
- **This is Cisco's recommended best practice!**



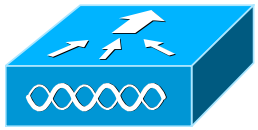


Controller Redundancy Designs—N:1



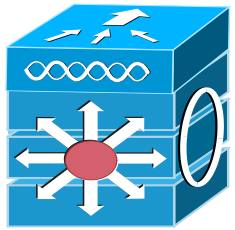
Campus WLAN Controller Options

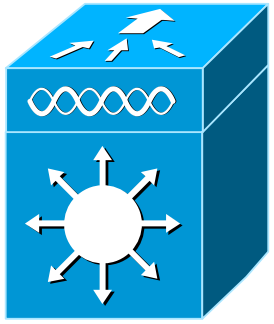
- Standalone appliance controller
  - Routed network exists on another platform
  - Dot1Q trunk to switched/routed network
- Integrated controller
  - Routed network can exist on the same platform
  - Layer 2 connection is internal
  - Layer 2 or 3 connection to network routed network



440x

Appliance





Cisco 3750G Integrated WLAN Controller

WiSM

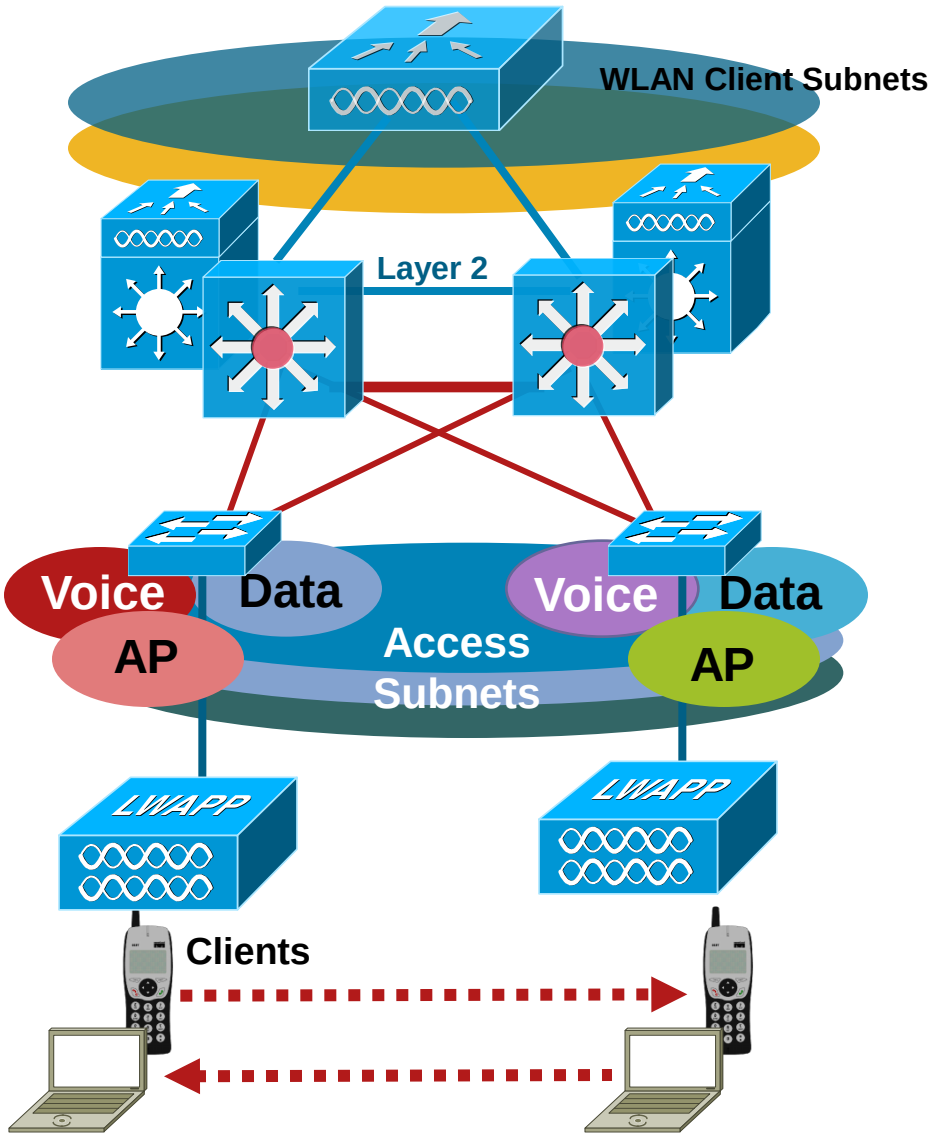
Integrated

Where to Place a WLAN Controller?

Distributed Designs

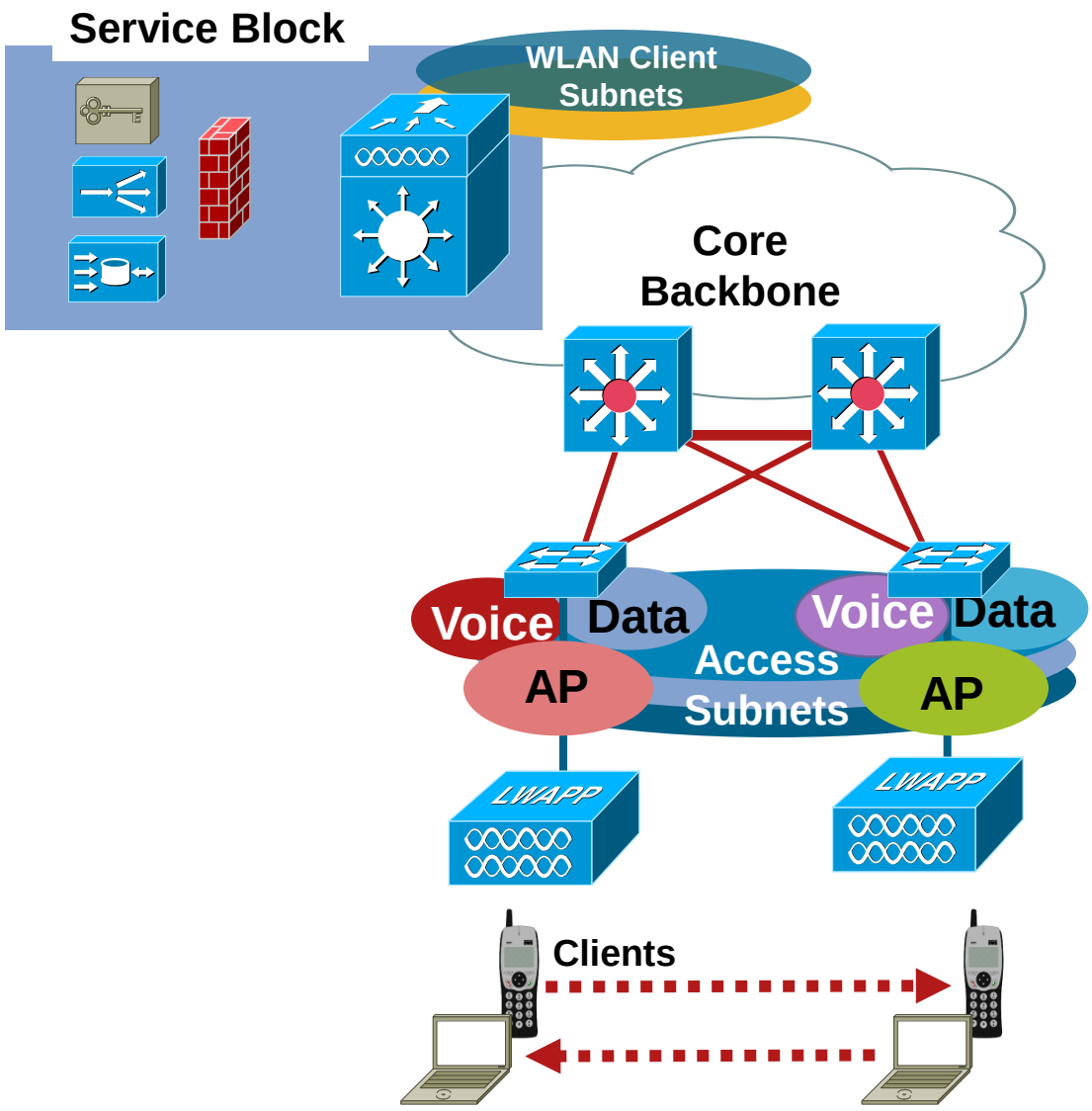
- WiSM(s) or 440x WLAN controller(s) connected at distribution layer
- Controller redundancy
- Key design considerations:
  - Spanning tree
  - HSRP/GLBP
  - Traffic flow
    - Load balancing
    - Resiliency
  - Access layer “collapsed” into distribution layer
    - Access layer IP addressing
    - Access layer features need to be implemented in the distribution layer

Mobility!



Where to Place a WLAN Controller?

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

Branch Office Deployment—Hybrid REAP

Design Considerations:

- Supported on 1130 and 1240 AP platforms
- Allows bridging/tagging of traffic locally (local switching) by WLAN
- Allows simultaneous tunneling of traffic to WLC (central switching) by WLAN
- “Connected Mode”—LWAPP control centralized
- “Standalone Mode” (WAN outage)
  - Locally switched WLANs stay up
  - Some lost functionality
- ← 100 msecs latency between APs and WLC
- H-REAP APs should be connected to trunk ports—allow only the relevant, locally switched VLANs
- No optimization for:
  - Fast, secure roaming (CCKM, PKC)
  - Voice (no CAC or TSPEC support in standalone mode)

Single Client for Uniform Security and Services

- Key Features:

  802.1X authentication for wired and wireless devices

  Windows XP/2000 support

- EAP:

  EAP-FAST, EAP-MD5, PEAP-MSCHAP, PEAP-GTC, EAP-TLS, EAP-TTLS, Cisco LEAP

- Encryption:

  WEP, Dynamic WEP, TKIP, AES

- Standards:

  WPA and WPA2

Cisco Secure Services Client

Features

- Unified wired and wireless client
- Support for industry standards
- Endpoint integrity
- Single sign-on capable
- Enabling of group policies
- Administrative control

Benefits

- Reduces client software
- Simple, secure device connectivity
- Minimizes chances of network compromise from infected devices
- Reduces complexity
- Restricts unauthorized network access
- Centralized provisioning

Delivering Network Unification

Catalyst 3750G
Integrated WLAN Controller

Intelligent Access

4400 Wireless LAN
Controller

Distribution

Wireless Integrated Services
Module (WiSM)

Network Core

Ease of Deployment

Lower TCO

Cisco Unified Wireless Network

Scalability

High Availability

Flexibility

Investment Protection

Branch Office

Wireless LAN
Controller for
ISR Series Routers

2106 Wireless LAN
Controller

Remote Office

Hybrid Remote Edge
Access Points (H-REAP)

Cisco Wireless Control System (WCS)

World-Class Network Management

Features

- Client troubleshooting (via CCX)
- Planning, configuration, monitoring, location, IDS/IPS, and troubleshooting
- Hierarchical maps
- Intuitive GUI and templates
- Policy based networking (QoS, security, RRM, etc.)

Benefits

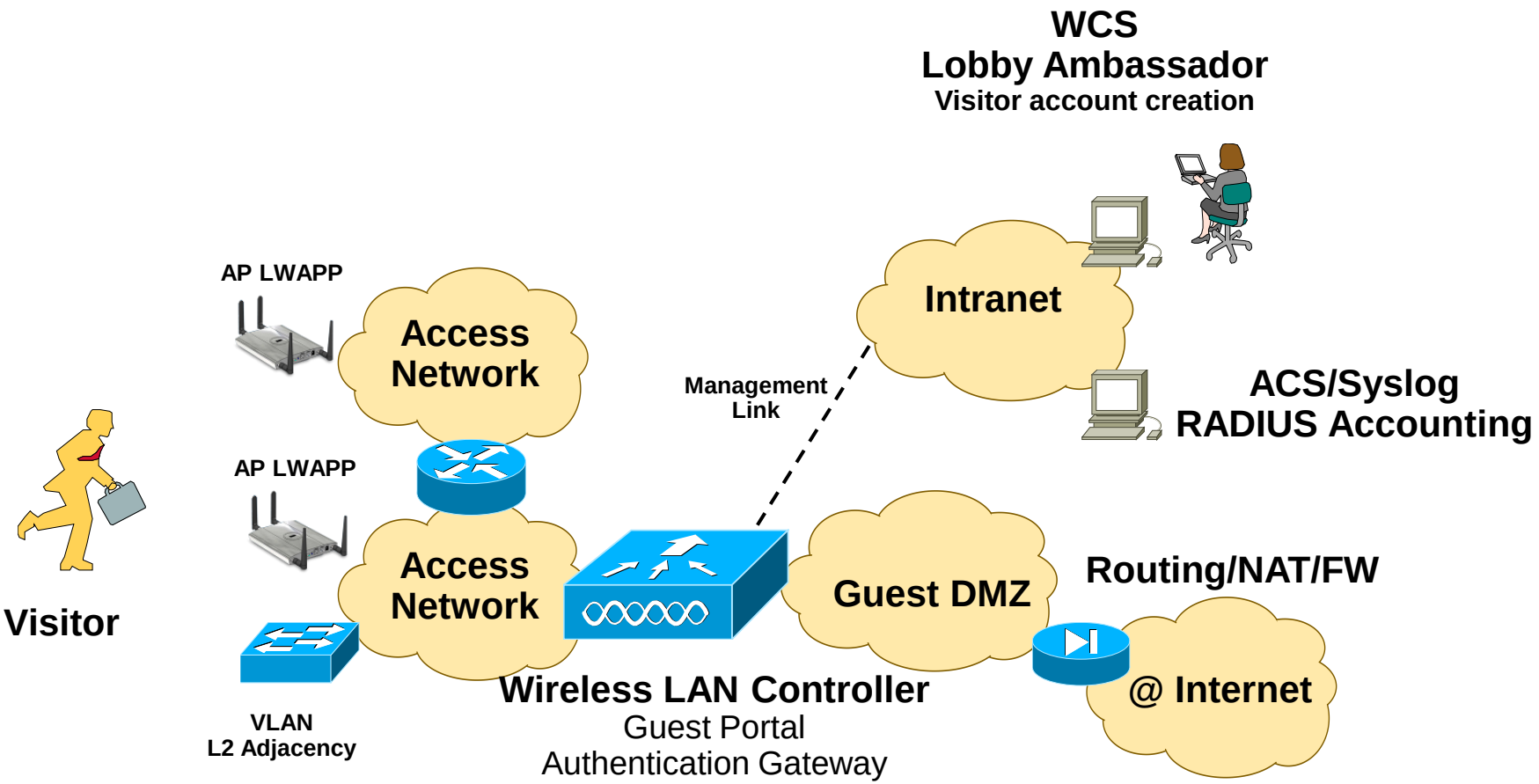
- Lower OPEX and CAPEX
- Better visibility and control of the air space
- Consolidate functionality into a single management system
- Determines location and voice readiness

Guest Access

Definition : Guest Access

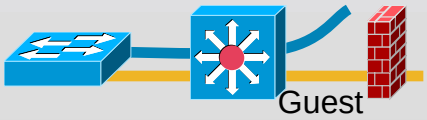
- A solution to offer Internet access to visitors/partners without putting at risk the enterprise Information System.
- It's characteristics are generally :
  - It's Free
  - It uses existing enterprise network infrastructure
  - Guest traffic must be isolated from intranet traffic
  - It does not guaranty radio communication security to guest (no encryption)
  - It does it best to protect against impersonation
  - It must follow local legal rules (tracking, …)

Guest Access Overview



Components of a Guest Access Solution

Network Segmentation



- Tunnels or VLANs

Guest Policy Management

- Differentiated access by guest

Guest Provisioning

- Guest provisioning web portal

Guest Login Portal

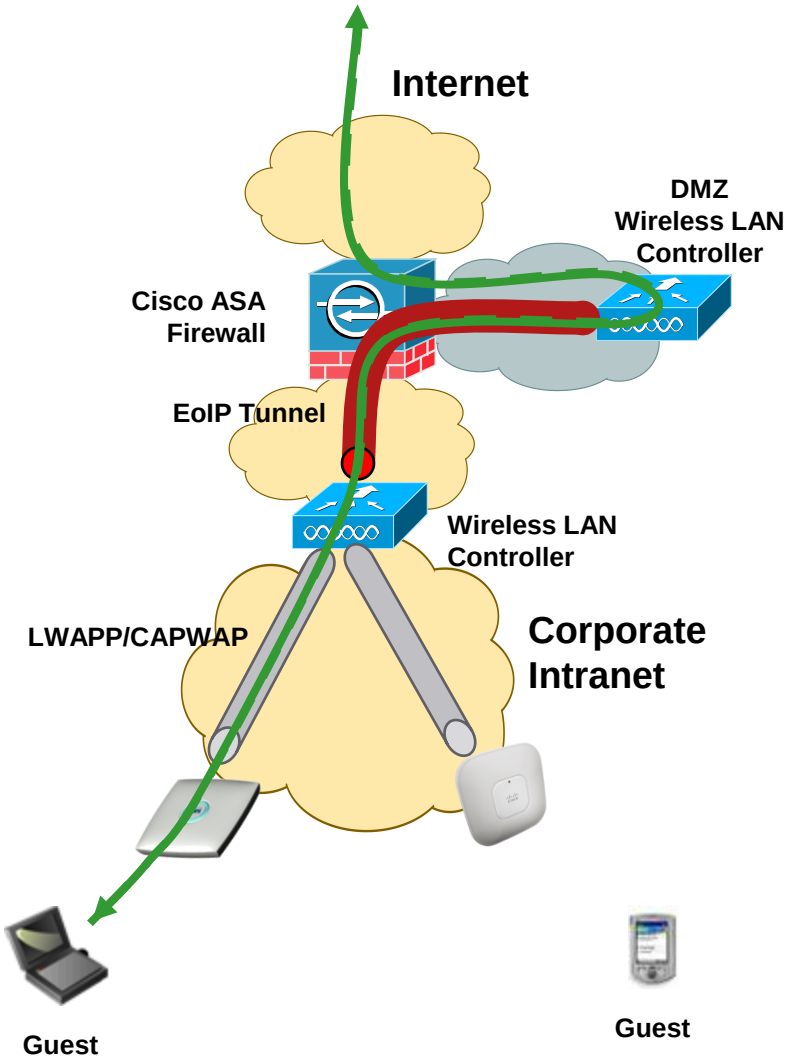
- Guest user intercept web auth portal

Reporting, Tracking

- Audit trails
- Legal tracking

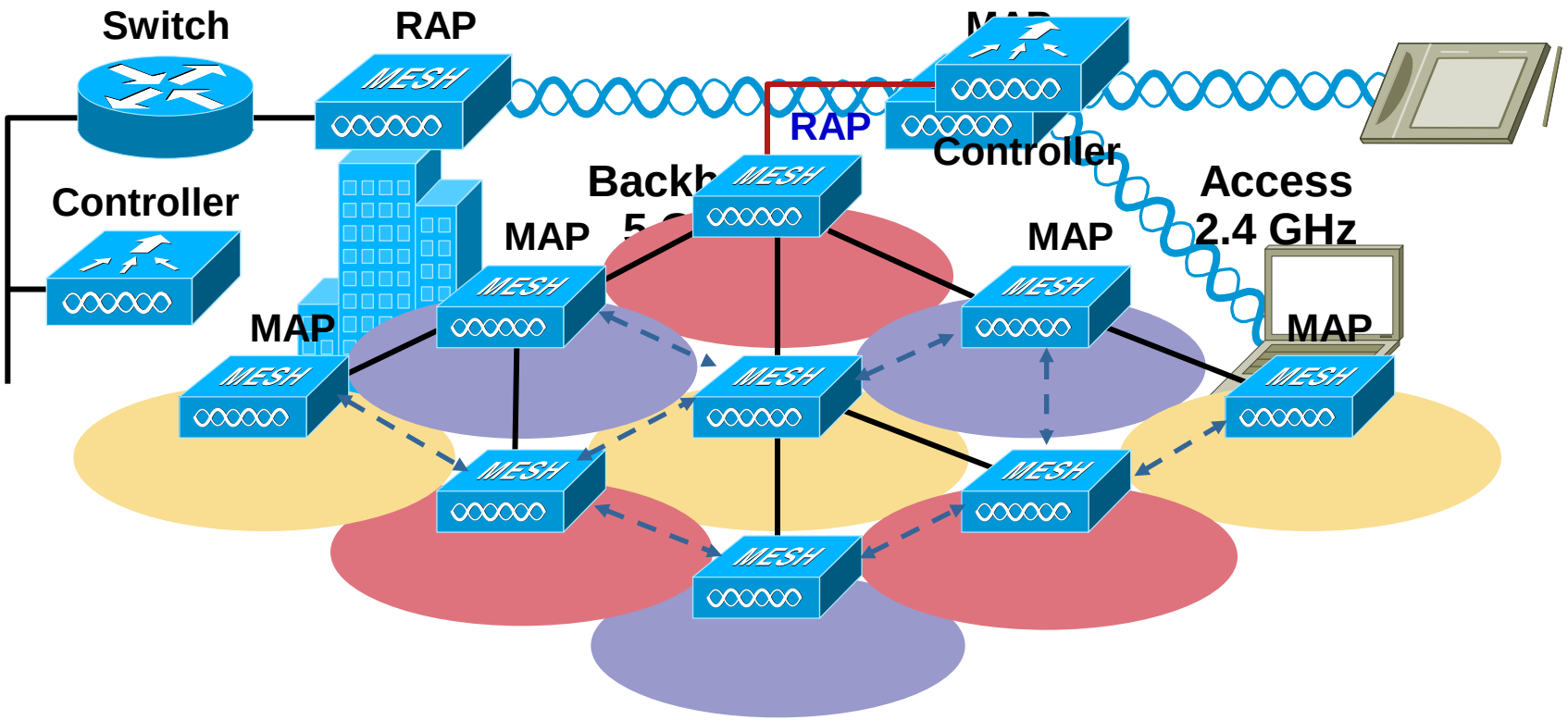
Guest isolation with Guest DMZ
Overview

- Guest service can use a Wireless Controller inside a Guest DMZ.
- Guest traffic will always be encapsulated on the corporate network.
- Guest Wireless traffic is transformed in ethernet traffic in Guest DMZ
- Guest Traffic can be controled and policed by Cisco ASA Firewall



Wireless Mesh

Wireless Bridging/Mesh Architectures



Installation—RAP Is All About Location

Mount Your Root AP on a Roof Top or Tower That Has a Good View of the Coverage Area

Ideally, You Should See Your RAP Site from the Streetlight or Coverage Area Looking Up

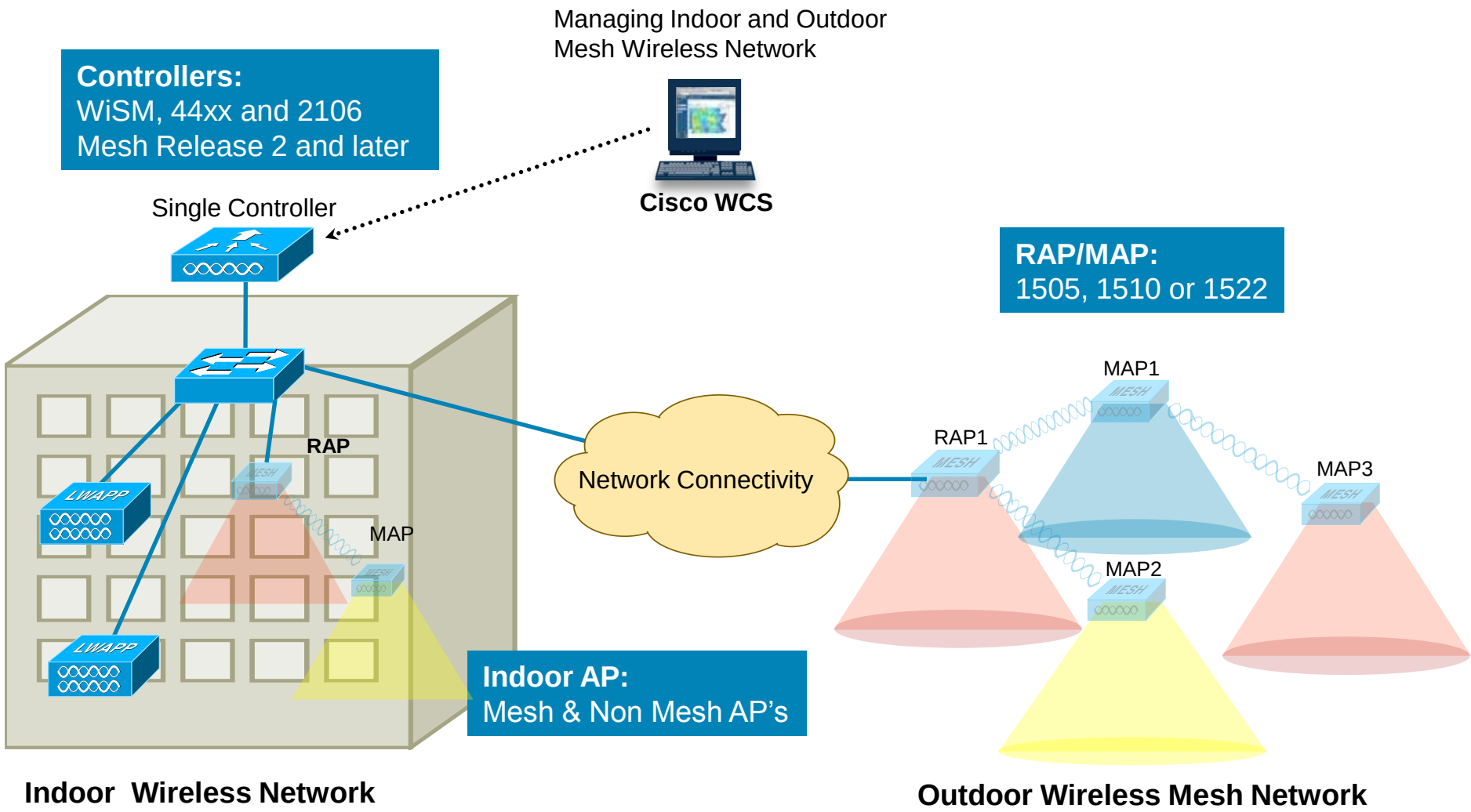
Mesh Roles—Root Access Point “RAP”

Mesh Roles—Mesh Access Point “MAP”

Antennas Installed on the Top of Pole

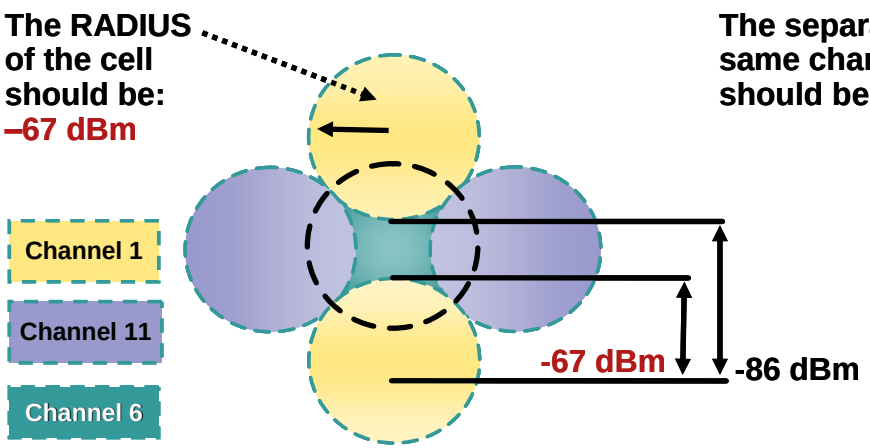
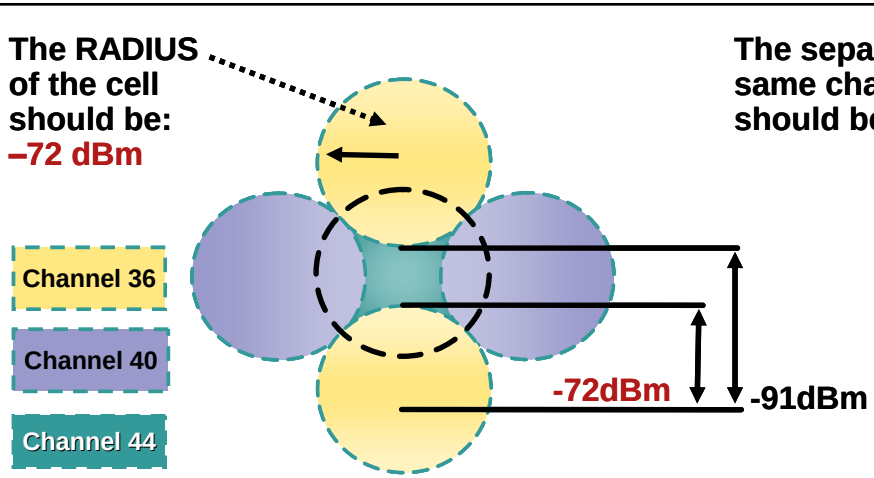
Indoor and Outdoor Deployment with Single Controller

iMesh – AP1131 AG & AP1242



VoIP over WiFi Cell Design

Ideal cell size and channel separation

	VoWLAN cell edge designs for 2.4GHz and 5GHz
802.11 b/g/n	
802.11 a/n	

Q and A