Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Design and Deployment of Enterprise WLANs

BRKEWN-2010

TOMORROW starts here.

Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

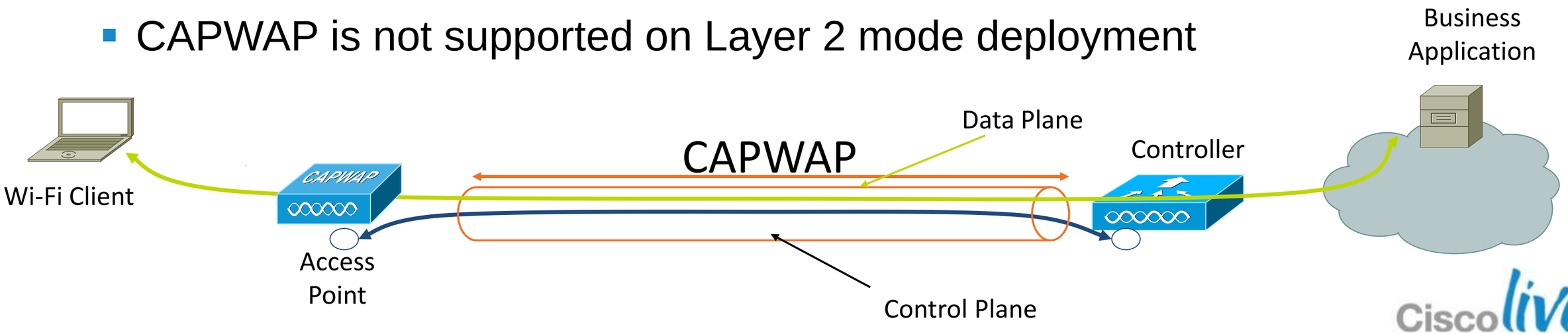
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

Centralised Wireless LAN Architecture

What Is CAPWAP?

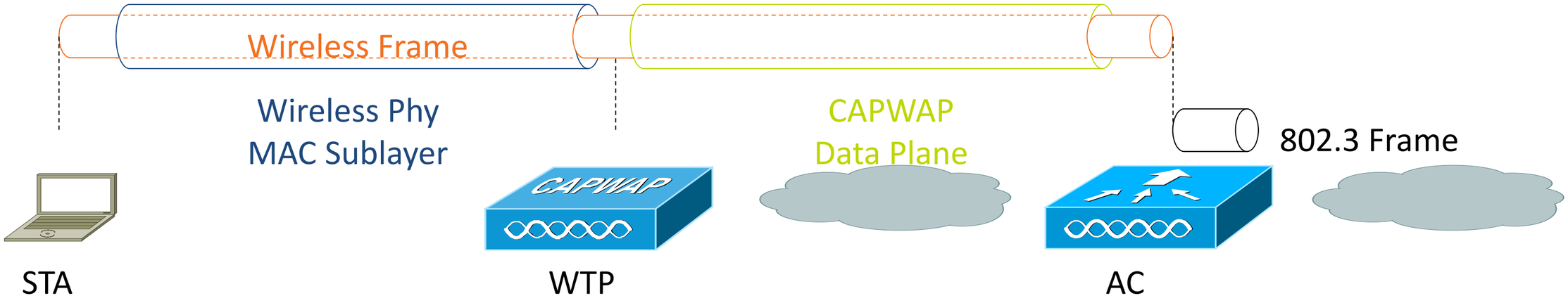
- CAPWAP: Control and Provisioning of Wireless Access Points is used between APs and WLAN controller and based on LWAPP
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (optional)
- LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless
- CAPWAP is not supported on Layer 2 mode deployment



CAPWAP Modes

Split MAC

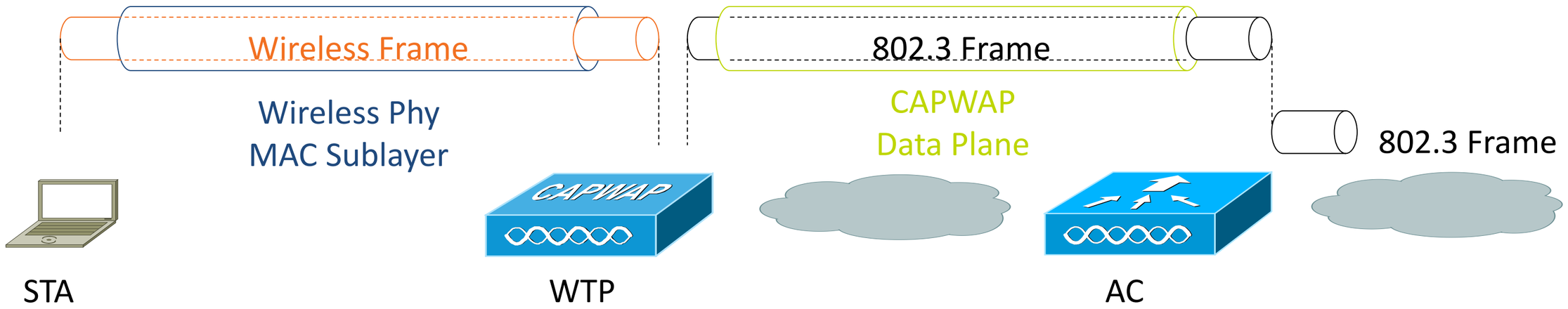
- The CAPWAP protocol supports two modes of operation
  - Split MAC (centralised mode)
  - Local MAC (H-REAP or FlexConnect)
- Split MAC



CAPWAP Modes

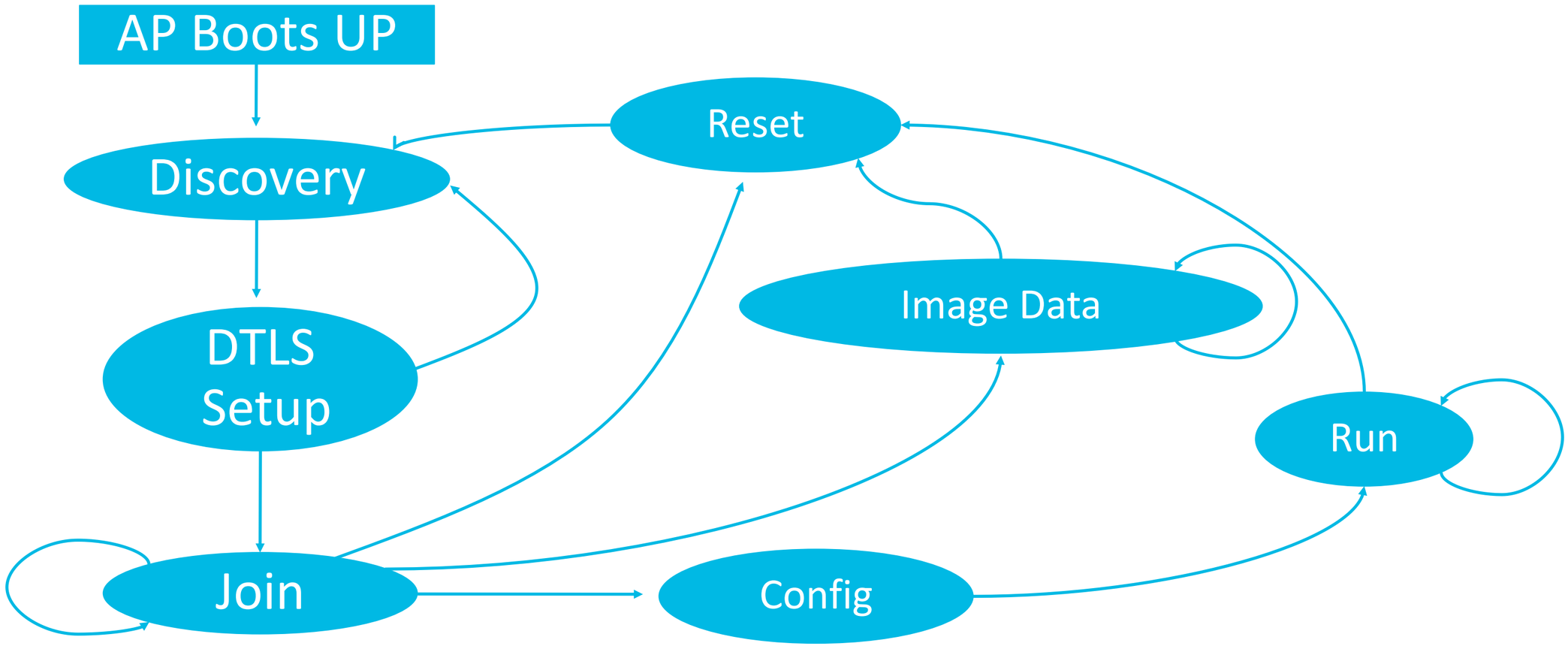
Local MAC

- Local MAC mode of operation allows for the data frames to be either locally bridged or tunneled as 802.3 frames
- Tunneled as 802.3 frames



- Tunnelled local MAC is not supported by Cisco
- H-REAP/FlexConnect support locally bridged MAC and split MAC per SSID

CAPWAP State Machine



AP Controller Discovery

Controller Discovery Order

- Layer 2 join procedure attempted on LWAPP APs
  - (CAPWAP does not support Layer 2 APs)
  - Broadcast message sent to discover controller on a local subnet
- Layer 3 join process on CAPWAP APs and on LWAPP APs after Layer 2 fails
  - Previously learned or primed controllers
  - Subnet broadcast
  - DHCP option 43
  - DNS lookup

Efficient CAPWAP Operation

Best Practices

- Define the Wireless Access Point Device DHCP Scopes
- Default router IP Address for Access Point scope
- Helper address (forwarding UDP 5246 to the WLCs management interface)
- Domain name
- Appropriate DHCP Lease timer for Aps
- Pool sizes for WLAN devices in accordance to different types of sites
- If NAT is used, static 1-to-1 NAT to an outside address is recommended

Sample Port Configuration

Controller Port

```
interface GigabitEthernet<port>
description <WLC name>
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan <vlan-list>
switchport mode trunk
switchport nonegotiate
mls qos trust cos
spanning-tree portfast trunk
```

AP Port Configuration

```
ip forward-protocol udp 5246
interface vlan <SVC>
ip helper-address <WLC1managementInterface>
ip helper-address <WLC2managementInterface>
```

6.0, 7.0, 7.2, 7.3 ? Which Version Should I Use?

- Latest Releases
  - 7.2.111.3(ED)
  - 7.0.235.3(ED)
- All Releases
  - 7.3
    - 7.3 ED Release
      - 7.3.101.0(ED)
  - 7.2
    - 7.2 ED Release
  - 7.1
    - 7.1 ED Release
  - 7.0
    - 7.0 ED Release
  - 6.0
    - 6.0 MD Release
    - 6.0 ED Release

- **WLC 5508 supports 6.0, 7.0 and 7.2 & 7.3**
- **WLC7500, WiSM-2 and WLC2504 only supported in 7.0 onwards**
- **7.0.220 is the latest MD AssureWave (Blue Ribbon)** AssureWave
- **Please note the current revision of 7.0-7.0.235.3 which is the recommended one for you today**

Agenda

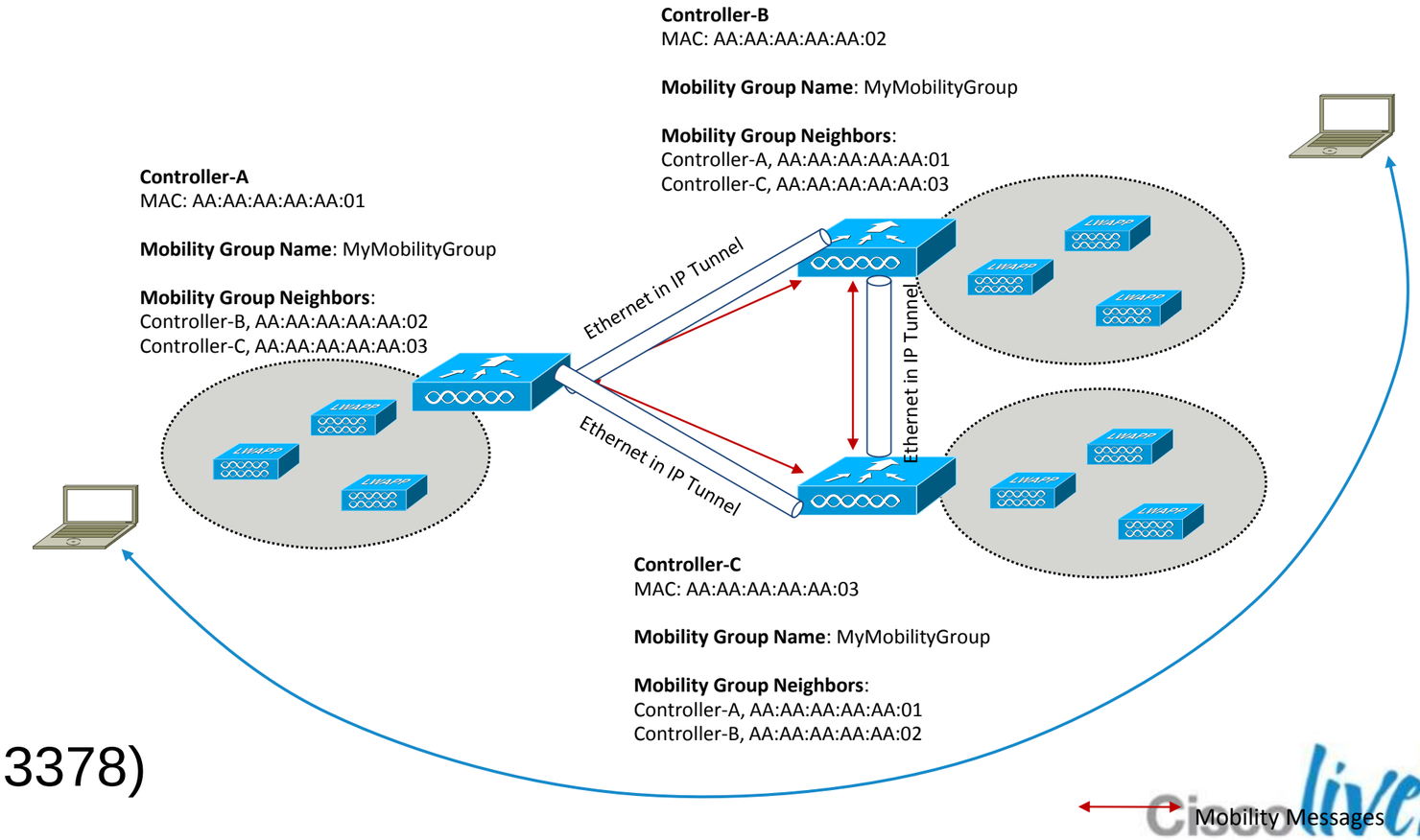
- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

Mobility Defined

- Mobility is a key reason for wireless networks
- Mobility means the end-user device is capable of moving location in the networked environment
- Roaming occurs when a wireless client moves association from one AP and re-associates to another, typically because it's **mobile!**
- Mobility presents new challenges:
  - Need to scale the architecture to support client roaming—roaming can occur intra-controller and inter-controller
  - Need to support client roaming that is seamless (fast) and preserves security

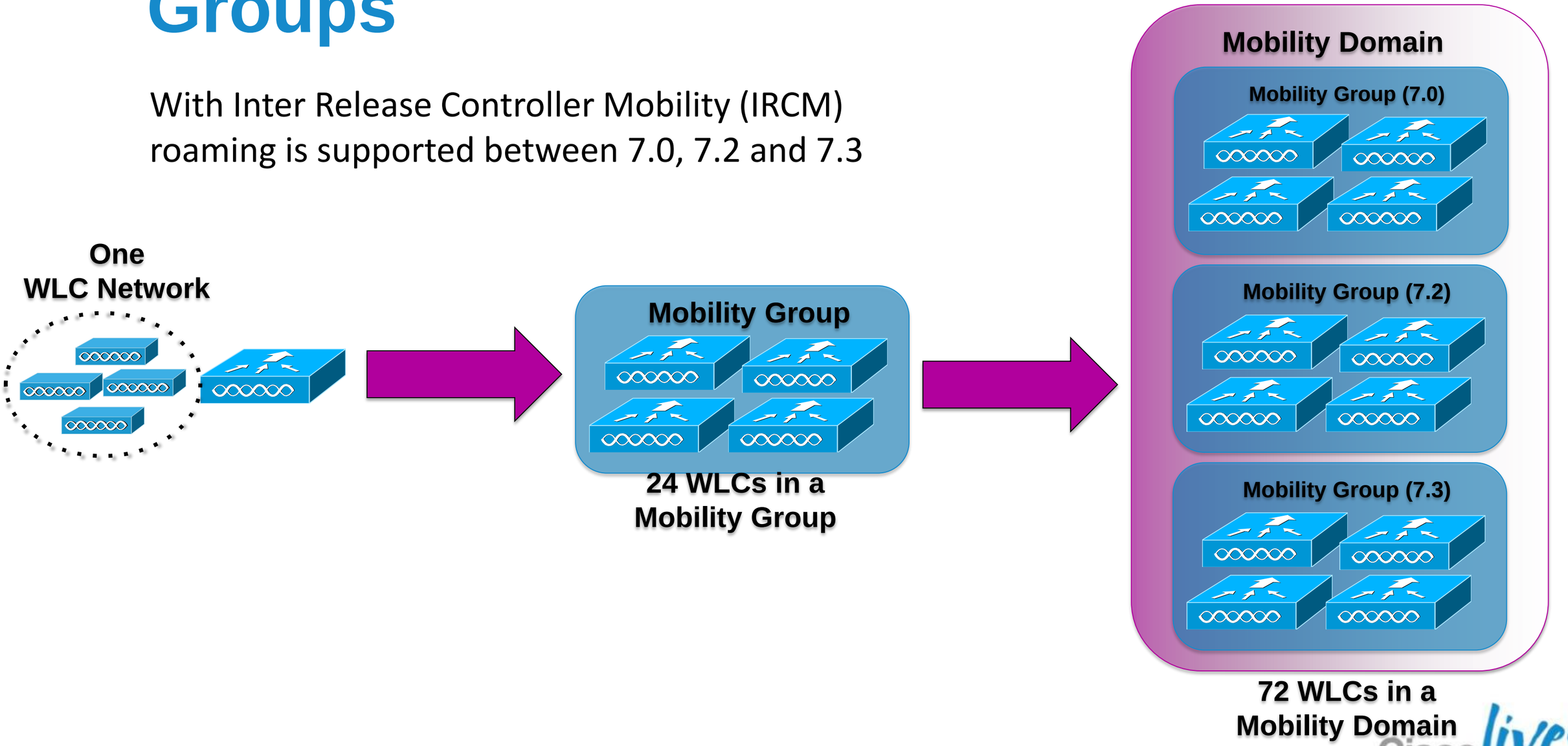
Scaling the Architecture with Mobility Groups

- 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 CAPWAP Join process
- Support for up to 24 controllers, 24000 APs per mobility group
- Mobility messages exchanged between controllers
- Data tunneled between controllers in EtherIP (RFC 3378)



Scaling the Architecture with Mobility Groups

With Inter Release Controller Mobility (IRCM) roaming is supported between 7.0, 7.2 and 7.3



How Long Does an STA Roam Take?

- Time it takes for:
  - –Client to disassociate +
  - –Probe for and select a new AP +
  - –802.11 Association +
  - –802.1X/EAP Authentication +
  - –Rekeying +
  - –IP address (re) acquisition
- All this can be on the order of seconds… Can we make this faster?

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

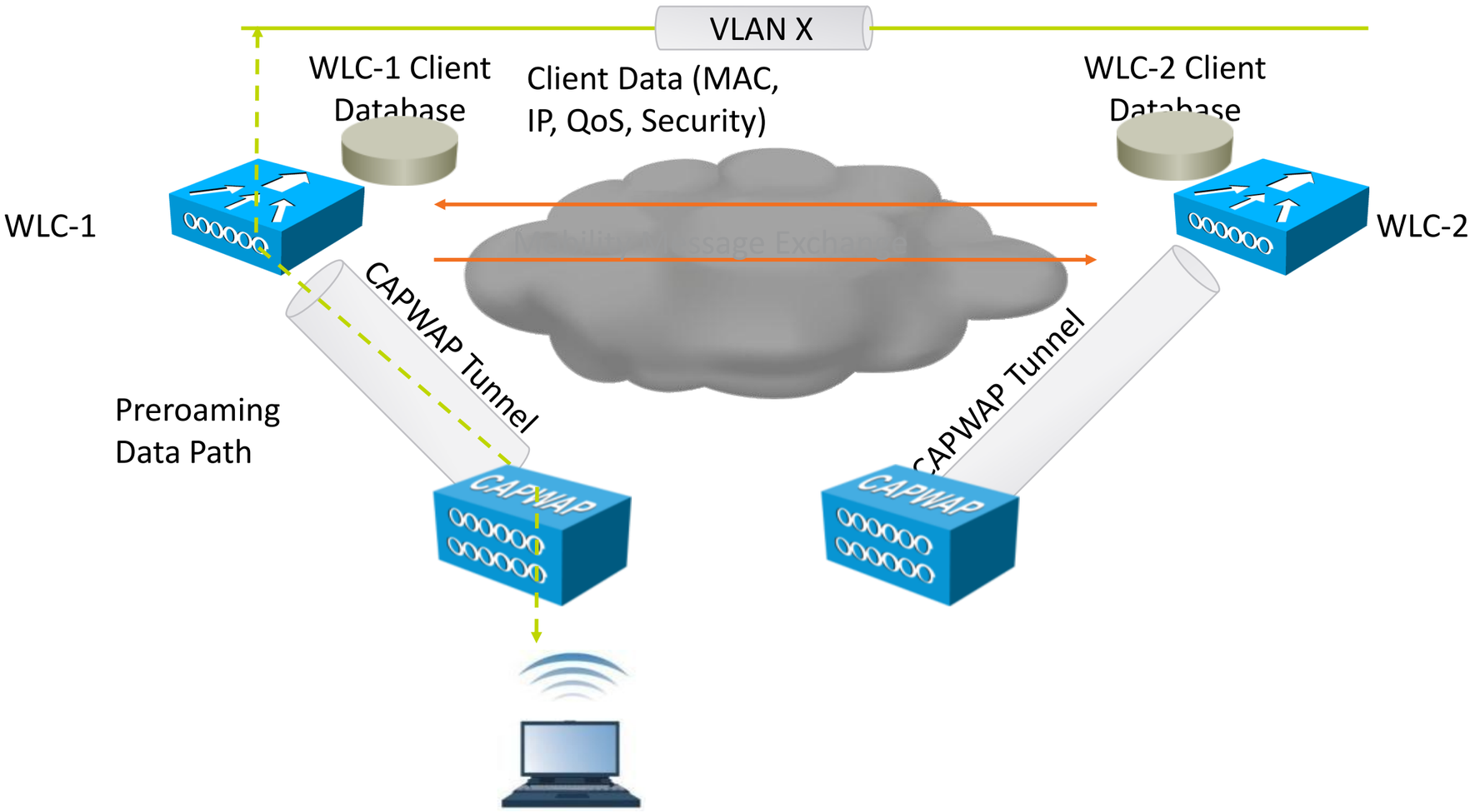
How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact

- Eliminating the (re)IP address acquisition challenge
- Eliminating full 802.1X/EAP reauthentication

Intra-Controller Roaming:

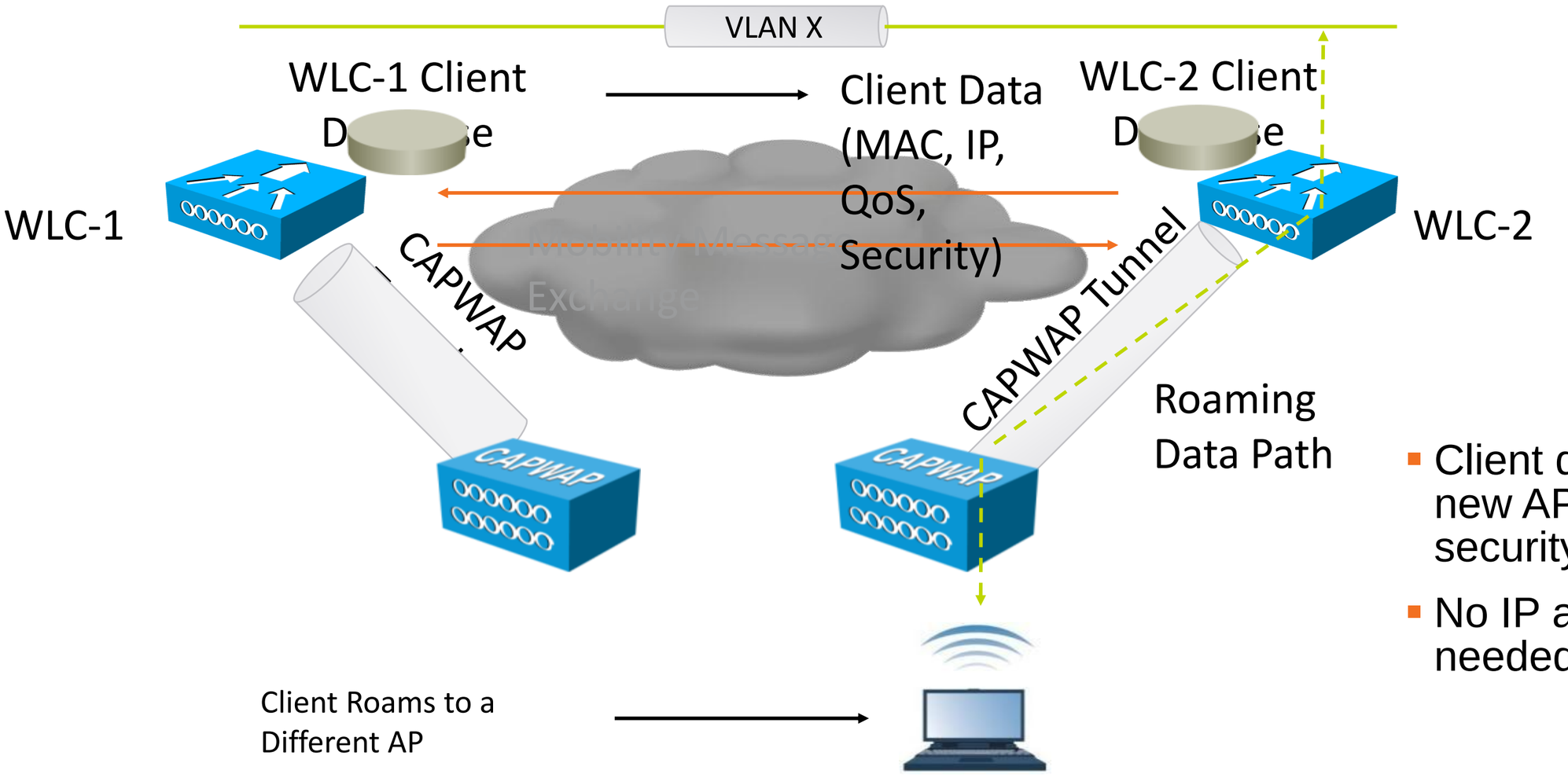
Layer 2



- 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

Intra-Controller Roaming:

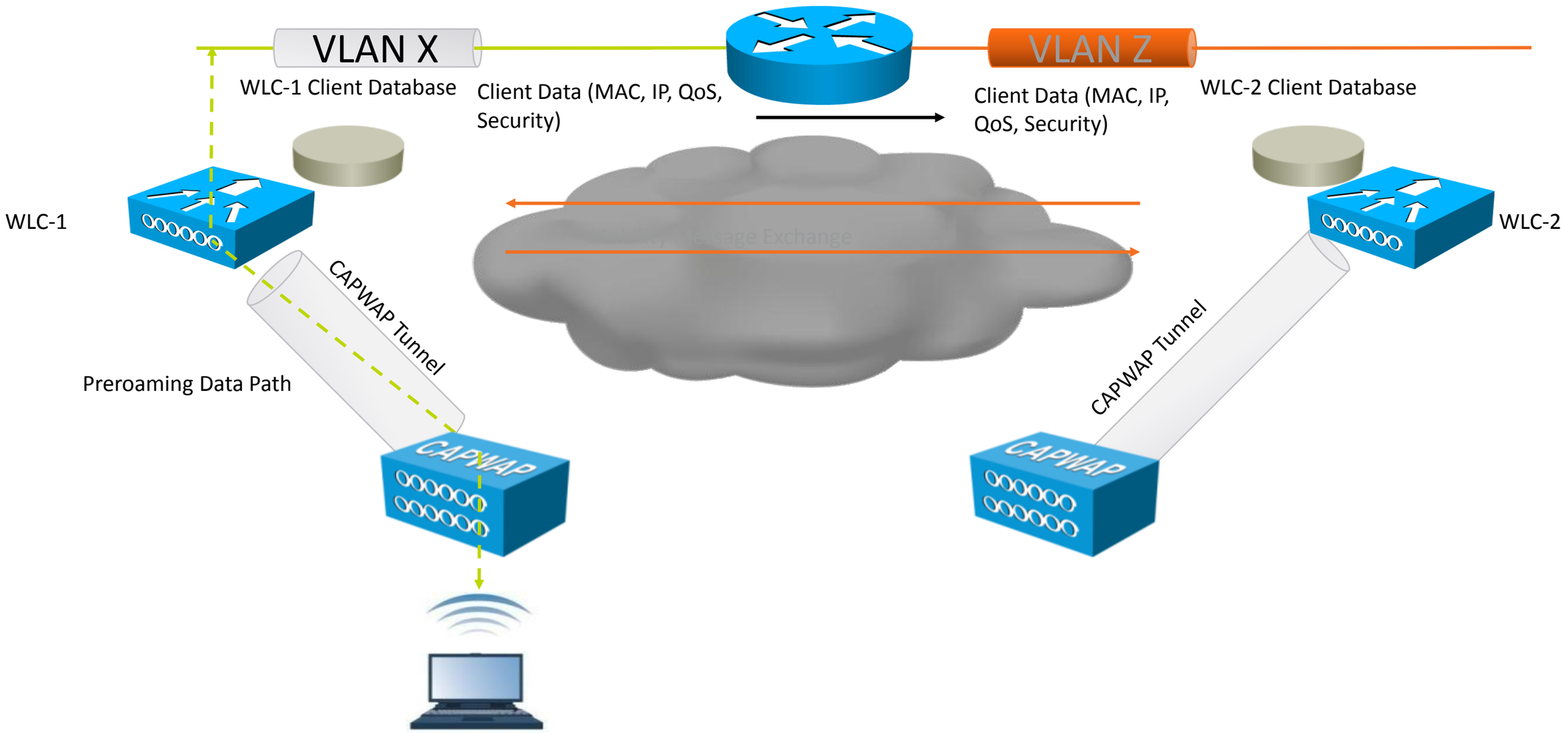
Layer 2 (Cont.)



- Client database entry with new AP and appropriate security context
- No IP address refresh needed

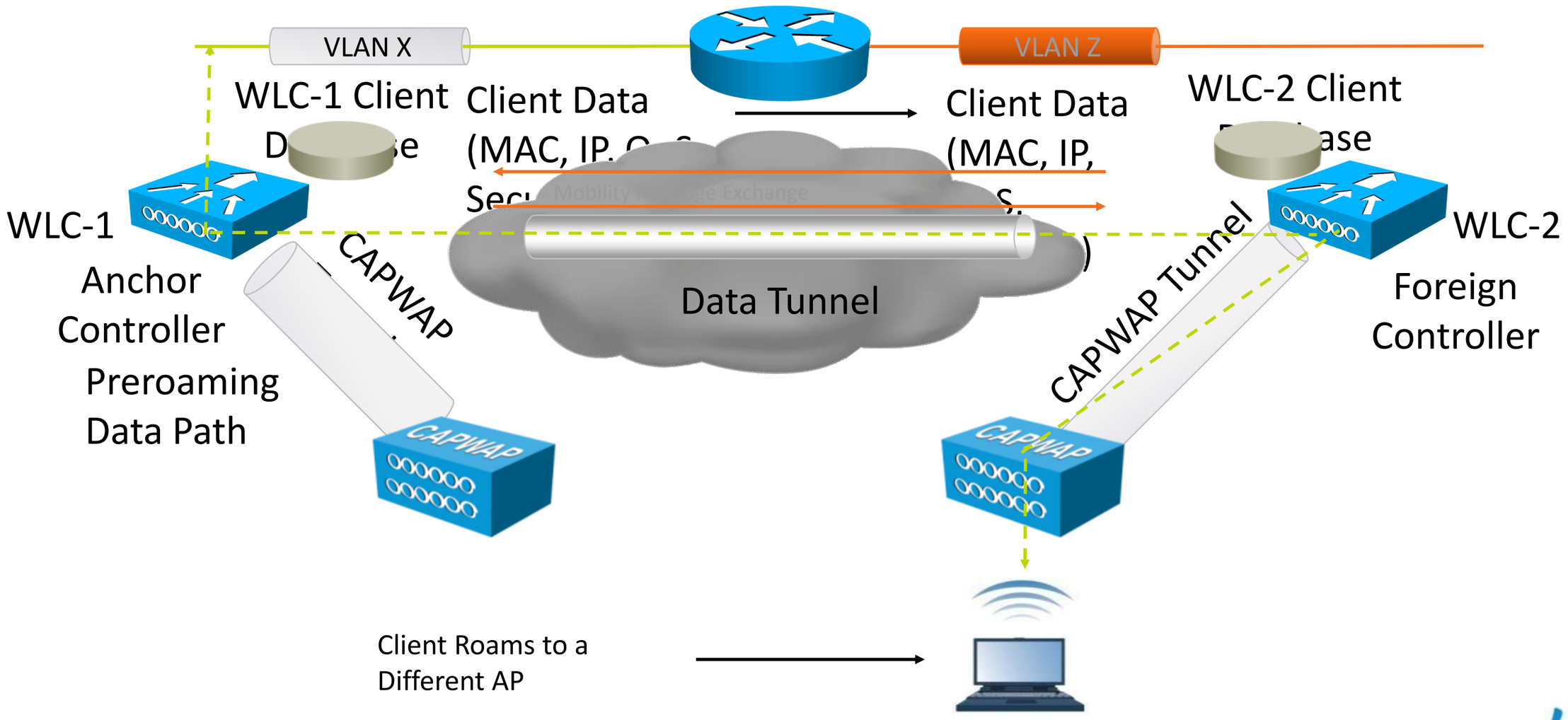
Intra-Controller Roaming:

Layer 3



Client Roaming Between Subnets:

Layer 3 (Cont.)



Roaming: Inter-Controller

Layer 3

- L3 inter-controller roam: STA moves association between APs joined to the different controllers but client traffic bridged onto different subnets
- Client must be re-authenticated and new security session established
- Client database entry copied to new controller – entry exists in both WLC client DBs
- Original controller tagged as the “anchor”, new controller tagged as the “foreign”
- WLCs must be in same mobility group or domain
- No IP address refresh needed
- Symmetric traffic path established -- asymmetric option has been eliminated as of 6.0 release
- Account for mobility message exchange in network design

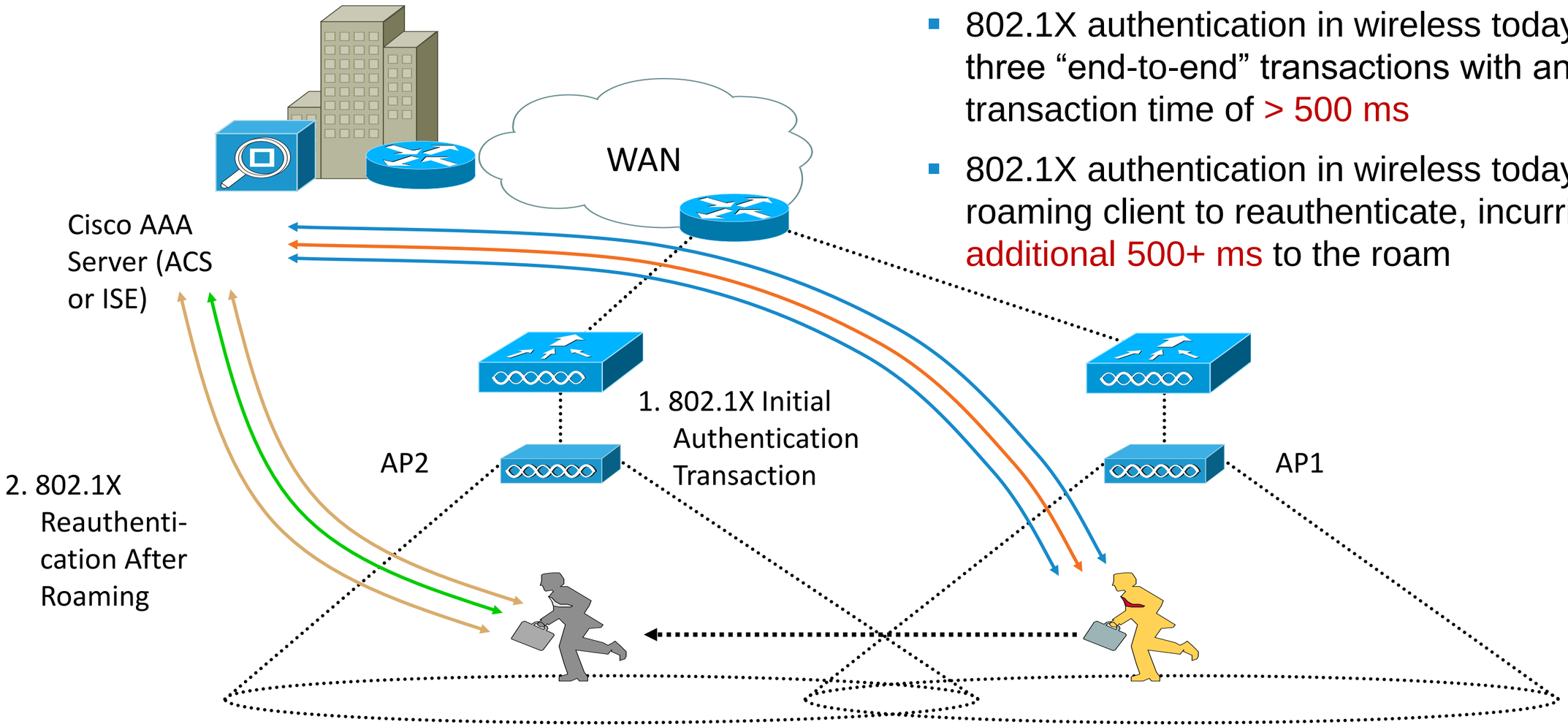
How Are We Going to Make Roaming Faster?

Focus on Where We Can Have the Biggest Impact

- ✓ Eliminating the (re)IP address acquisition challenge
- Eliminating full 802.1X/EAP reauthentication

Fast Secure Roaming

Standard Wi-Fi Secure Roaming



- 802.1X authentication in wireless today requires three “end-to-end” transactions with an overall transaction time of > 500 ms
- 802.1X authentication in wireless today requires a roaming client to reauthenticate, incurring an additional 500+ ms to the roam

Note: Mechanism Is Needed to Centralise Key Distribution

Cisco Centralised Key Management (CCKM)

- Cisco introduced CCKM in CCXv2 (pre-802.11i), so widely available, especially with application specific devices (ASDs)
- CCKM ported to CUWN architecture in 3.2 release
- In *highly controlled test environments*, CCKM roam times consistently measure in the 5-8 msec range!
- CCKM is most widely implemented in ASDs, especially VoWLAN devices
- To work across WLCs, WLCs must be in the same mobility group
- CCX-based laptops may not fully support CCKM – depends on supplicant capabilities
- CCKM is standardised in 802.11r, Apple iOS 6.0

802.11r Introduction

- IEEE Standard for Fast Roaming – CCKM / OKC.
- Introduces a new concept of roaming where the handshake with the new AP is done even before the client roams to the target AP.
- The initial handshake allows the client and APs to do PTK calculation in advance, thus reducing roaming time.
- The pre-created PTK keys are applied to the client and AP once the client does the re-association request / response exchange with new target AP.
- 802.11r provides 2 ways of roaming:
  1. Over-the-Air
  2. Over-the-DS (Distribution System)
- The FT (Fast Transition) key hierarchy is designed to allow the client to make fast BSS transitions between APs without the need to re-authenticate at every AP.
- WLAN configuration will have new AKM type called FT (Fast Transition)

802.11r – Fast Transition (FT)

WLAN Authentication Configuration

Legacy clients may not associate with a WLAN that has 802.11r enabled along with 802.11i. If the driver or the supplicant that is responsible for parsing the Robust Security Network Information Element (RSN IE) is old and confused by the additional AKM (Authentication Key Management) suites advertised in the IE (IE48), the driver will not attempt to start the association process.

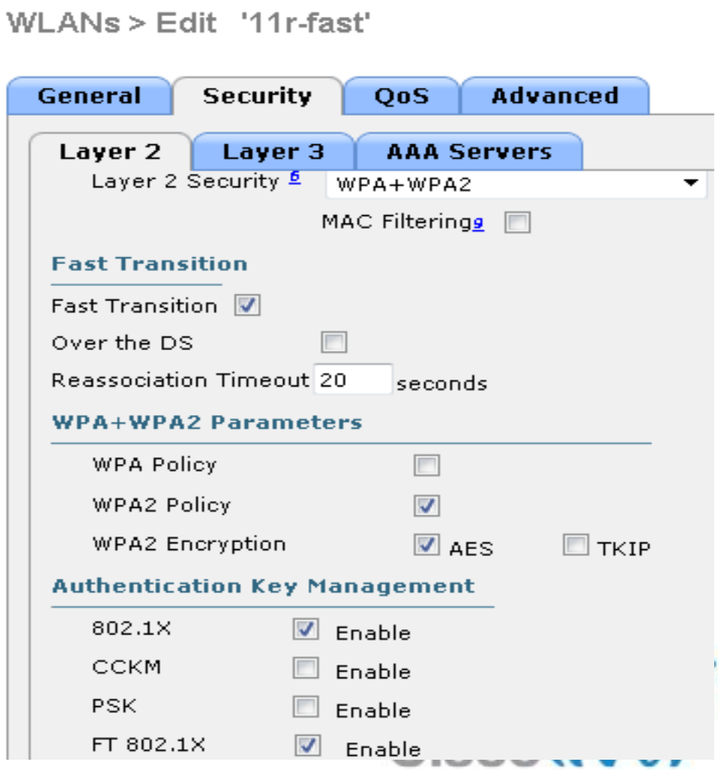
Due to this limitation, legacy clients cannot send association requests to WLANs with a FT PSK or FT 802.1x configuration.

These legacy clients, however, can still associate with non-802.11r WLANs.

Therefore the recommendation is to have a new unique WLAN. With unique SSIDs for the addition 802.11r FT WPA clients. And an additional WLAN for the 802.11r FT 802.1x clients.

An iPhone with 6.0 iOS could Authenticate to WLAN with both of these AKM's. But because of legacy clients this is NOT recommended.

A non-6.0 iOS client can't associate.



PSK & FT PSK Authentication Types

- RSN (Robust Security Network Information Exchange)
- AKMP (Authentication Key Management Protocol)
  -
- PSK (Pre Shared Key)

- AKMP – 02 is PSK
- AKMP – 04 is Fast Transition PS

```
RSN Information
    Element ID:                 48  RSN Information [108]
    Length:                     24 [109]
    Version:                    1 [110-111]
    Group Cipher OUI:           00-0F-AC [112-114]
    Group Cipher Type:          4  CCMP - default in an RSN [115]
    Pairwise Cipher Count:      1 [116-117]
    PairwiseKey Cipher List
        Pairwise Cipher OUI:    00-0F-AC-04  CCMP - default in an RSN [118-121]
    AuthKey Mngmnt Count:       2 [122-123]
    AuthKey Mngmnt Suite List
        AKMP Suite OUI:         00-0F-AC-02  None [124-127]
        AKMP Suite OUI:         00-0F-AC-04 [128-131]
    RSN Capabilities:           %0000000000101000 [132-133]
        xxxx.... ........ Reserved
        ....0... ........ SPP A-MSDUs Allowed
        .....0.. ........ SPP A-MSDU Not Supported
        ......0. ........ PeerKey Handshake Not Supported
        .......x xx...... Reserved
        ........ ..10.... GTKSA Replay Ctr: 2 - 4 replay counters
        ........ ....10.. PTKSA Replay Ctr: 2 - 4 replay counters
        ........ ......0. Does not Support No Pairwise
        ........ .......0 Does Not Support Pre-Authentication
Mobility Domain
    Element ID:                 54  Mobility Domain [134]
    Length:                     3 [135]
    Mobility Domain Id:         0xC4D0 [136-137]
    FT Capability:              %00000000 [138]
```

802.1x & FT 802.1x Authentication Types

- AKMP – 01 is 802.1x
- AKMP – 03 is

  Fast Transition 802.1x

- The Mobility Domain ID is

  different for each Mobility Domain

```
RSN Information
    Element ID:                 48  RSN Information [108]
    Length:                     24 [109]
    Version:                    1 [110-111]
    Group Cipher OUI:           00-0F-AC [112-114]
    Group Cipher Type:          4  CCMP - default in an RSN [115]
    Pairwise Cipher Count:1 [116-117]
    PairwiseKey Cipher List
        Pairwise Cipher OUI:    00-0F-AC-04  CCMP - default in an RSN [118-121]
    AuthKey Mngmnt Count:       2 [122-123]
    AuthKey Mngmnt Suite List
        AKMP Suite OUI:         00-0F-AC-01  802.1X Authentication [124-127]
        AKMP Suite OUI:         00-0F-AC-03 [128-131]
    RSN Capabilities:           %0000000000101000 [132-133]
                                xxxx.... ........ Reserved
                                ....0... ........ SPP A-MSDUs Allowed
                                .....0.. ........ SPP A-MSDU Not Supported
                                ......0. ........ PeerKey Handshake Not Supported
                                .......x xx...... Reserved
                                ........ ..10.... GTKSA Replay Ctr: 2 - 4 replay counters
                                ........ ....10.. PTKSA Replay Ctr: 2 - 4 replay counters
                                ........ .......0 Does not Support No Pairwise
                                ........ .......0 Does Not Support Pre-Authentication
Mobility Domain
    Element ID:                 54  Mobility Domain [134]
    Length:                     3 [135]
    Mobility Domain Id:         0xC4D0 [136-137]
    FT Capability:              %00000000 [138]
```

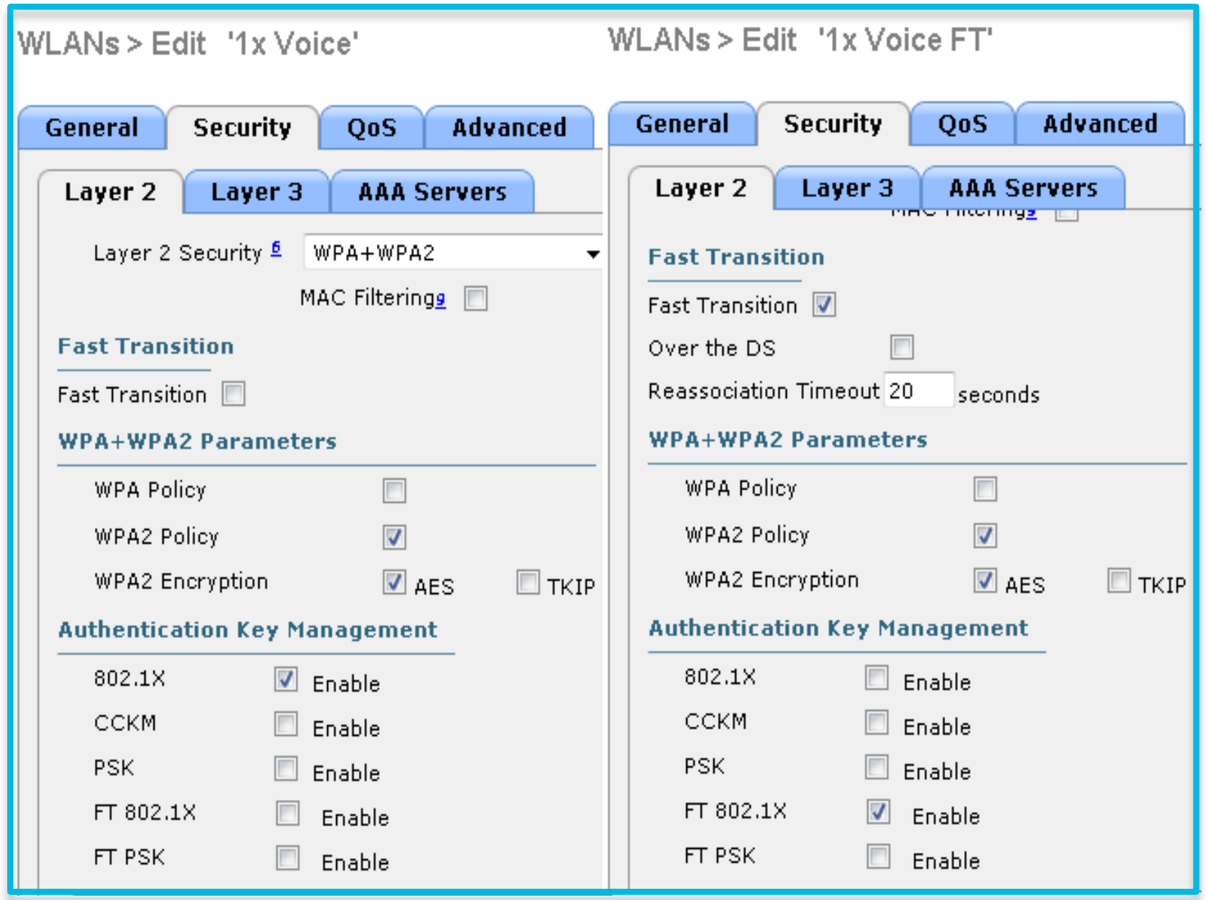
Example of the Recommended WLAN Configurations if using 802.11r -- Fast Transition .

- The next page shows our configuration recommendation for adding 802.11r Fast Transition support to your Wi-Fi network.
- These examples show a unique SSID for the two authentication types that crossover with the two new authentication types add by 802.11r.
- Our recommendation is have unique SSIDs for each of the types. Legacy clients that cannot do 802.11r can become confused by the additional information of 802.11r.
- This type of thing has happened before in 802.11. When 802.11g was approved, there were some 802.11b clients that were not 802.11g aware. And 802.11g had to be disabled to allow those clients to join the Wi-Fi network.

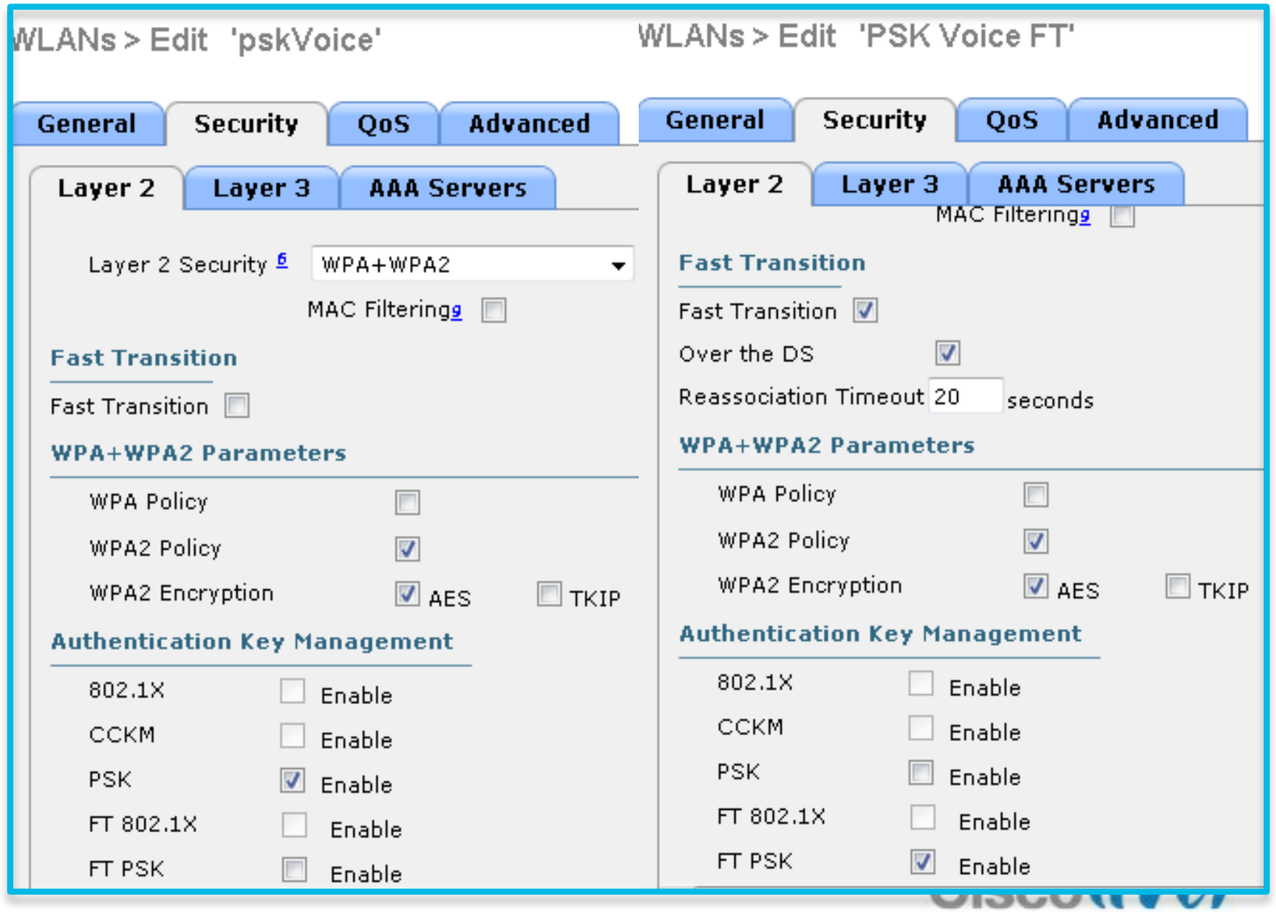
Multiple WLANs for Multiple Auth Types Each with a Unique SSID

WLAN ID	Type	Profile Name	WLAN SSID	Status	Security Policies
6	WLAN	1x Voice	1Voice	Enabled	[WPA2][Auth(802.1X)]
7	WLAN	1x Voice FT	1VoiceFT	Enabled	[WPA2][Auth(FT 802.1X)]
8	WLAN	PSK Voice	pskVoice	Enabled	[WPA2][Auth(PSK)]
9	WLAN	PSK Voice FT	pskVoiceFT	Enabled	[WPA2][Auth(FT-PSK)]

802.1x & 802.1x FT WLANs Unique SSIDs



PSK & PSK FT WLANs With Unique SSIDs



Limitations with 802.11r BSS Fast Transition

- This feature is supported only on open and WPA2 configured WLANs.
- Legacy client don't know the 802.11r elements in Probe and Association Responses.
  - **The above packet decode shows "Element ID: 48" used by 802.11r**
  - **And therefore will not associate to 802.11r enabled WLANs.**
- The workaround is to enable or upgrade the driver of the legacy client to work with the new 802.11r AKMs. After which the legacy clients can successfully associate with 802.11r enabled WLANs.
- Another workaround is to add with a unique SSID security settings for FT. (Shown in the WLAN Security Configuration Screens.)
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three Fast Transition handshakes with different APs.

Designing a Mobility Group/Domain

Design Considerations

- Less roaming is better – clients and apps are happier
- While clients are authenticating/roaming, WLC CPU is doing the processing – not as much of a big deal for 5508 which has dedicated management/control processor
- L3 roaming & fast roaming clients consume client DB slots on multiple controllers – consider “worst case” scenarios in designing roaming domain size
- Leverage natural roaming domain boundaries
- Mobility Message transport selection: multicast vs. unicast
- Make sure the right ports and protocols are allowed

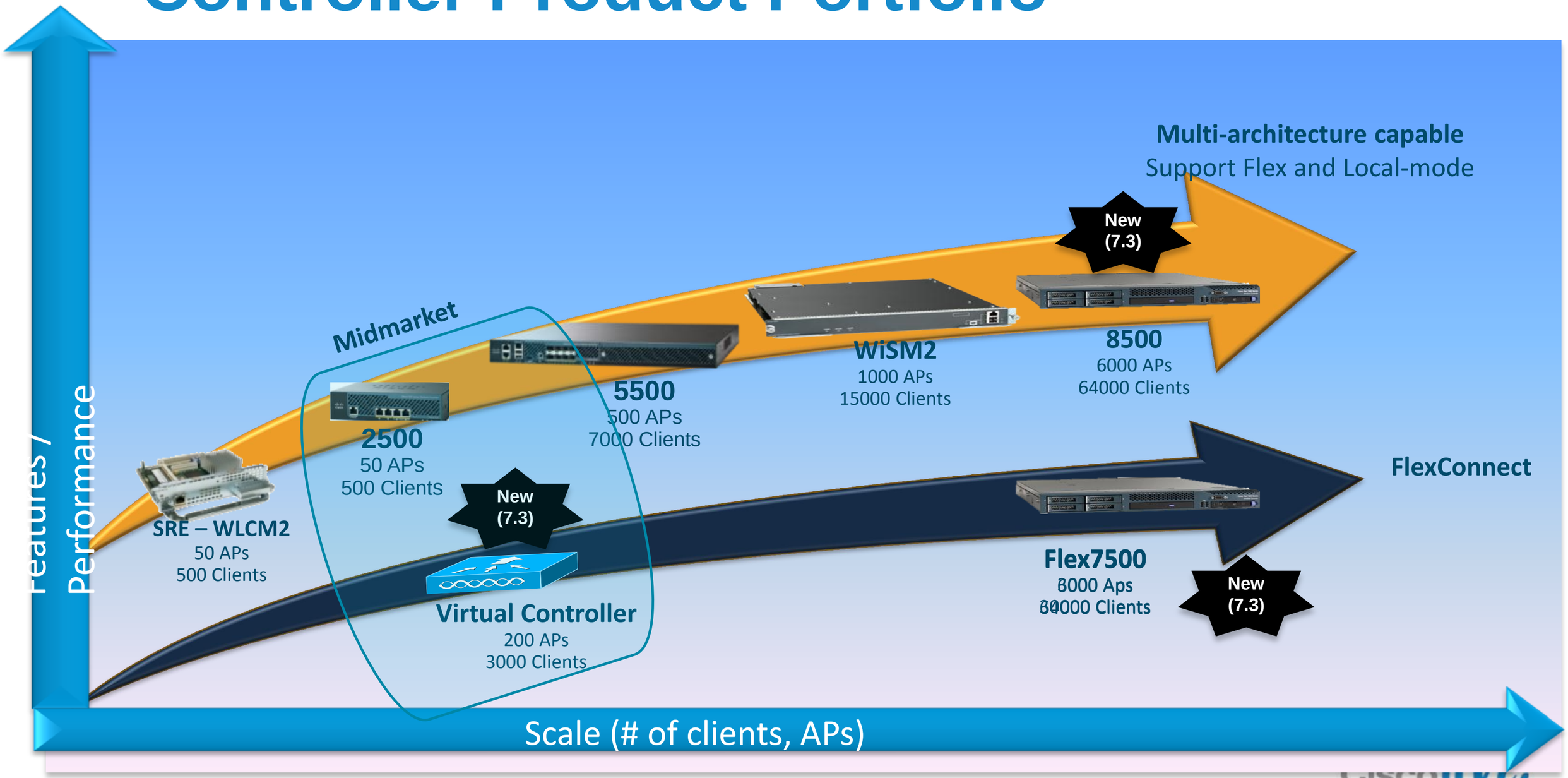
Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

CUWN Release - Key Controller Features

S/W Release	May 2012	September 2012	Q1 CY13
	7.2MR1	7.3	7.4
Unified Access WLAN Infrastructure	Outdoor AP Internal Antenna	AP 2600 802.11n G2	AP1600 802.11n G2
		Outdoor AP Uni Band Antenna	AP3600 Security Module
	Outdoor AP Honeywell integration	WLC 8500 Target customer - SP	Application visibility and control (AVC)
		Virtual Controller	Bonjour Gateway
	802.11r L2 Fast Roaming	Scale Flex7500 6K APs	Voice Enterprise Certification**
		HA - AP SSO HA Licensing	Scale WLC 2500
	ISE -Flex integration Flex / Local Mode parity with ISE	FlexConnect Split Tunneling	HA Licensing, N:1
		802.11r – Flex Modes	LAG on Flex7500, WLC 8500, WLC 2500
	Local and FlexConnect support on RAP	Bi-directional rate-limiting	
		Voice/Video: 11n CAC	Guest Anchor on WLC2500
		PMIPv6 on WLC	

Controller Product Portfolio



Virtual Controller

Midmarket-Focused Solution

Product Scope

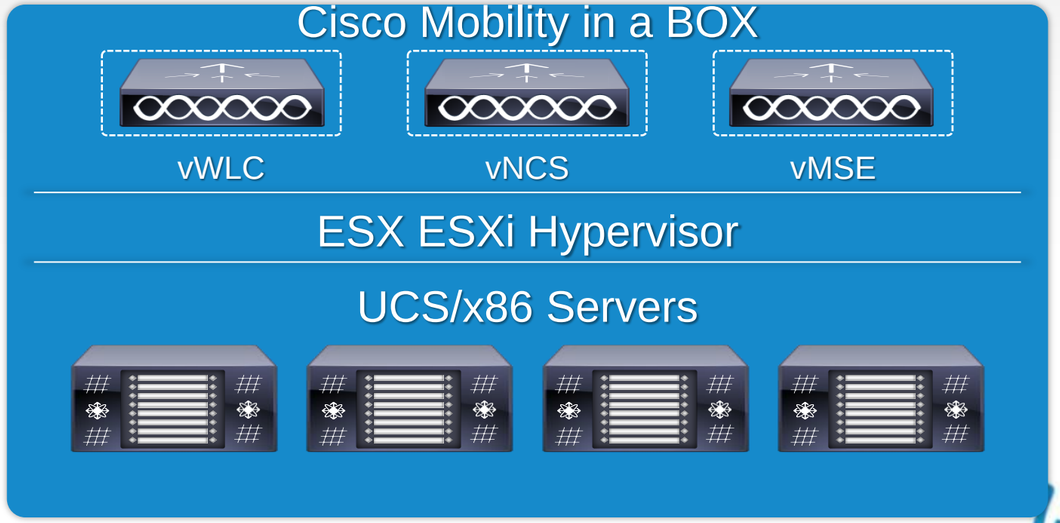
- 5 to 200 AP support, 3,000 clients
- One AP adder license
- FlexConnect mode only
- Support on VMware ESX/ESXi at FCS (similar to NCS and MSE)
- Support on Cisco UCS C-Series and B-Series and equivalent servers

Pricing

- Base SKU (with five AP licenses) = $750
- One AP Adder license = $150

Target Market

- Mid-market with spare compute platform
- Alternative to Flex 7500 for customers with fewer branches
- Partner/MSP-hosted Wi-Fi service
- NOT for large campus



Cisco 8510 Series Controller

Optimised for High-Scale Deployments

New in 7.3

Access Points	3000–6,000
Clients	64,000
Branches/Locations	6,000 (2,000 Groups)
Access Points per FlexConnect Group	100
Deployment Model	Local, FlexConnect, and Mesh
Form Factor	1 RU
IO Interface and Redundancy	Dual Redundant 10GE Ports*
Power Options	AC and DC*
Power Redundancy	Dual Redundant Power Supplies Installed*

*Unique 8500 features

- High scale for SP and large campus deployments
  - 6,000 local mode APs and 64,000 clients in 1RU*
  - 4K VLANs
- Rich features with deployment flexibility (7.3 release)
  - High availability with subsecond stateful switchover Outdoor AP support
  - FlexConnect, local mode, and mesh support*
  - 3G packet core integration: PMIPv6 MAG solution with ASR5K (LMA)
  - FlexConnect with HS2.0 for 3G offload

Cisco Aironet Access Points

TELEWORKER

600

- Basic Connectivity
- Deployment Flexibility

ENTERPRISE CLASS

1600

Q2FY 13

- Enterprise Class Performance
- Video/Voice/Multi-Media

MISSION CRITICAL

2600

New

- Any Device/BYOD Optimised
- Client Scalability
- RF Interference Mitigation

BEST IN CLASS

3600

- High Client Density
- Investment Protection
- 802.11ac Support
- HD Video/VDI
- Best In Class Security

Entry Level → Sm/Med → Sm/Med/Large → Med/Large Enterprise

Cisco Aironet 802.11n Indoor Access Point

* Basic SI only, ** Future Support

AP Model (availability)	3600 Series	2600 Series	1600 Series (Q4)	600 Series
Max Data Rate	1.3 Gbps	450 Mbps	300 Mbps	300 Mbps
Radio Design (MIMO: Spatial Streams)	.11n: 4X4:3 .11ac: 3x3:3	3X4:3	3X3:2	2X2:2
CleanAir	✔	✔	*	
ClientLink	ClientLink 2.0	ClientLink 2.0	ClientLink 2.0	
BandSelect	✔	✔	✔	
VideoStream	✔	✔	✔	
Rogue AP Detection	✔	✔	✔	
Adaptive wIPS	✔	✔	✔	✔
OfficeExtend	✔	✔	✔	✔
FlexConnect	✔	✔	✔	✔
Wireless Mesh	✔	✔	✔	
Autonomous	✔	✔	✔	
Power	802.3af	802.3af	802.3af	100 to 240 VAC, 50-60 Hz
Wi-Fi Standards	802.11 a/b/g/n/ac	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n

Agenda

- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

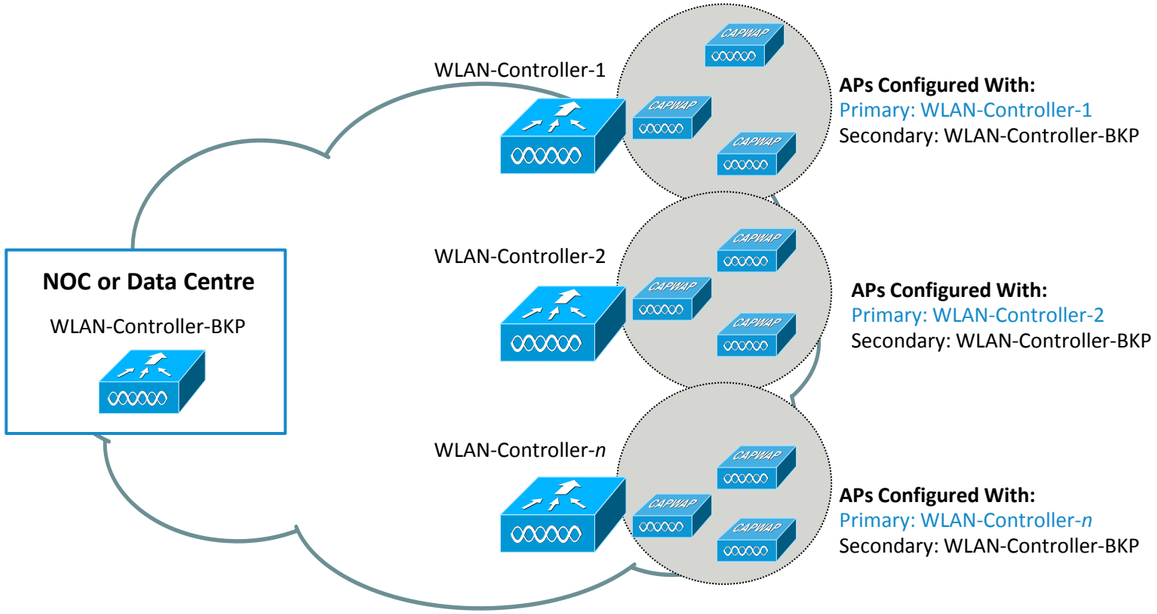
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

Controller Redundancy

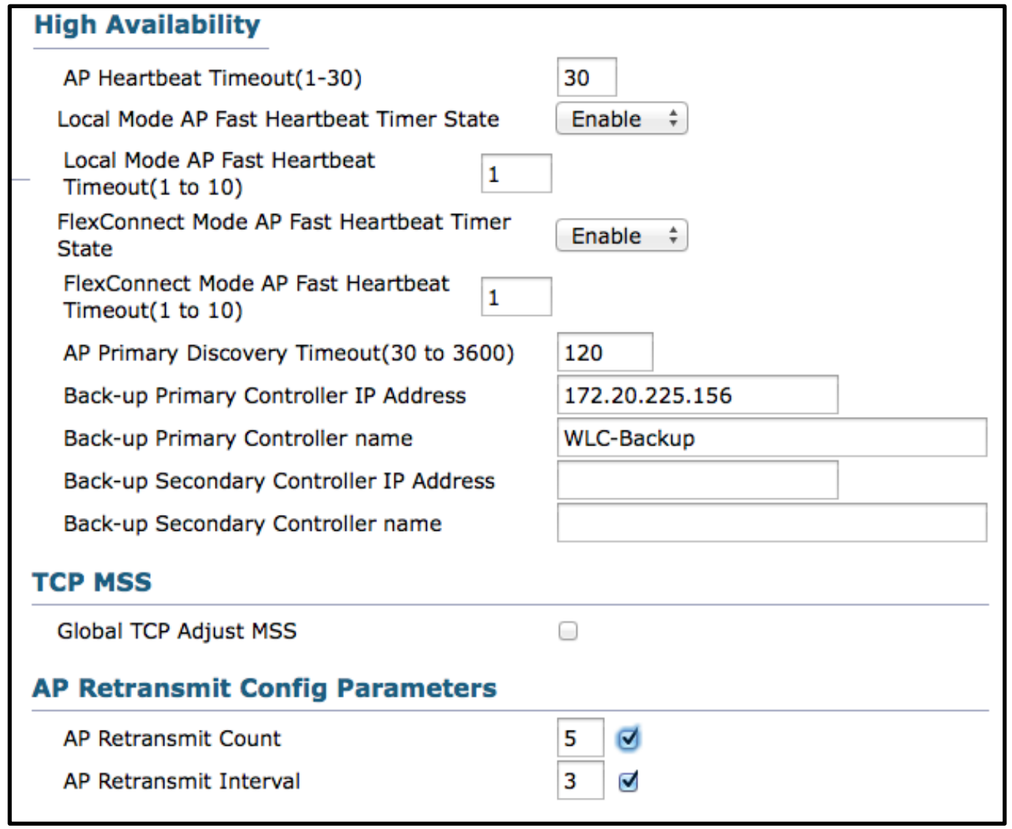
Most Common (N+1)

- Redundant WLC in a geographically separate location
- Layer-3 connectivity between the AP connected to primary WLC and the redundant WLC
- Redundant WLC need not be part of the same mobility group
- Configure high availability (HA) to detect failure and faster failover
- Use AP priority in case of over subscription of redundant WLC



Controller Redundancy – High Availability

- High Availability Principles :
  - ⇨ AP is registered with a WLC and maintain a backup list of WLC.
  - ⇨ AP use heartbeats to validate WLC connectivity
  - ⇨ AP use Primary Discovery message to validate backup WLC list
  - ⇨ When AP loose 3 heartbeats it start join process to first backup WLC candidate
  - ⇨ Candidate Backup WLC is the first alive WLC in this order : primary, secondary, tertiary, global primary, global secondary.
  - ⇨ AP does not re-initiate discovery process.



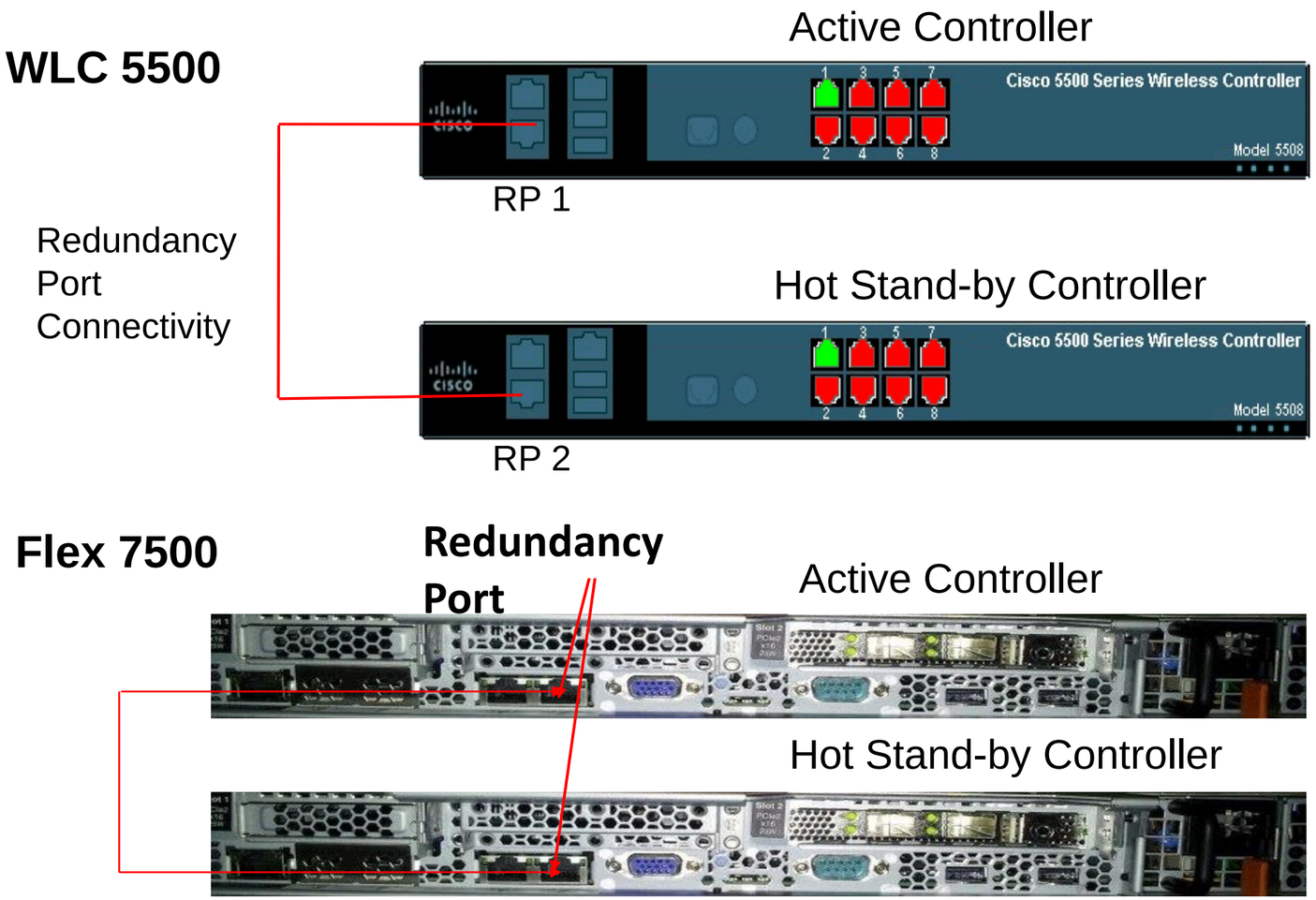
	New Timers 7.2
Heartbeat Timeout	**1-30 secs**
Fast Heartbeat Timer	**1-10 secs**
AP Retransmit Interval	**2-5 secs**
AP Retransmit with FH Enabled	**3-8 Times**
AP Fallback to next WLC	**12 secs**

True High Availability in 7.3 release

- Box to Box High Availability i.e. 1:1
- One WLC in Active state and Second WLC in Hot Standby State monitors the health of Active WLC via Redundant Port
- Configuration on Active is synched to Standby WLC via Redundant Port
- Both the WLC shares the same set of configuration including the IP Address of management interface.
- APs CAPWAP State (Only APs which are in RUN state) also synched. APs does not go in Discovery state when Active WLC fails
- Downtime between failover reduced to 5 - 1000 msec in case of Box failover and up to 3 seconds in case of Network Issues
- Supported on 5500 / 7500 / 8500 and WiSM-2

HA Connectivity on 5500 / 7500 / 8500 WLC

- 5500/7500/8500 WLC have dedicated Redundancy Port which is used to synch configuration from Active to Standby WLC
- Keepalives are sent on RP port from Standby to Active WLC every 100 msec (default timer) to check the health of Active WLC.
- ICMP packets are also sent every one second from each WLC to check reachability to gateway using Redundant Management interface.



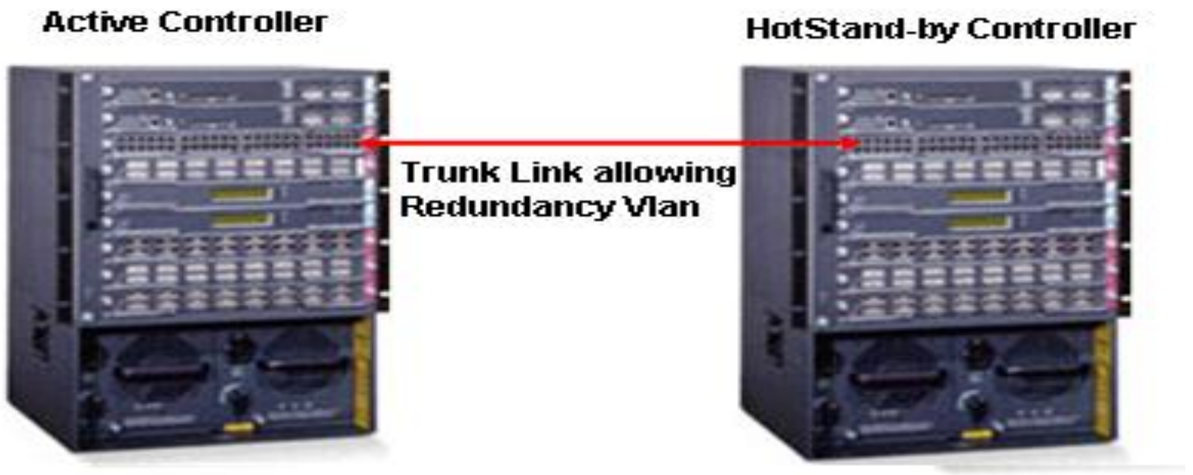
High Availability Connectivity on WiSM-2 WLC

- WiSM-2 WLC have dedicated **Redundancy Vlan** which is used to synch configuration from Active to Standby WLC
- Keepalives are sent on Redundancy Vlan from Standby to Active WLC every 100 msec (default timer) to check the health of Active WLC.
- To achieve HA between WiSM-2 WLCs it can be deployed in single chassis OR can also be deployed between multiple chassis using VSS as well as by extending Redundancy Vlan between two chassis.

WISM2 configuration on Cat6k

Multi Chassis Connectivity

```
wism service-vlan 192 (service port Vlan)
wism redundancy-vlan 169( redundancy port Vlan)
wism module 6 controller 1 allowed-vlan 24-38(data vlan)
```

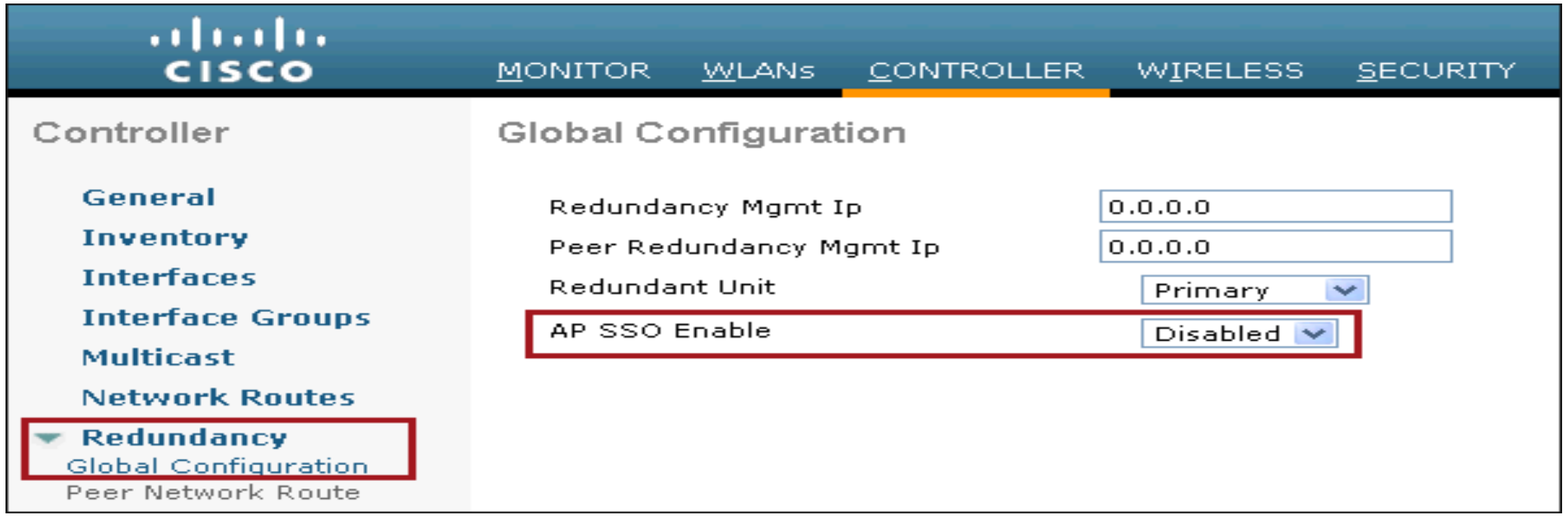


Single Chassis HA Setup

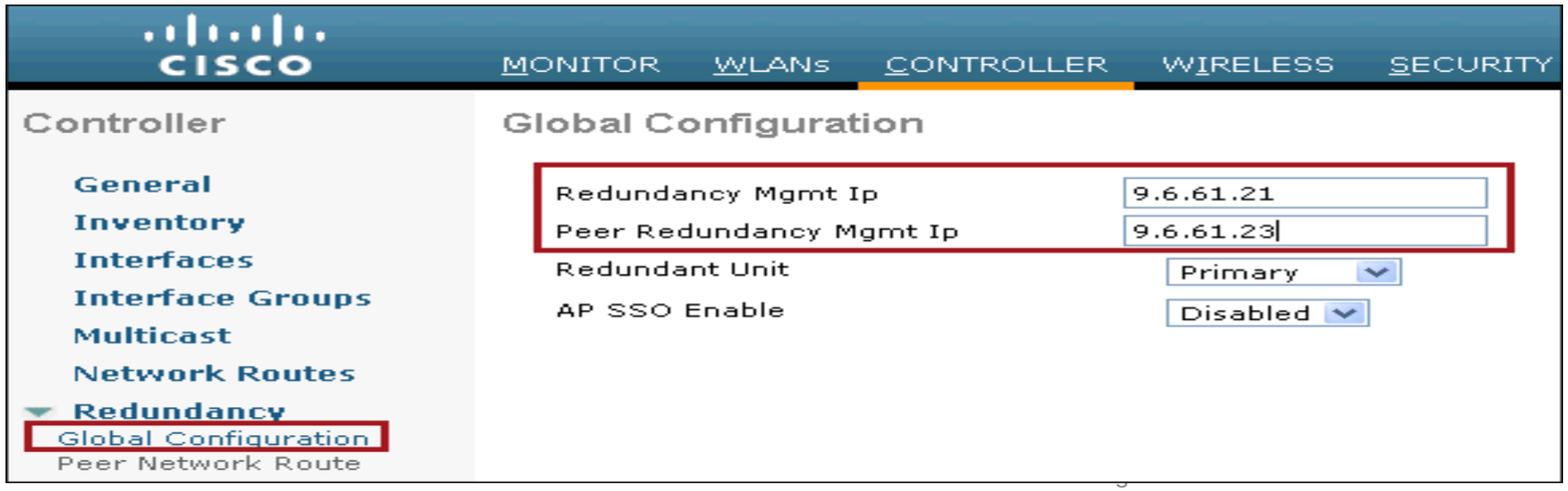
Slot 8: Active WiSM-2
Slot 9: Hot Stand-By WiSM-2

High Availability Configuration

- By default HA is disabled.

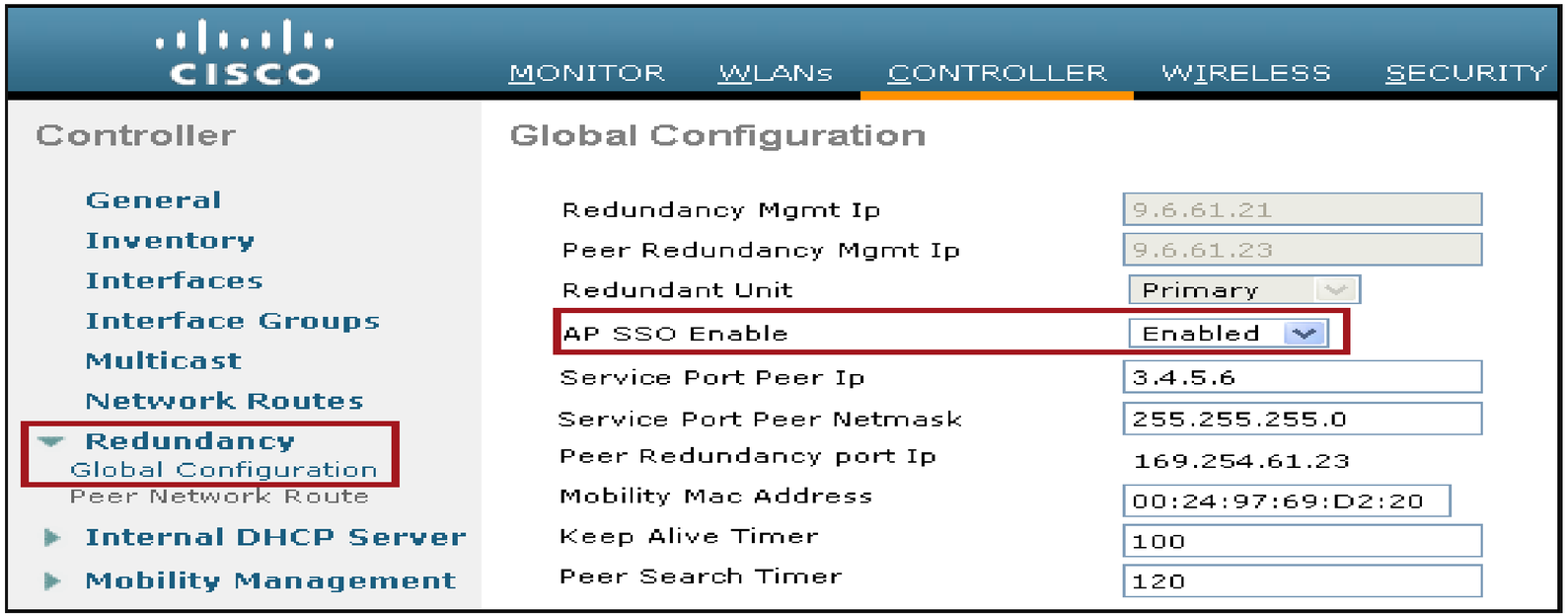


- Configure Redundant Management and Peer Redundant Management IP first before enabling AP SSO



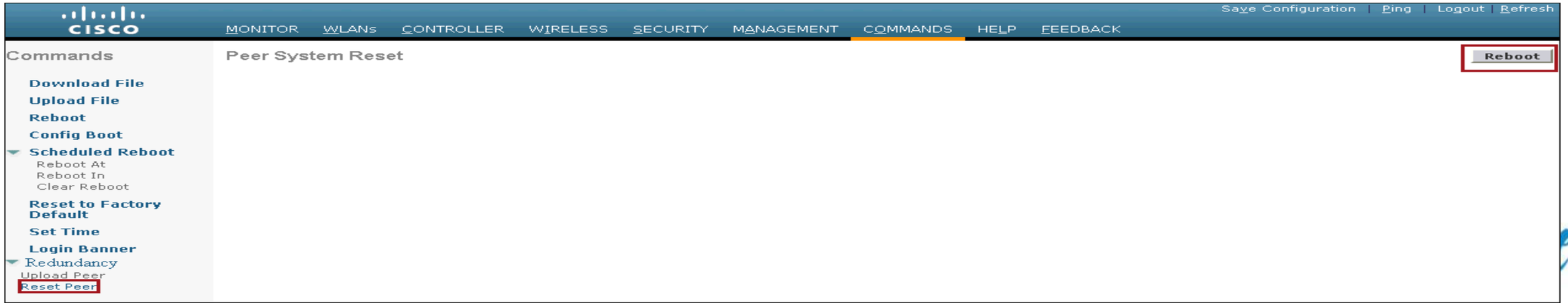
High Availability Configuration

- Configure AP SSO selecting “Enable” from drop down



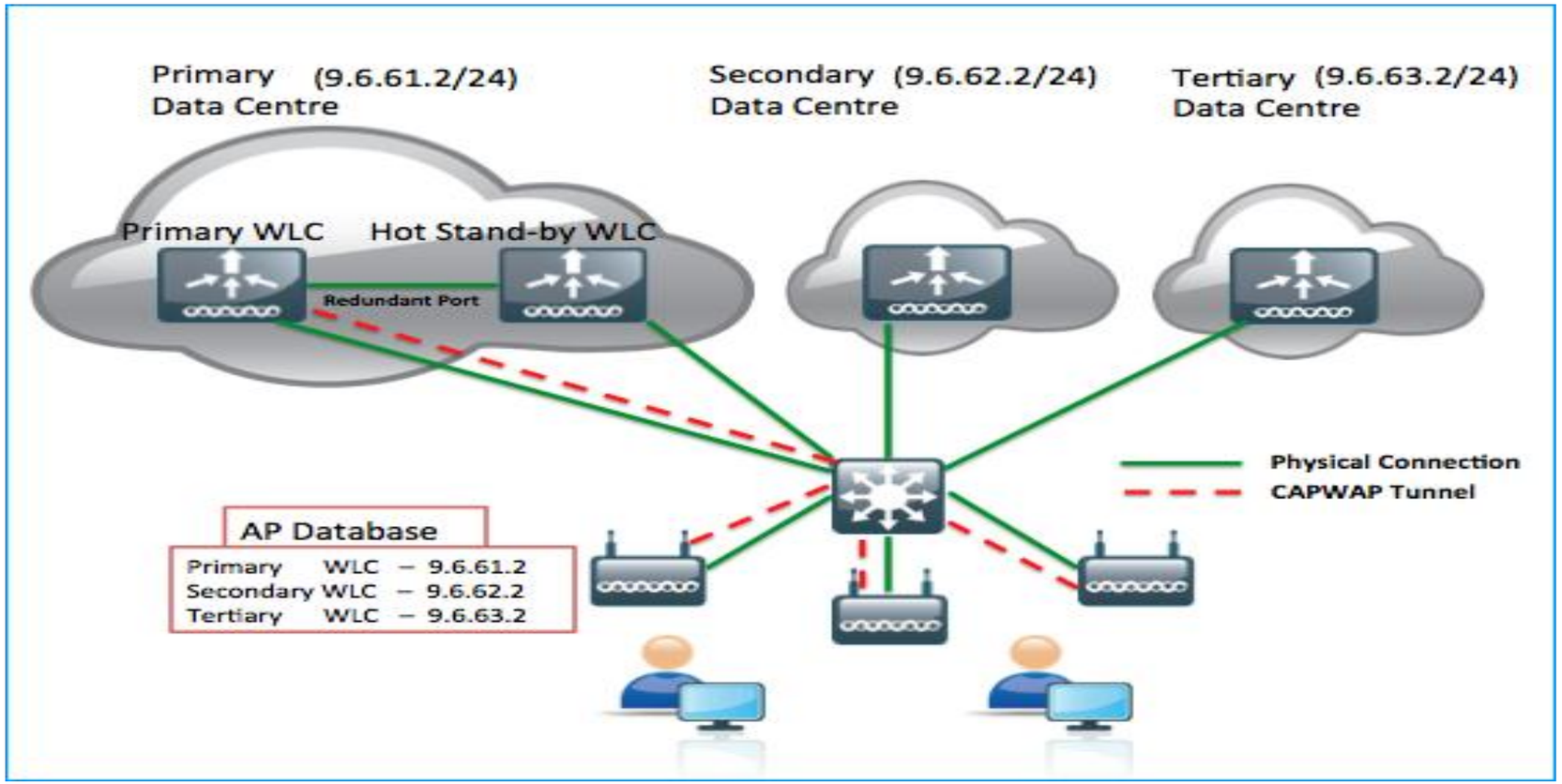
All other optional configuration like Service Port Peer IP, Mobility MAC Address, Keep Alive and Peer Search Timer can be configured on same page

- To Reset Peer WLC click on Commands -> Redundancy -> Reset Peer



AP SSO with Legacy High Availability

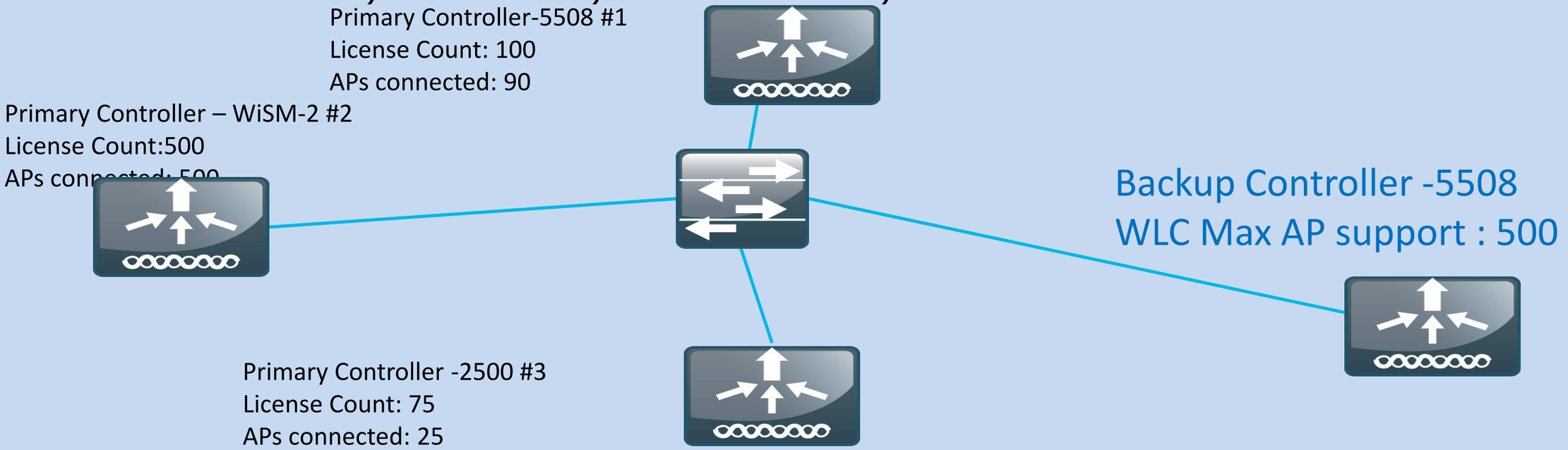
- AP SSO can be deployed with Secondary and Tertiary Controllers
- Both Active and Standby combined in AP SSO setup should be configured as primary.
- On failure of both Active and Standby WLC in AP SSO setup, APs will fall back to secondary and further to configured tertiary controller.



HA-SKU as secondary WLC (with AP-SSO disabled)

- This feature enables HA-SKU controller as secondary controller
  - HA-SKU controller allowed for use as secondary controller for 90 days without nagging
  - If HA feature disabled the controller used as secondary controller for the maximum capacity of supported APs.

Note: HA-SKU ; 5508 50AP, WiSM2 100AP, 7500/8500 300AP will work as Standby



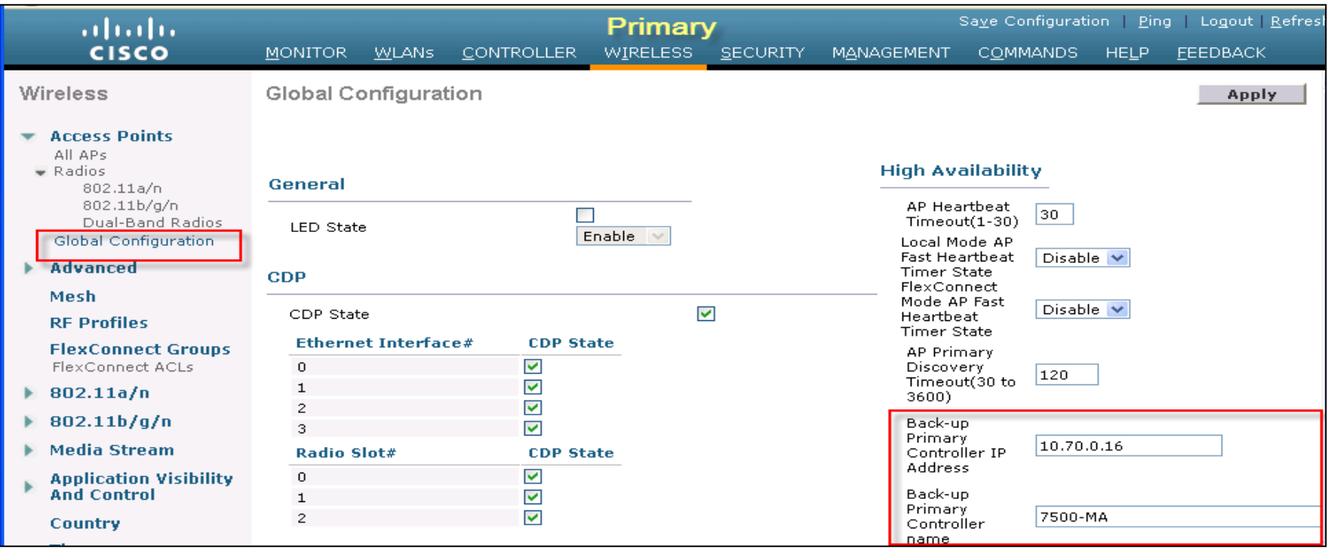
HA-SKU as secondary WLC - configuration

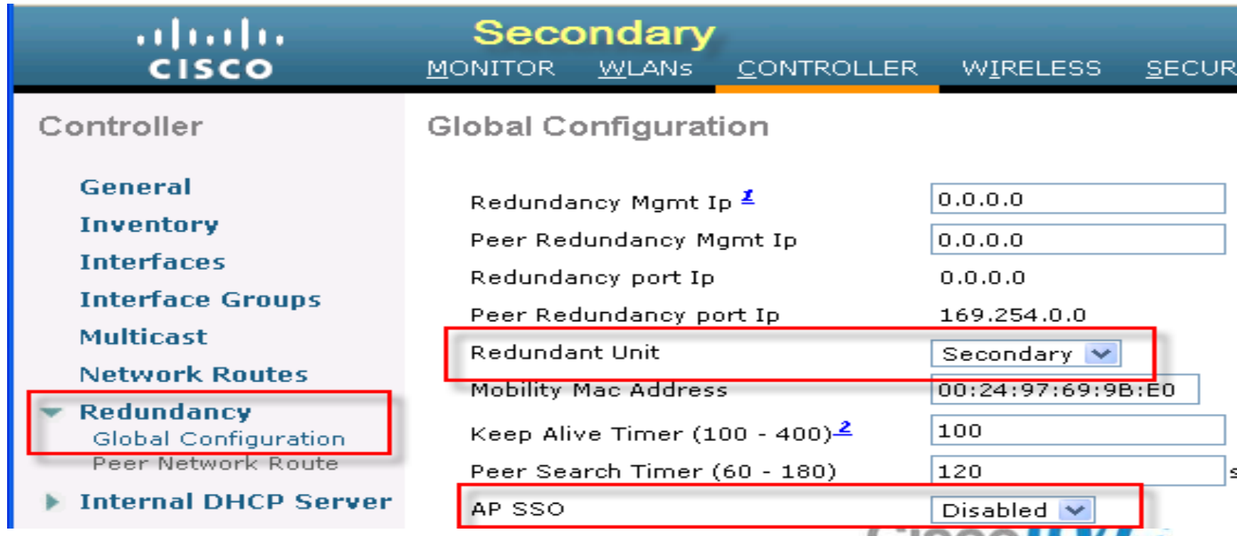
- *CLI Secondary: config redundancy unit secondary*
- *CLI Primary: config ap primary-base <Switch Name> <Cisco AP> <Switch IP Addr>'*

```
(Cisco Controller) >show redundancy summary
 Redundancy Mode = SSO DISABLED
      Local State = ACTIVE
       Peer State = N/A
             Unit = Secondary - HA SKU
          Unit ID = 70:81:05:CE:C8:40
Redundancy State = N/A
     Mobility MAC = 70:81:05:CE:C8:40

Redundancy Management IP Address................... 0.0.0.0
Peer Redundancy Management IP Address............. 0.0.0.0
Redundancy Port IP Address........................ 0.0.0.0
Peer Redundancy Port IP Address................... 169.254.0.0
```

GUI configuration:





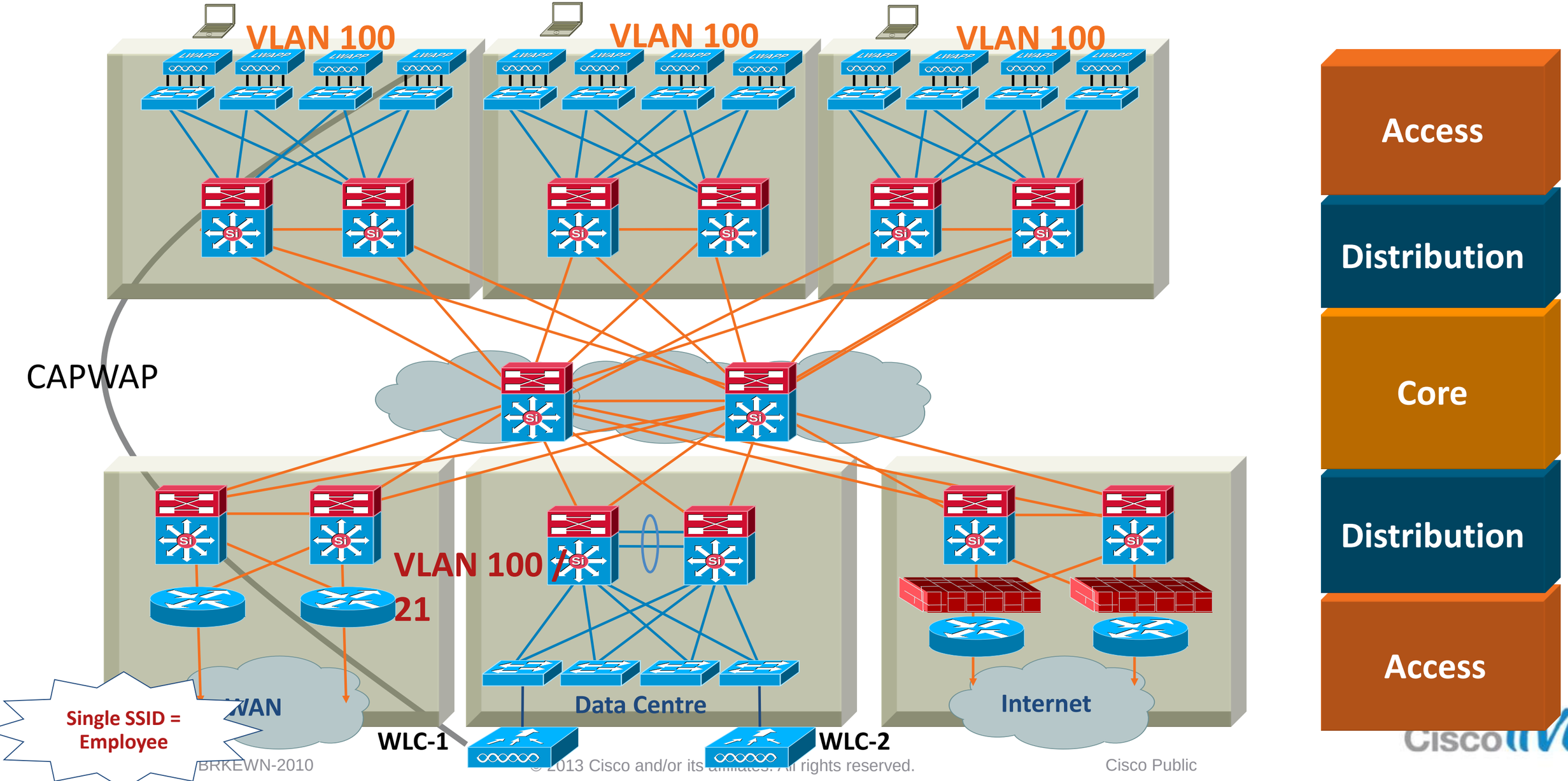
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

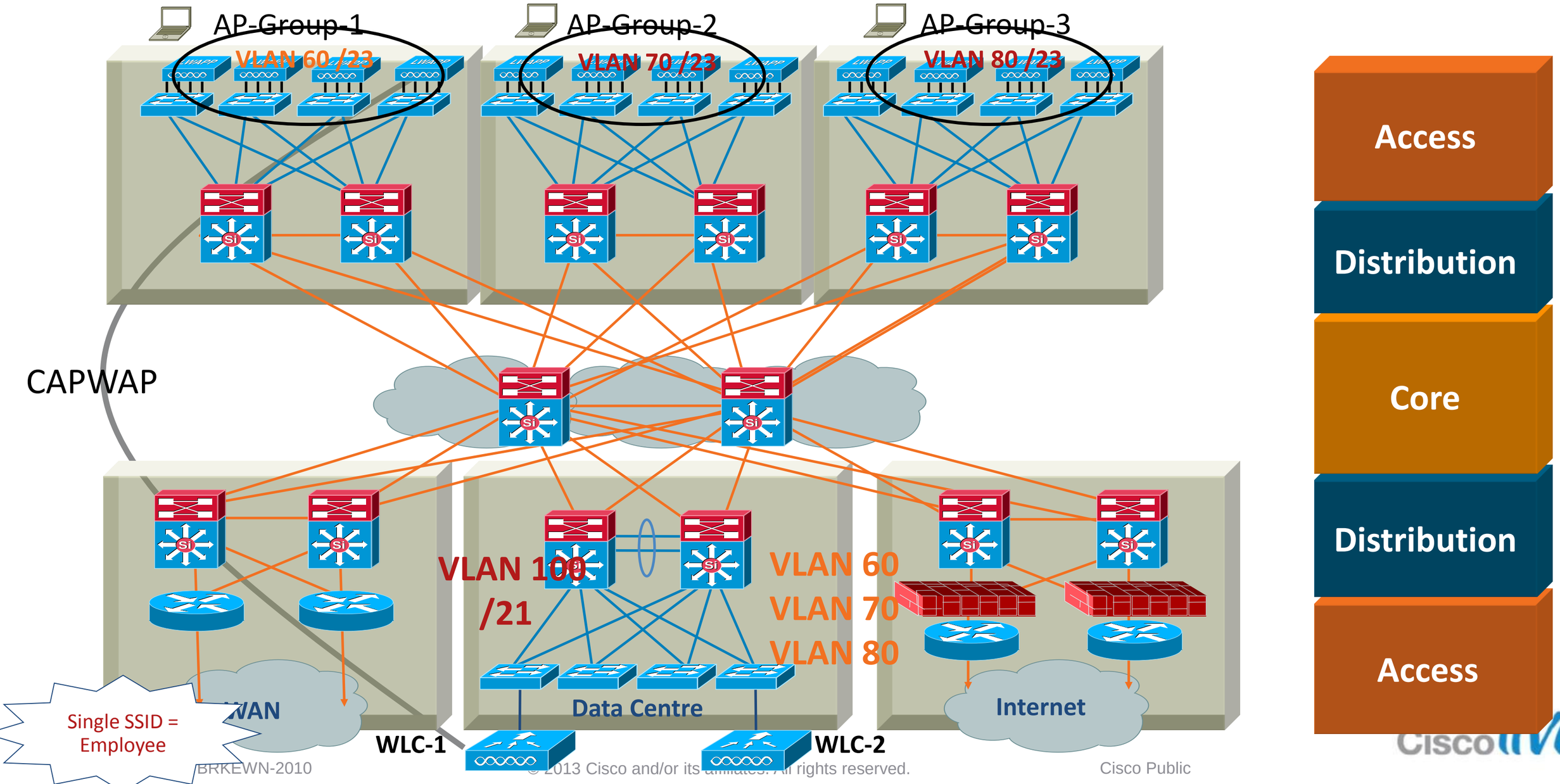
AP-Groups - Default AP-Group

- The first 16 WLANs created (WLAN IDs 1–16) on the WLC are included in the default AP-Group
- Default AP-Group cannot be modified
- APs with no assignment to an specific AP-Group will use the Default AP-Group
- The 17th and higher WLAN (WLAN IDs 17 and up) can be assigned to any AP-Groups
- Any given WLAN can be mapped to different dynamic interfaces in different AP-Groups
- WLC 2106 (AP groups: 50), WLC 2504 (AP groups:50)
  WLC 4400 and WiSM (AP groups: 300),
  WLC 5508 & WiSM-2 (AP groups: 500),
  WLC 7500 (AP Groups : 500)

AP-Grouping in Campus



AP-Grouping in Campus



Default AP-Group

Network Name

WLAN ID	Type	Profile Name	WLAN SSID
1	WLAN	Employee	Employee
17	WLAN	test123	test123

Default AP Group

WLANs

WLANs
WLANs
Advanced
AP Groups

Ap Groups > Edit 'default-group'

General | WLANs | APs

AP Group Name default-group
AP Group Description Defaulg-Group

Only WLANs 1–16 Will Be Added in Default AP Group

Ap Groups > Edit 'default-group'

General | WLANs | APs

WLAN ID	WLAN SSID	Interface Name
1	Employee	management

Multiple AP-Groups

AP Group 1

Ap Groups > Edit 'AP-Group-1'

General | WLANs | RF Profile | APs | 802.11u

WLAN ID	WLAN SSID	Interface/Interface
1	Employee	vlan60

AP Group 2

Ap Groups > Edit 'AP-Group-2'

General | WLANs | RF Profile | APs | 802.11u

WLAN ID	WLAN SSID	Interface/Interface
1	Employee	vlan70

AP Group 3

Ap Groups > Edit 'AP-Group-3'

General | WLANs | RF Profile | APs | 802.11u

WLAN ID	WLAN SSID	Interface/Interface
1	Employee	vlan80

RF-Profiles

7.2 and 7.3

- RF Profiles allow the administrator to tune groups of AP's sharing a common coverage zone together.
  - Selectively changing how RRM will operate the AP's within that coverage zone
- RF Profiles are created for either the 2.4 GHz radio or 5GHz radio
  - Profiles are applied to groups of AP's belonging to an AP Group, in which all AP's in the group will have the same Profile Settings
- There are two components to this feature:
  - RF Profile – New in 7.2 providing administrative control over:
    - Min/Max TPC values
    - TPCv1 Threshold
    - TPCv2 Threshold
    - Data Rates
    - High Density
    - Client Load Balancing

RF Profiles

- Create an RF profile for a or b/g radio
- Select if required the minimum and/or Maximum TPC settings
- Select a custom TPC power threshold for either Version 1 or Version 2 of TPC
- Select the data rates to be applied to the AP's

RF Profile > Edit 'Profile-1'

General | 802.11 | RRM | High Density | Client Distribution

Profile Name Profile-1
Radio policy 802.11a
Description High Density

RF Profile > Edit 'Profile-1'

General | 802.11 | RRM

Data Rates[1]

6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

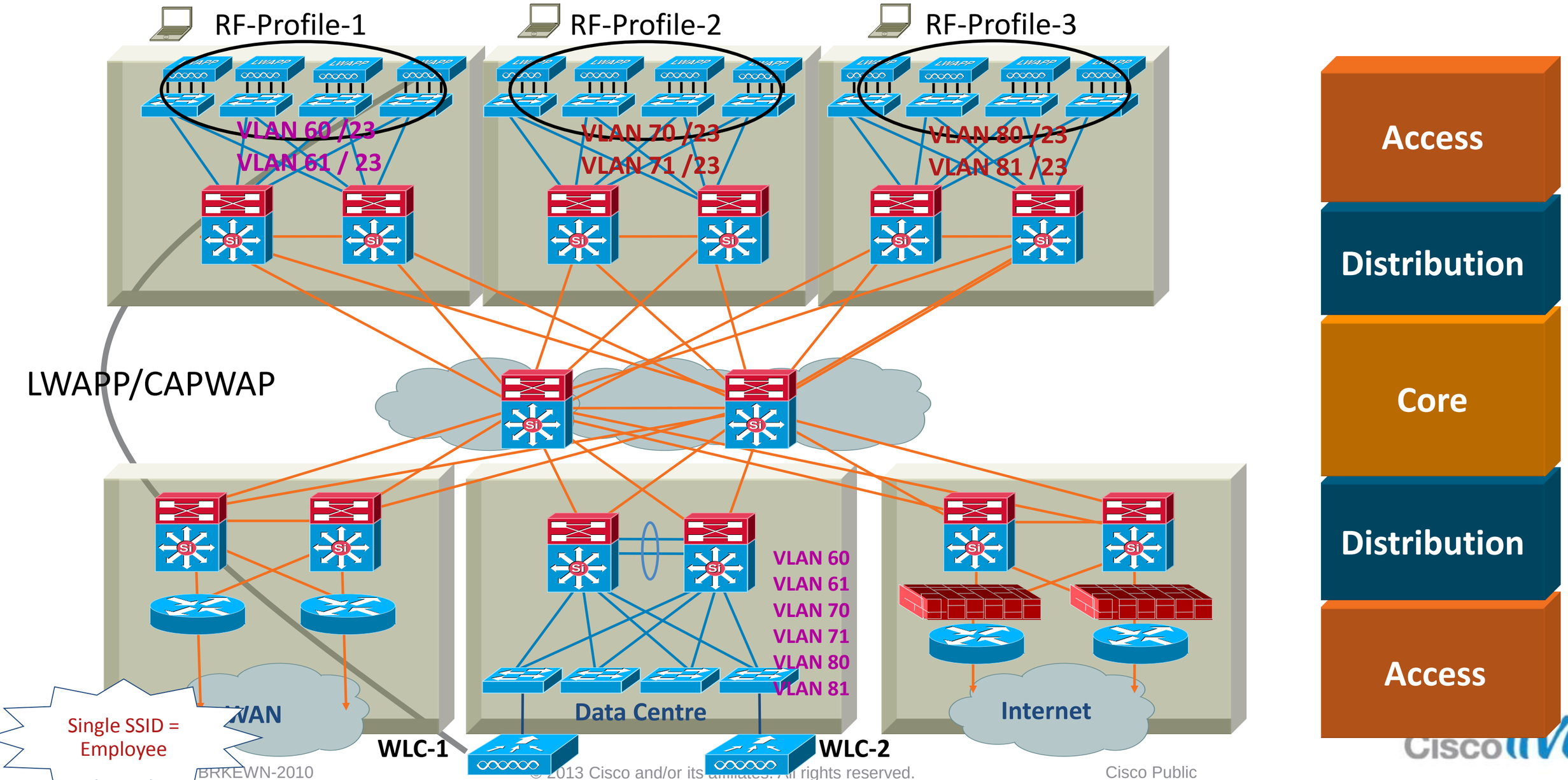
RF Profile > Edit 'Profile-1'

General | 802.11 | RRM | High Density | Client D

TPC

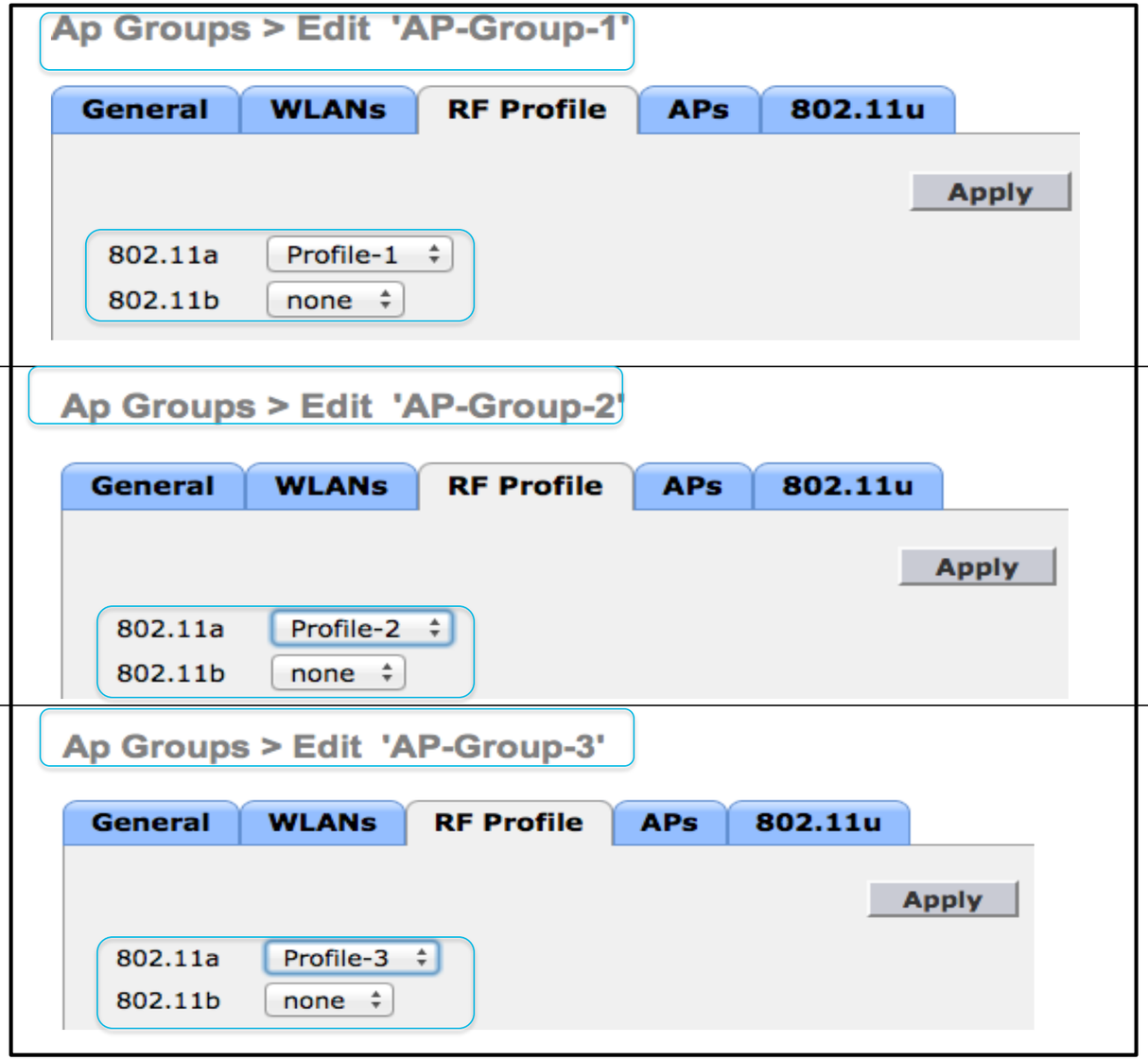
Maximum Power Level Assignment (-10 to 30 dBm)	30
Minimum Power Level Assignment (-10 to 30 dBm)	-10
Power Threshold v1(-80 to -50 dBm)	-70
Power Threshold v2(-80 to -50 dBm)	-67

RF-Profile in Campus



Multiple RF-Profiles

RF Profile -1



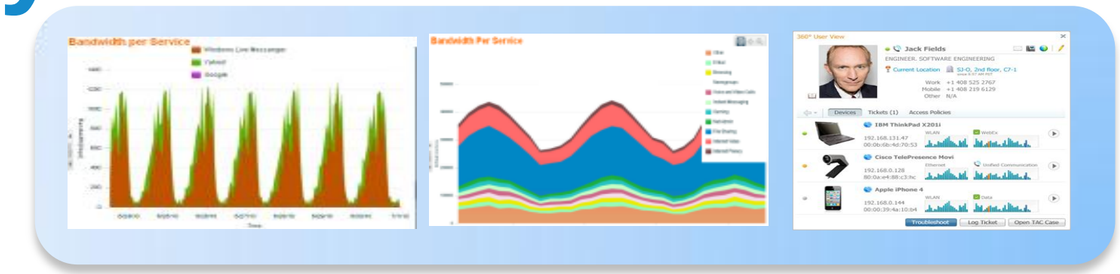
RF Profile -2

RF Profile -3

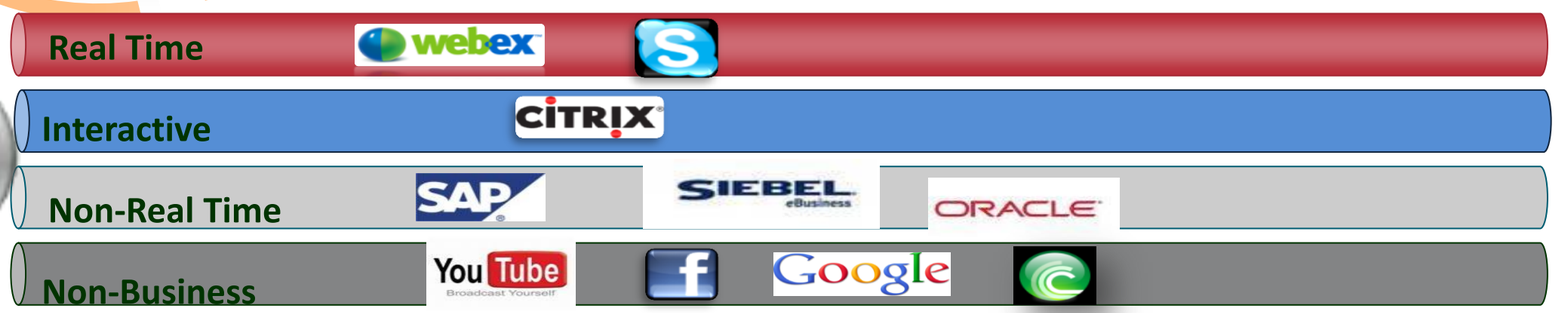
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

Application Visibility & Control



Congestion!



What applications are in the air?
Why is my key application running slow?
How do I support a new application for a set of users?

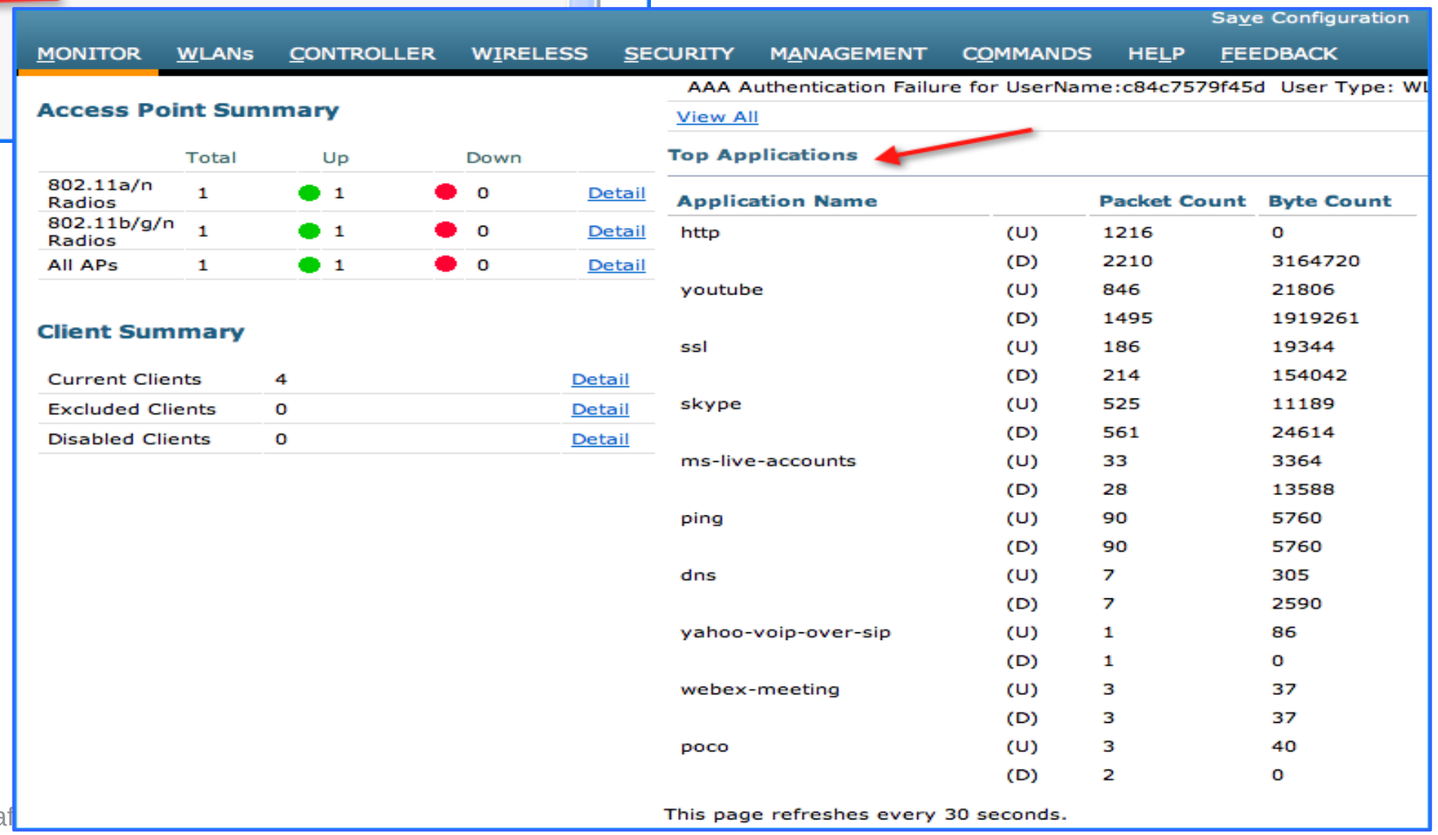
NBAR supported features

- Classification : Identification of Application/Protocol, supports Stateful L4 - L7 classification. WLC can classify 1039 applications.

- AVC (Application Visibility Control): Provides visibility of classified traffic and also gives an option to control the same, using – Drop OR Mark (DSCP) action.
  - Action DROP (Traffic for that application will be dropped)
  - Action MARK (Particular applications can be marked with different QOS profiles available on WLC OR administrator can custom define DSCP value for that application)
  - AVC Marking overrides all other QoS markings

- NetFlow: Updating NBAR stats to Netflow collector like Cisco Prime Assurance Manager (PAM)
- NBAR is supported on 2500, 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs
- WLC can support 16 AVC profiles
- WLAN can support only 1 AVC profile and each profile can contain 32 rules, thus each WLAN can support 32 application actions of mark or drop.

Enabling AVC



- Global summary of top applications on Controller Monitor screen

AVC Application

Save Configuration | Ping | Logout | Refresh

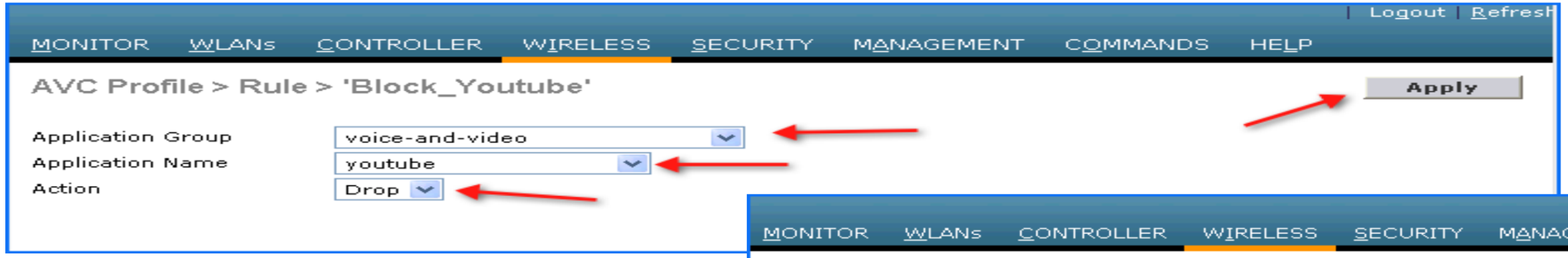
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

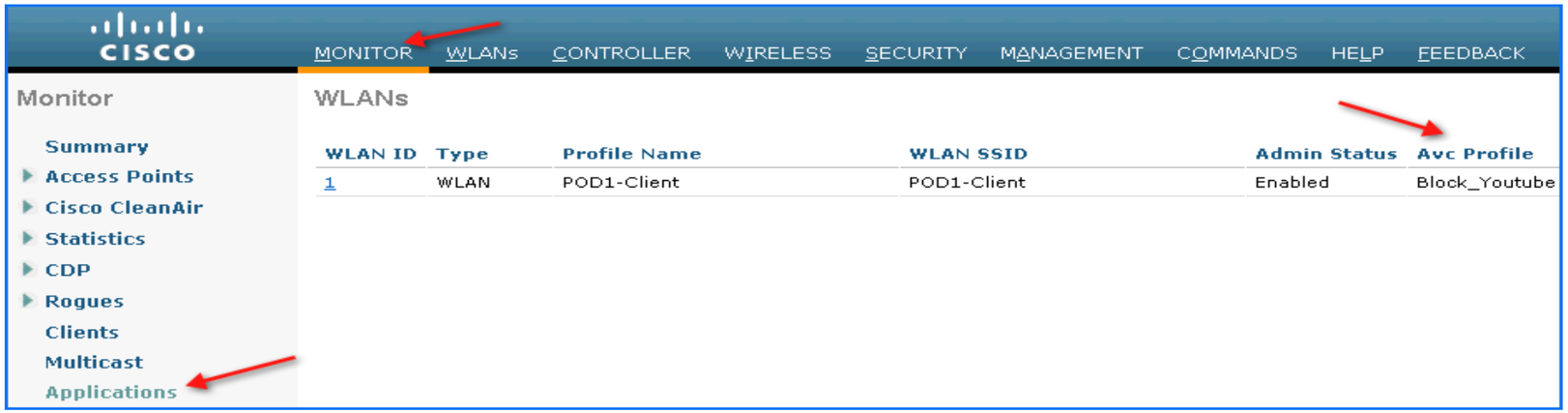
- Access Points
  - All APs
  - Radios
    - 802.11a/n
    - 802.11b/g/n
    - Dual-Band Radios
  - Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Groups
  - FlexConnect ACLs
- 802.11a/n
- 802.11b/g/n
- Media Stream
- Application Visibility And Control
  - AVC Applications
  - AVC Profiles
- Country
- Timers
- Netflow
- QoS

mpp	email	1115	3	218
mptn	industrial-protocols	312	3	397
mrm	net-admin	587	3	679
ms-dynamics-crm-online	business-and-productivity-tools	1443	13	508
ms-iis	other	1411	13	482
ms-live-accounts	other	1434	13	498
ms-lync	business-and-productivity-tools	1466	13	531
ms-lync-media	voice-and-video	1467	13	532
ms-netlogon	other	1412	13	483
ms-ocs-file-transfer	other	1356	3	6891
ms-office-365	other	1431	13	495
ms-olap	business-and-productivity-tools	686	3	2393
ms-rome	other	484	3	569
ms-rpc	other	1310	13	1310
ms-shuttle	other	483	3	568
ms-sms	other	1413	13	484
ms-sql-m	business-and-productivity-tools	685	3	1434
ms-streaming	other	1355	3	1755
ms-update	other	1432	13	497
ms-wbt	net-admin	689	3	3389
ms-win-dns	net-admin	1410	13	481
msdp	net-admin	548	3	639
msexch-routing	email	599	3	691
msft-gc	business-and-productivity-tools	687	3	3268
msft-gc-ssl	business-and-productivity-tools	688	3	3269
msg-auth	other	916	3	31

AVC Profile

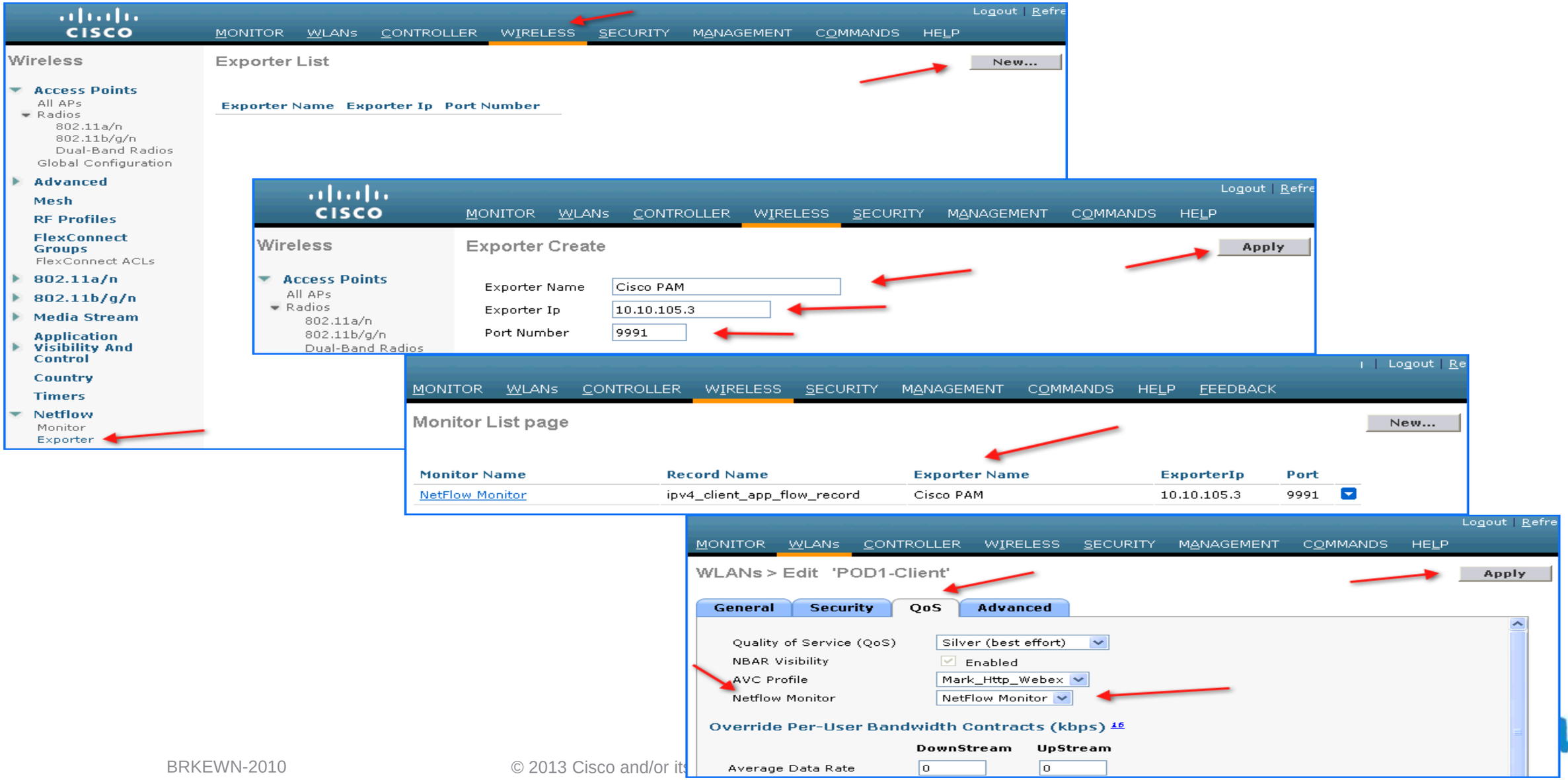


- Apply the custom profile per WLAN



Netflow Monitor

- Configuring Netflow Exporter on the Controller and apply to WLAN



AVC Summary

- Application Statistics per WLAN with more details UP/Down Streams

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

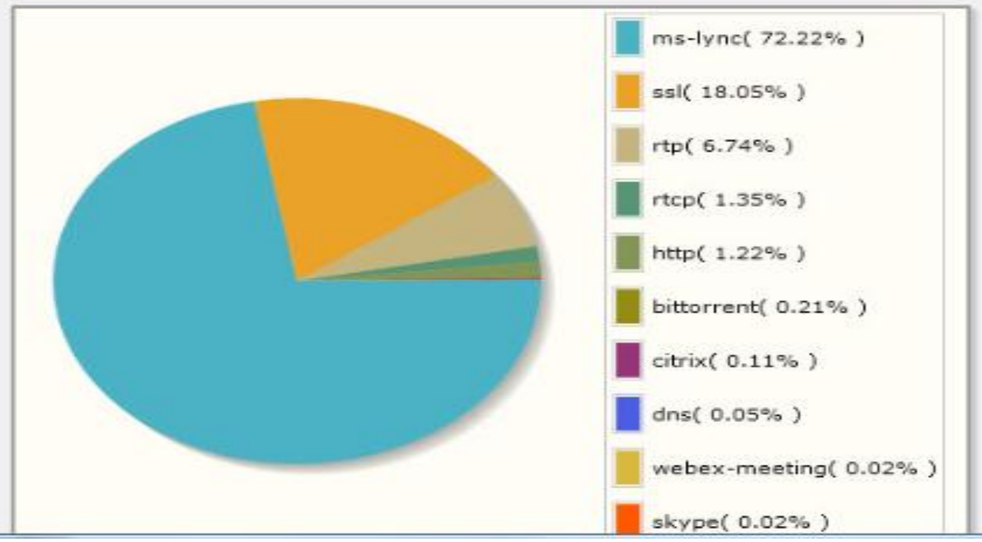
WLANs > Application Statistics

Aggregate | Upstream | Downstream

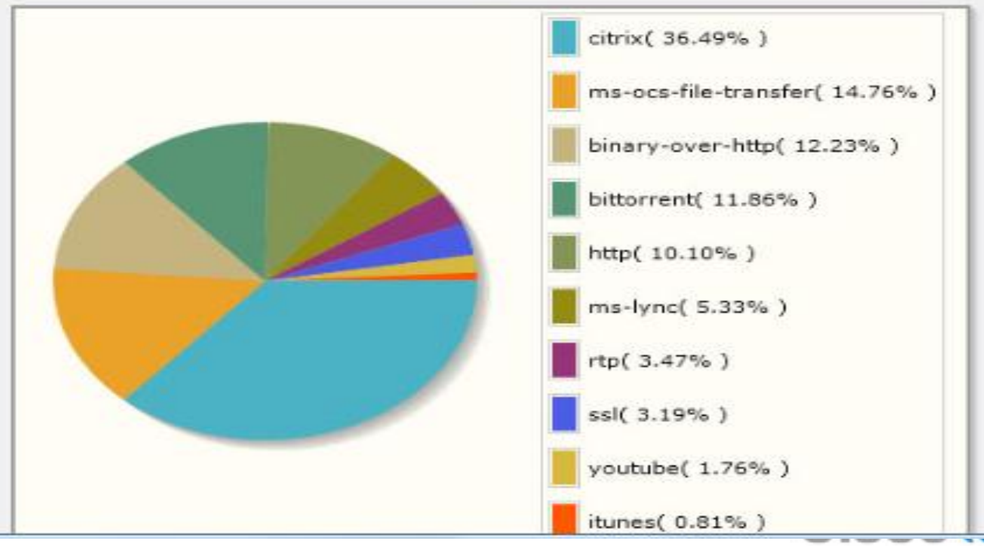
App Name	Packet Count	Byte Count	Average Packet Size	Usage(%)
ms-lync	35970	19368158	538	72.22
ssl	5482	4840784	883	18.05
rtp	6830	1806702	264	6.74
rtcp	578	362678	627	1.35
http	296	328084	1108	1.22
bittorrent	457	57236	125	0.21
citrix	345	30003	86	0.11
dns	61	12831	210	0.05
webex-meeting	15	5925	395	0.02
skype	65	5449	83	0.02

App Name	Packet Count	Byte Count	Usage(%)
citrix	1806809	676350770	36.49
ms-ocs-file-transfer	318410	273665176	14.76
binary-over-http	195928	226772935	12.23
bittorrent	815460	219756102	11.86
http	183250	187127941	10.10
ms-lync	160894	98699034	5.33
rtp	123502	64324358	3.47
ssl	88478	59217362	3.19
youtube	28738	32543822	1.76
itunes	13637	15043237	0.81

Application Last 90 Secs Usage(%)



Application Cumulative Usage(%)



Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

The Protocol Problem

- Why Bonjour services need modifications?

?

?

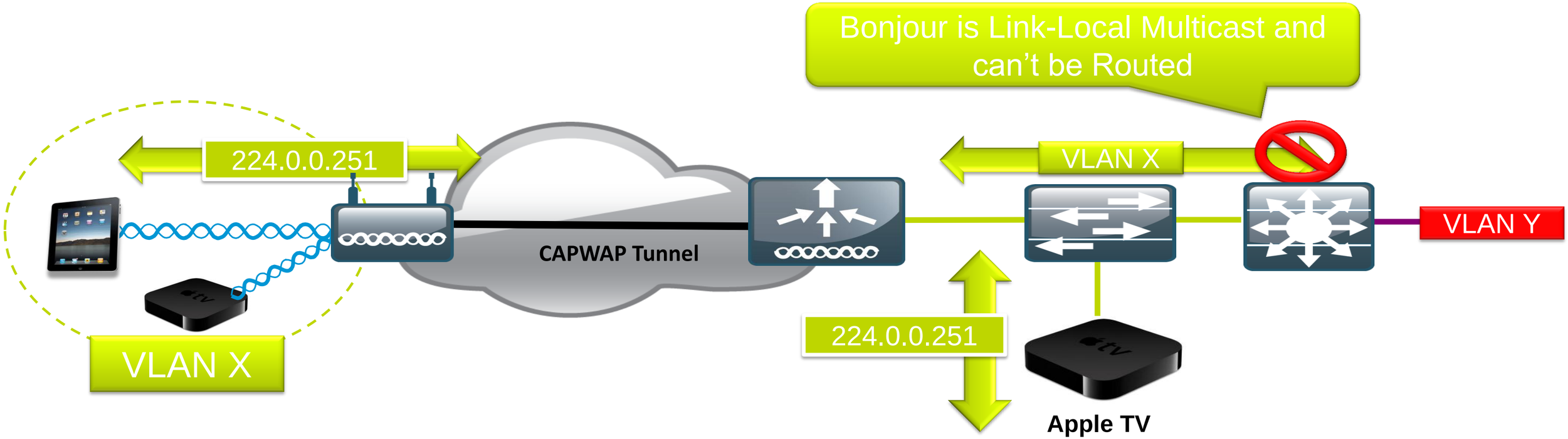
?

Bonjour

- Apple service discovery protocol
- mDNS packets advertise and discover services clients
- Does not cross subnets or VLANs.

Result: Clients can’t see services on other subnets

Deployment Challenges



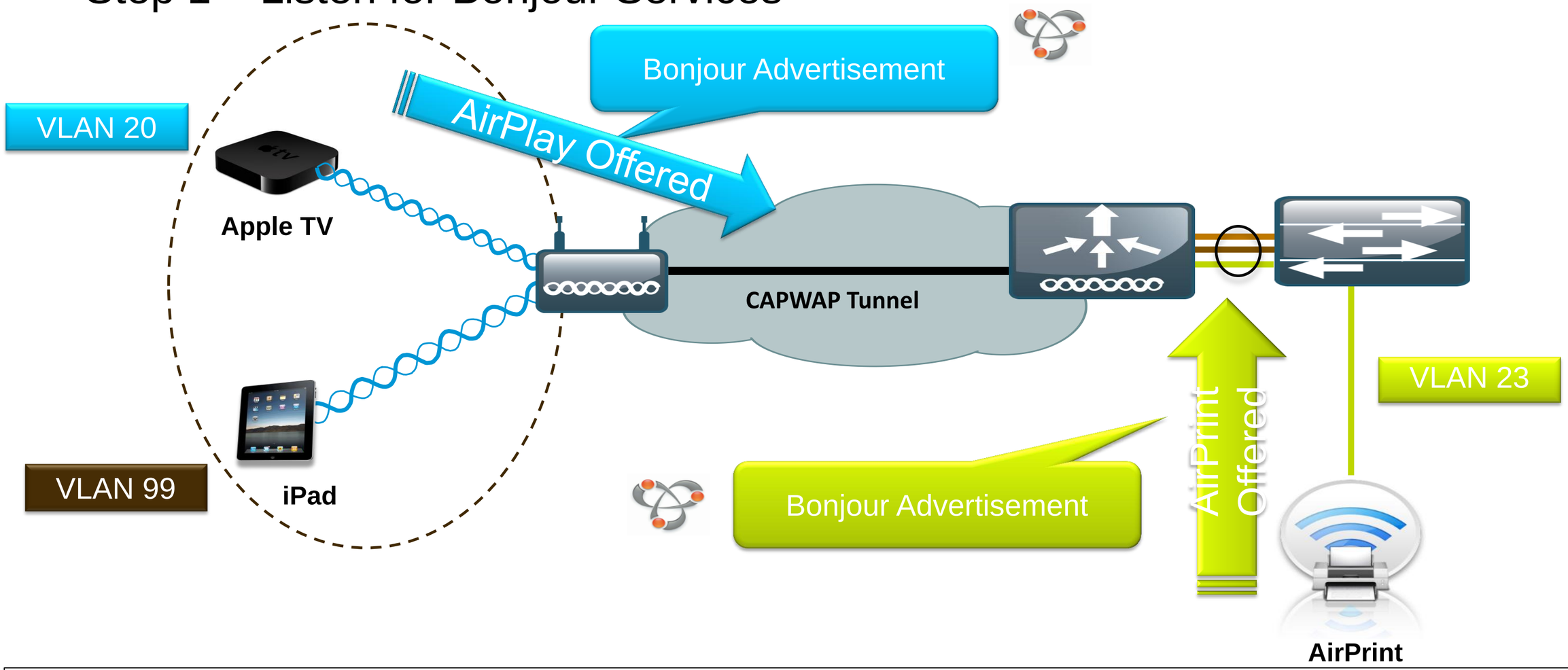
- Bonjour is link local multicast and thus forwarded on Local L2 domain
- AirPlay (Apple TV) and AirPrint supported only on a single VLAN
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:

  IPv4 Group Address – 224.0.0.251

  IPv6 Group Address – FF02::FB

Bonjour mDNS GW on WLC

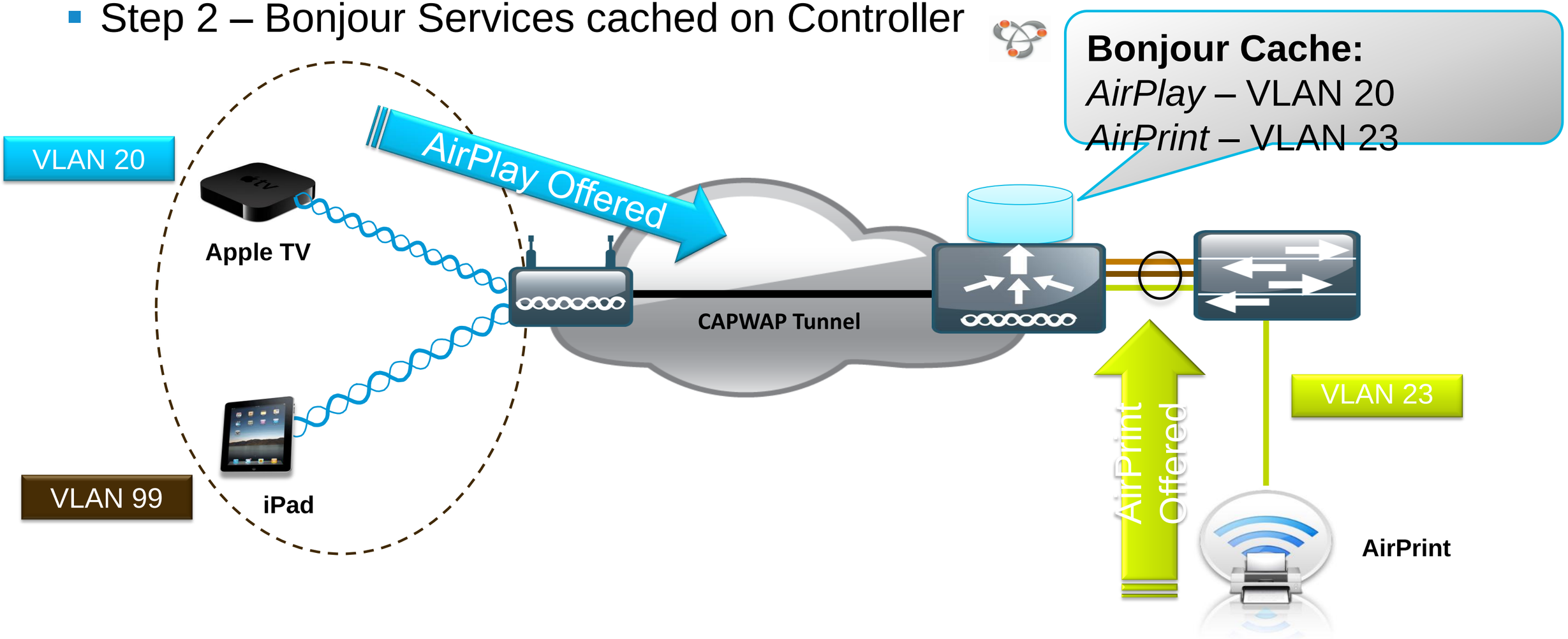
- Step 1 – Listen for Bonjour Services



- In 7.4 Bonjour Services with mDNS gateway on the controller don't require multicast services to be enabled.

Bonjour mDNS GW on WLC

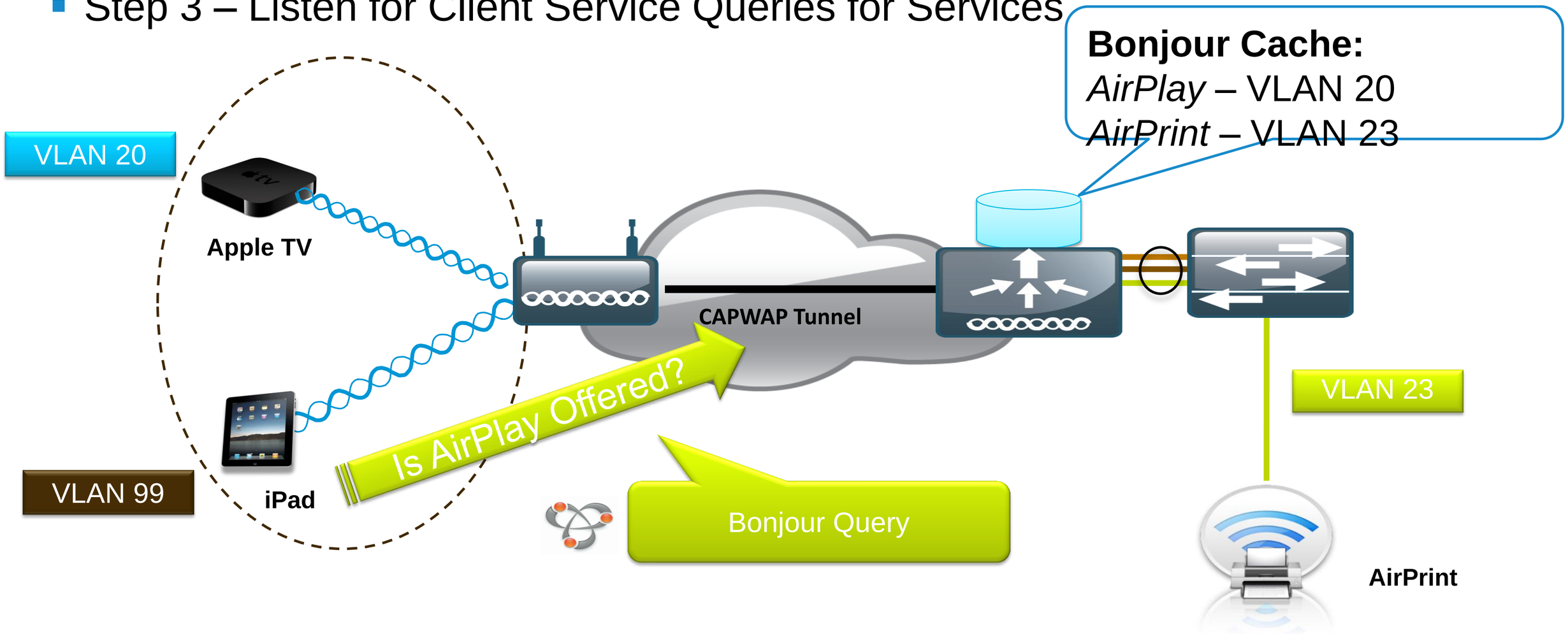
- Step 2 – Bonjour Services cached on Controller



With deployment of mDNS gateway Bonjour Services don't flood subnet with mDNS advertisements

Bonjour GW on WLC

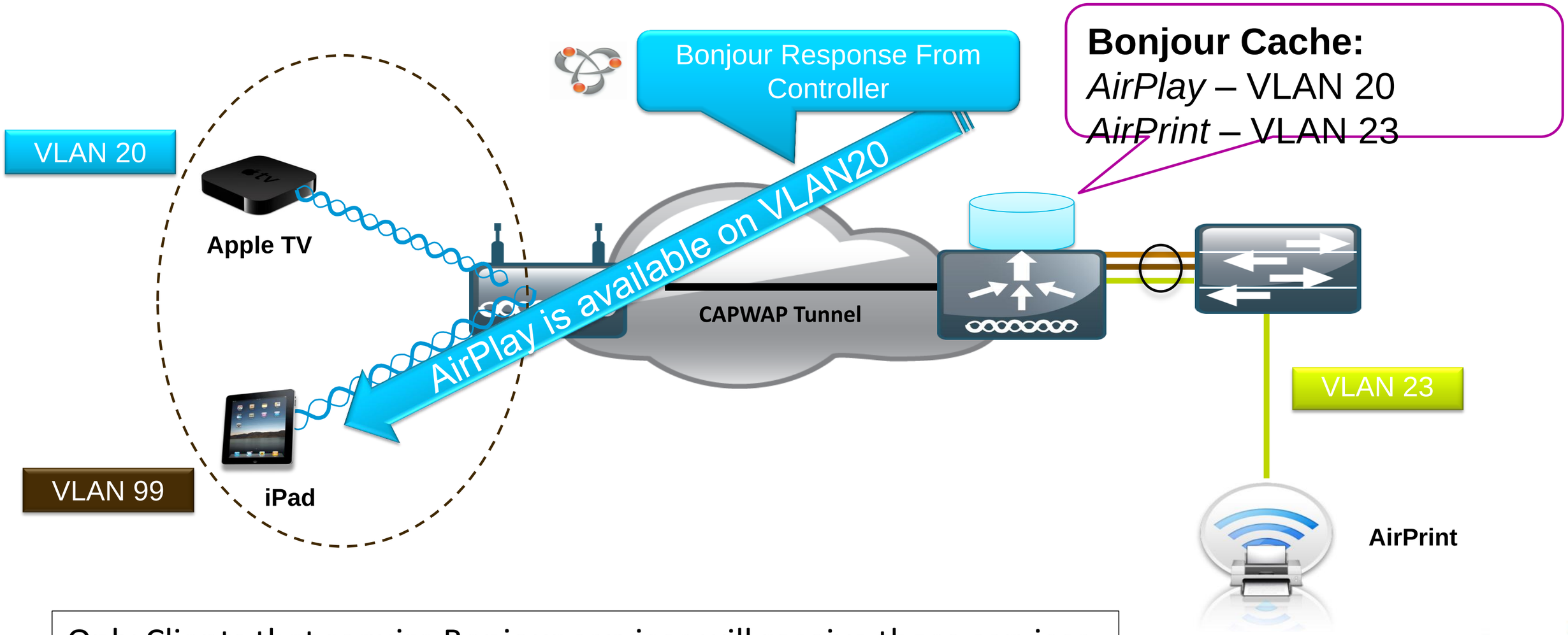
- Step 3 – Listen for Client Service Queries for Services



WLC will snoop all Bonjour discovery packets and will not forward the same on AIR or Infra network

Bonjour GW on WLC

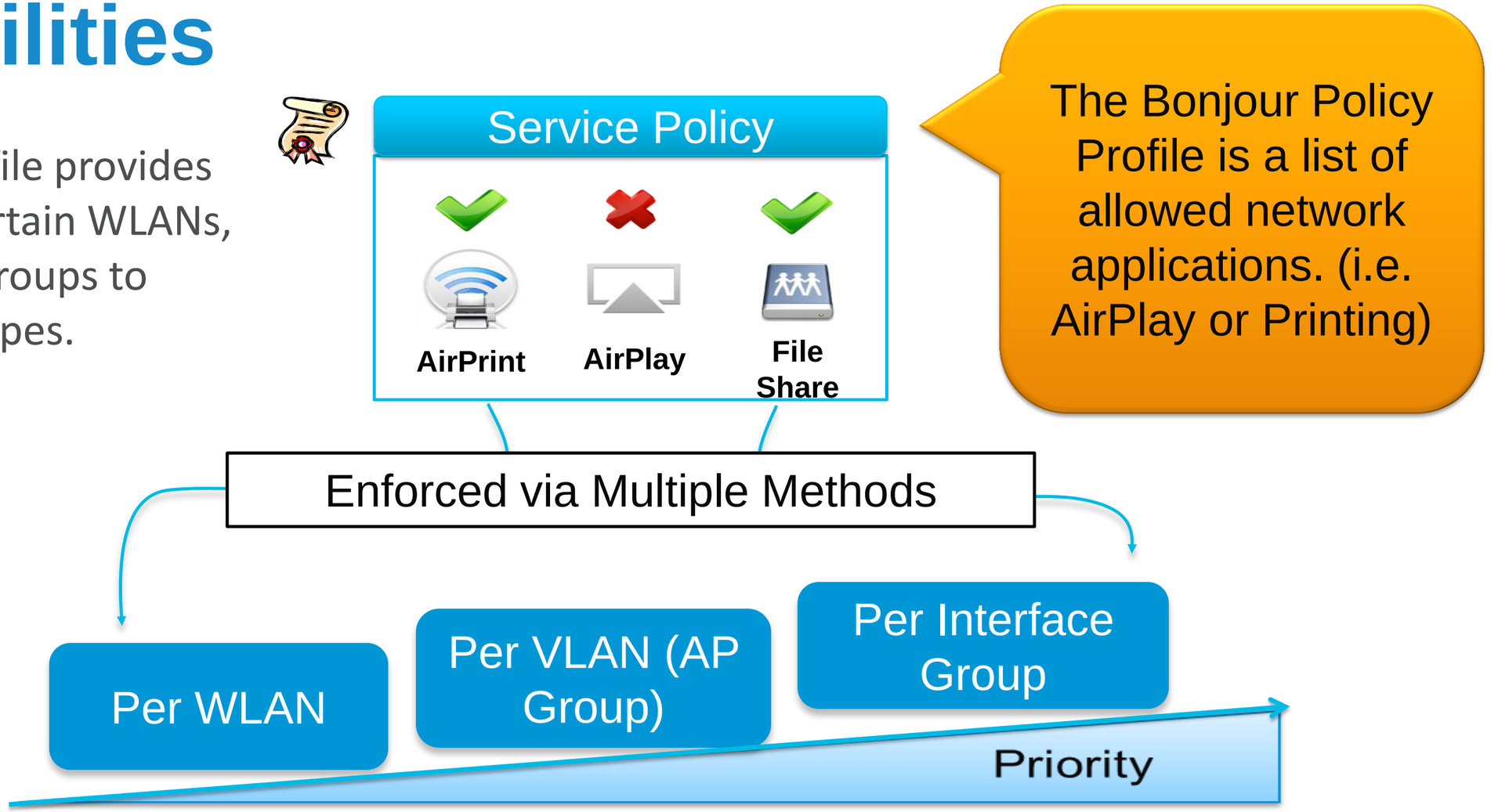
- Step 4 – Respond to Client Queries for Bonjour Services



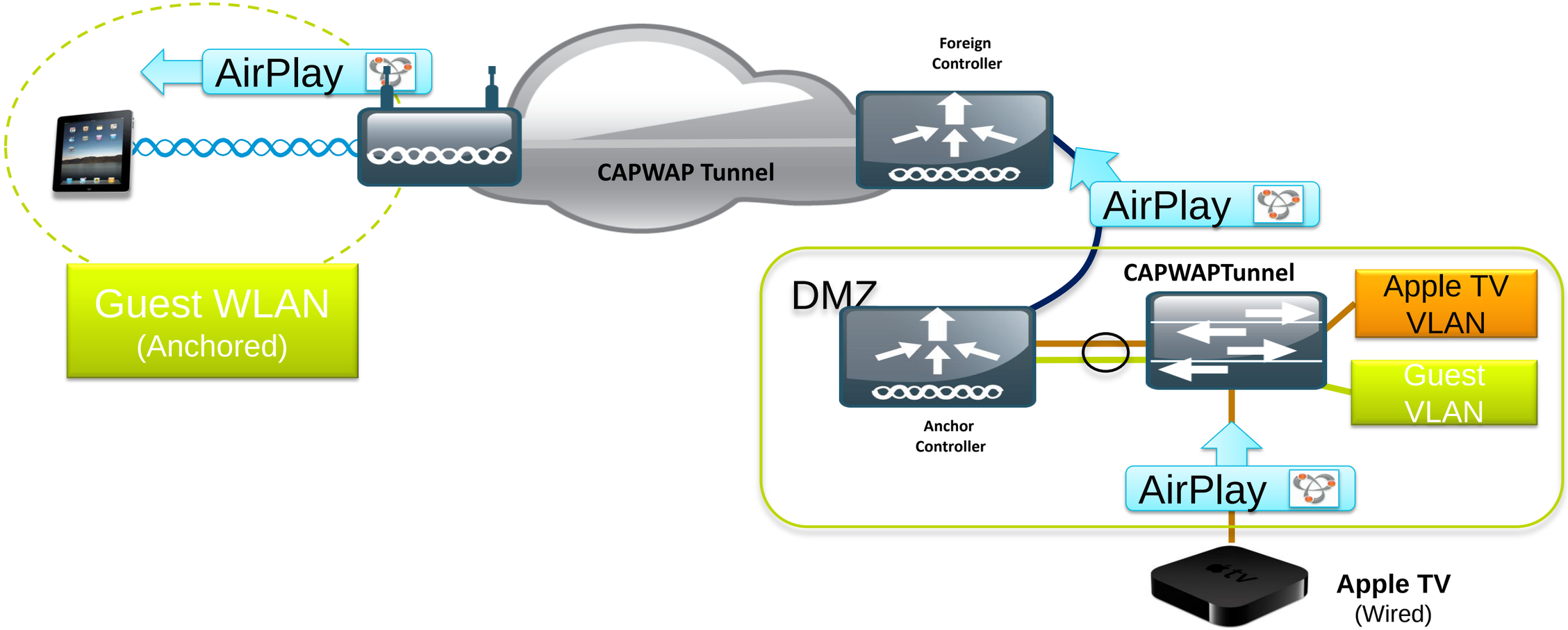
Only Clients that require Bonjour services will receive those services

Bonjour Services Directory Policy Capabilities

The Bonjour service profile provides filtering to allow only certain WLANs, Interfaces or Interface Groups to access specific service types.

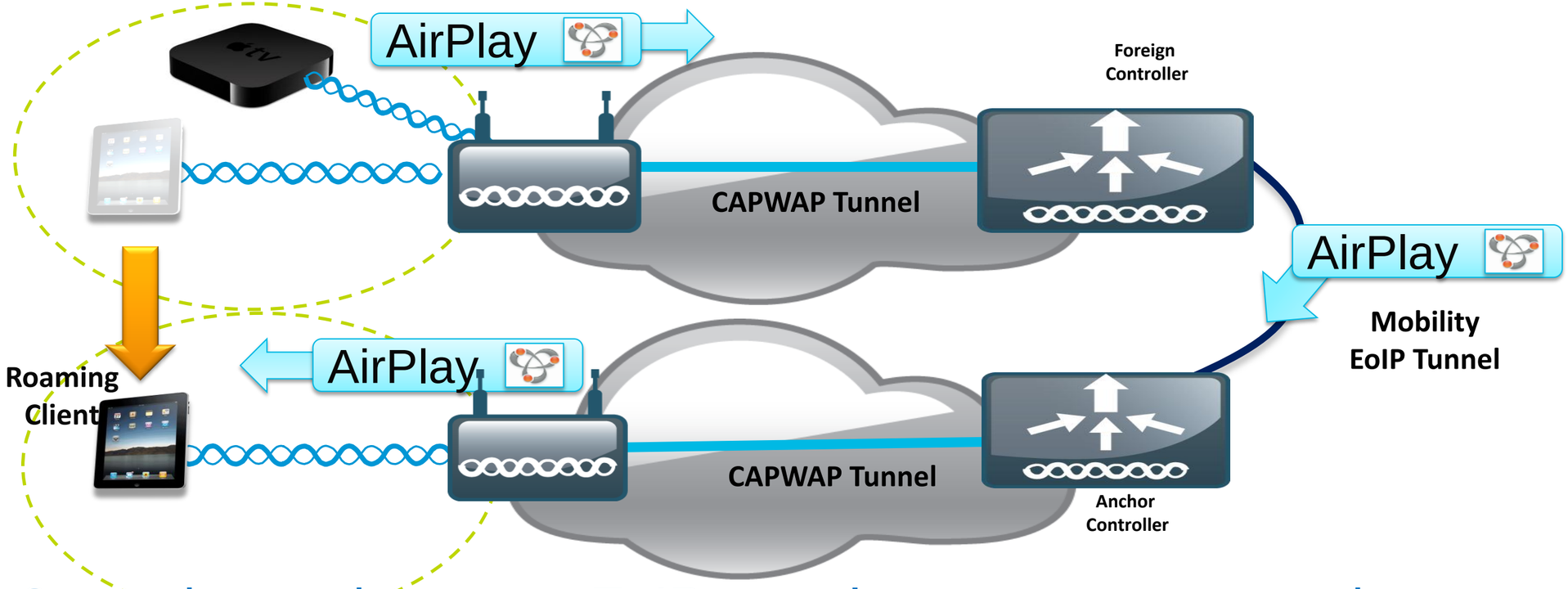


Bonjour and Guest Anchoring



- The guest WLAN will be able to see Bonjour services advertised to the anchor controller.
- The Bonjour queries and advertisements will be sent inside the CAPWAP tunnel.

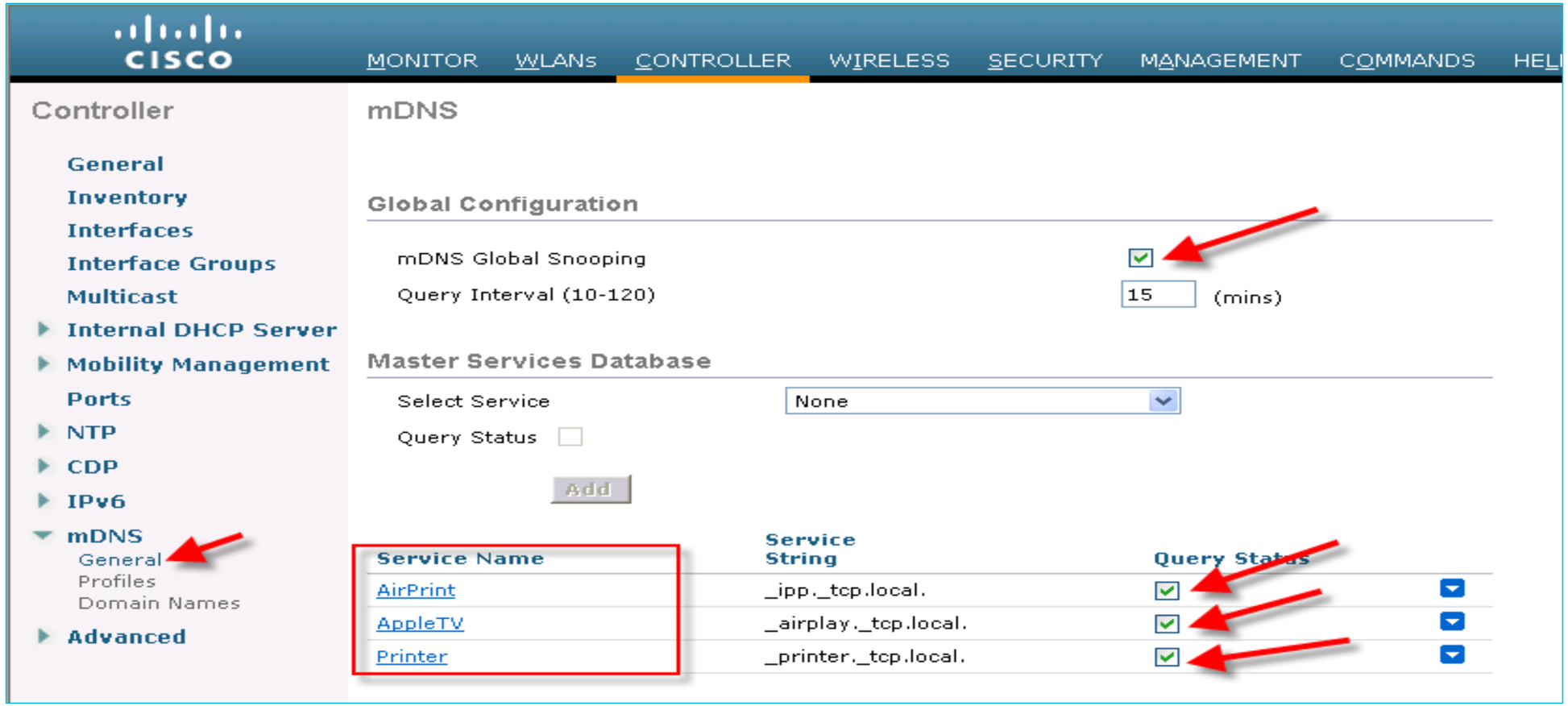
Bonjour L3 Roaming



- Layer 3 roaming works across EoIP tunnel to ensure users moving amongst APs on different controllers continue to see the devices they saw on the original controller.
- The Bonjour services on the anchor controller will be displayed to the client including both wired and wireless devices.

Configuring mDNS Snooping

- Enable mDNS snooping globally and add services



Maximum of 100 services can be configured *

* Subject to change by FCS

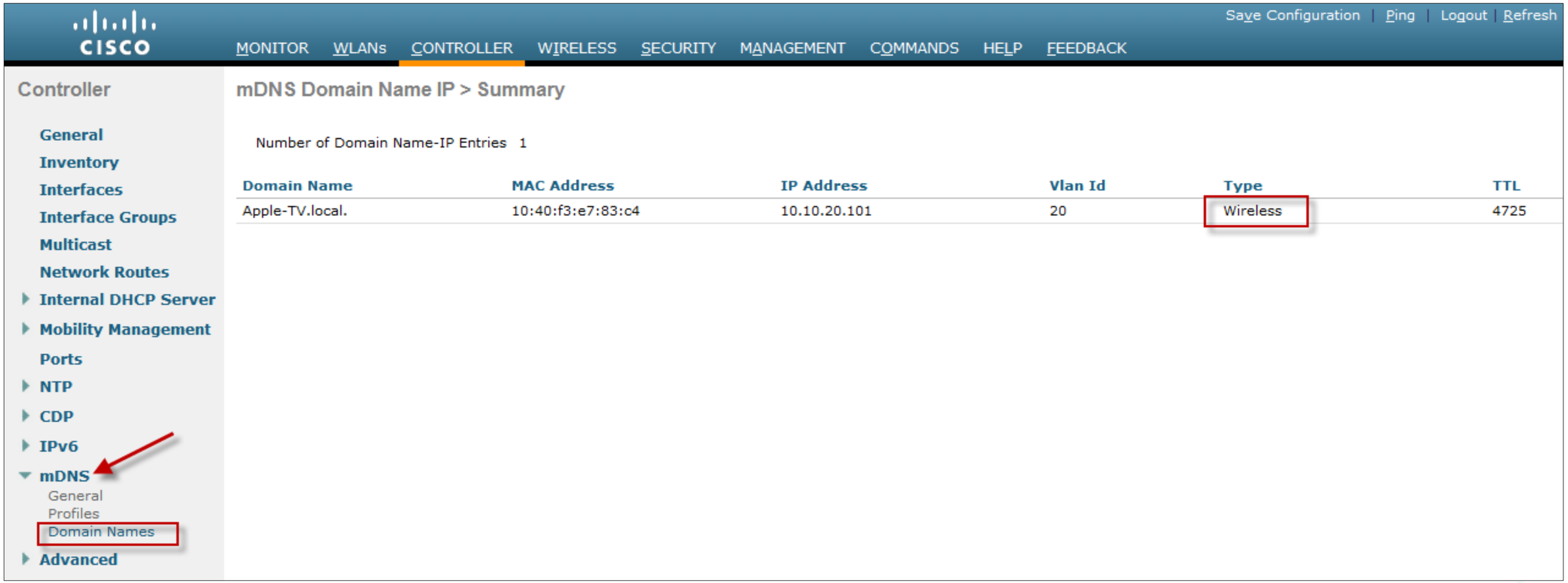
Configure mDNS profile per WLAN

- Create custom profile per WLAN

Enable mDNS snooping profile on the desired VLAN or WLAN

Summary of Bonjour enabled devices

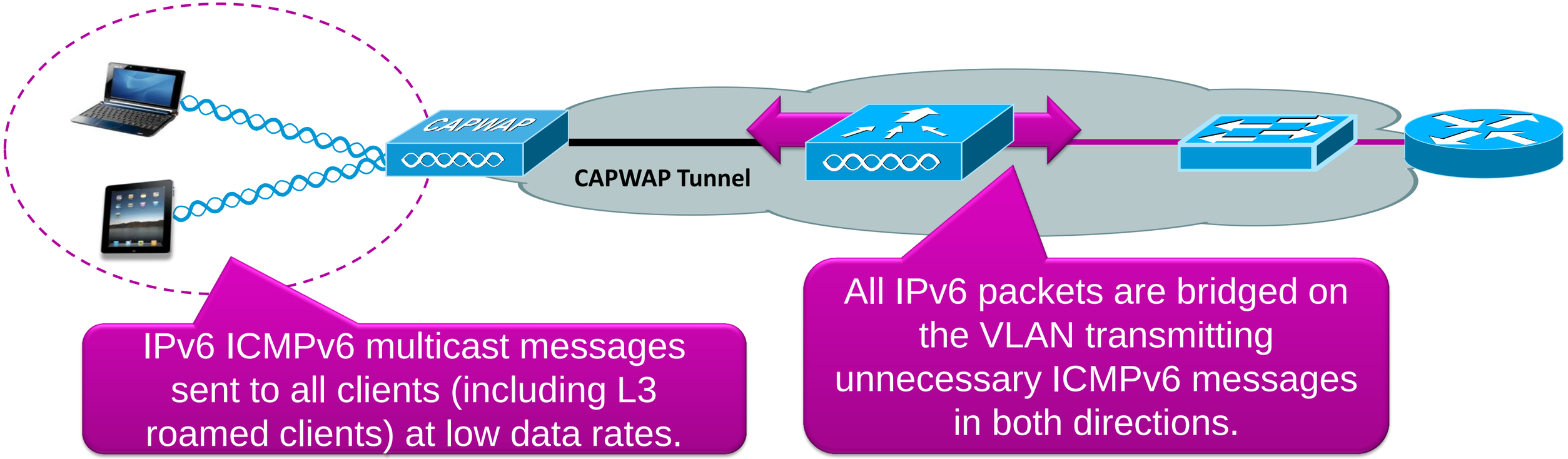
- Bonjour enabled devices advertising service is shown as Domain Name



Deploying the Cisco Unified Wireless Architecture

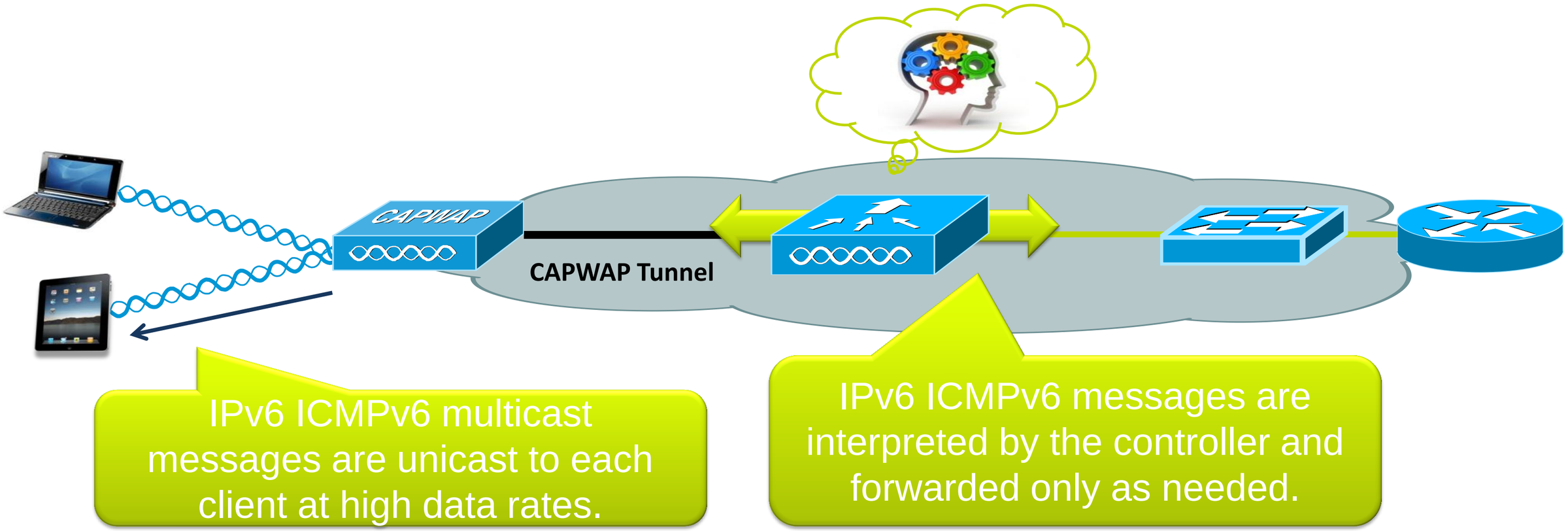
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

Wireless IPv6 Support - Pre-v7.2



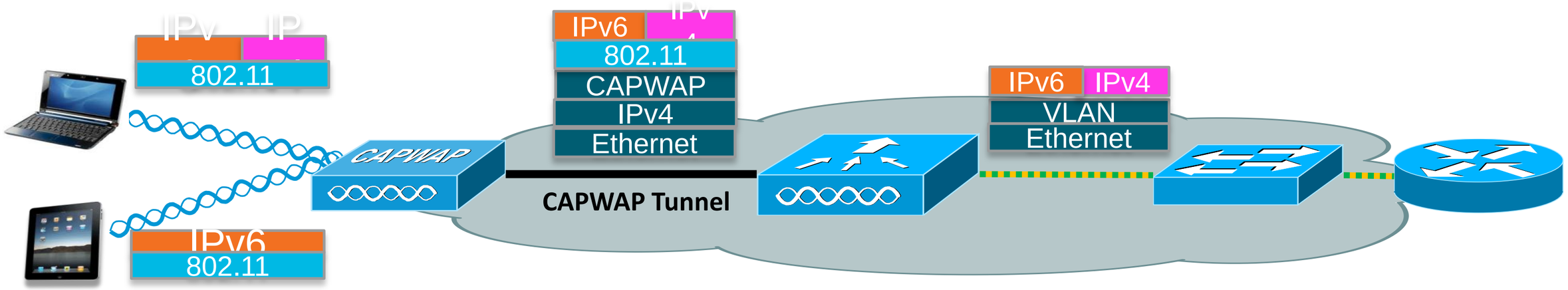
- In releases prior to 7.2, enabling IPv6 bridging provided a limited solution with no Layer 3 mobility and non-optimised delivery of essential ICMPv6 messages to clients.

Wireless IPv6 Support - Post-v7.2



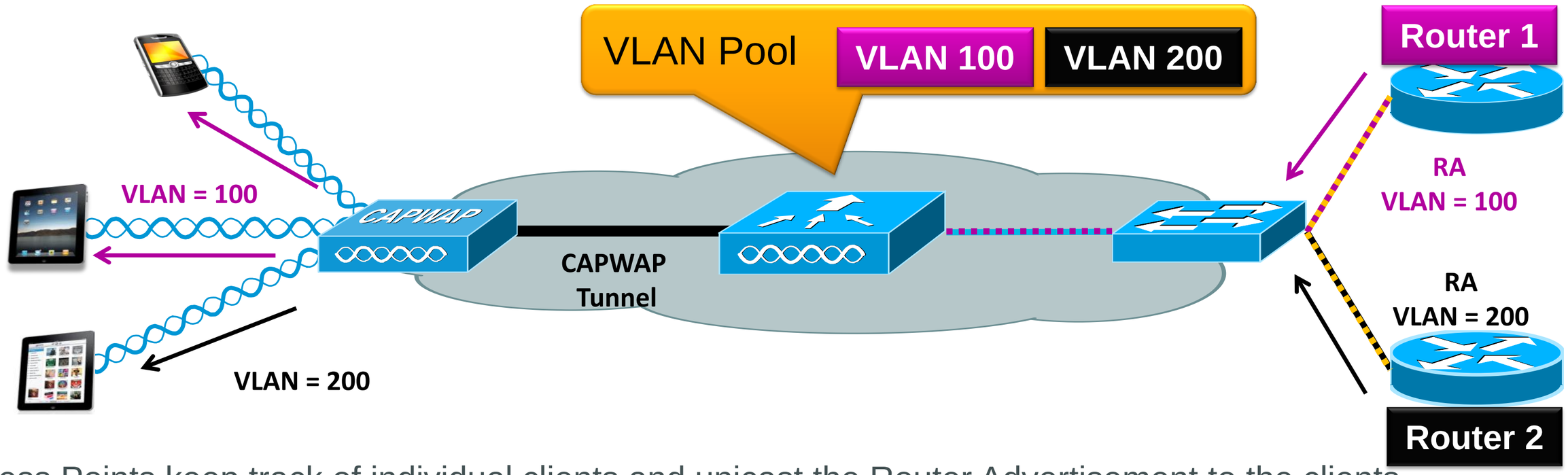
- In releases 7.2, the controller now processes ICMPv6 messages allowing for optimised delivery, Layer 3 mobility and first hop security.

Wireless IPv6 Client Support



- Supports IPv4, Dual Stack and Native IPv6 clients on single WLAN simultaneously
- Supports the following IPv6 address assignment for wireless clients:
  - IPv6 Stateless Autoconfiguration [SLAAC]
  - Stateless, Stateful DHCPv6
  - Static IPv6 configuration
- Supports up to 8 IPv6 addresses per client
- Clients will be able to pass traffic once IPv4 or IPv6 address assignment is completed after successful authentication

IPv6 Client Connectivity on Multiple WLANs



- Access Points keep track of individual clients and unicast the Router Advertisement to the clients depending on the WLAN they belong to.
- Access Point support up to 16 WLANs/SSIDs for dual stack clients.
- To maintain proper routing capability, mobile clients need to have proper global unique unicast prefix from router within their own network.

Cisco Supports Many IPv6 Addresses Per Client

- Support for many IPv6 addresses per client is necessary because:
  - Clients can have multiple address types per interface
  - Clients can be assigned addresses via multiple methods such as SLAAC and DHCPv6
  - Most clients automatically generate a temporary address in addition to assigned addresses

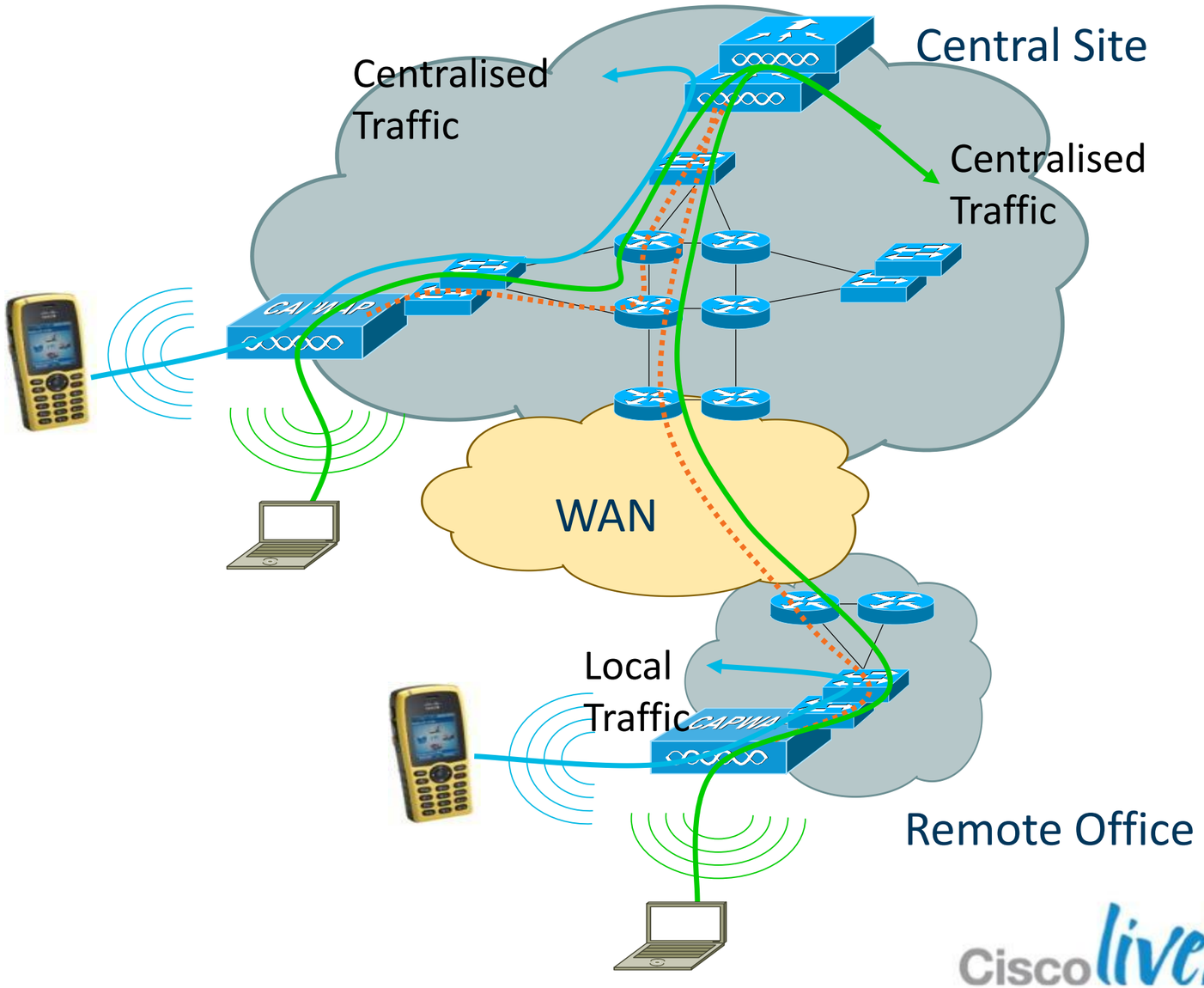
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
  - Understanding FlexConnect AP Deployment
  - Understanding Branch Controller Deployment
- Guest Access Deployment
- Home Office Design

Branch Office Deployment

FlexConnect

- Hybrid architecture
- Single management and control point
  - –Centralised traffic (split MAC)
  - –Or
  - –Local traffic (local MAC)
- HA will preserve local traffic only



FlexConnect Design Considerations

For Your Reference

WAN limitations apply

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	128 kbps	300 ms	5	25
Data + Voice	128 kbps	100 ms	5	25
Data	128 kbps	1 sec	1	1
Monitor	128 kbps	2 sec	5	N/A
Data	1.44 Mbps	300 ms	50	1000
Data + Voice	1.44 Mbps	100 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Monitor	1.44 Mbps	2 sec	50	N/A

Economies of Scale for Lean Branches

Flex 7500 Wireless Controller

Access Points	300 - 6,000
Clients	64,000
Branches	2000
Access Points / Branch	100
Deployment Model	FlexConnect
Form Factor	1 RU
IO Interface	2x 10GE
Upgrade Licenses	100, 200, 500, 1K

Key Differentiation

- WAN Tolerance
  - High Latency Networks
  - WAN Survivability
- Security

  802.1x based port authentication
- Voice support
  - Voice CAC
  - OKC/CCKM

Flex 7500 Scale Update (7.2 vs. 7.3)

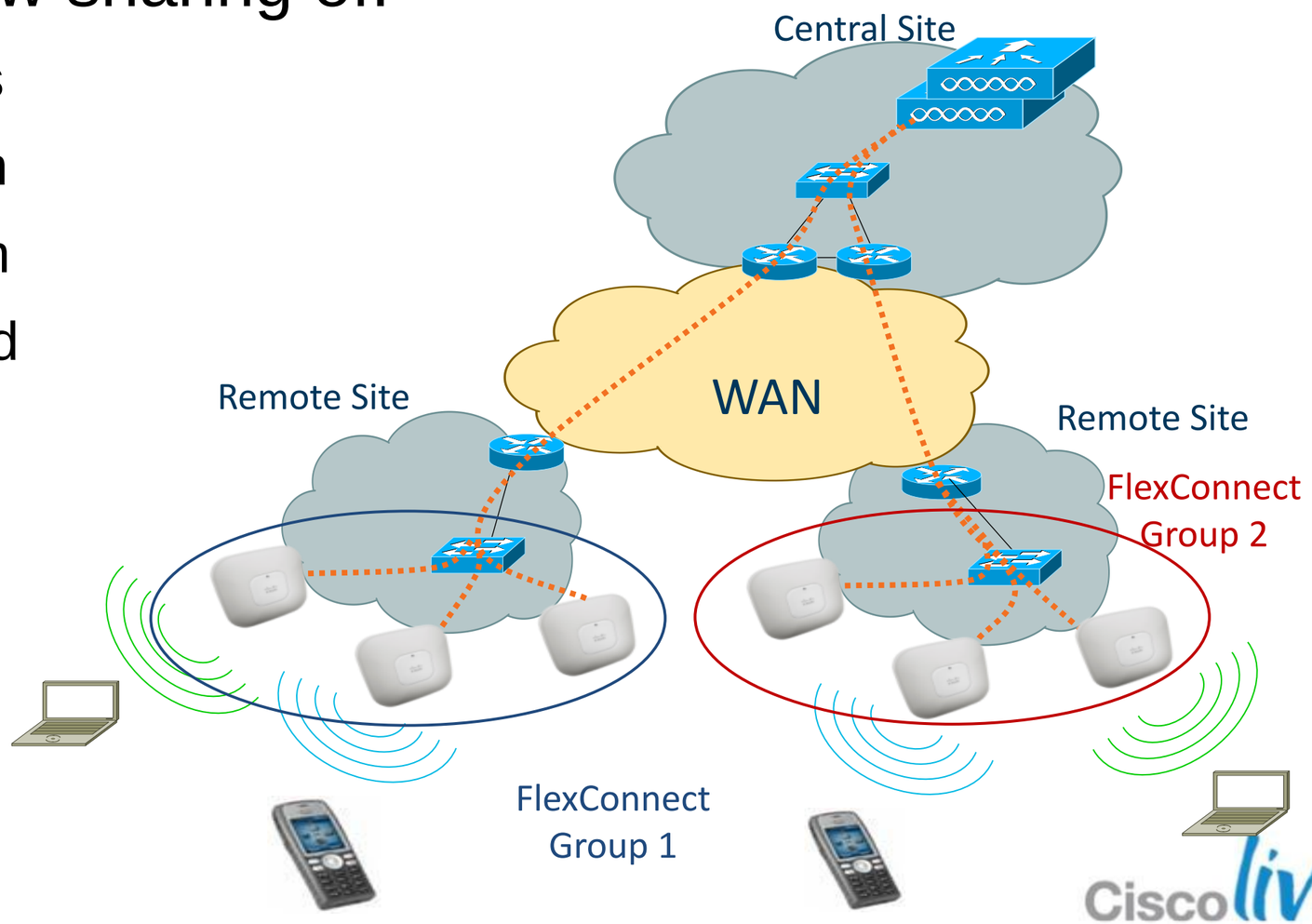
Scalability	7.2	7.3
Total APs	3000	6000
Total Clients	30,000	64,000
Total FlexConnect Group	1000	2000
Maximum APs per FlexConnect Group	50	100
Total Rogue AP	12000	24000
Total Rogue Client	15000	32000
Number of Vlan Support	512	4095
Number of RFID	20000	50000
Maximum APs per RRM Group	6000	12000

Understanding FlexConnect Groups

- FlexConnect groups allow sharing of:
  - –CCKM fast roaming keys
  - –Local user authentication
  - –Local EAP authentication
  - –Efficient Image Download

- Scaling information

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504
FlexConnect Groups	1000	100	100	20
AP per Flex Group	50	25	25	25



FlexConnect Improvements in 7.2

- Smart AP Image Upgrade
- ACL's on FlexConnect AP
- AAA Over-ride of VLAN - dynamic VLAN assignment for locally switched clients
- FlexConnect Re-branding
- Fast Roaming for Voice Clients
- Peer to Peer Blocking

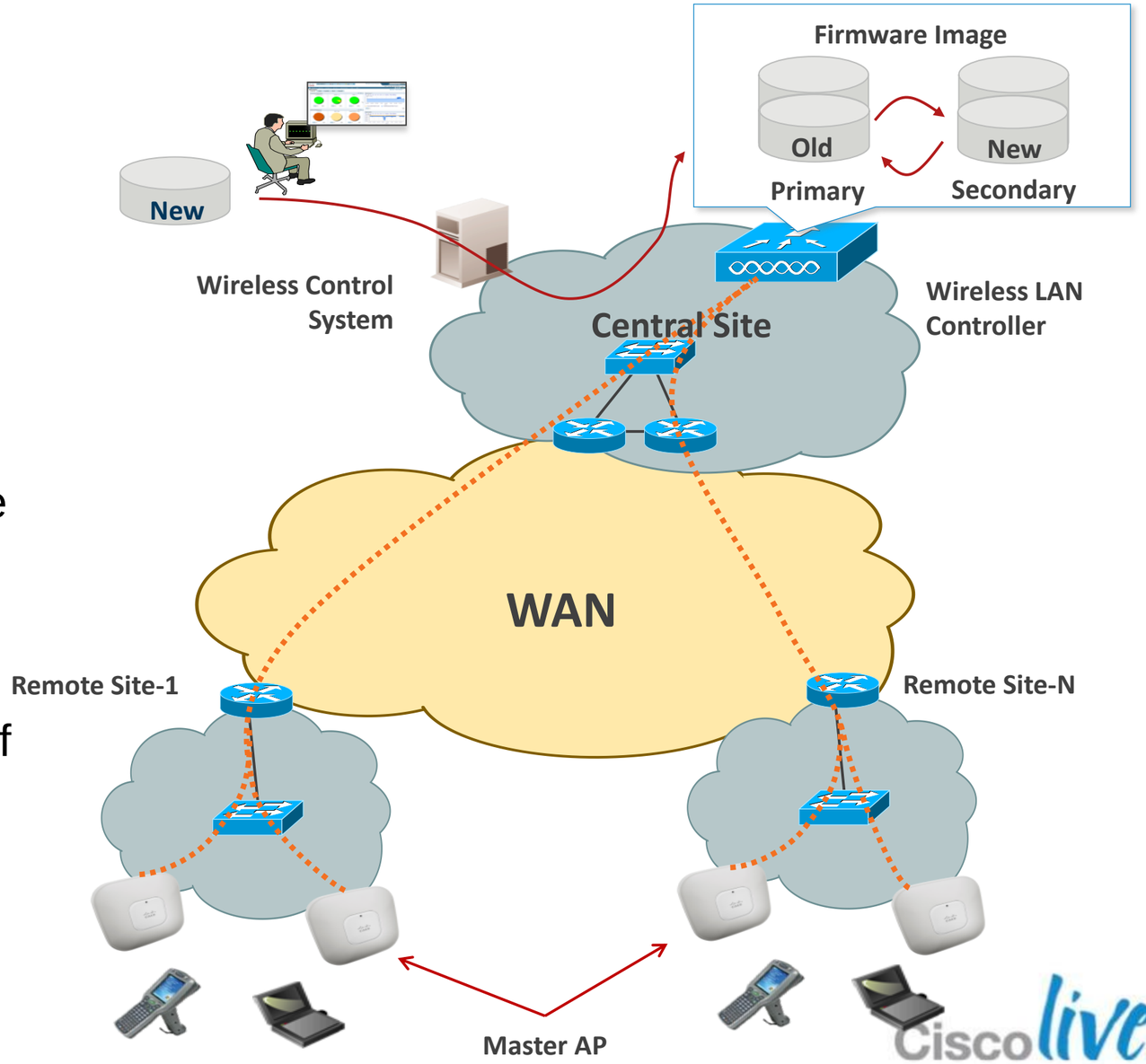
FlexConnect Smart AP Image Upgrade

Description

Smart AP Image Upgrade use a « master » AP in each FlexConnect Group to download the code.

Other FlexConnect AP download the code from the master locally

1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)



New in 7.2

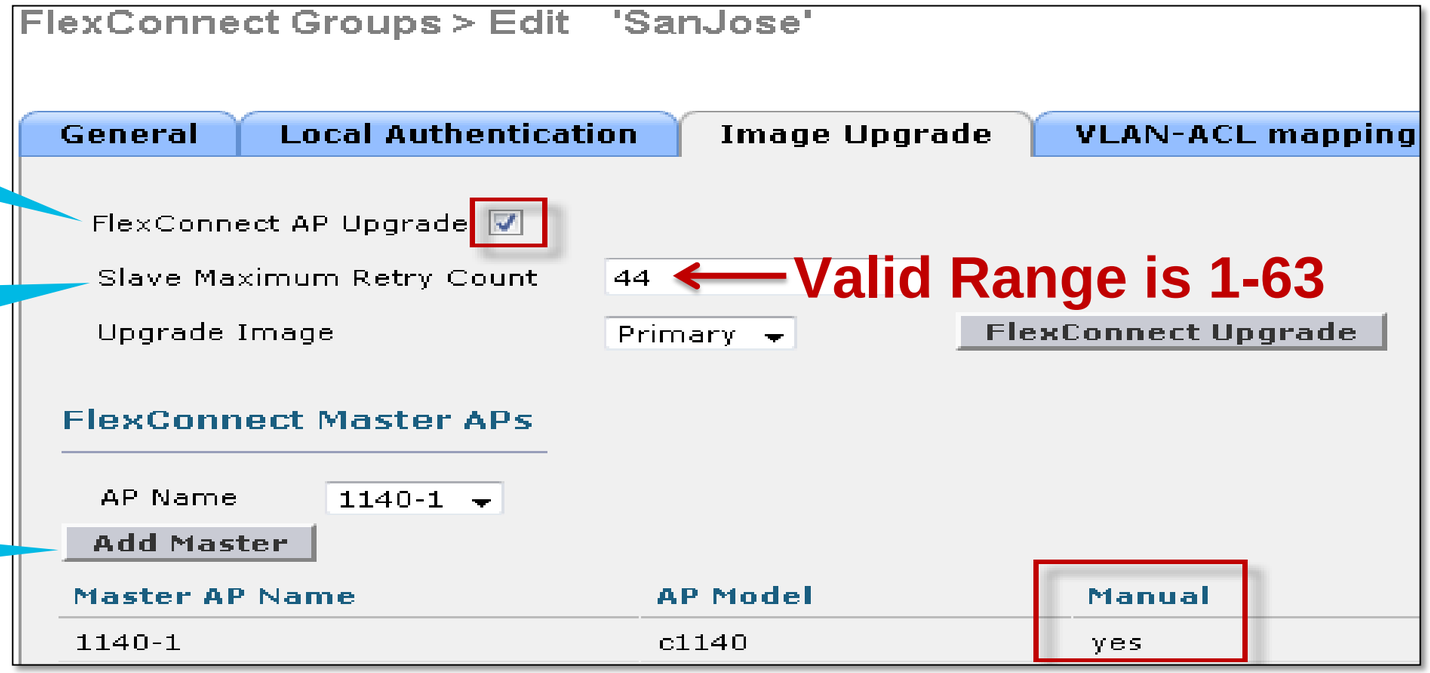
FlexConnect Smart AP Image Upgrade

Configuration

Enable Efficient AP Image Upgrade

Random Backoff Interval (100-300sec) between each retry

Master AP Selection is Optional



"FlexConnect AP Upgrade" checkbox has to be enabled for each FlexConnect Group.

By default, Master AP for each FlexConnect Group is selected using Lower-MAC algorithm.

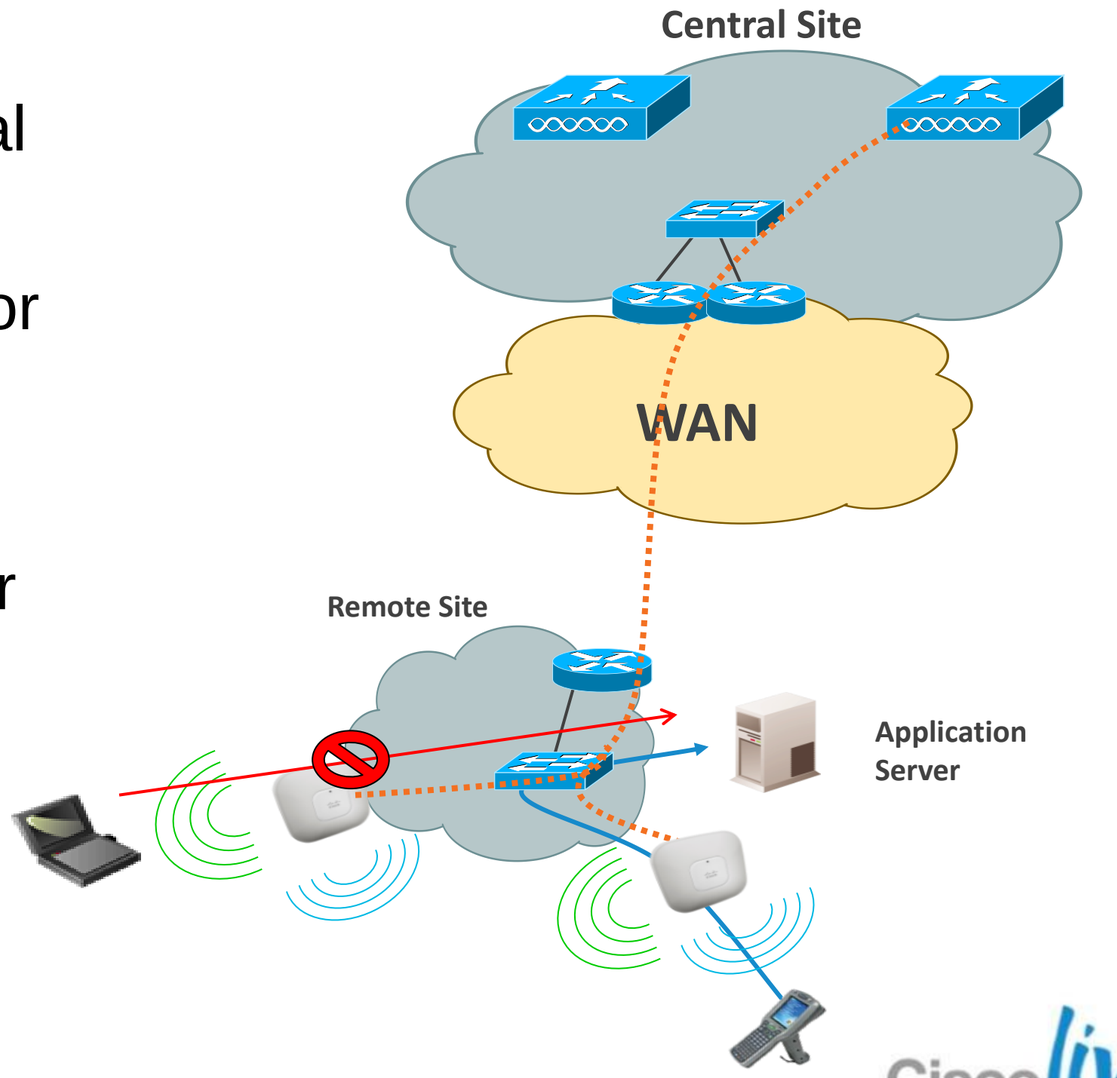
One Master select per AP type.

New in 7.2

Local Switching Access Lists

Description

- Support for ACL in FlexConnect local switching mode
- ACL mapped to local VLAN per AP or FlexConnect Group
- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL

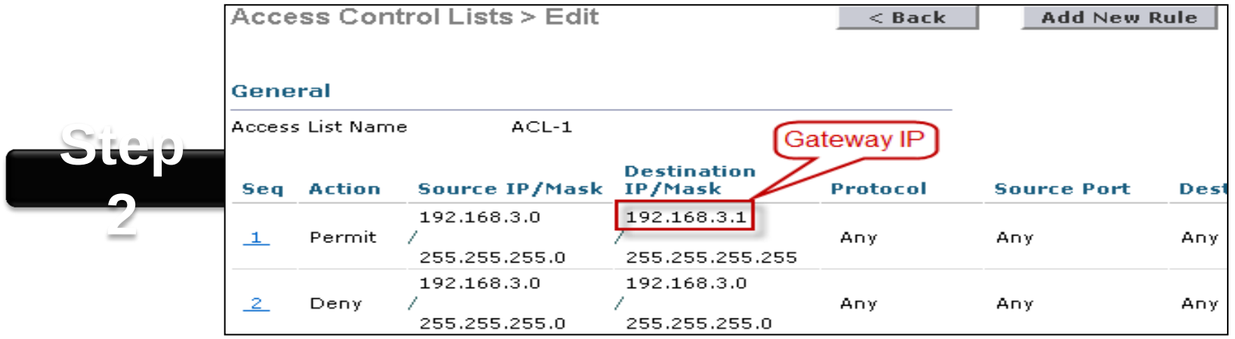


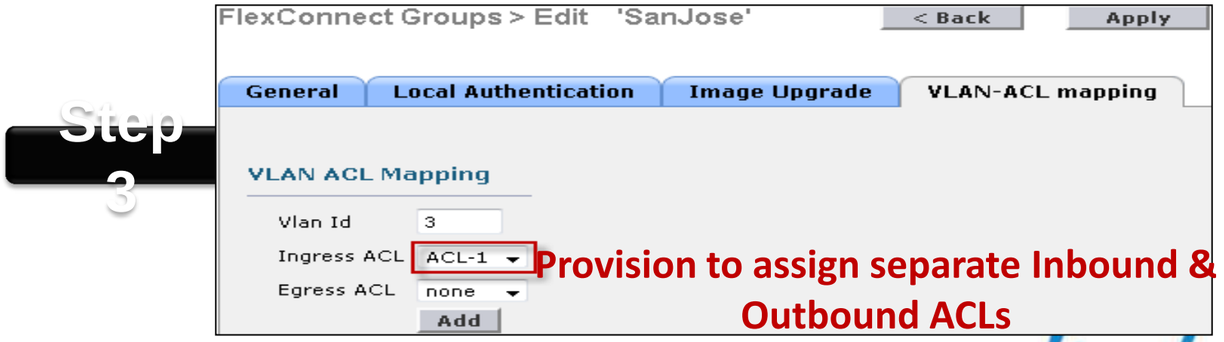
New in 7.2

Local Switching Access Lists

Configuration

- ACL rule creation and application for FlexConnect is identical to WLC rule creation for Local Mode



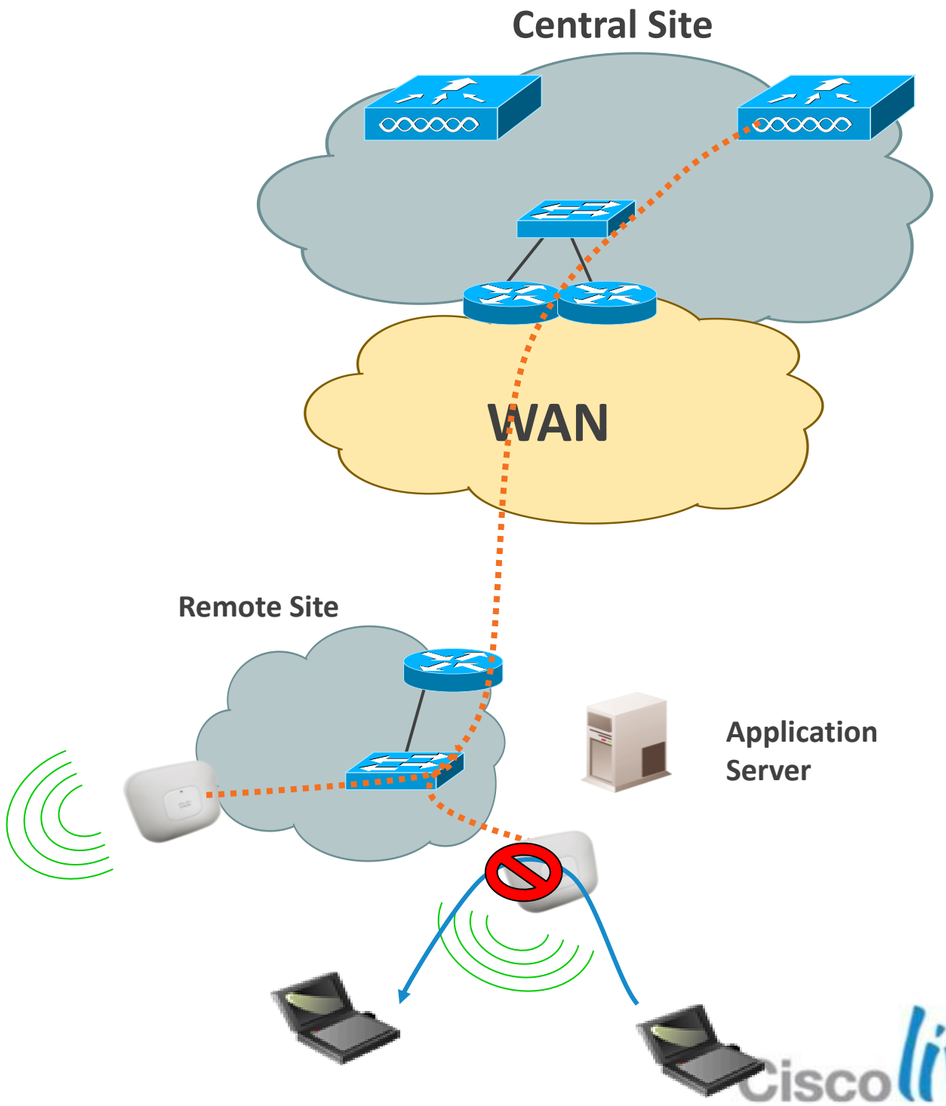


New in 7.2

Local Switching Peer-to-Peer Blocking

Description

- Support for Peer-to-Peer blocking in FlexConnect AP
- Apply for clients on same FlexConnect AP
- P2P blocking modes : disable or drop
- For P2P blocking inter-AP use ACL or Private VLAN fonction

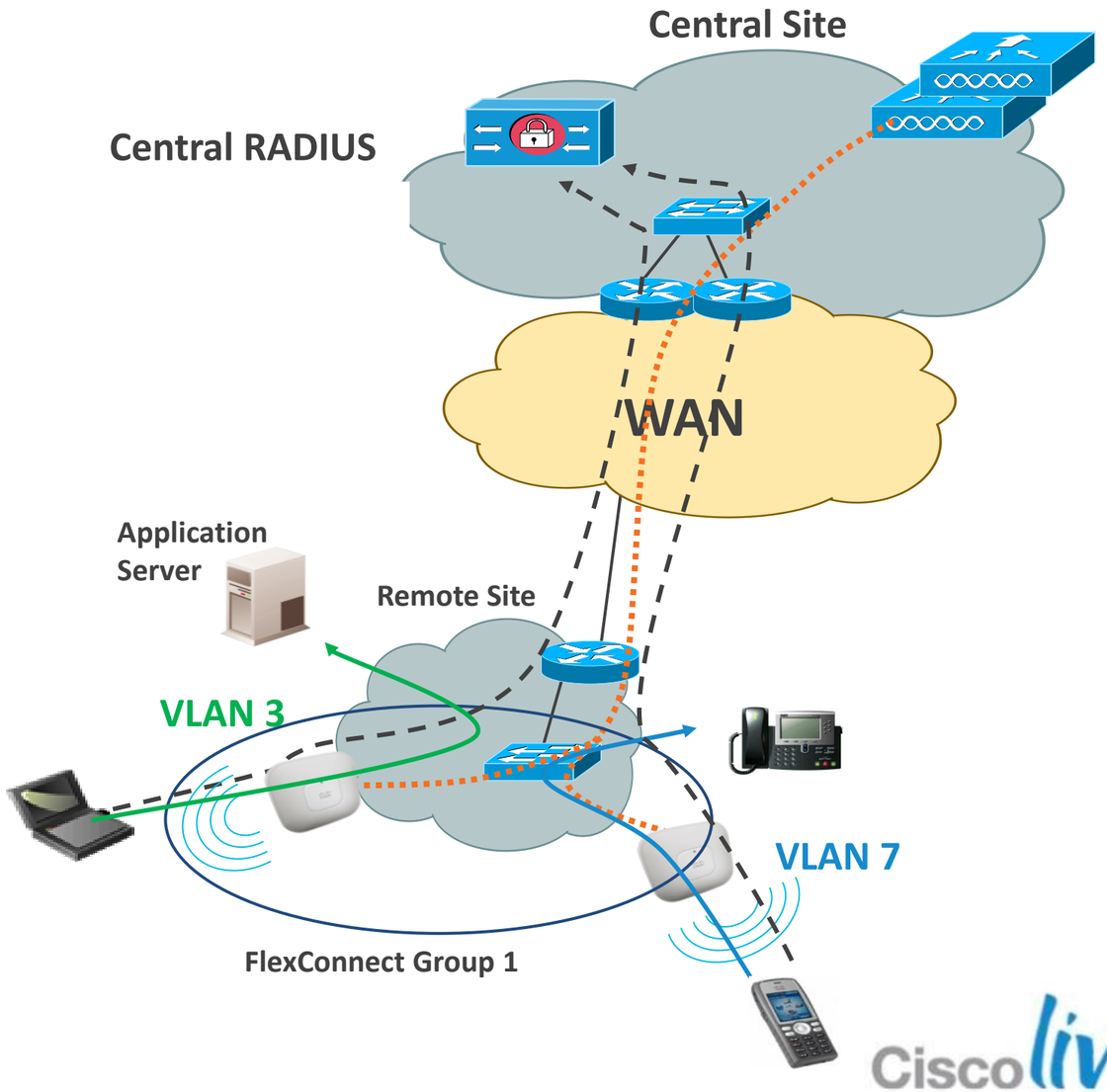


New in 7.2

FlexConnect AAA VLAN Override

Description

- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used
- QoS and ACL Override is not supported.

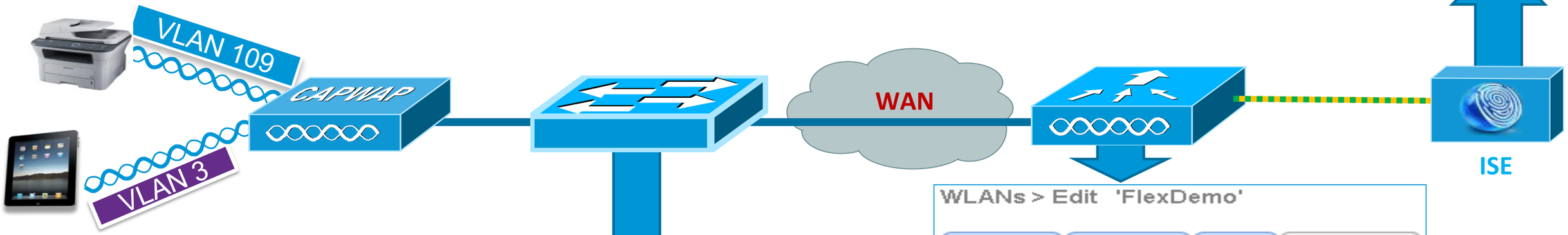


New in 7.2

FlexConnect AAA VLAN Override

Configuration

	Attribute	Type	Value
IETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802
IETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN
IETF 81	Tunnel-Private-Group-ID	Tagged String	[T:1] 3




```
interface GigabitEthernet1/0/4
 description AP-3600-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

WLANs > Edit 'FlexDemo'

General | Security | QoS | Advanced

Allow AAA Override ☑ Enabled

FlexConnect Groups > Edit 'SanJose'

General | Local Authentication | Image Upgrade | VLAN-ACL mapping

VLAN ACL Mapping

Vlan Id 3

Ingress ACL none

Egress ACL none

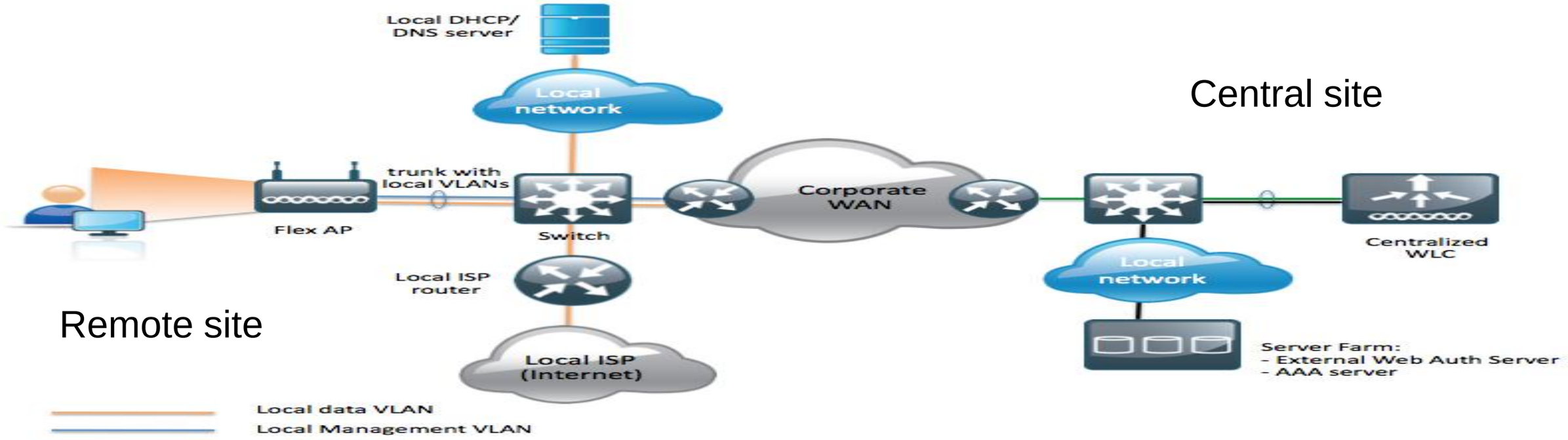
Add

Create Sub-Interface on FlexConnect AP

New in 7.2

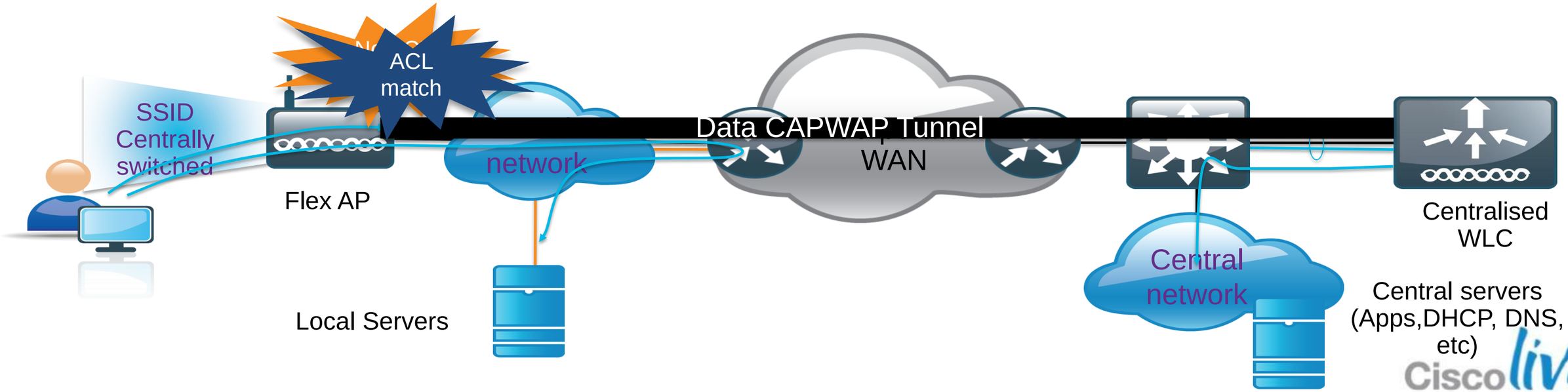
Flex: External Web Auth with Local Switching

- **What**: starting with 7.2 MR1 it is possible for WLC to perform Web authentication with an external server on a locally switched WLAN
- **Why**: This addresses Retail and Hot Spot requirement where the portal is centralised but the traffic needs to exit locally to save WAN bandwidth
- **How**: A pre-auth Flex ACL at the AP is used to match the traffic that is allowed to be locally switched before authentication is completed.



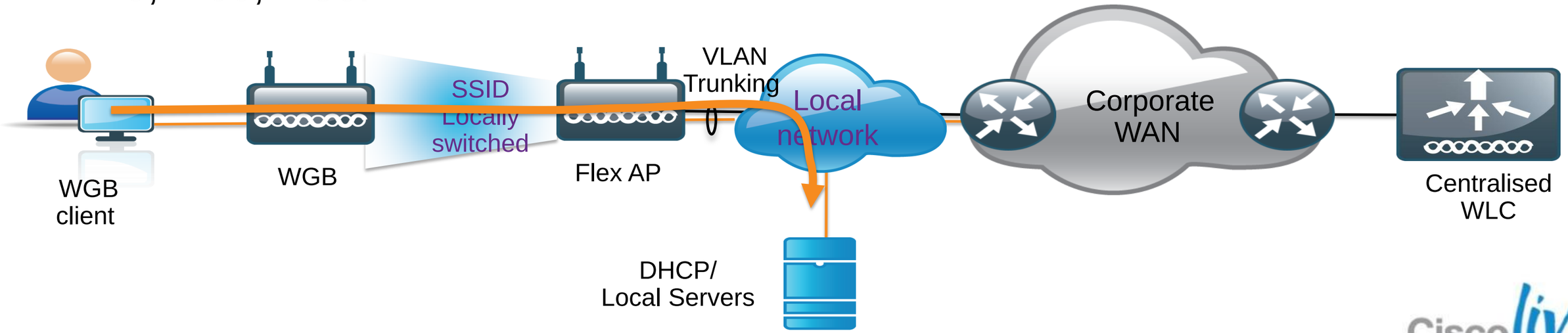
Flex: Local Split Tunnelling

- **What**: on a centrally switched WLAN, this feature gives the flexibility to decide what traffic gets tunneled to WLC and what traffic is bridged locally at the AP
- **Why**: Local Spilt Tunnelling improves WAN bandwidth utilisation and may simplify subnet/routing design for remote sites.
- **How**: Flex ACL is used to match traffic for local switching. Port Address Translation (PAT) is used to switch packets to the local LAN using BVI's IP address.

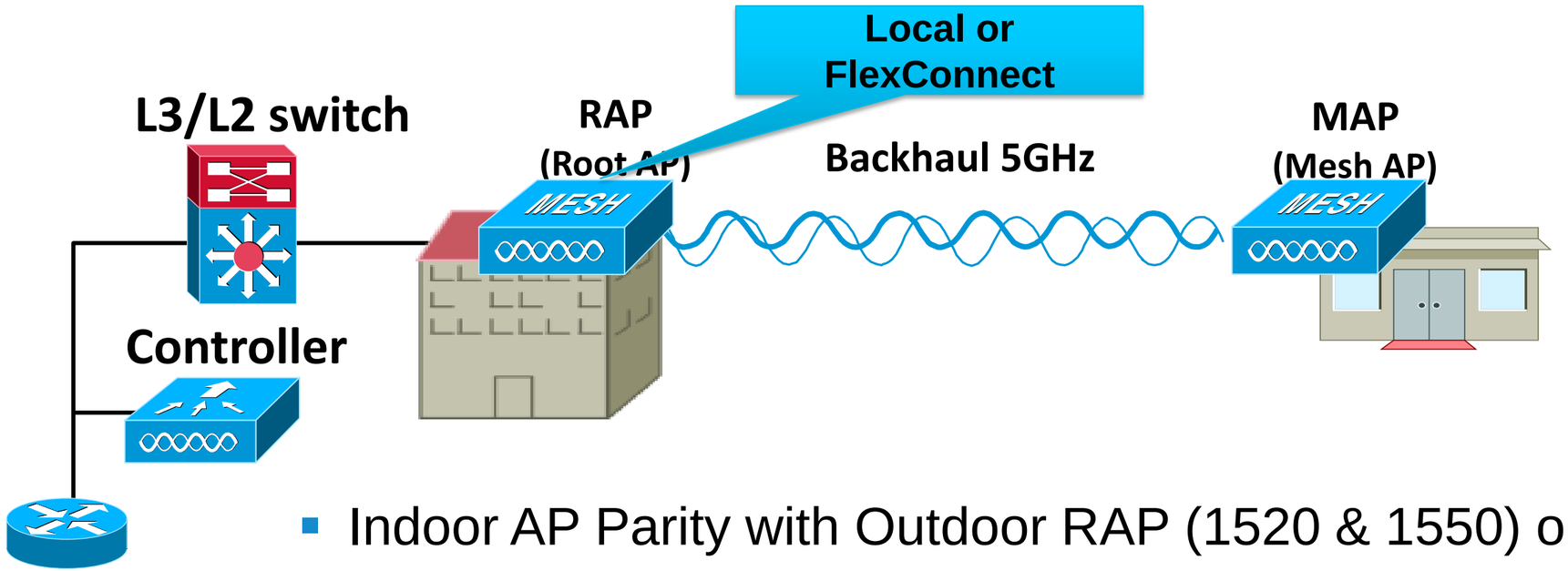


Flex: WGB/uWGB support for Local switching

- **What**: this feature extends support of CUWN for WGB/uWGB associated to a locally switched WLAN on Flex mode APs
- **Why**: simplifies deployment of wired-only devices in remote locations when traffic is designed to stay local. Manufacturing is the main Vertical
- **How**: this capability has been extended to Flex APs for locally switched WLANs; no configuration required. WGB is supported on an IOS AP: 1240, 1130, 1140,1260,1250.



FlexConnect and AP1500 (Outdoor)



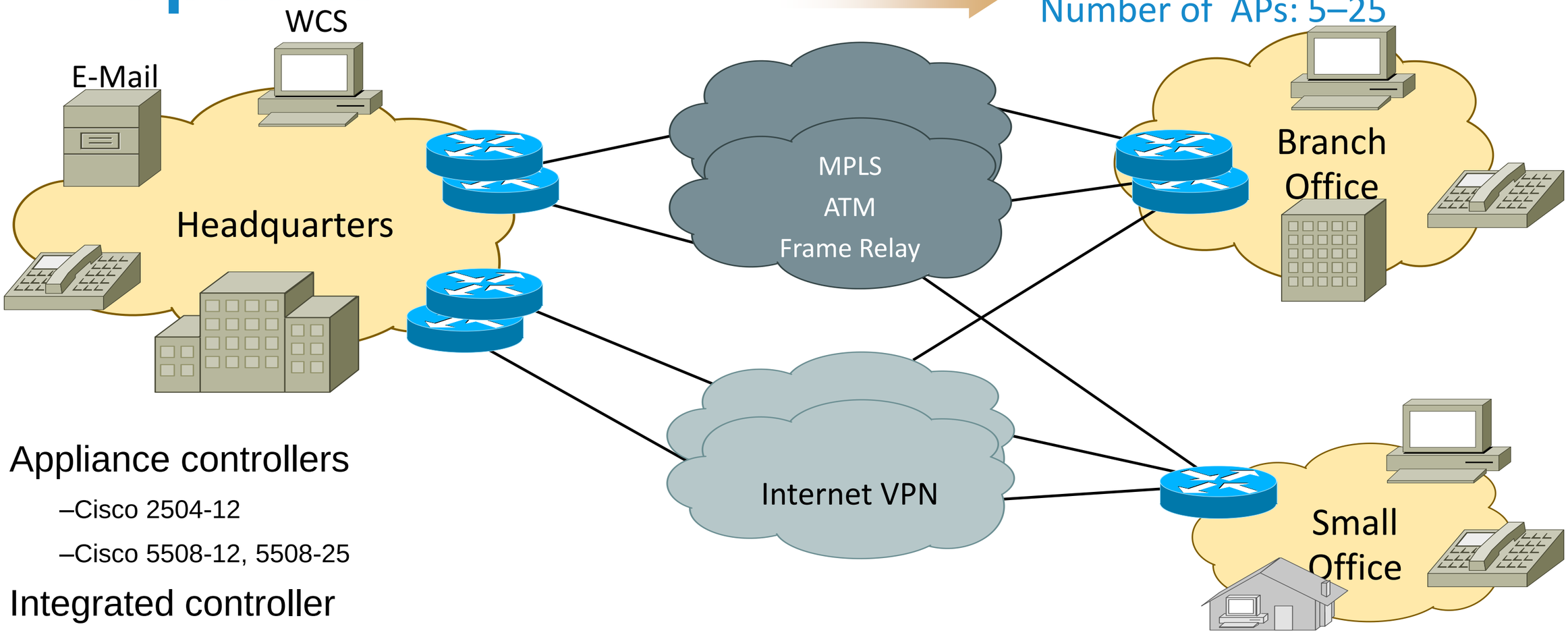
- Indoor AP Parity with Outdoor RAP (1520 & 1550) only
  - Local Mode
  - FlexConnect Mode
  - No MAP functionality in this release
- Flex Mode will have support for Central and Local Switching

Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
  - Understanding FlexConnect AP Deployment
  - Understanding Branch Controller Deployment
- Guest Access Deployment
- Home Office Design

Branch Office WLAN Controller Options

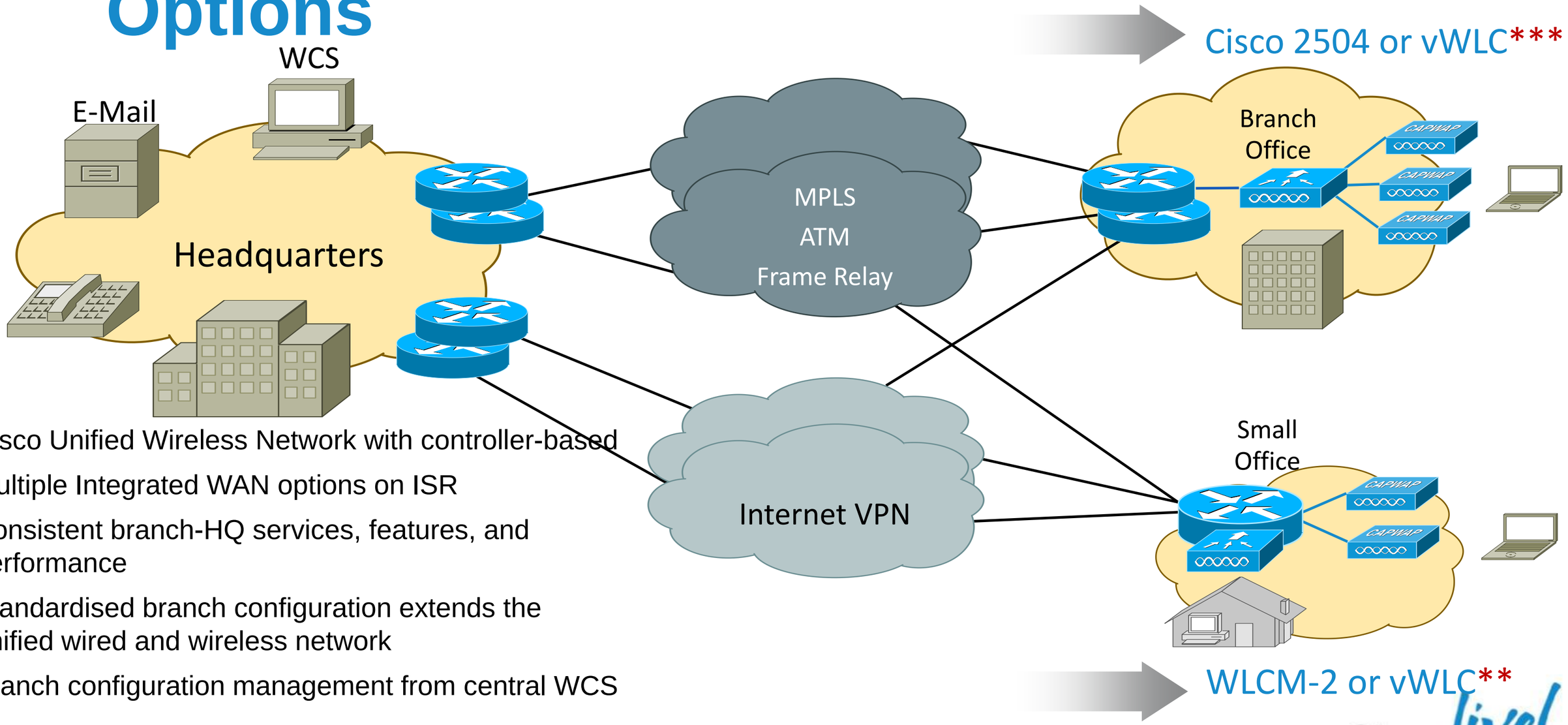
Number of Users: 100–500
Number of APs: 5–25



- Appliance controllers
  - –Cisco 2504-12
  - –Cisco 5508-12, 5508-25
- Integrated controller
  - –WLAN controller module (WLCM-2) for ISR G2
- Virtual WLC (vWLC)

Number of Users: 20–100
Number of APs: 1–5

Branch Office WLAN Controller Options



- Cisco Unified Wireless Network with controller-based
- Multiple Integrated WAN options on ISR
- Consistent branch-HQ services, features, and performance
- Standardised branch configuration extends the unified wired and wireless network
- Branch configuration management from central WCS

**AP Count Vary Depending on Channel Utilisation and Data Rates

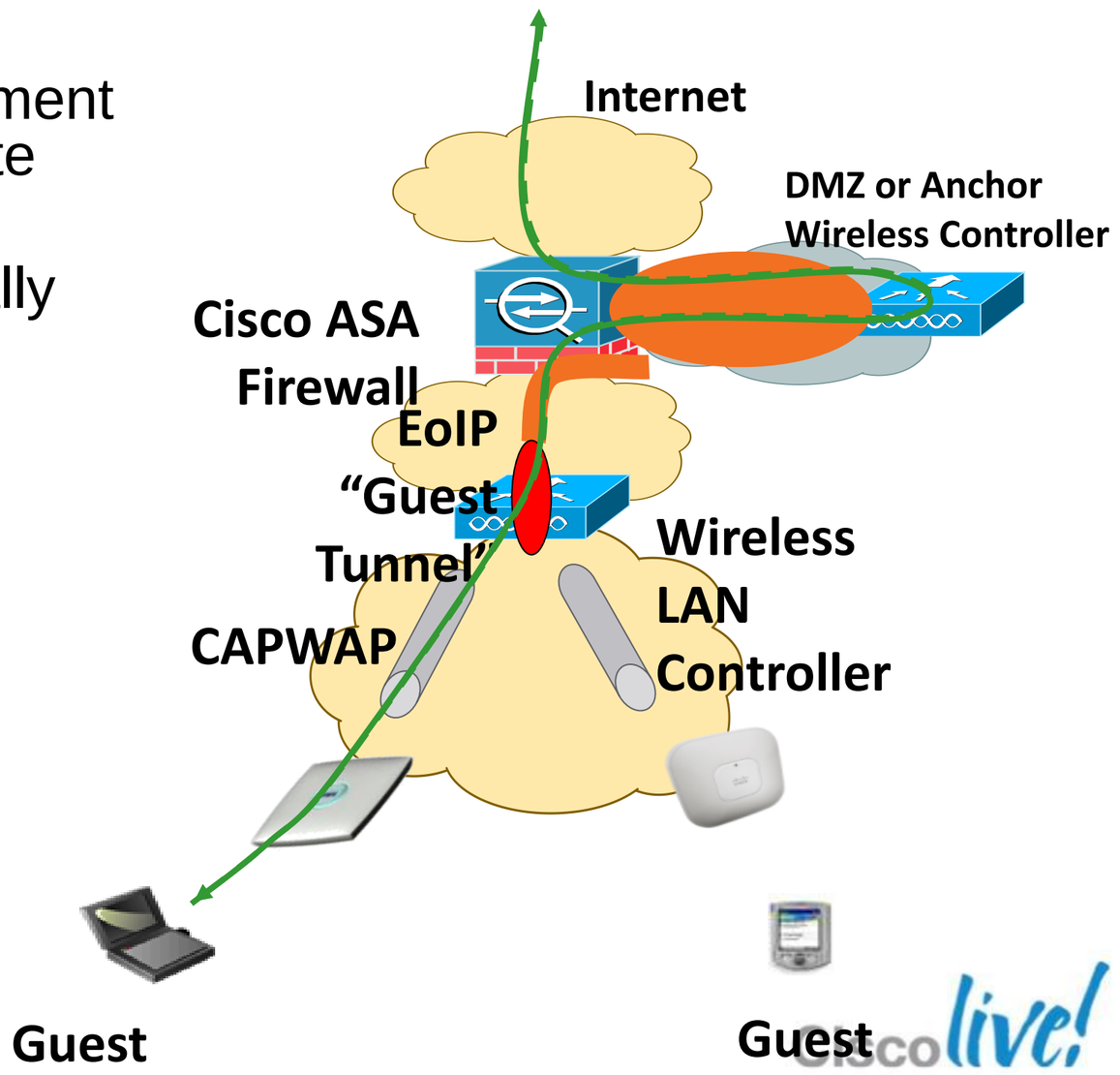
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

Guest Access Deployment

WLAN Controller Deployments with EoIP Tunnel

- Use of up to 71 EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers
- Other traffic (employee for example) still locally bridged at the remote controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the remote controllers
- Original guest's Ethernet frame maintained across CAPWAP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- 2504 series and WLCM-2 models cannot terminate EoIP connections (no anchor role)

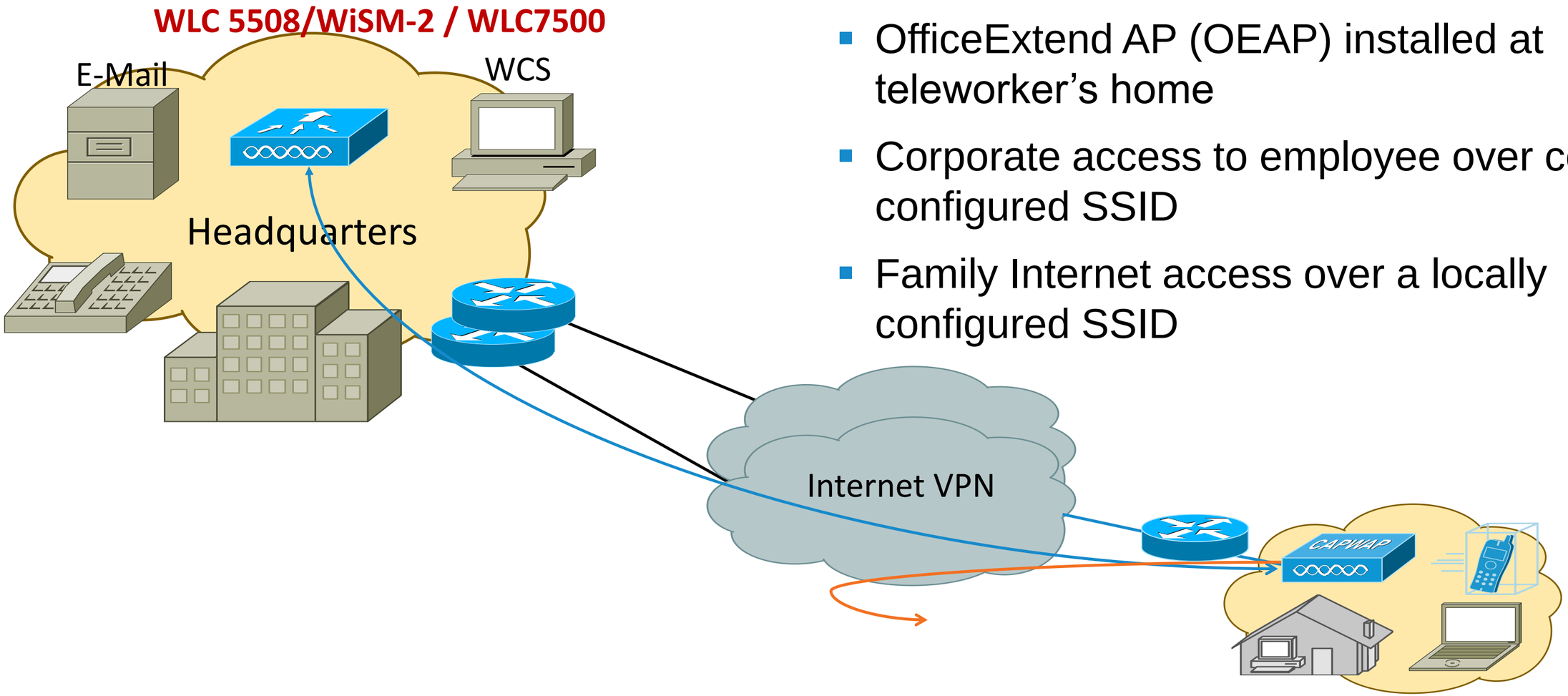


Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- Bonjour Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Designs

Home Office Design

OEAP AP



- Cisco controller installed in the DMZ of the corporate network
- OfficeExtend AP (OEAP) installed at teleworker's home
- Corporate access to employee over centrally configured SSID
- Family Internet access over a locally configured SSID

OEAP 600

- 802.11n AP with dual concurrent 2.4GHz and 5GHz radios for teleworker home
- 4 local Ethernet ports
- 1 Corporate-bound port, 3 for local Ethernet devices
- Up to 4 clients behind the corporate port
- Corporate SSID and user-configurable Personal SSID
- Traffic segmenting supported (corporate vs. personal traffic)
- Local DHCP and NAT support
- Control and data plane encryption

Summary – Key Takeways

- Take advantage of the standards (CAPWAP, DTLS,802.11 i, e, k, r…..)
- Wide range of architecture / design choices
- Brand new controllers (WiSM-2, WLC 7500,WLC 8500, WLC 2504, Virtual WLC) portfolio with investment protection
- Take advantage of innovations from Cisco (CleanAir, BandSelect, ClientLink, Security, CCX, FlexConnect, etc)
- Cisco's investment into technology – Cisco Prime, ISE, New hardware, Cloud controller

Documentation

Virtual WLC Deployment Guide http://www.cisco.com/en/US/products/ps12723/products_tech_note09186a0080bd2d04.shtml

HA Deployment Guide http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bd3504.shtml

Flex 7500 Deployment Guide http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

AP2600 Deployment Guide : http://www.cisco.com/en/US/products/ps11983/products_tech_note09186a0080bd3d10.shtml

Wireless Bi-Directional Rate Limiting Deployment Guide
: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bd3900.shtml

WLC8500 Deployment Guide: http://www.cisco.com/en/US/products/ps12722/products_tech_note09186a0080bd6504.shtml

WiSM-2 : http://www.cisco.com/en/US/products/hw/modules/ps2706/products_tech_note09186a0080bb2500.shtml

Flex7500 Deployment Guide

http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

Bonjour Deployment Guide

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_tech_note09186a0080bb1d7c.shtml

MSE HA Deployment Guide : http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a0080bb490d.shtml

MSE Virtual Appliance Deployment Guide :
http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a0080bb497f.shtml

IPv6 Deployment Guide http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bae506.shtml

VLAN Select Deployment Guide : http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bb4900.shtml

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

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

Cisco live!