TOMORROW starts here.

cisco

Cisco live!

Design and Deployment of Enterprise WLANs

BRKEWN-2010

Sujit Ghosh

Senior Manager Technical Marketing

Enterprise Networking Group

Cisco live!

Agenda

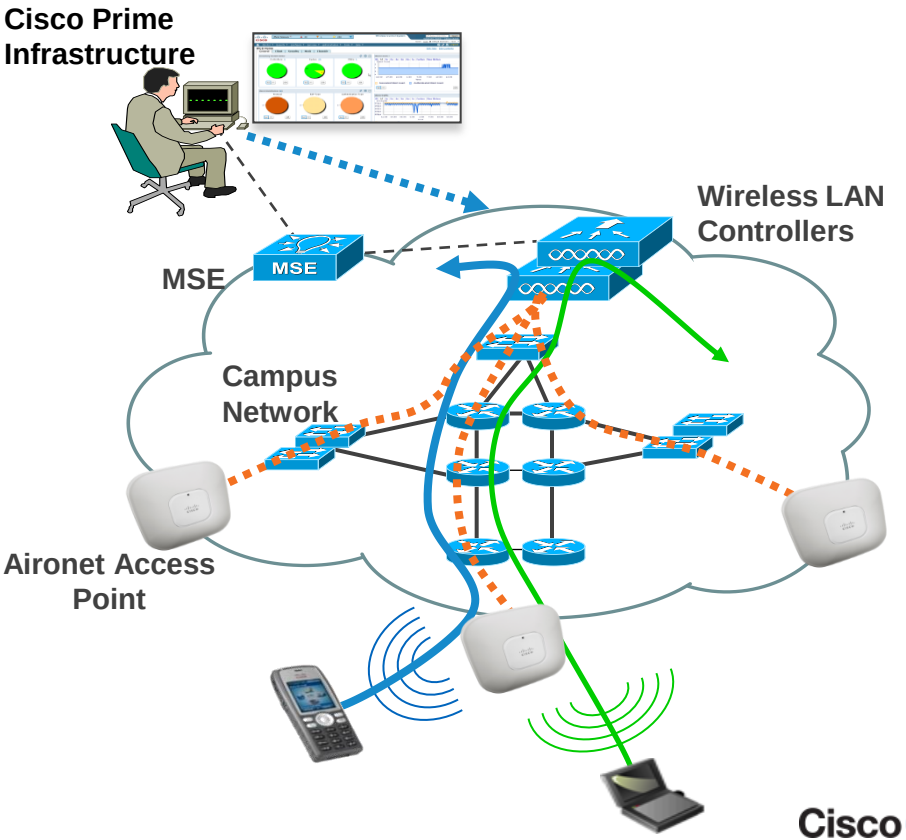
- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

Agenda

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

Cisco Unified Wireless Principles

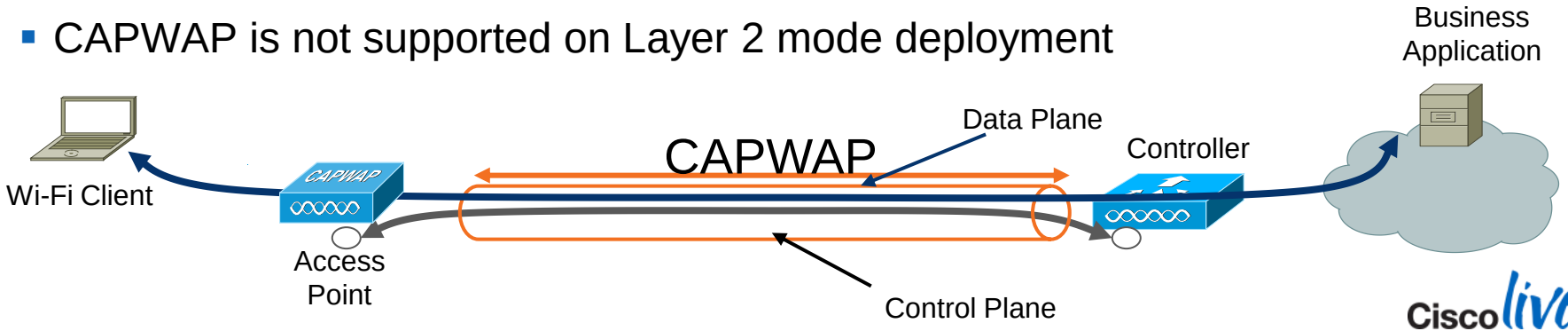
- Components
  - Wireless LAN controllers
  - Aironet access points
  - Management (Prime Infrastructure)
  - Mobility Service Engine (MSE)
- Principles
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC



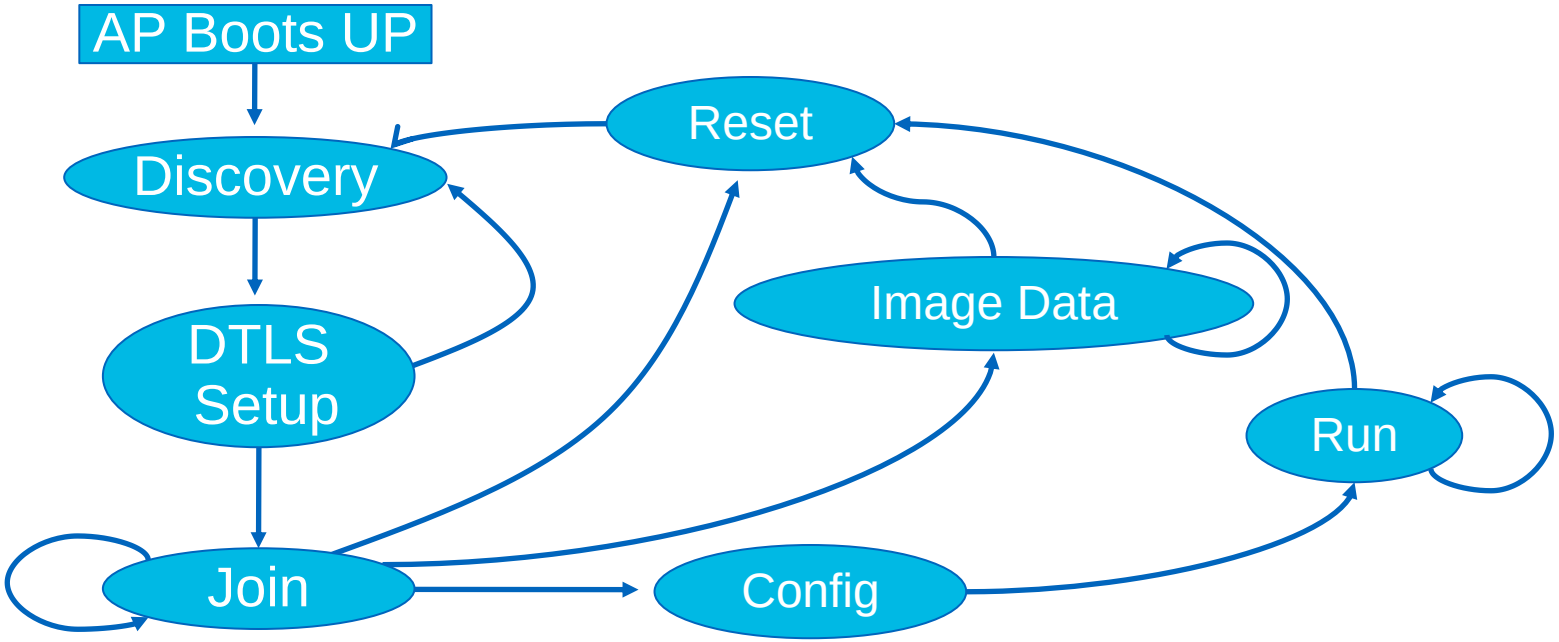
Centralised Wireless LAN Architecture

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 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

7.4, 7.5, 7.6 ? Which Version Should I Use?

- Latest Releases
  - 7.6.100.0(ED)
  - 7.4.121.0(ED)
  - 7.5.102.0(ED)
  - 7.2.115.2(ED)
- All Releases
  - 7.6
    - 7.6 ED Release
  - 7.5
    - 7.5 ED Release
  - 7.4
    - 7.4 ED Release
      - 7.4.121.0(ED)
      - 7.4.110.0(ED)
  - 7.3
    - 7.3 ED Release
  - 7.2
    - 7.2 ED Release
  - 7.1
    - 7.1 ED Release
  - 7.0

- **WLC 5508 supports 6.0 and above**
- **WLC7500, WiSM-2 and WLC2504 only supported in 7.0 onwards**
- **7.4.110 is the latest MD AssureWave (Blue Ribbon)**
- **Please note the current revision of 7.4.121 is the recommended one for you today with latest fixes**
- **AP3700 (7.6), AP3600+11ac (7.5), AP1600(7.4), AP2600 (7.3), AP3600(7.2)**

Release Recommendations

Software Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train	7.4 MD release train
Early Deployment (ED) releases for pre-802.11ac deployments	7.2 ED releases 7.3 ED releases	7.4 MD release train (7.4.121.0 is the minimum recommended release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release	7.6 ED release

Software Release	ISE	Prime Infra	MSE
7.0 (MD train)	1.2	2.0	7.6
7.4 (MD train)	1.2	2.0	7.6
7.6 (ED)	1.2	1.4.1	7.6

Detailed release recommendations in Software release bulletin:
http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps12722/bulletin-c25-730741.pdf

Agenda

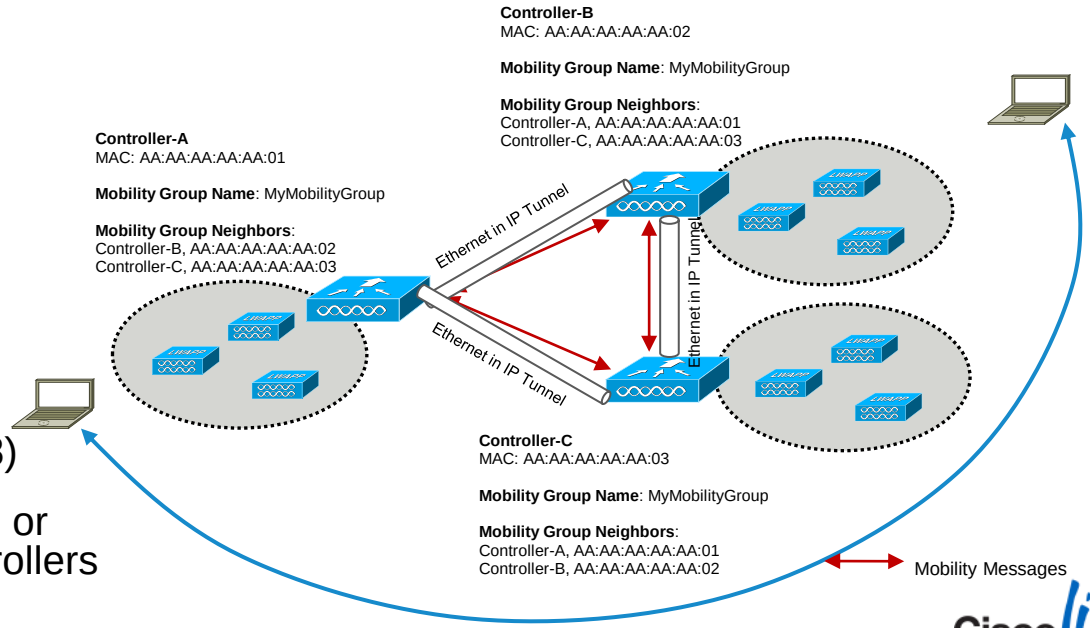
- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

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

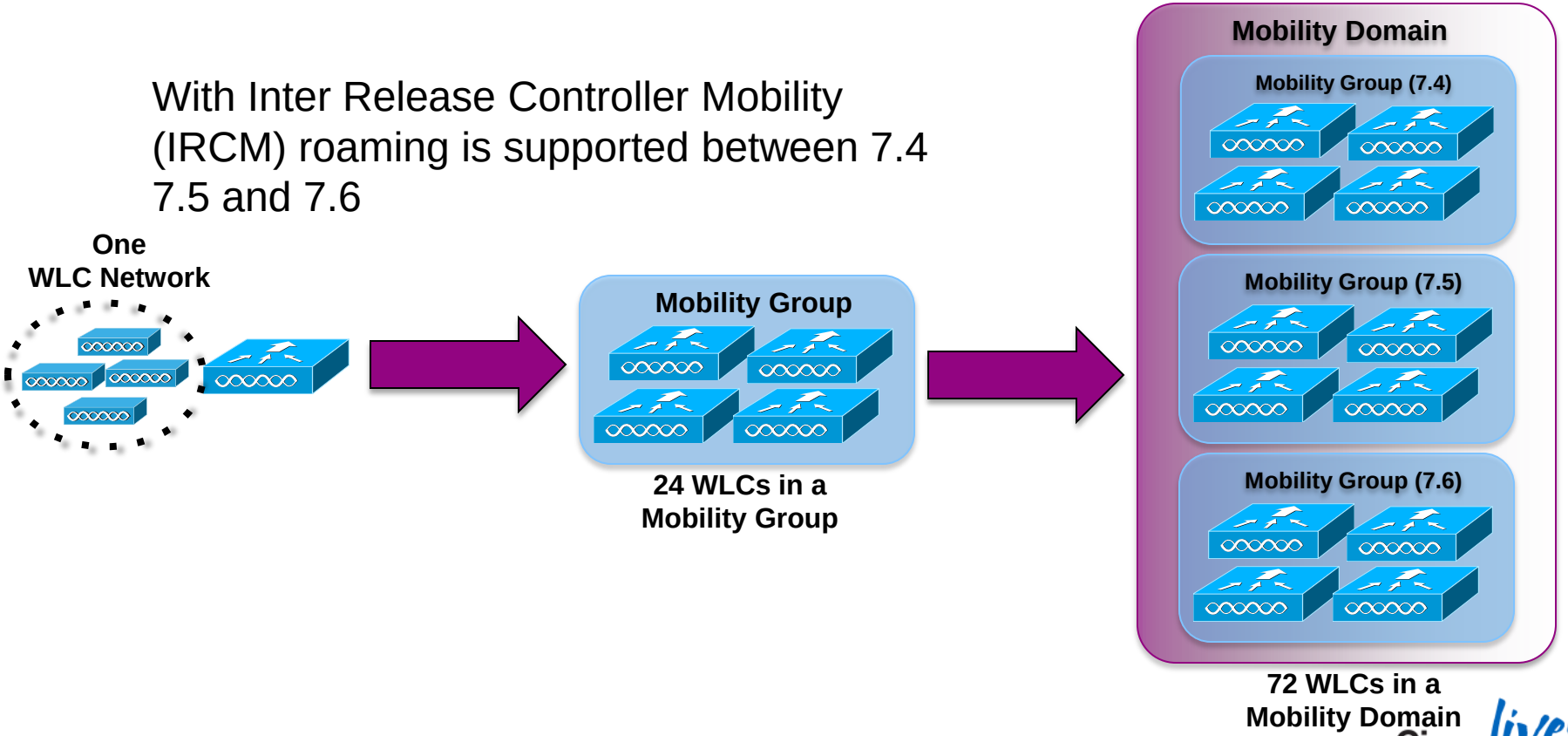
Scaling the Architecture with Mobility Groups

- 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)
- 7.5 has the option of using EOIP or CAPWAP tunnels between controllers



Scaling the Architecture with Mobility Groups

With Inter Release Controller Mobility (IRCM) roaming is supported between 7.4 7.5 and 7.6



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

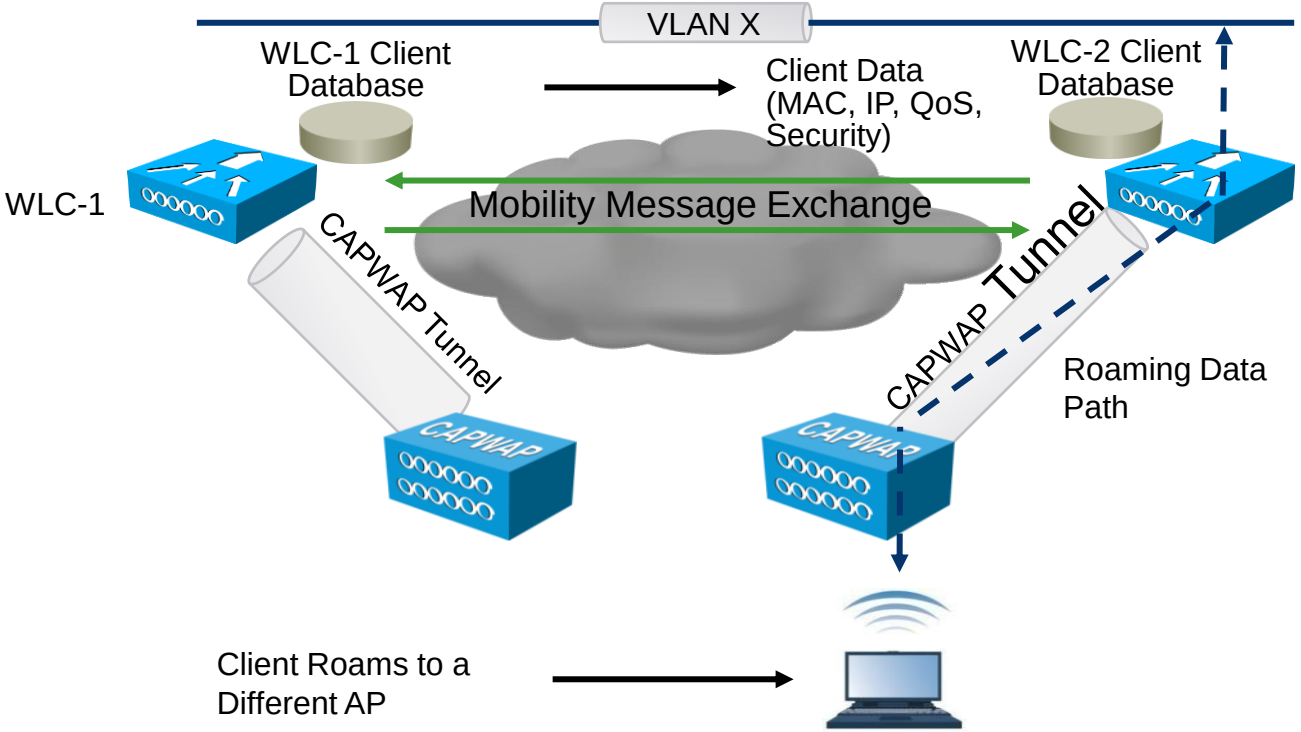
How Are We Going to Make Roaming Faster?

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:

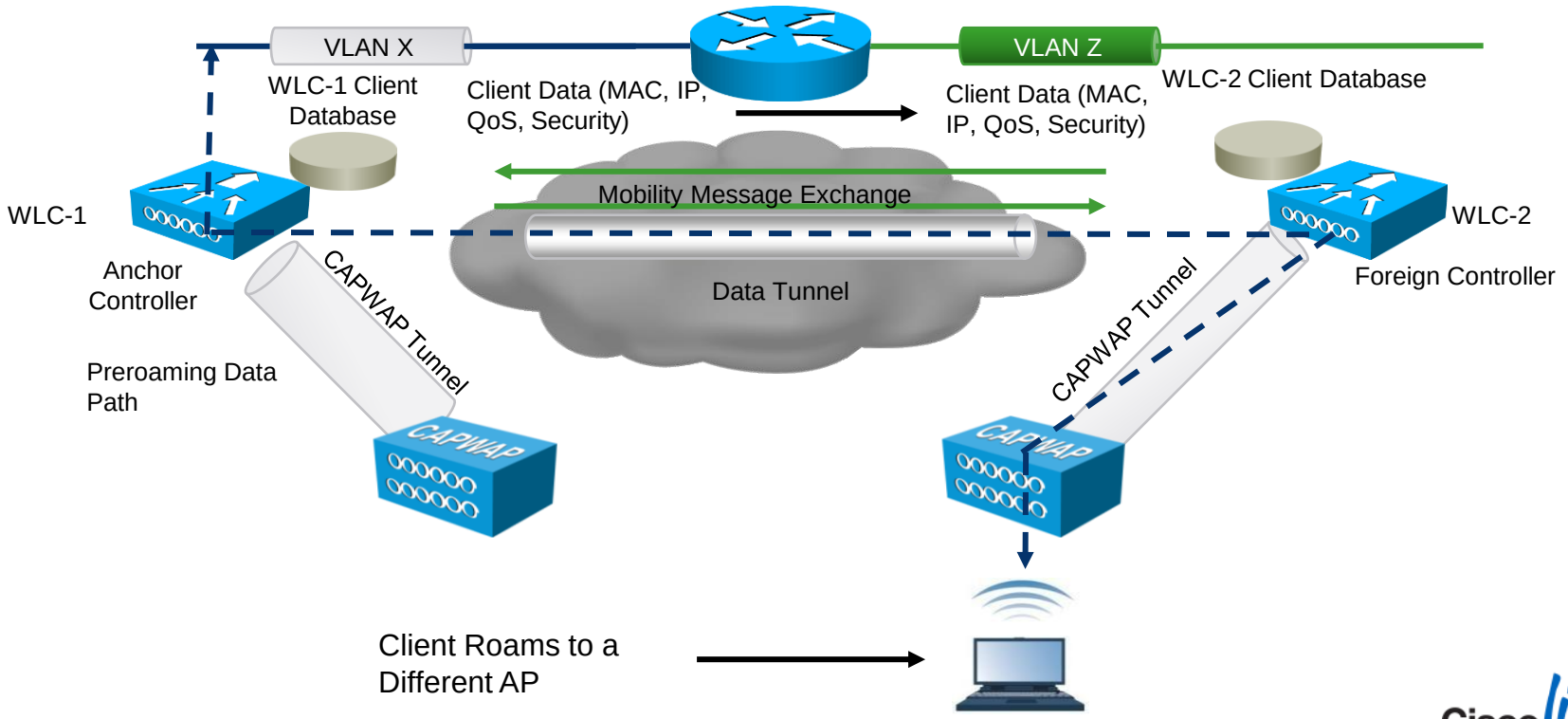
Layer 2 Roaming



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

Client Roaming Between Subnets:

Layer 3



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?

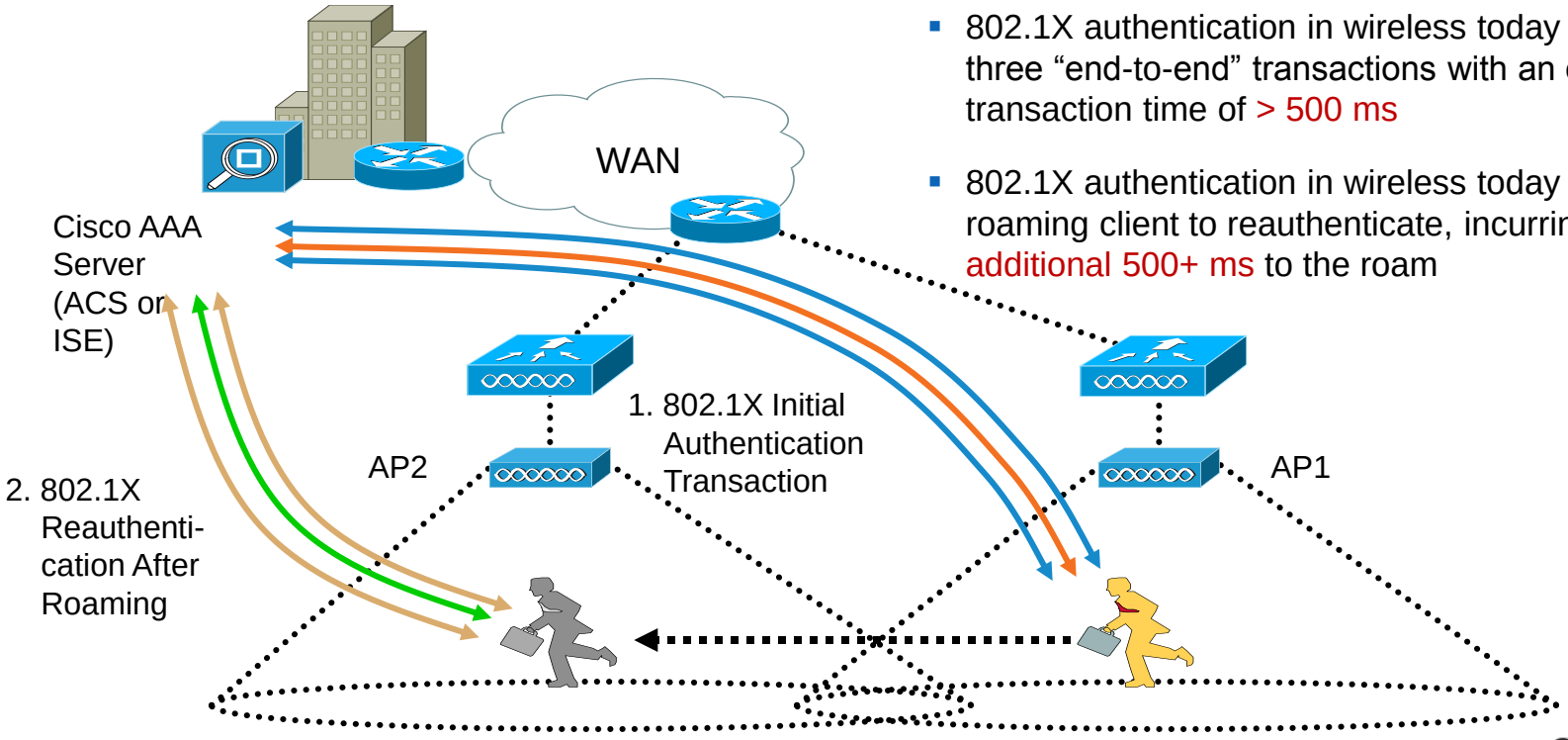
Focus on Where We Can Have the Biggest Impact

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

Fast Secure Roaming

Standard Wi-Fi Secure Roaming

Note: Mechanism Is Needed to Centralise Key Distribution



- 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

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, iOS 7.0

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

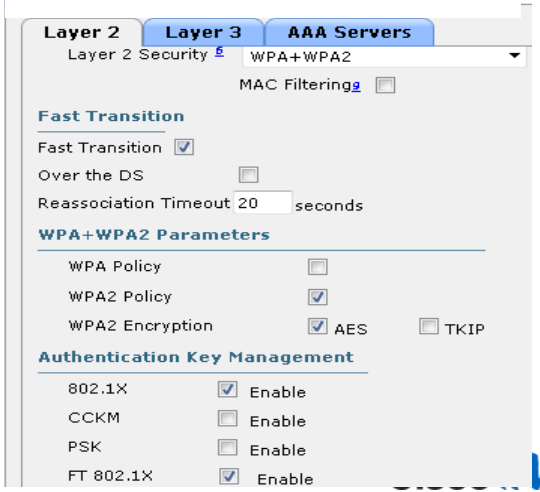
Legacy clients may not associate with a WLAN that has 802.11r enabled along with 802.11i. If the driver or the supplicant that is responsible for parsing the Robust Security Network Information Element (RSN IE) is old and confused by the additional AKM (Authentication Key Management) suites advertised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

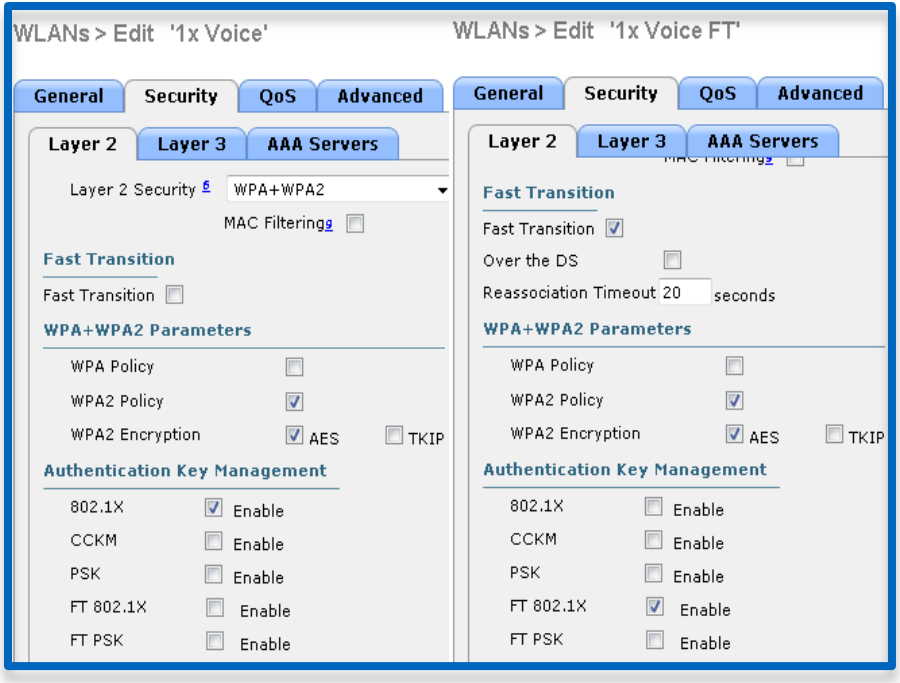
An iPhone with 6.0 or 7.0 iOS could Authenticate to WLAN with both of these AKM's. But because of legacy clients this is NOT recommended.
A non-6.0/7.0 iOS client can't associate.



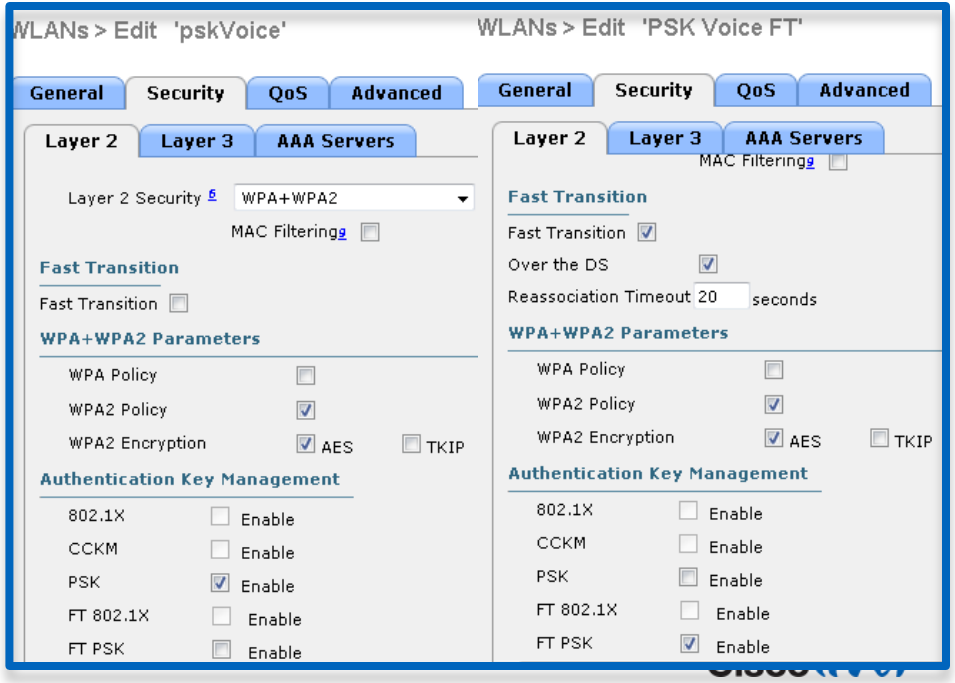
Multiple WLANs for Multiple Auth Types Each with a Unique SSID

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

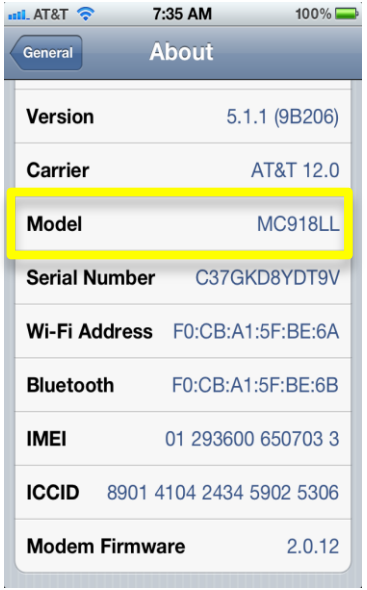


802.11r (Fast Transition) and Client Devices

It can get a little Complex…

- An iPhone with iOS 6.0 can authenticate to a WLAN with and without “FT”.
- A non-6.0 iOS client can’t associate.
- Both iPhone 4 models will take the 6.0iOS upgrade.
- But iPhone 4 does **not** do 11r.
- The iPhone 4s does 11r

(The iPhone 5 also).



- So, which one is it?

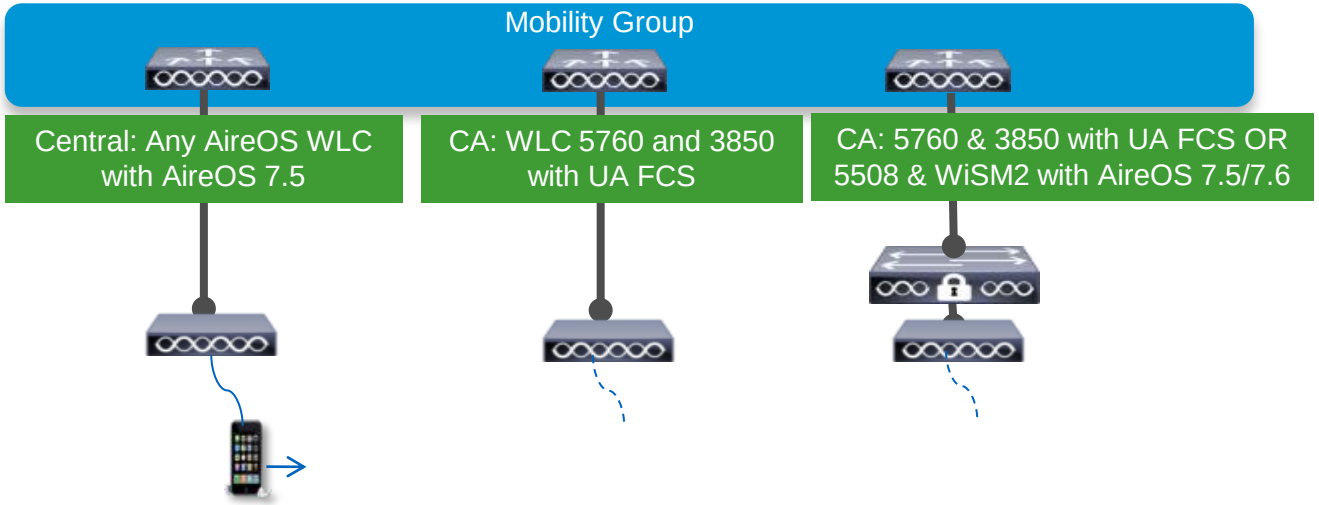
Do an internet search to find the Model if unsure.

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 with latest controllers 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

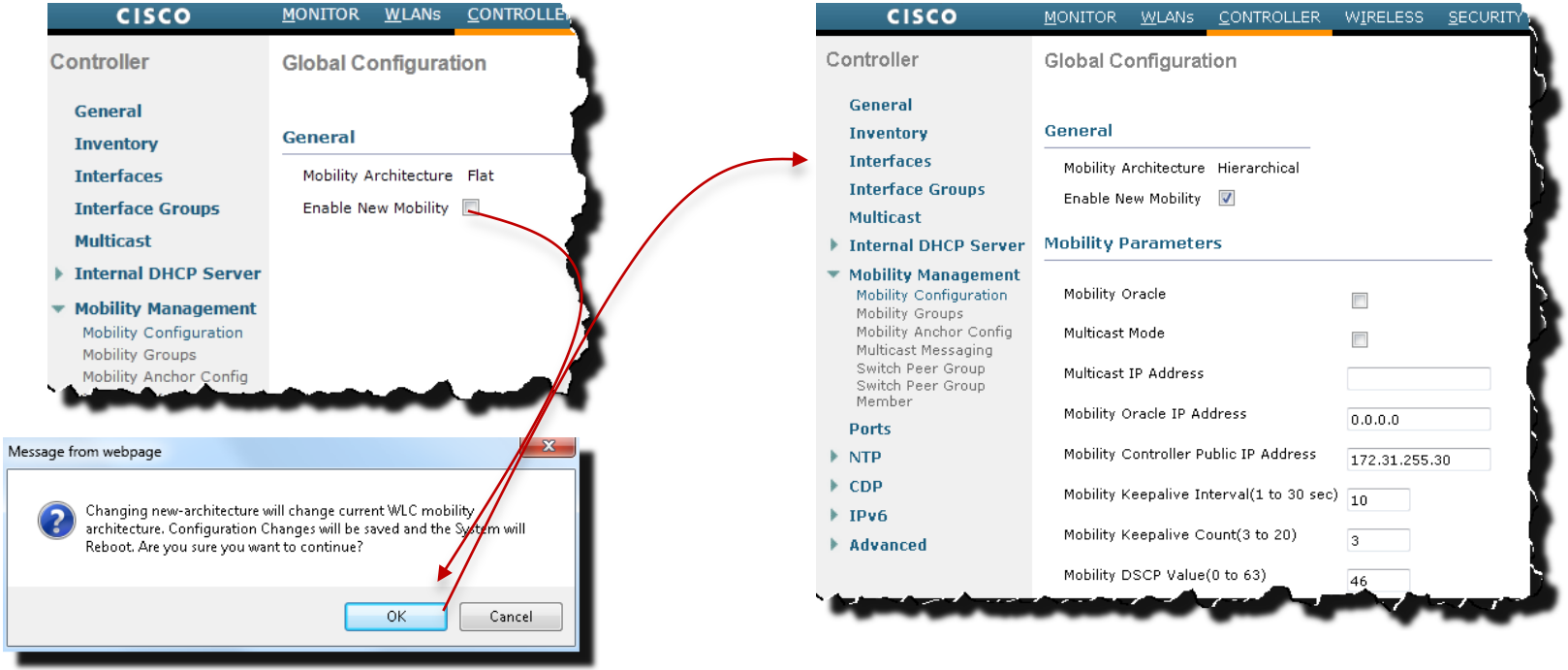
New Mobility and MC Support



- New mobility enables client to roam across AireOS and IOS based solutions in Central as well as Converged Access mode
- Client cannot roam across AireOS WLC1 configured with old mobility and another AireOS WLC2 configured with new mobility
- UA FCS - 5508 & WiSM2 can operate on 7.5/7.6 & 7.3.112

New Mobility Configuration

- You have to change your mobility mode from Flat to Hierarchical



Agenda

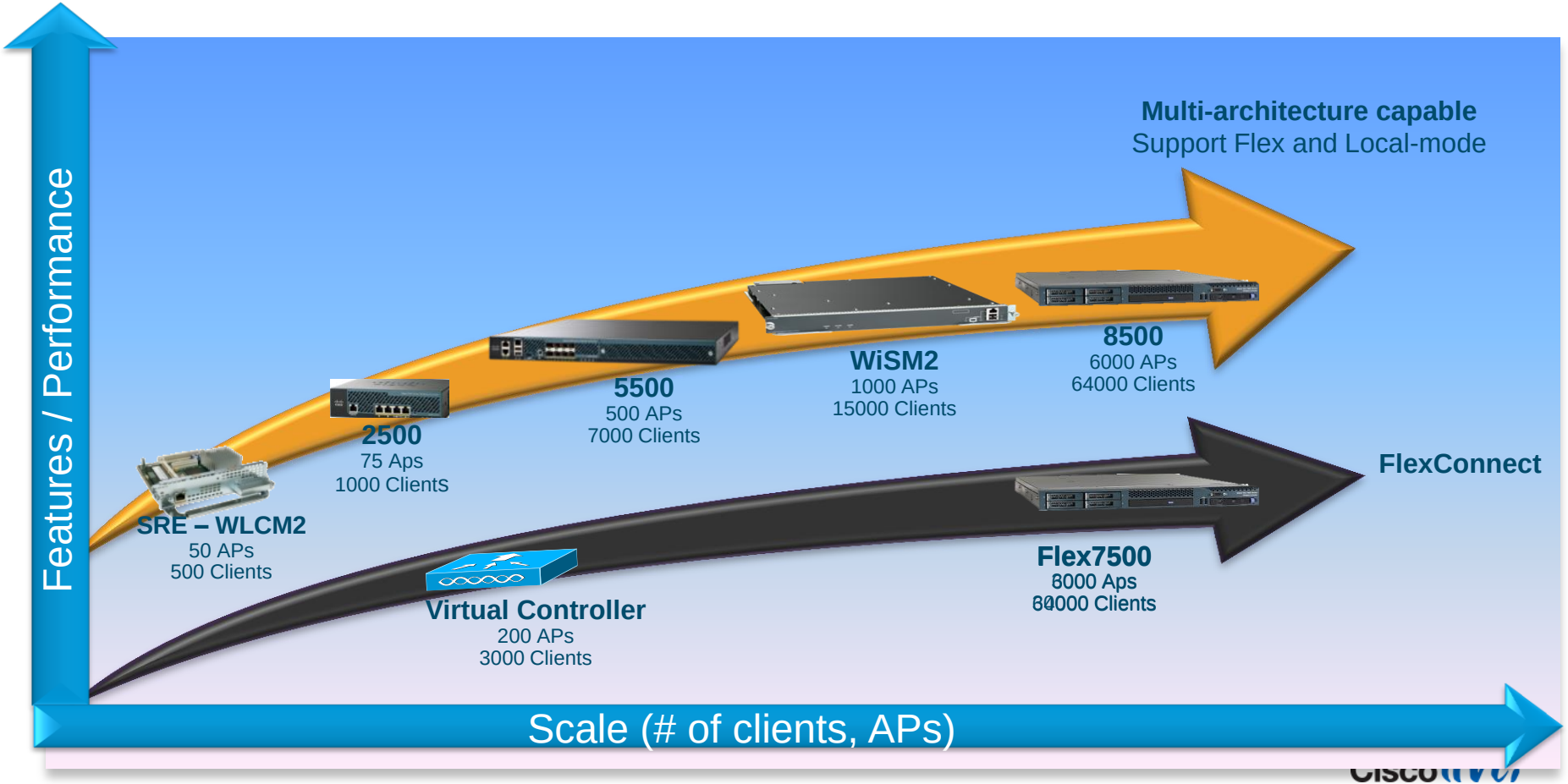
- Controller-Based Architecture Overview
- Mobility in the Cisco Unified WLAN Architecture
- Architecture Building Blocks
- Deploying the Cisco Unified Wireless Architecture

CUWN Release - Key Controller Features

Unified Access – WLAN Infrastructure

	May 2012	Sep 2012	Dec 2012	May 2013
s/w release	7.2MR1	7.3	7.4	7.5
	Outdoor AP Internal Antenna	AP 2600 802.11n G2	AP1600 802.11n G2	AP3600 11ac module
		Outdoor AP Uni Band Antenna	AP3600 Security Module	AP 700
	Outdoor AP Honeywell integration	WLC 8500 Target customer - SP	Application visibility and control (AVC)	OEAP 600 Split Tunnelling
		Virtual Controller	Bonjour Services Directory Phase 1	Profiling and Policy on WLC
	802.11r L2 Fast Roaming	Scale Flex7500 6K APs	AP neighbor list (Subset of 802.11k)	Guest Anchor on WLC8500
		Controller Resiliency- AP SSO HA Licensing	Scale WLC 2500	Controller Resiliency Client SSO Over any L2
	ISE - Flex integration Flex / Local Mode parity with ISE	FlexConnect Split Tunnelling	HA Licensing, N:1	Bonjour Services Directory Phase 2
		802.11r – Flex Modes	802.11w (local mode) Protected Mgmt Frame	
		Bi-directional rate-limiting	LAG on Flex7500, WLC 8500, WLC 2500	FlexConnect Additions: PEAP / EAP-TLS AAA ACL and QoS 802.11w
	Local and FlexConnect support on RAP	Voice/Video: 11n CAC		
		PMIPv6 on WLC	Guest Anchor on WLC2500	N+1 Redundancy with WLC2504

Controller Product Portfolio



Roadmap is highly confidential and reflects current plan. Subject to change without notice

Cisco Aironet 3700 Access Point Series

Best-in-Class 802.11ac

New (7.6)

- Industry's first 4x4 MIMO:3 SS 802.11ac AP
- 3X performance of 802.11n 5Ghz WiFi
  - higher performance at a greater distance
- RF Excellence enabled in hardware
- High Density Experience Technology
  - Client density scale and performance
- Future proof,
  - Modular Architecture = investment protection
  - Security, 3G Small Cell or Wave 2 802.11ac module options

Cisco Aironet Indoor Access Point

Industry's Best 802.11n and 802.11ac Series

Mission Specific
600 & 700

NEW

- Up to 600 Mbps
- 702w: Wall Plate AP
  - Dorms, hospitality
- 702i: Compact Mid-market AP
- 600: Teleworker

Enterprise Class
1600

- Up to 600 Mbps
- CleanAir Express*
- ClientLink 2.0
- VideoStream

Mission Critical
2600

- Up to 900 Mbps
- High Client Scalability
- CleanAir
- ClientLink 2.0
- VideoStream

Best in Class
3700

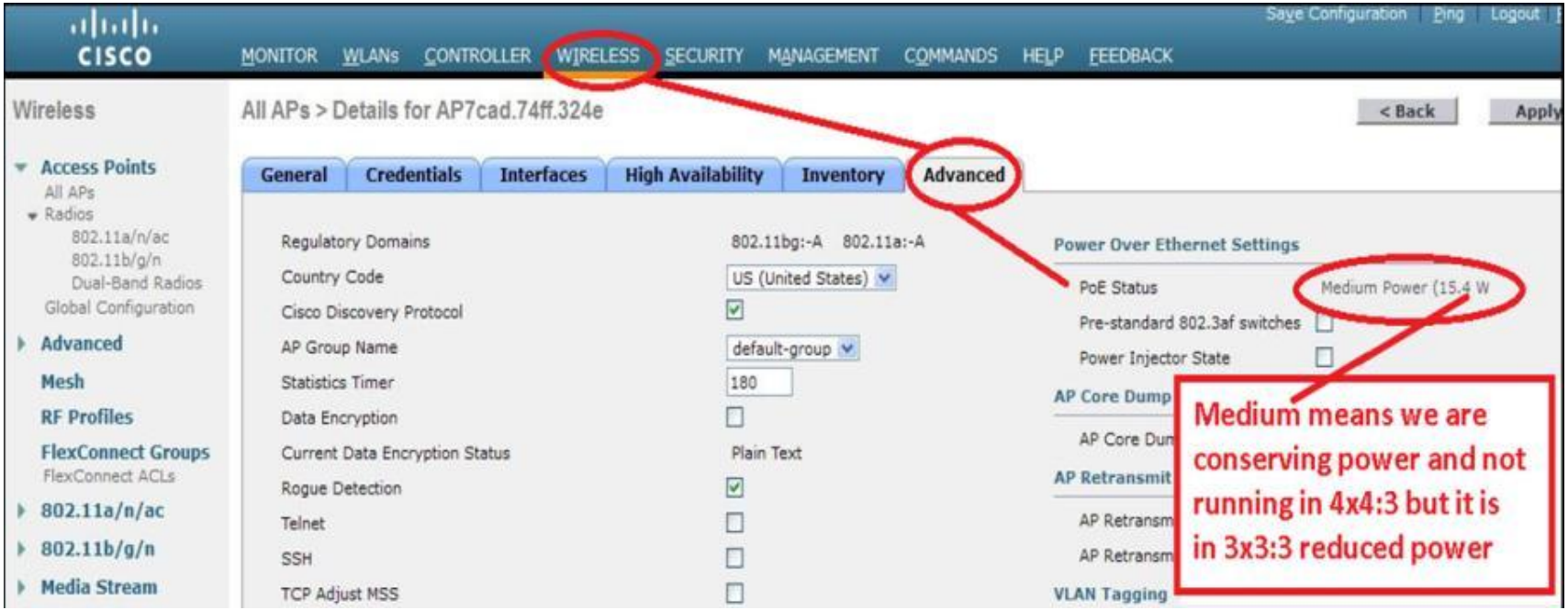
NEW

- Over 1 Gbps, 802.11ac support
- High Density Experience
- CleanAir 80 MHz, ClientLink 3.0, VideoStream
- Future proof modularity: Security, 3G Small Cell or Wave 2 802.11ac

Value-Based → Enterprise → Mission Critical → Best In Class

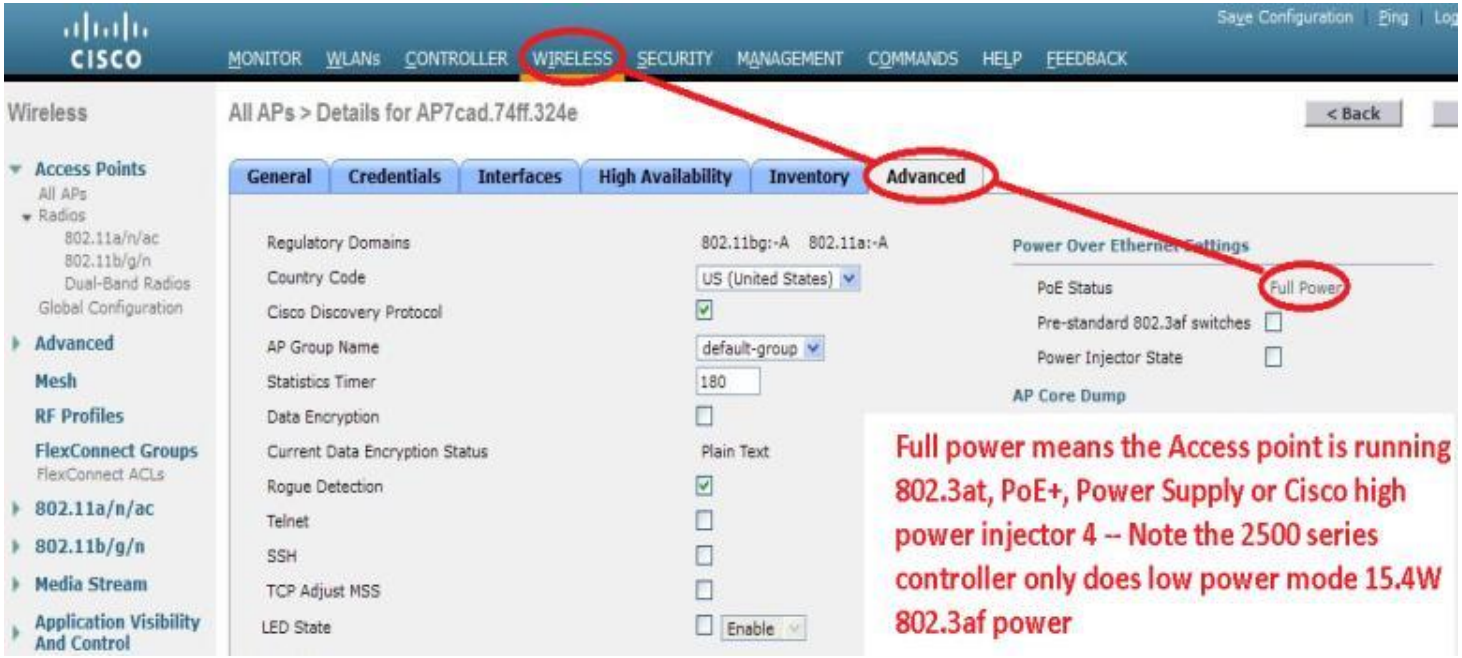
Understanding PoE with AP-3700 using 15.4W (802.3af)

- AP3700 supports full 3x3:3 using the lower 15.4 Watt (802.3af) PoE



Understanding PoE with AP-3700 using PoE+ (802.3at)

- 3700 supports full 4x4:3 using higher power (802.3at), Local Power supply or the AIR-PWRINJ-4 injector

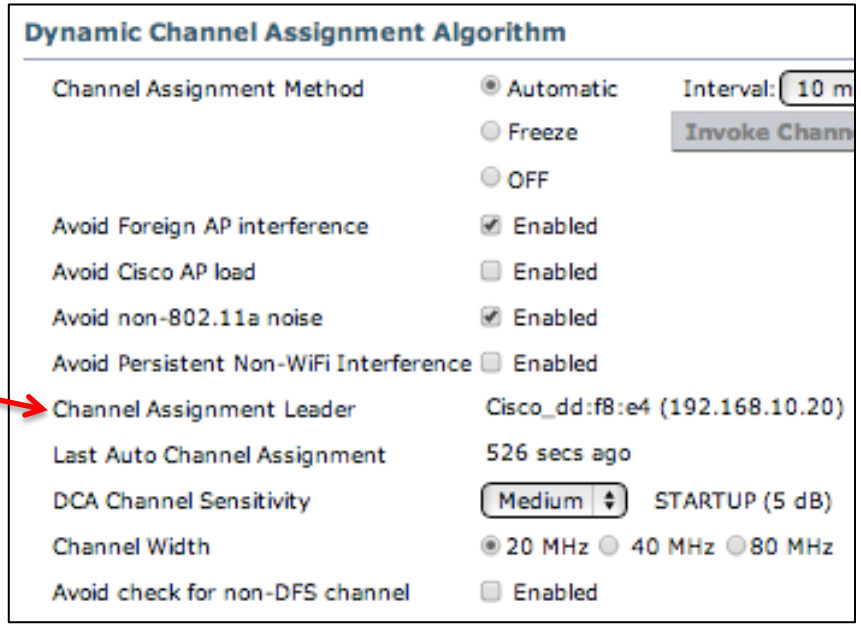


Channel Planning, 802.11ac,and DCA Best Practices

- Do you have spectrum available for 80 Mhz?
  - Evaluate by Regulatory
- Do you use 40 MHz for 802.11n AP's today?
  - If not – why not?
  - Does it make sense to use 80 MHz?
- Plan the Implementation – and understand that this is a major change to your existing spectrum plan
- Let DCA help you

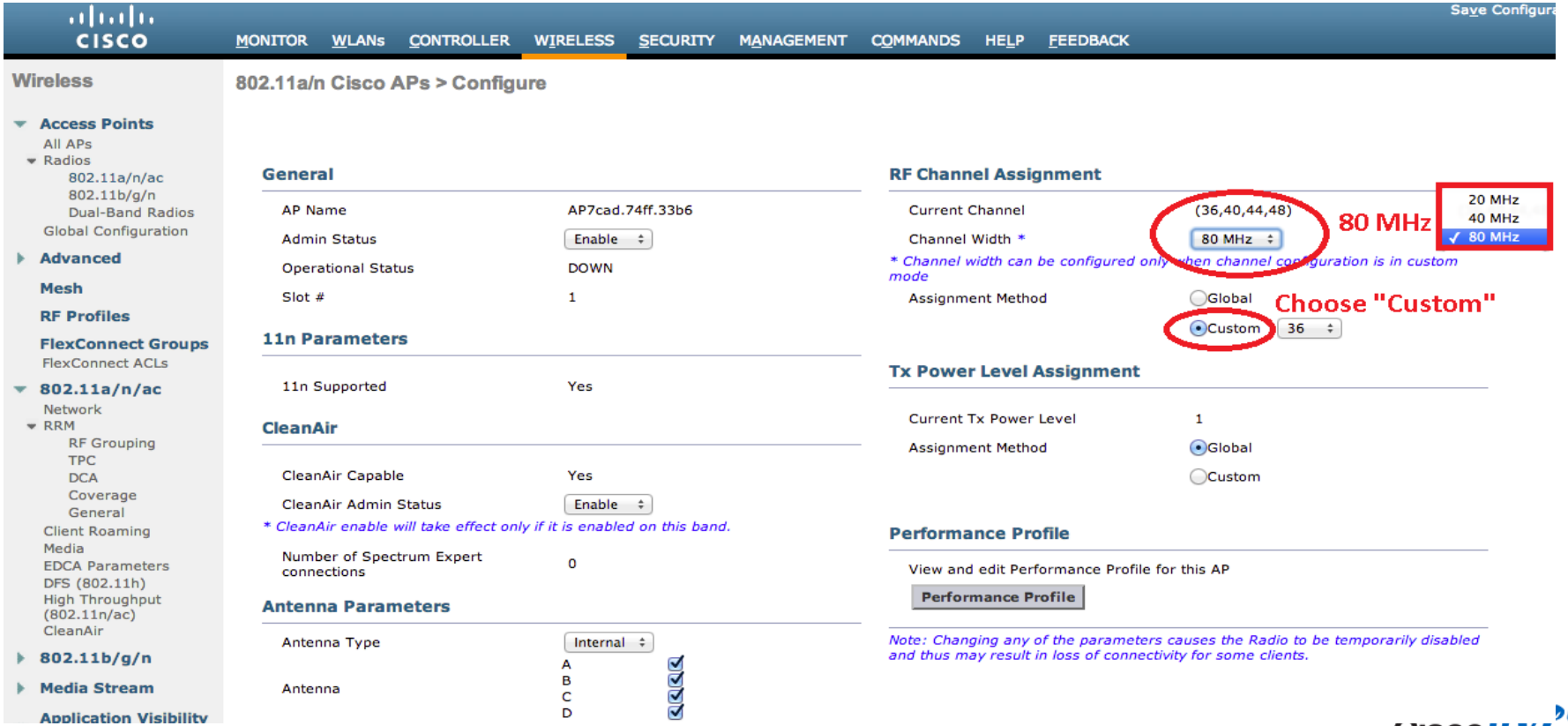
Best Practices for Implementing 802.11ac

- Decide what Channel Width you will use
- Implement new hardware
- Initialise DCA in Startup Mode – FROM the RF group Leader(s)
- Remember – all of this is 5 GHz only!

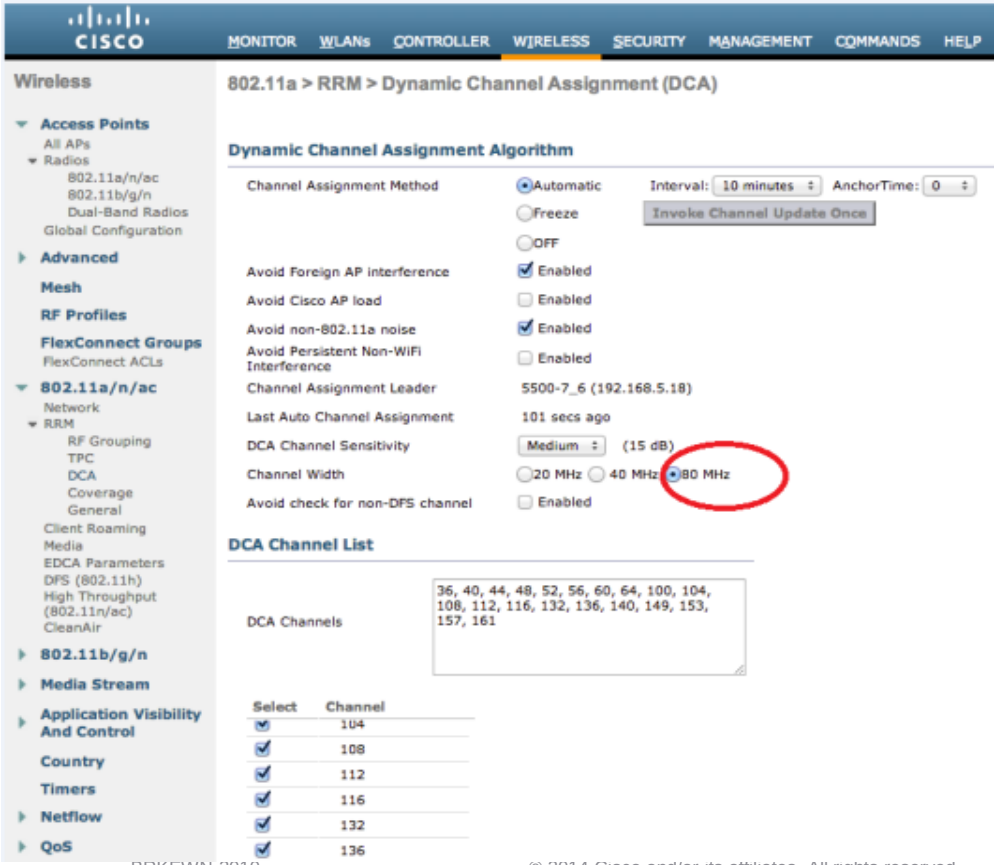


7.3 and above – from the CLI - ***Config 802.11a channel global restart***

AP-3700 Setting 80 MHz (Manually)



AP-3700 (DCA) and RF Grouping



RF Group leader should be configured with 80MHz channel width

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

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

Client Profiling

- ISE offers a rich set of BYOD features: e.g. device identification, onboarding, posture and policy
- Customers who do not deploy ISE but still require some of ISE features directly in WLC:
  - Native profiling of identifying network end devices based on protocols like HTTP, DHCP
  - Device-based policies enforcement per user or per device policy on the network.
  - Statistics based on per user or per device end points and policies applicable per device.

Client Profiling

- WLC-based local policy consists of 2 separate elements.
  - **Profiling** can be based on:
    - *Role* - defining user type or the user group the user belongs to.
    - *Device type* – e.g. Windows, OS_X, iPad, iPhone, Android, etc.
    - *EAP Type* - check what EAP method the client is getting connected to.
  - **Action** is policy that can be enforced after profiling:
    - *VLAN* - override WLAN interface with VLAN id on WLC
    - *QoS level* – override WLAN QoS
    - *ACL* – override with named ACL
    - *Session timeout* – override WLAN session timeout value
    - *Time of day* – policy override based on time of the day, else default to WLAN.
    - 7.5 release contains 88 pre-existing profiles:

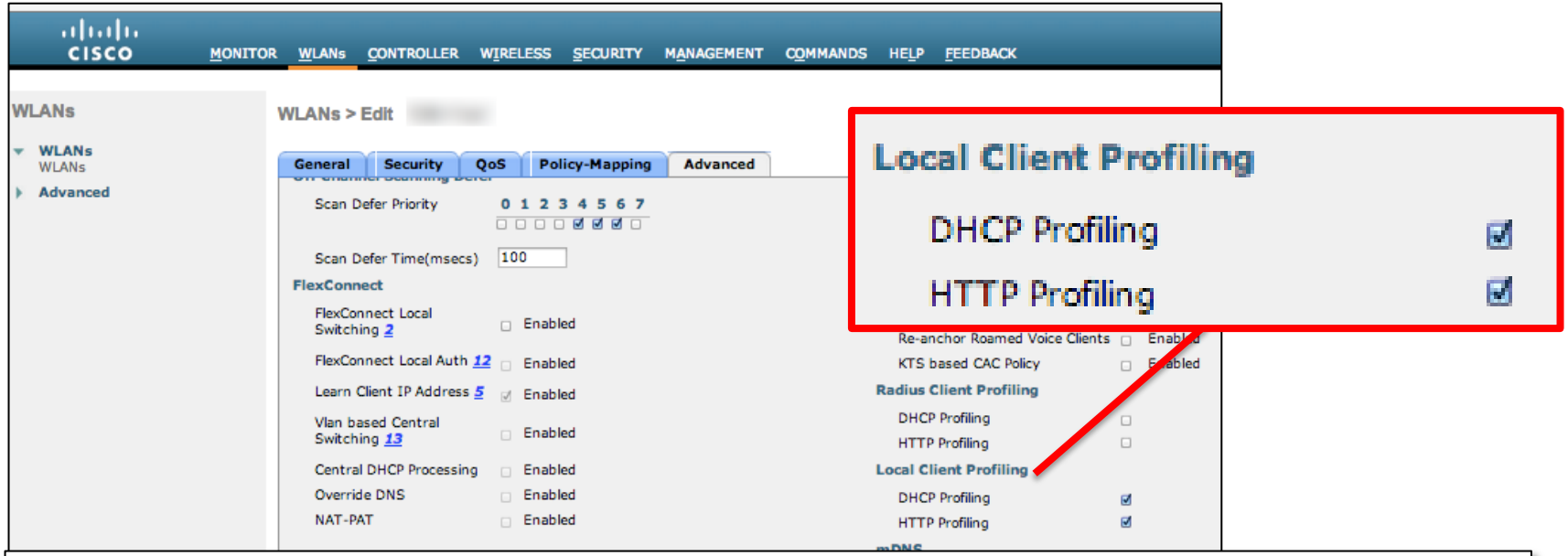
Configuring Client Profiles

- Client profiling uses pre-existing profiles in the controller
  - Custom profiles are not supported in this release
- Wireless clients are profiled based on the MAC OUI, DHCP,HTTP user agent
  - DHCP is required for DHCP profiling, Webauth for HTTP user agent
- 7.5 release contains 88 pre-existing profiles:

```
(Cisco Controller) >show profiling policy summary

Number of Builtin Classification Profiles: 88
ID   Name                                        Parent Min CM Valid
==== ========================================== ====== ====== =====
   0 Android                                                  None      30    Yes
    1 Apple-Device                                             None      10    Yes
    2 Apple-MacBook                                               1      20    Yes
    3 Apple-iPad                                                  1      20    Yes
    4 Apple-iPhone                                                1      20    Yes
     .../...
```

Local Client Profiling Configuration

- At the WLAN level, enable Local Client Profiling (DHCP and HTTP)
  - DHCP required is checked automatically when selecting DHCP profiling

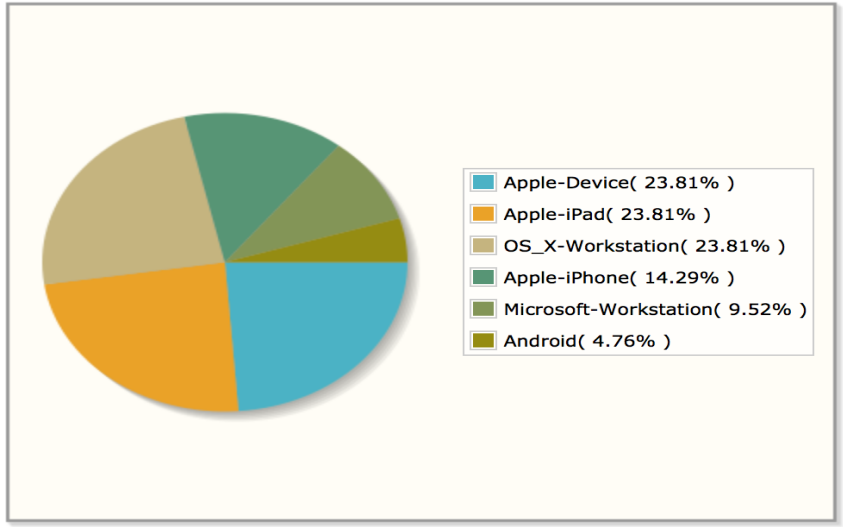



```
config wlan profiling {local | radius} {dhcp | http | all} <wlan ID>
(Cisco Controller) >config wlan profiling local all enable 1
```

Client Profiles in 7.6

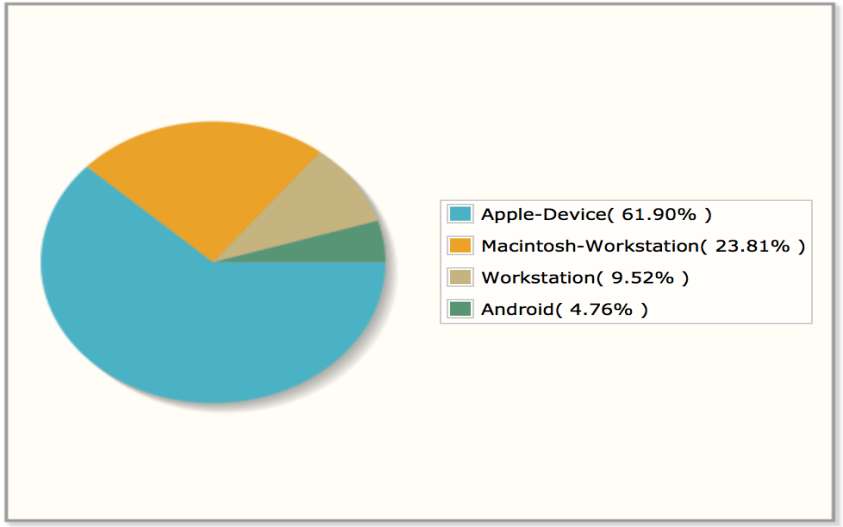
Local Profiling > Device Stats

Device Stats



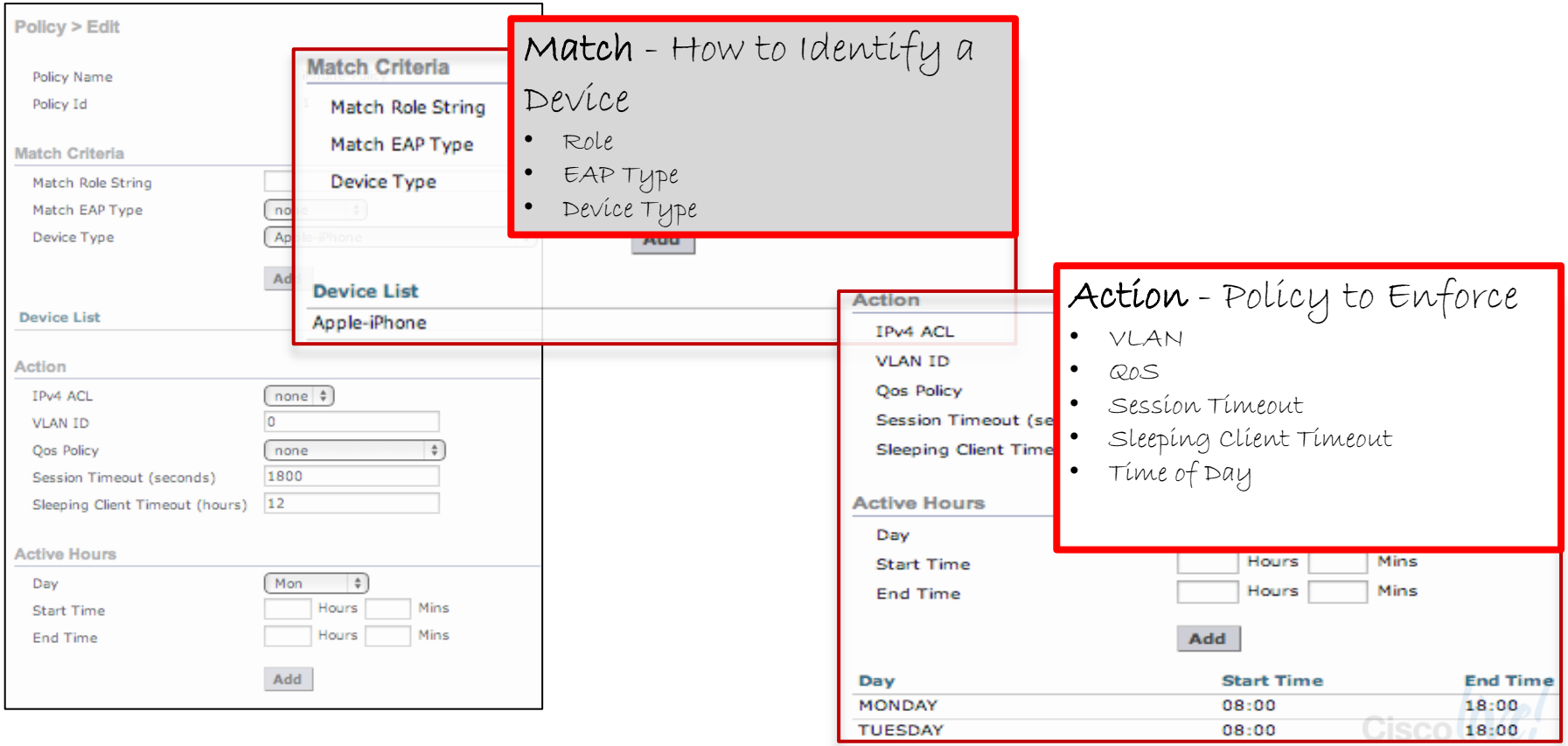
Device Type	Count	(%)
Apple-Device	5	23.81
Apple-iPad	5	23.81
OS_X-Workstation	5	23.81
Apple-iPhone	3	14.29
Microsoft-Workstation	2	9.52
Android	1	4.76

Manufacturer Stats



Manufacturer	Count	(%)
Apple-Device	13	61.90
Macintosh-Workstation	5	23.81
Workstation	2	9.52
Android	1	4.76

Security Local Policies



Match - How to Identify a Device

- Role
- EAP Type
- Device Type

Action - Policy to Enforce

- VLAN
- QoS
- Session Timeout
- Sleeping Client Timeout
- Time of Day

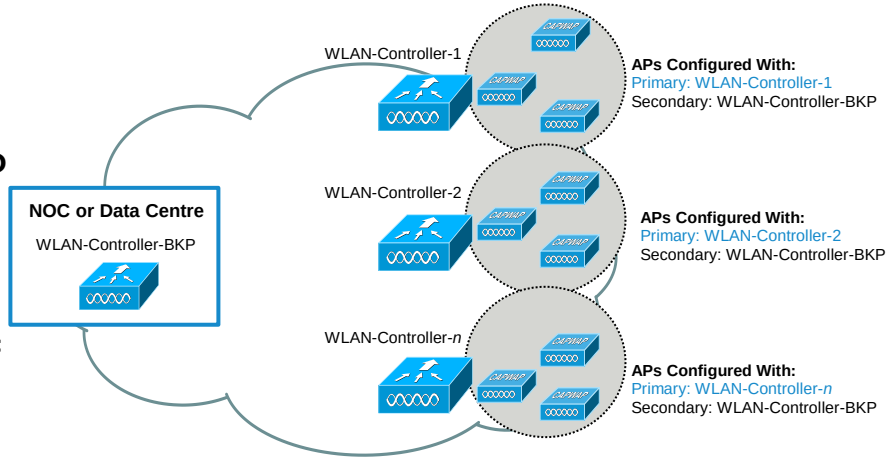
Deploying the Cisco Unified Wireless Architecture

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

Controller Redundancy

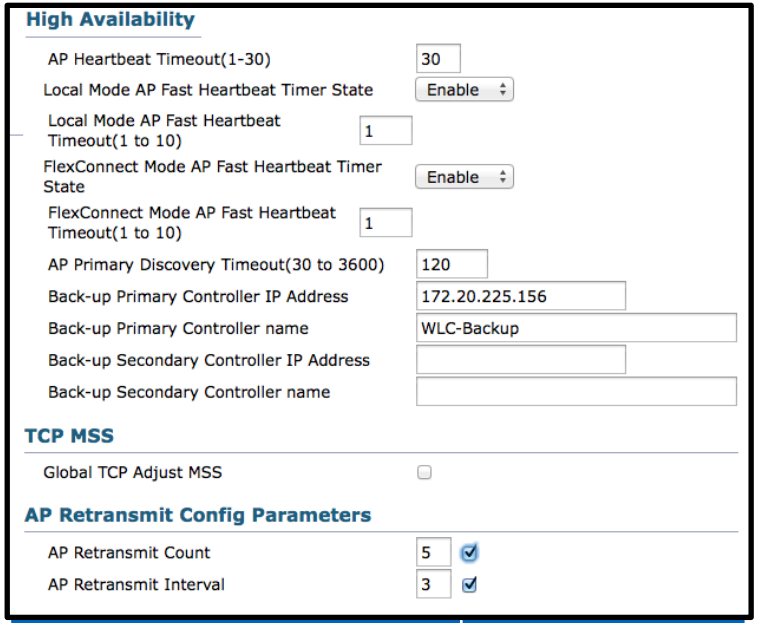
Most Common (N+1)

- 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

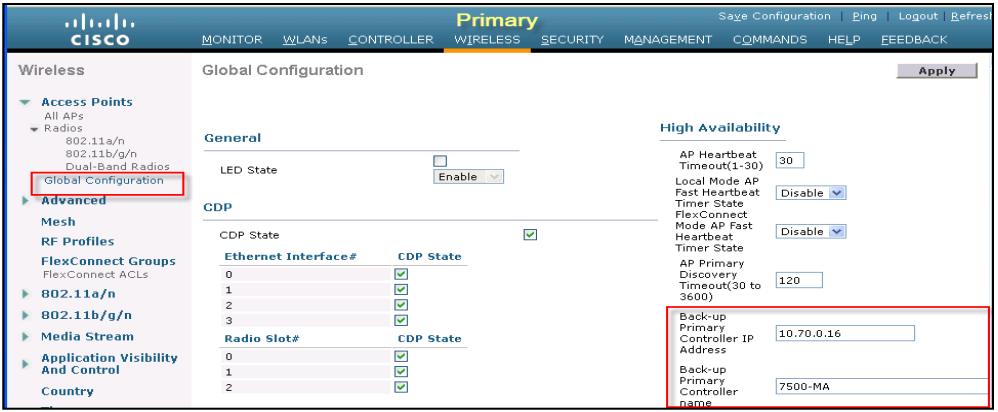
- High Availability Principles :
  - ⇨ AP is registered with a WLC and maintain a backup list of WLC.
  - ⇨ AP use heartbeats to validate WLC connectivity
  - ⇨ AP use Primary Discovery message to validate backup WLC list
  - ⇨ When AP loose 3 heartbeats it start join process to first backup WLC candidate
  - ⇨ 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.

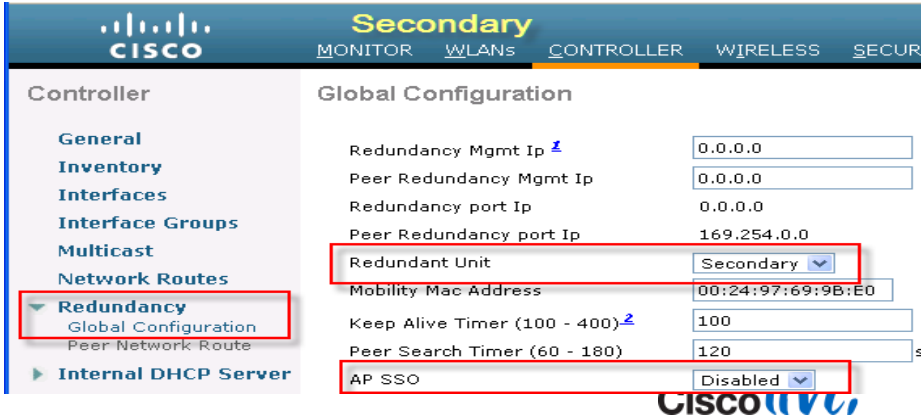


	New Timers 7.2
Heartbeat Timeout	1-30 secs
Fast Heartbeat Timer	1-10 secs
AP Retransmit Interval	2-5 secs
AP Retransmit with FH Enabled	3-8 Times
AP Fallback to next WLC	12 secs

HA-SKU as Secondary WLC - Configuration

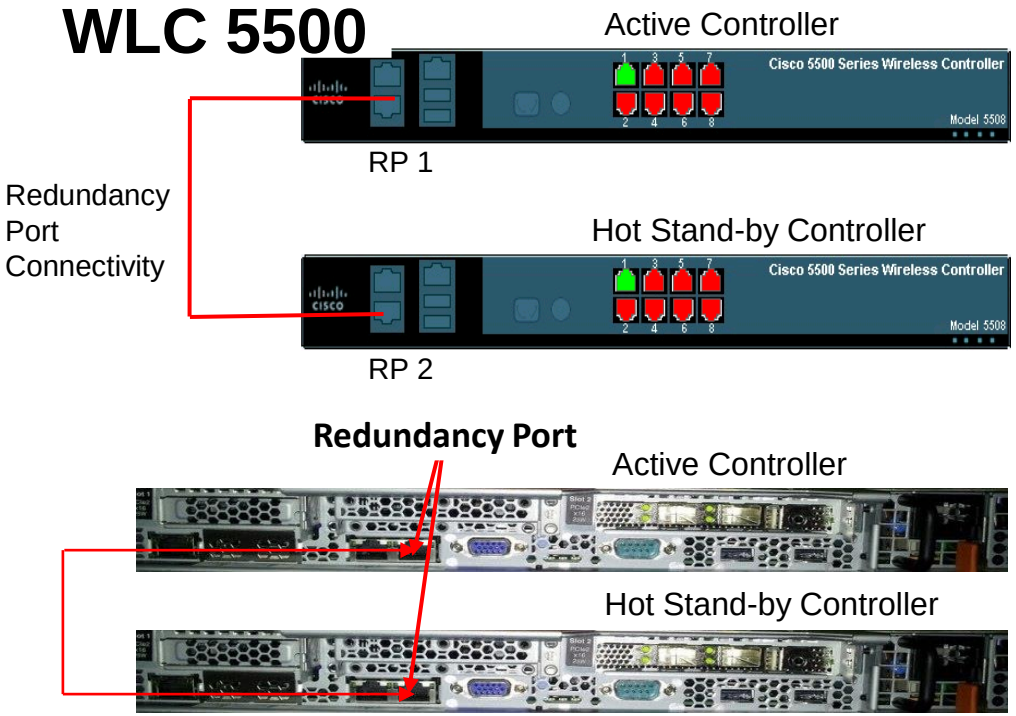
```
(Cisco Controller) >show redundancy summary
 Redundancy Mode = SSO DISABLED
      Local State = ACTIVE
       Peer State = N/A
             Unit = Secondary - HA SKU
          Unit ID = 70:81:05:CE:C8:40
Redundancy State = N/A
    Mobility MAC = 70:81:05:CE:C8:40

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
```





High Availability (AP and Client SSO)

- 5500/7500/8500 WLC have dedicated Redundancy Port which is used to sync 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 (RMI)



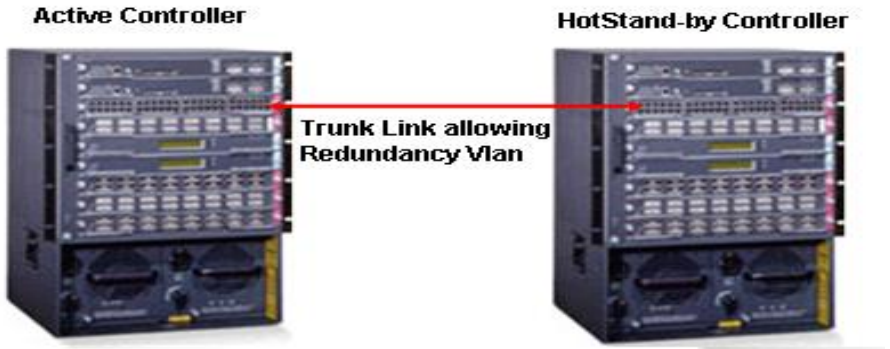
High Availability (AP and Client SSO)

- WiSM-2 WLC have dedicated **Redundancy Vlan** which is used to sync 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 AP SSO Support 7.3/7.4

- Model is 1:1 (Active : Hot-Standby)
- Supported on 5500 / 7500 / 8500 and WiSM-2
- Same hardware and software version
- Two new interfaces
  - Redundancy Port
  - Redundancy Management Interface
- Same management IP on Active and Standby
- Static & dynamic system configurations synced to standby.

- AP information synced to the standby.
  - Synced when AP Joins or it's configuration changes.
  - AP CAPWAP re-join is avoided on switchover.
- Detection time : 5-996 msec for box failover , 3-4 seconds for management gateway failover
- Back-to-back Connectivity on the Redundancy Port between the two WLCs
- Clients are de-authenticated on failover ; forced to re-associate

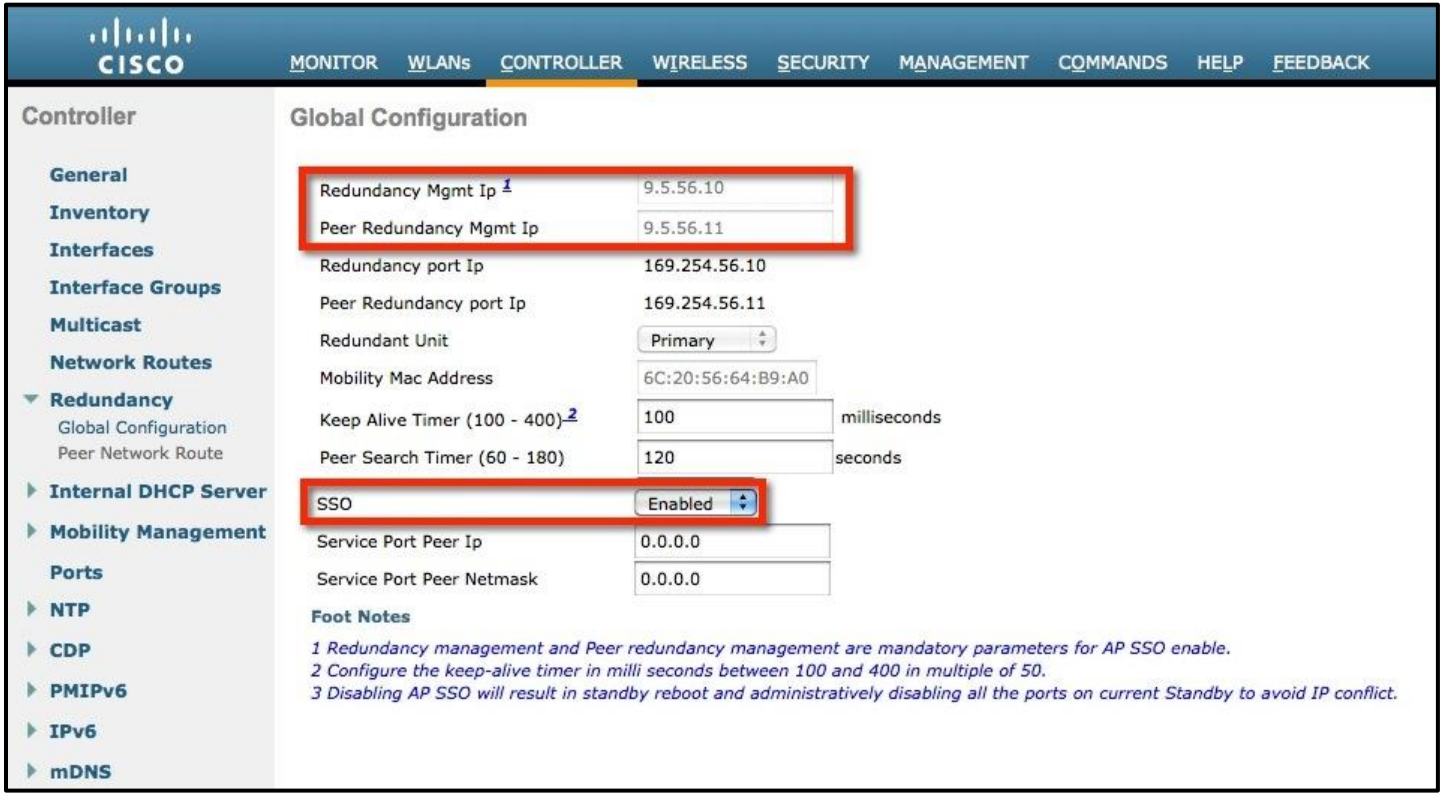
Effective service downtime – Detection time + Switch Over Time (Network recovery/convergence) + Client re-association time

Stateful HA with Client SSO 7.5

- Client's information is synced to the Standby
  - ✓ Client information is synced when client moves to RUN state.
  - ✓ Client re-association is avoided on switch over
- Fully authenticated clients(RUN state) are synced to the peer.
- The intermediate client state events are not synced
- Transient clients are dis-associated after switch over.

Effective service downtime – Detection time + Switch Over Time (Network recovery/convergence)

Web-GUI Configuration

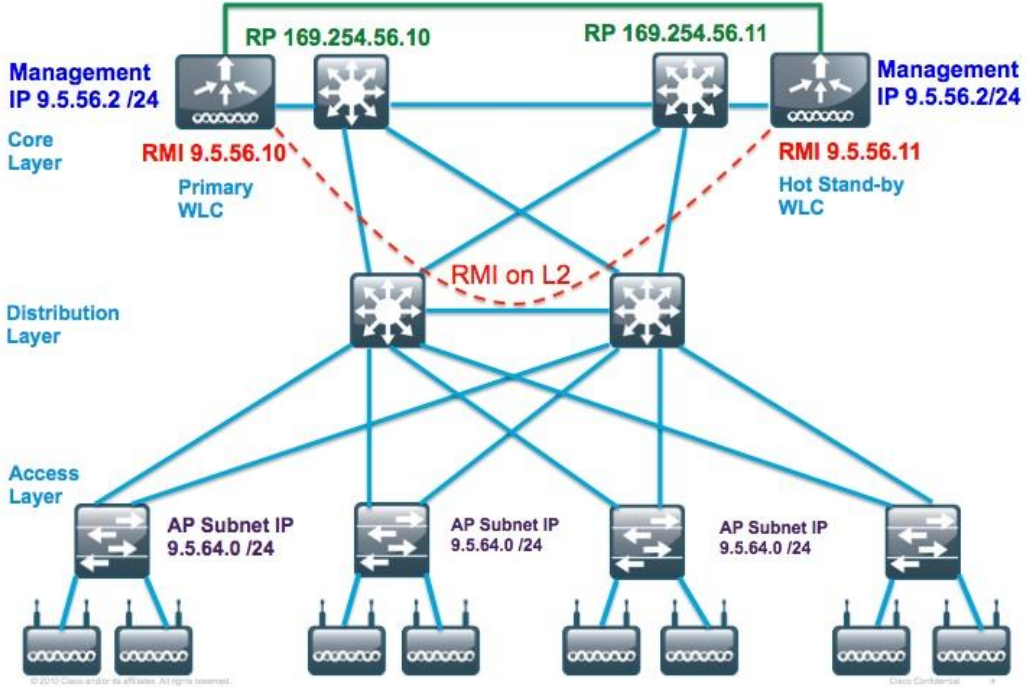


Supported HA Topologies – 7.5

1. Two 5508 , 7500 or 8500 connected via back-to-back RP port in the same Data Centre
2. Two 5508 , 7500 or 8500 connected via RP port over L2 VLAN/fibre in the same or different Data Centre
3. Two 5508, 7500 or 8500 connected to a VSS pair.

1. Two WiSM-2 on the same chassis
2. Two WiSM-2 on different chassis with redundancy VLAN extended over L2 network
3. Two WiSM-2 on different chassis in VSS mode

WLC 5508/7500/8500 Back-to-back RP Connectivity



Management GW is monitored with 12 pings (~15 sec)

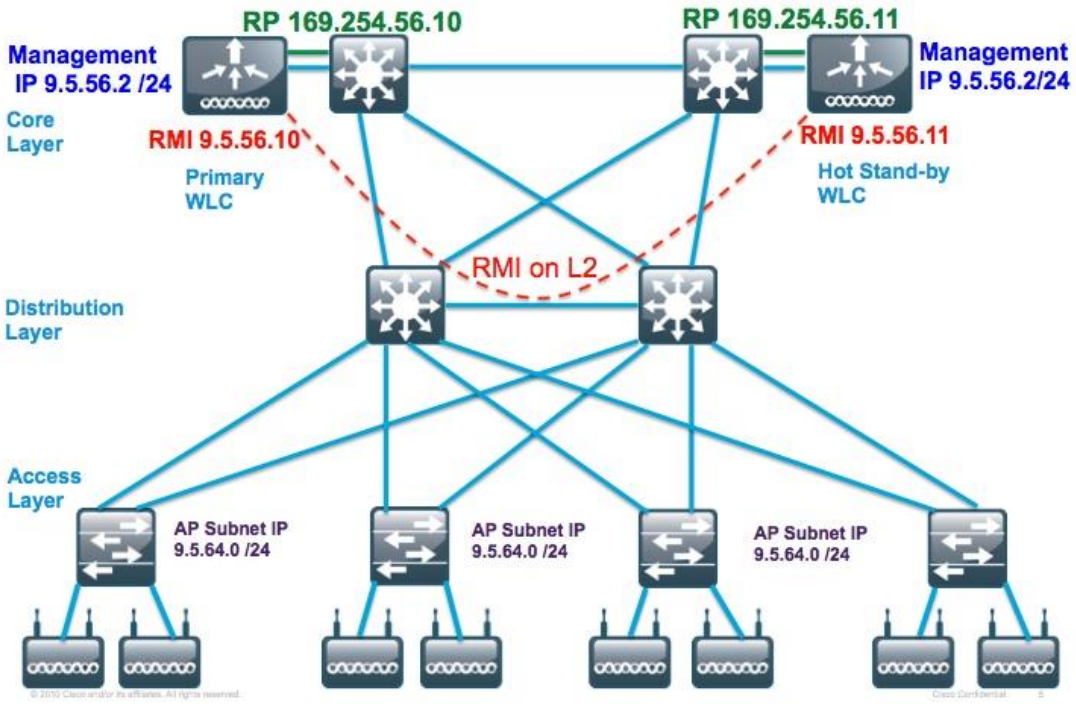
Configuration on Primary WLC:

- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

Configuration on Hot Standby WLC:

- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

WLC 5508/7500/8500 RP Connectivity via Switches



.RTT Latency : 80 ms or less default ; Bandwidth: 60 Mbps or more ; MTU: 1500

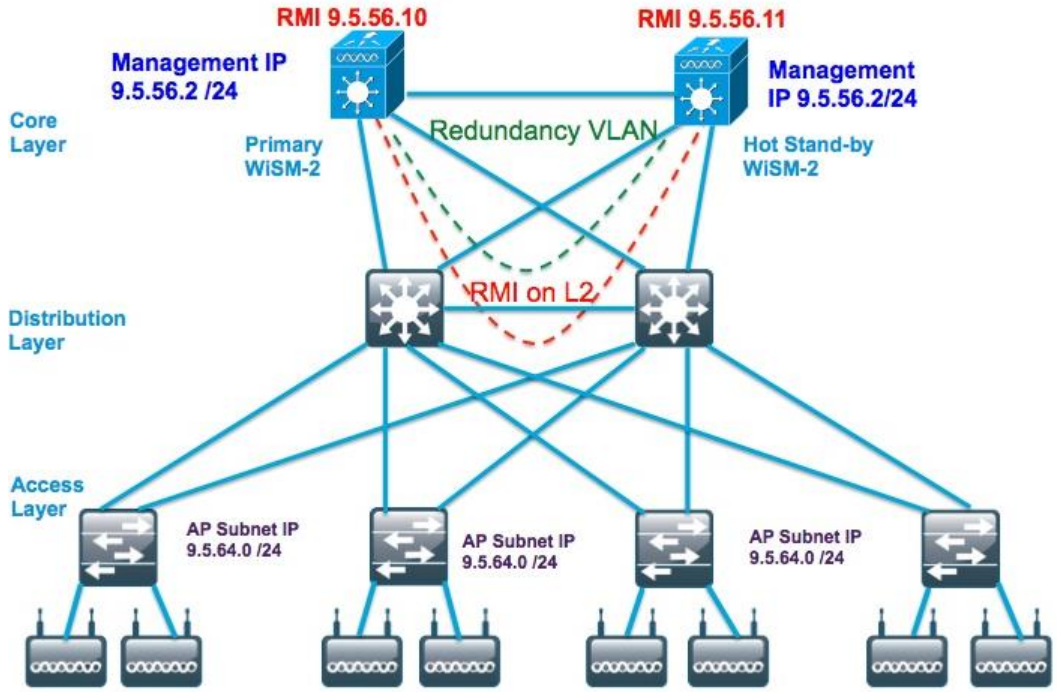
Configuration on Primary WLC:

- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

Configuration on Hot Standby WLC:

- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

WiSM-2 Connectivity Over L2 Redundancy VLAN



Configuration on Cat6k

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)

SSO Behaviour and Recommendations

- RTT latency on Redundancy Link : 80 milliseconds or less. 80% of keepalive timer.
- Preferred MTU on Redundancy Link : 1500 or above.
- Bandwidth on Redundancy Link : 60Mbps or more.

- 5500 / 7500 / 8500 : RP Connectivity between Active and Standby
  - ✓ Via Switches (7.5)
  - ✓ Back-to-back (7.3, 7.4, 7.5)
- WiSM-2 : single 6500 chassis OR different chassis using VSS setup/extending redundancy VLAN.

- Recommended to have Redundancy Link and RMI Connectivity between WLCs on different switches or on different L2 networks
- Keepalive/Peer Discovery timers should be left with default timer values for better performance
- Default box failover detection time is 3 *100 = 300+60 = 360 +jitter (12 msec)= ~400 msec

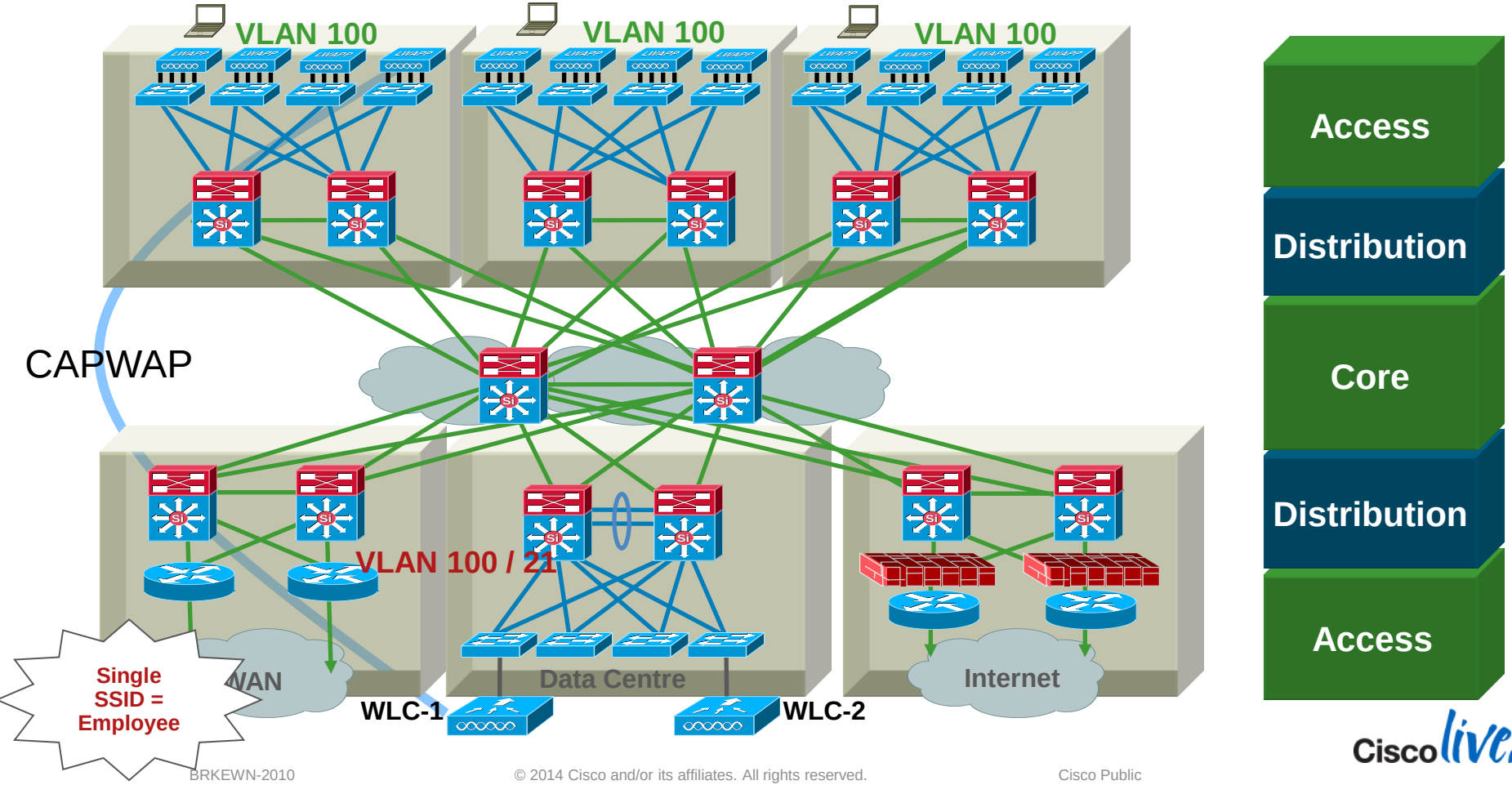
Deploying the Cisco Unified Wireless Architecture

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

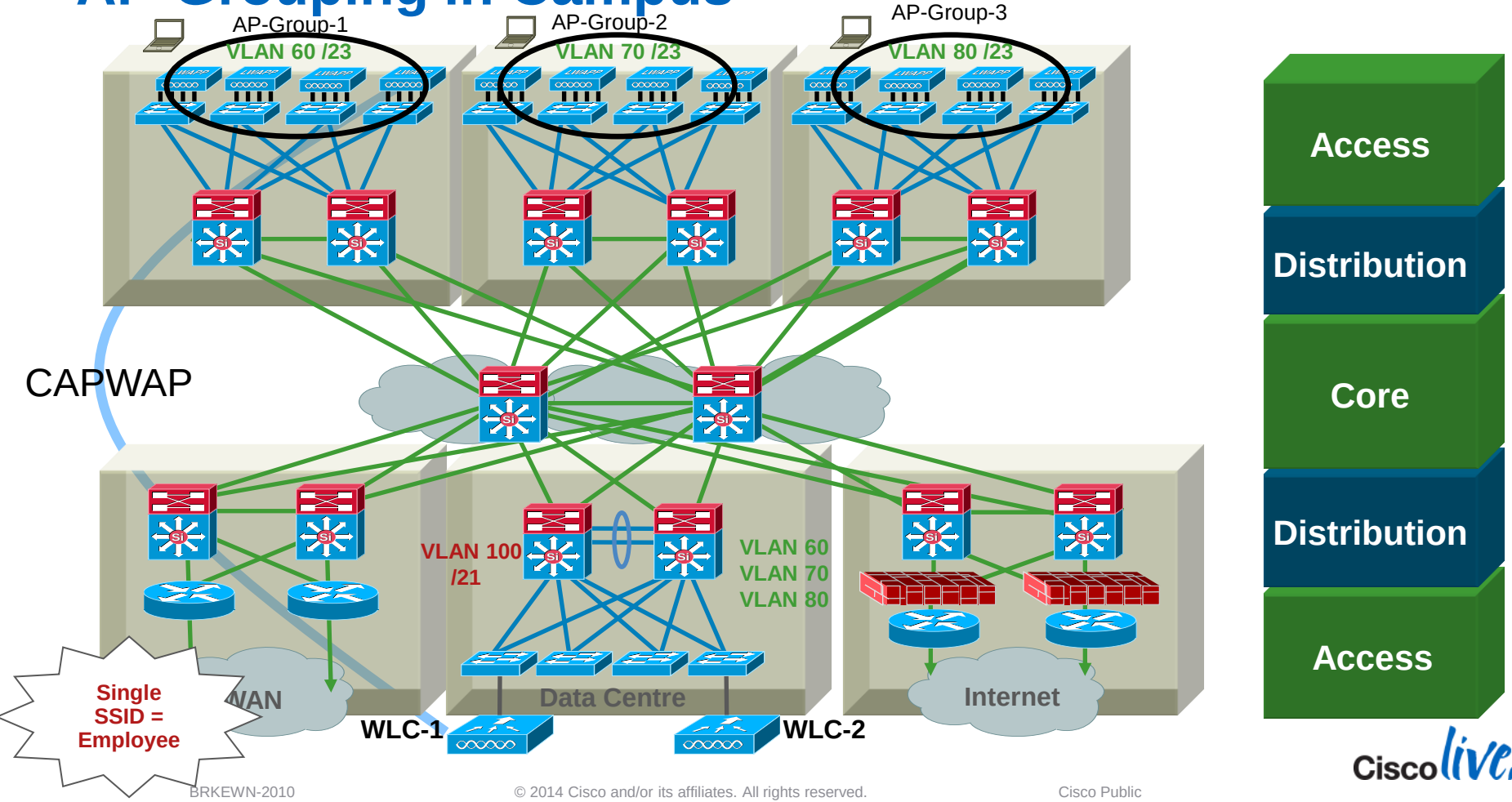
AP-Groups - Default AP-Group

- 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

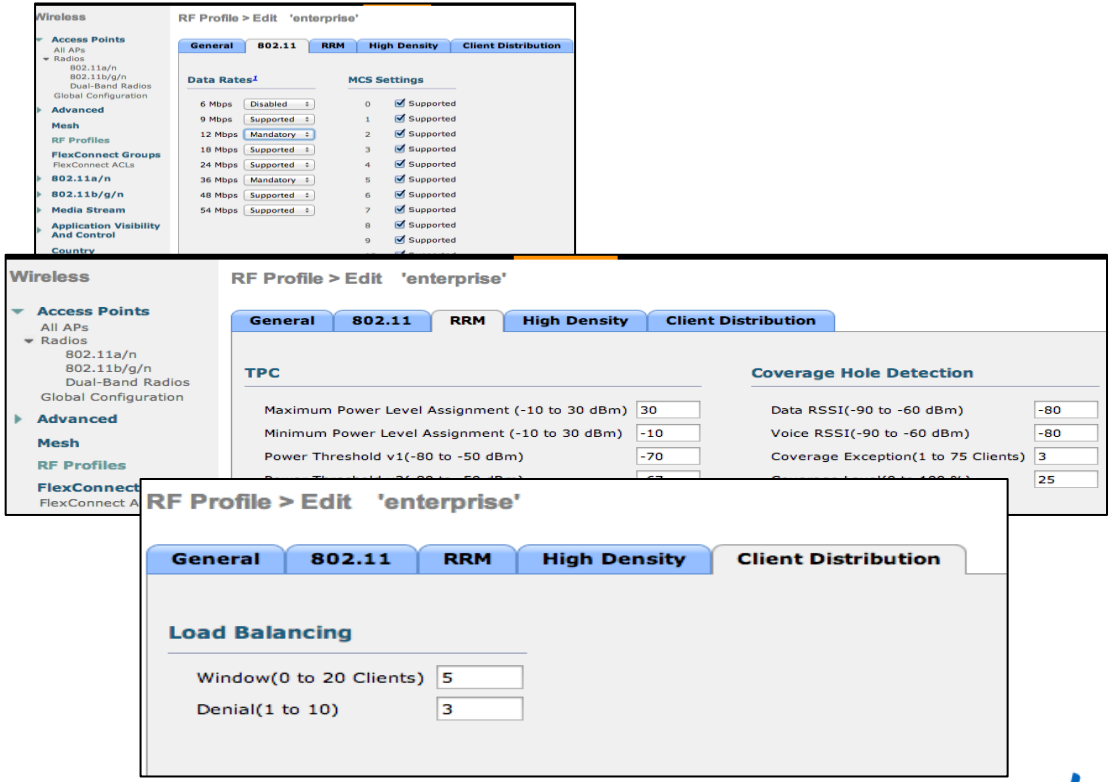
RF-Profiles

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

“Normal” Profile

- A normal profile can be built to match your exact criteria
- You may wish to increase the mandatory data Rate to match your coverage (higher if dense, lower if sparse)
- Change the RRM coverage thresholds to match your exact architecture
- Make a custom load balancing plan that suits the environment



High Density Profile

- For High Density, RF profiles will differ significantly

RF Profile > Edit 'HD_2_4'

General | 802.11 | RRM | High Density | Client Distribution

Data Rates[1]

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Disabled
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Mandatory

MCS Settings

0	Supported
1	Supported
2	Supported
3	Supported
4	Supported
9	Supported
	Supported
	Supported
	Supported
	Supported

Higher "Mandatory data Rate
More Disabled Rates

RF Profile > Edit 'HD_2_4'

General | 802.11 | RRM | High Density | Client Distribution

TPC

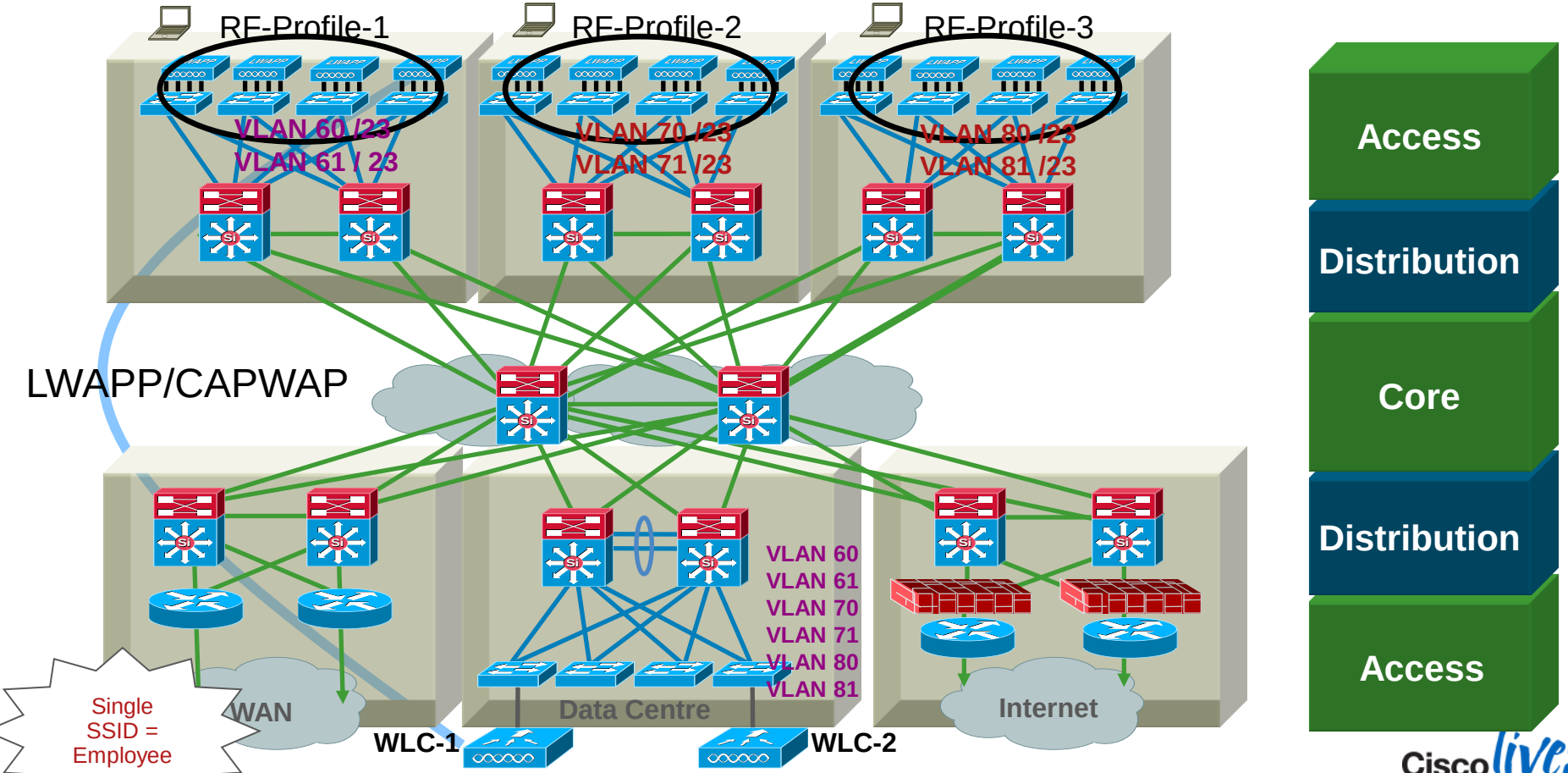
Maximum Power Level Assignment (-10 to 30 dBm)	30
Minimum Power Level Assignment (-10 to 30 dBm)	8
Power Threshold v1(-80 to -50 dBm)	-60
Power Threshold v2(-80 to -50 dBm)	-55

Coverage Hole D

Data RSSI(-90 to	
Voice RSSI(-90 to	
Coverage Exceptio	
Coverage Level(0 to 100 %)	25

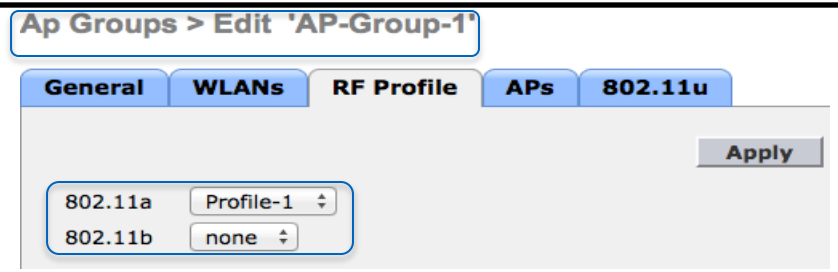
Enforce "Minimum Power"
TPCv1-2 thresholds hotter

RF-Profile in Campus

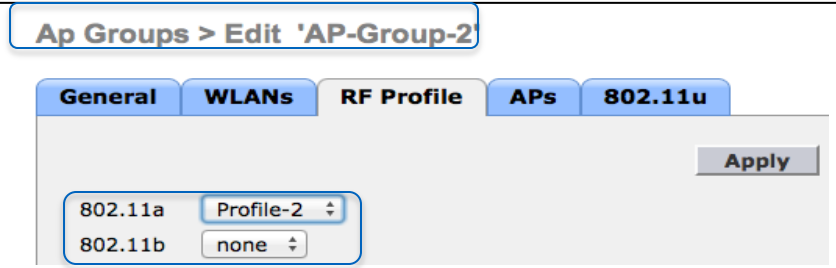


Multiple RF-Profiles

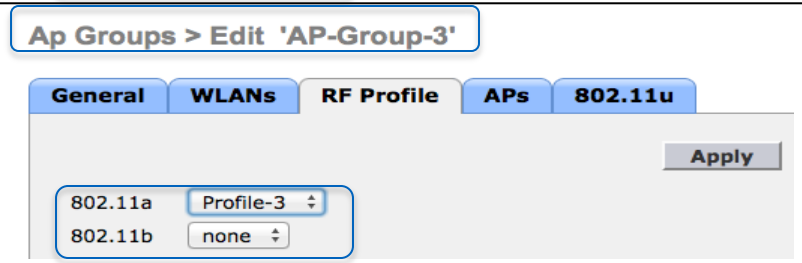
RF Profile -1



RF Profile -2



RF Profile -3

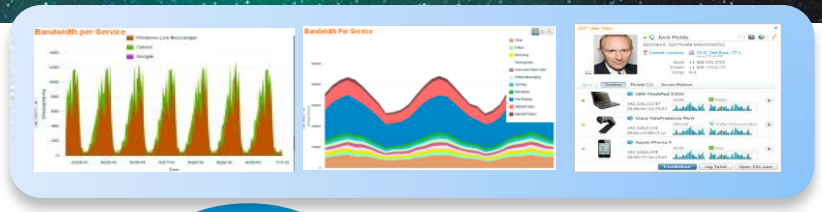


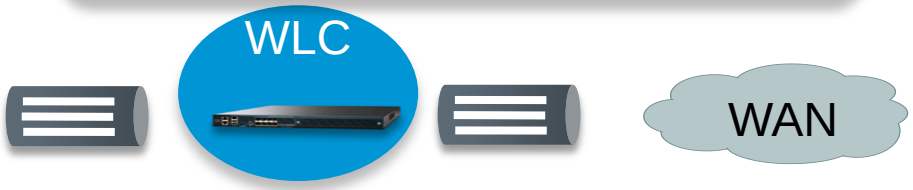
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS 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?

AVC Supported Features

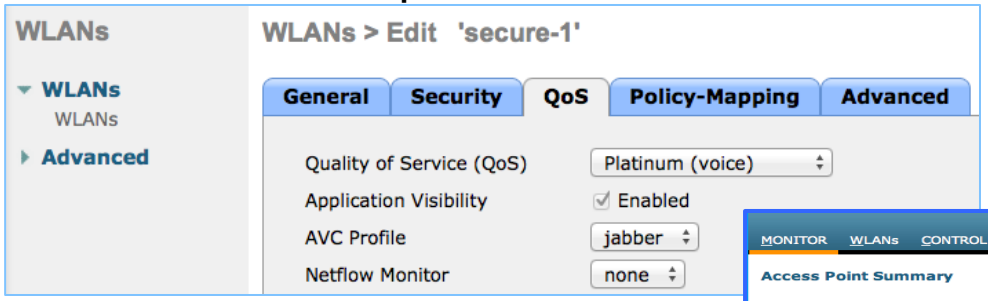
- Classification : Identification of Application/Protocol, supports Stateful L4 - L7 classification. WLC can classify 1039 applications.

- 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).

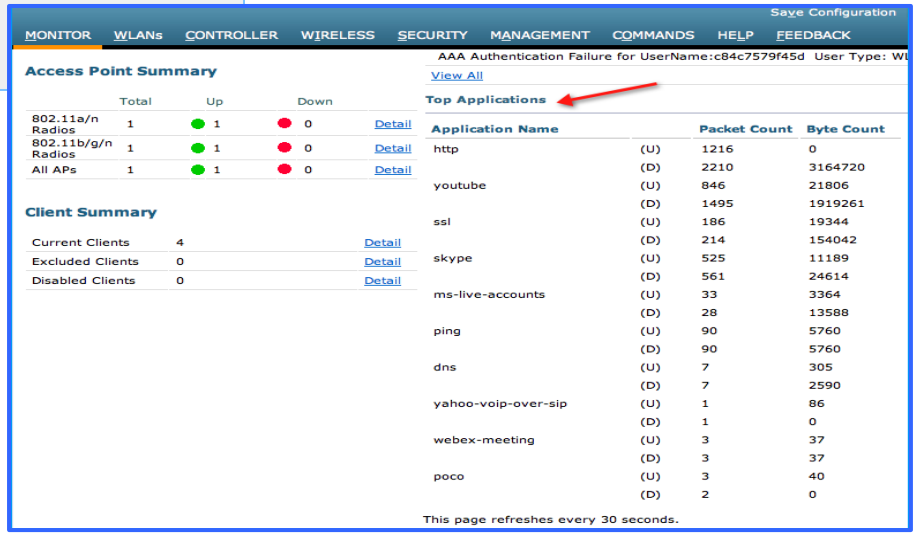
- AVC is supported on 2500, 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs
- WLC can support 16 AVC profiles
- WLAN can support only 1 AVC profile and each profile can contain 32 rules, thus each WLAN can support 32 application actions of mark or drop.

Enabling AVC

- AVC enabled on per WLAN basis

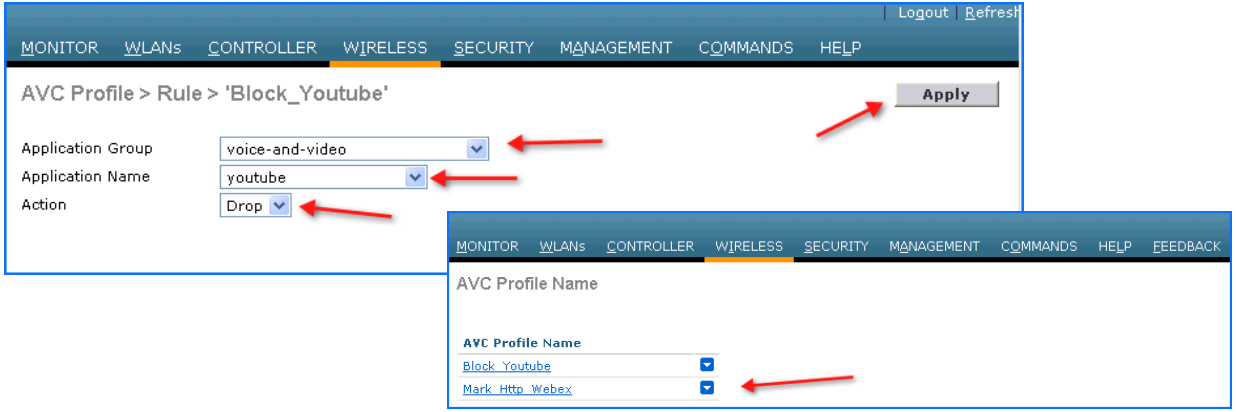


- Global summary of top applications on Controller Monitor screen



AVC Profile

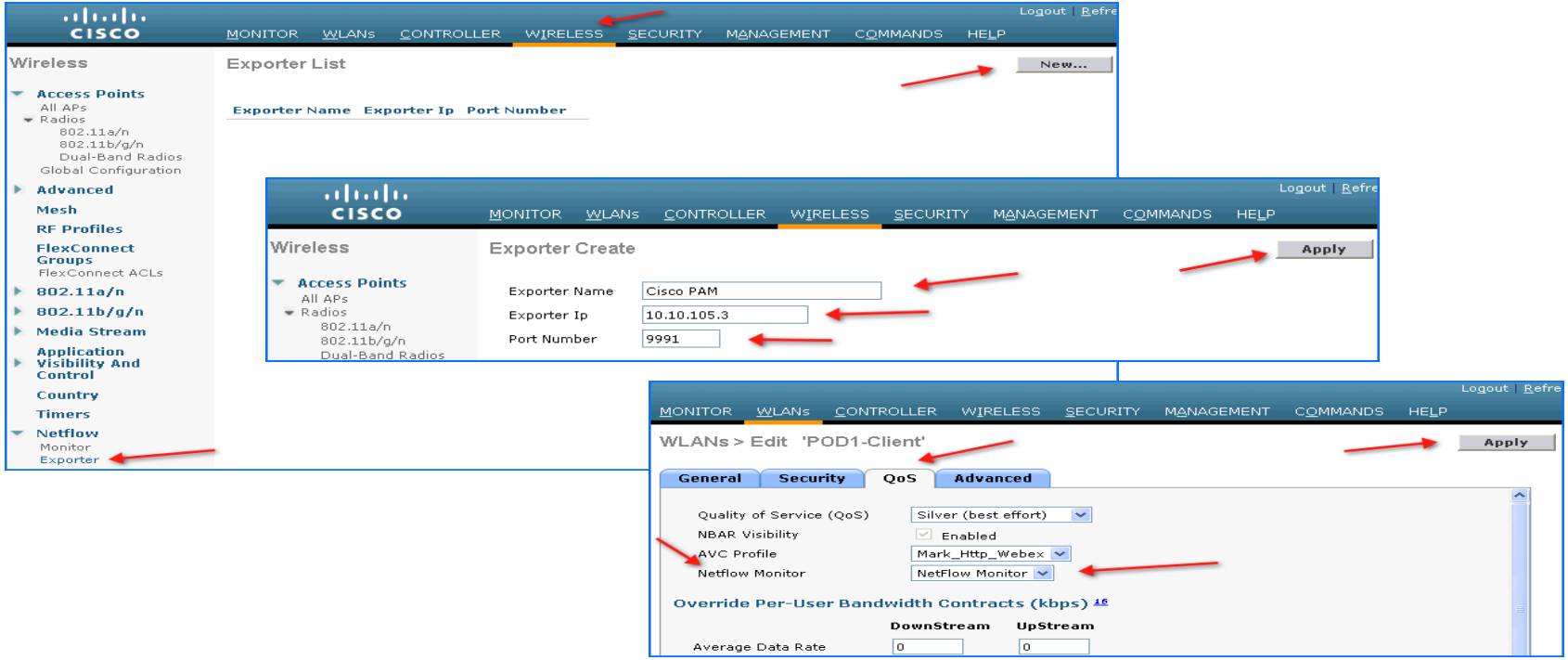
- Custom AVC Profiles created to do traffic shaping



- Apply the custom profile per WLAN

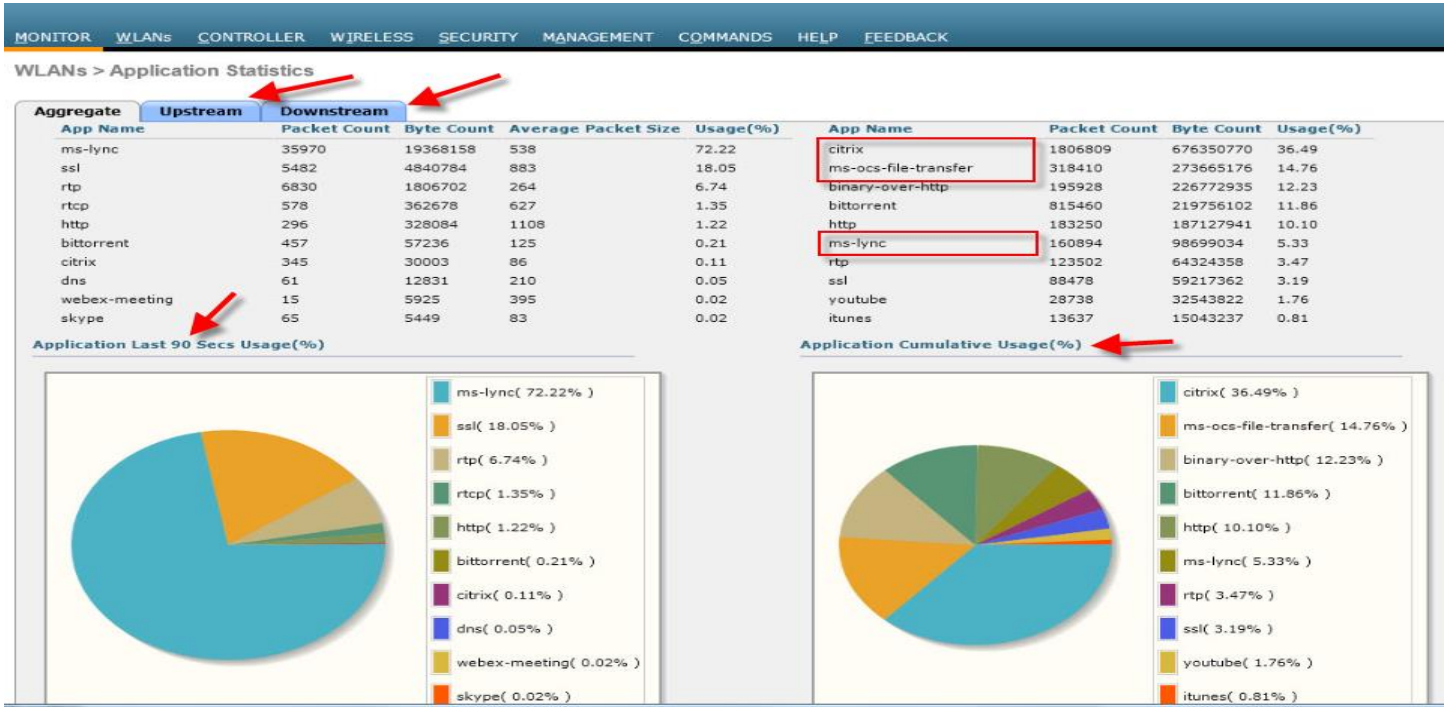
Netflow Monitor

- Configuring Netflow Exporter on the Controller and apply to WLAN



AVC Summary

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



http://technet.microsoft.com/en-us/lync/gg131938.aspx

AVC Client Stats – Microsoft Lync and Jabber

- This shows the current level of Lync Client 2013 identification
- The stats are updated on a 90 second interval.

WLANs > Application Statistics

Aggregate | Upstream | Downstream

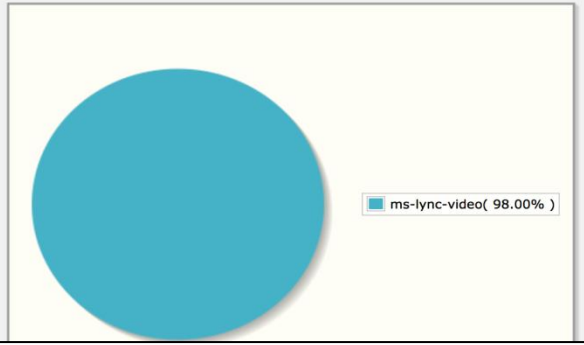
Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage(%)
ms-lync-video	109386	105.79 MB	1014	98.00
ms-lync-audio	10988	1.02 MB	97	0.00
rtcp	588	369.46 KB	643	0.00
google-services	33	12.66 KB	392	0.00
ssl	30	6.16 KB	210	0.00
http	15	5.29 KB	361	0.00
dns	9	1.42 KB	161	0.00

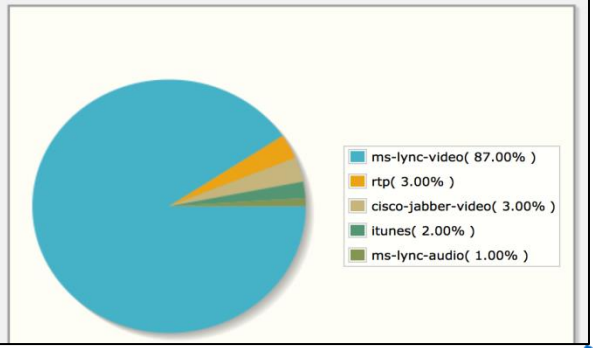
Application Cumulative Stats

App Name	Packet Count	Byte Count	Usage(%)
ms-lync-video	57056370	50.12 GB	87.00
rtp	3839873	1.90 GB	3.00
cisco-jabber-video	3390086	1.90 GB	3.00
itunes	1071447	1.20 GB	2.00
ms-lync-audio	8638938	825.49 MB	1.00
cisco-jabber-audio	5282917	473.11 MB	0.00
rtcp	1369613	318.99 MB	0.00
ms-update	272658	284.79 MB	0.00
http	50764	46.18 MB	0.00
cisco-jabber-control	1266834	44.43 MB	0.00

Application Last 90 Secs Usage(%)



Application Cumulative Usage(%)



http://www.cisco.com/en/US/prod/wireless/wireless_unified_communication.html

Protocol Pack - Compatibility

New (7.5)

- Protocol packs are released for specific NBAR engine versions
  - For example, rel 7.5 WLC has NBAR engine 13, so protocol packs for it are written for engine 13 (pp-adv-asr1k-152-4.S-**13**-3.0.0.pack)
- Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (13 in the example above).
- Therefore:
  - PP 3.0 for version 13 can be loaded on top of version 13 or version 14
  - BUT PP 3.0 for version 14 could not be loaded in engine version 13
  - Loading the wrong version will generate an error
- <u>It is strongly recommended to use the protocol pack that is the exact match for the engine</u>

Deploying the Cisco Unified Wireless Architecture

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

The Protocol Problem

- Why Bonjour services need modifications?

?

?

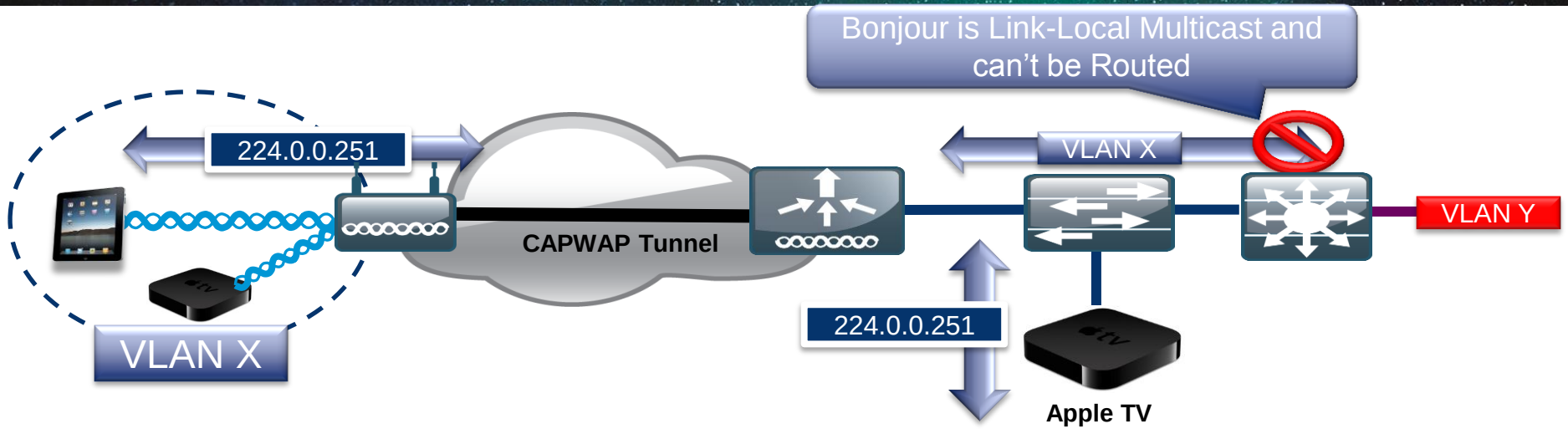
?

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



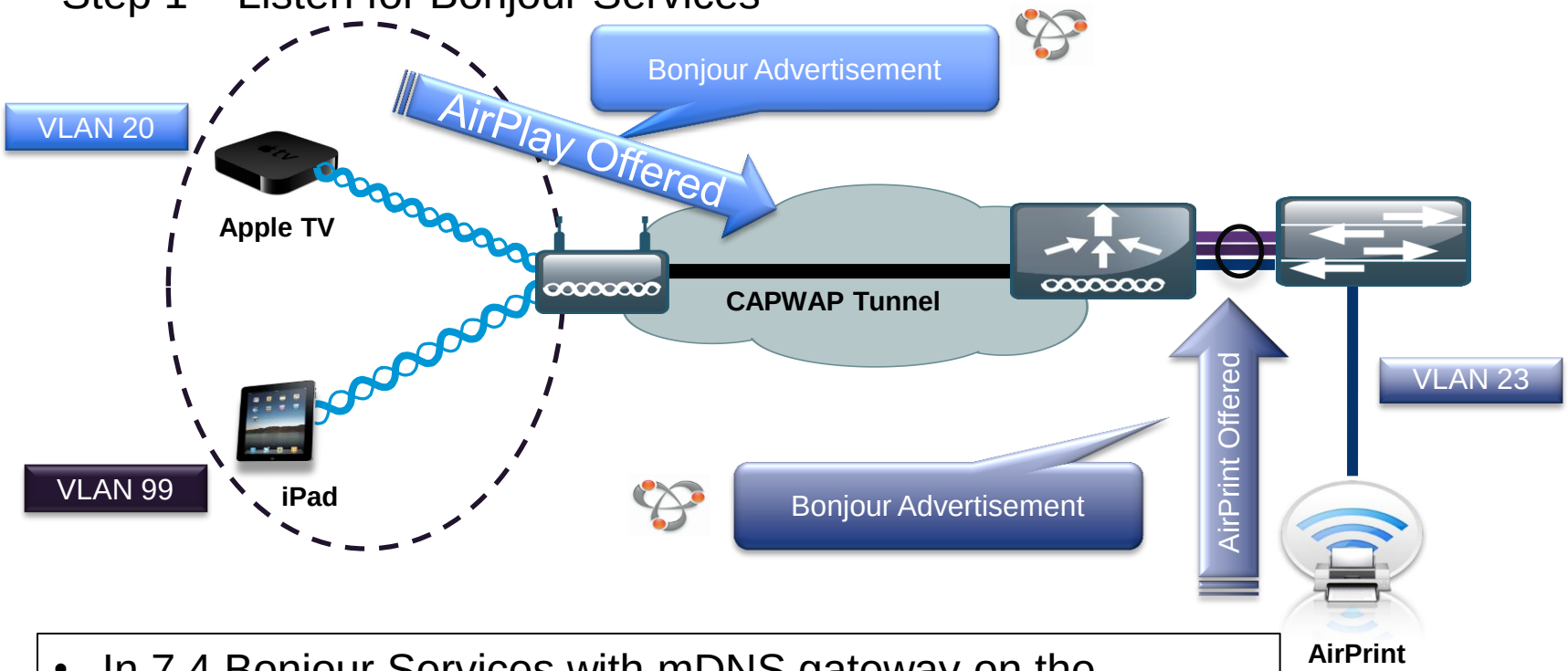
- Bonjour is link local multicast and thus forwarded on Local L2 domain
- AirPlay (Apple TV) and AirPrint supported only on a single VLAN
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:

  IPv4 Group Address – 224.0.0.251

  IPv6 Group Address – FF02::FB

Bonjour mDNS GW on WLC

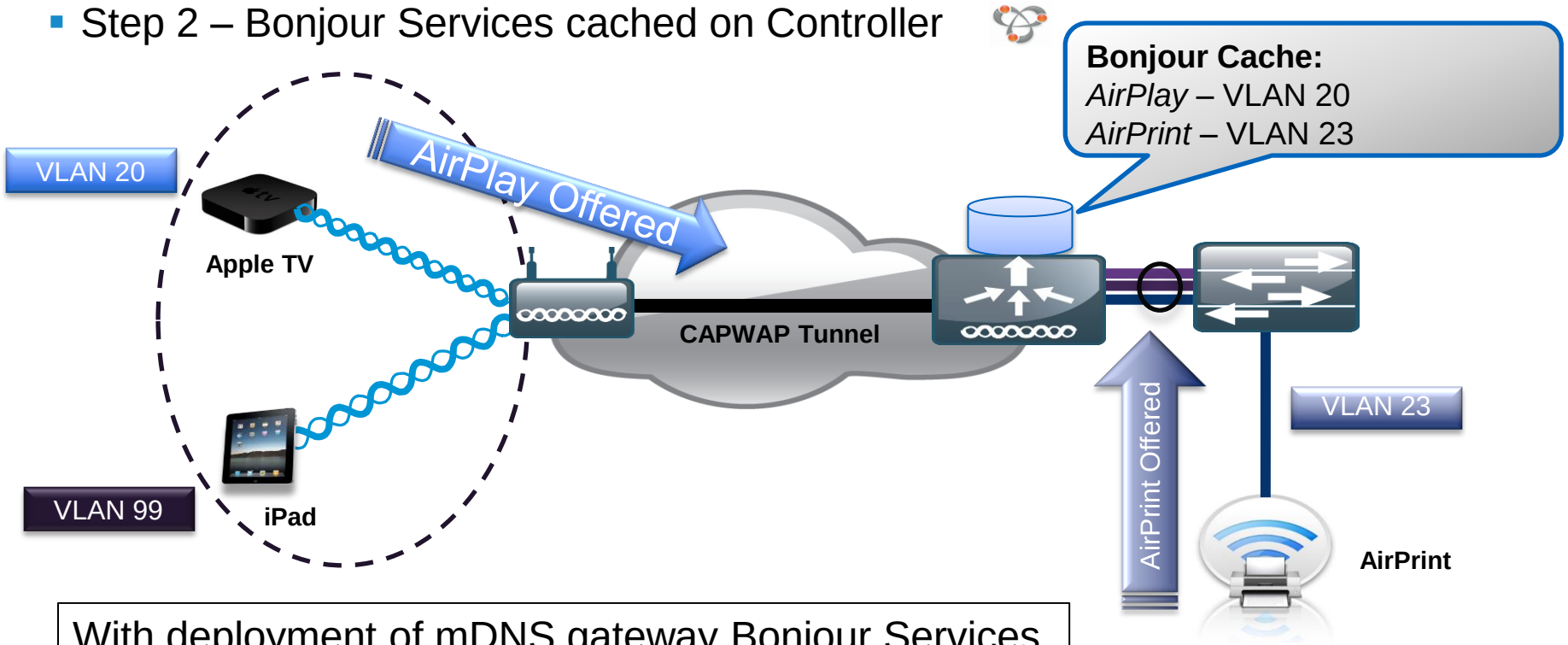
- Step 1 – Listen for Bonjour Services



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

Bonjour mDNS GW on WLC

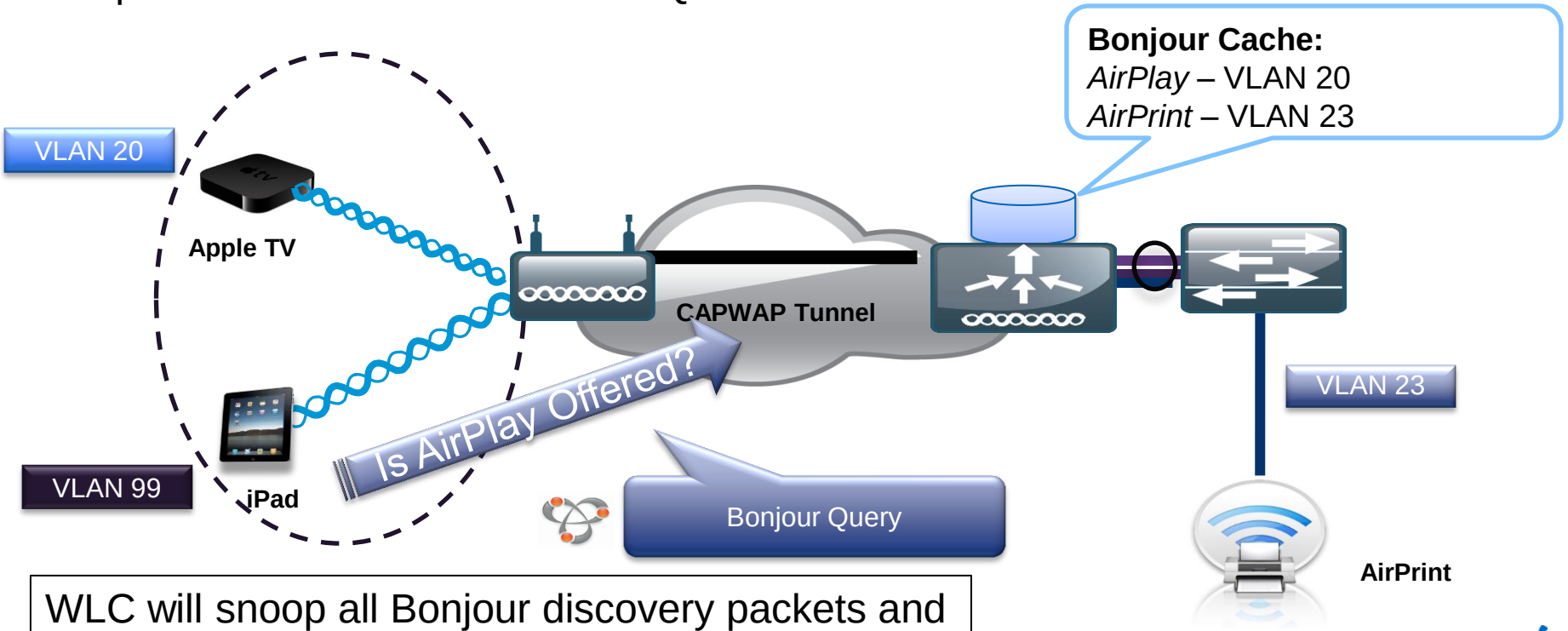
- Step 2 – Bonjour Services cached on Controller



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

Bonjour GW on WLC

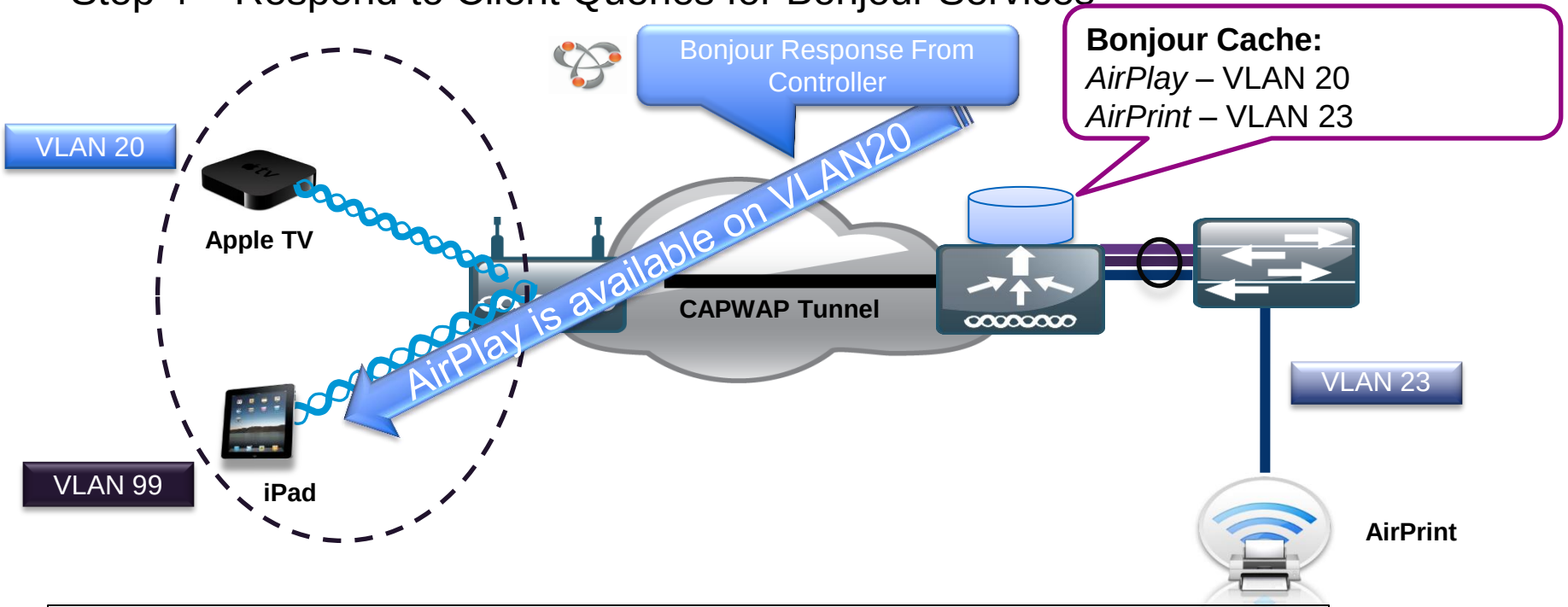
- Step 3 – Listen for Client Service Queries for Services



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

Bonjour GW on WLC

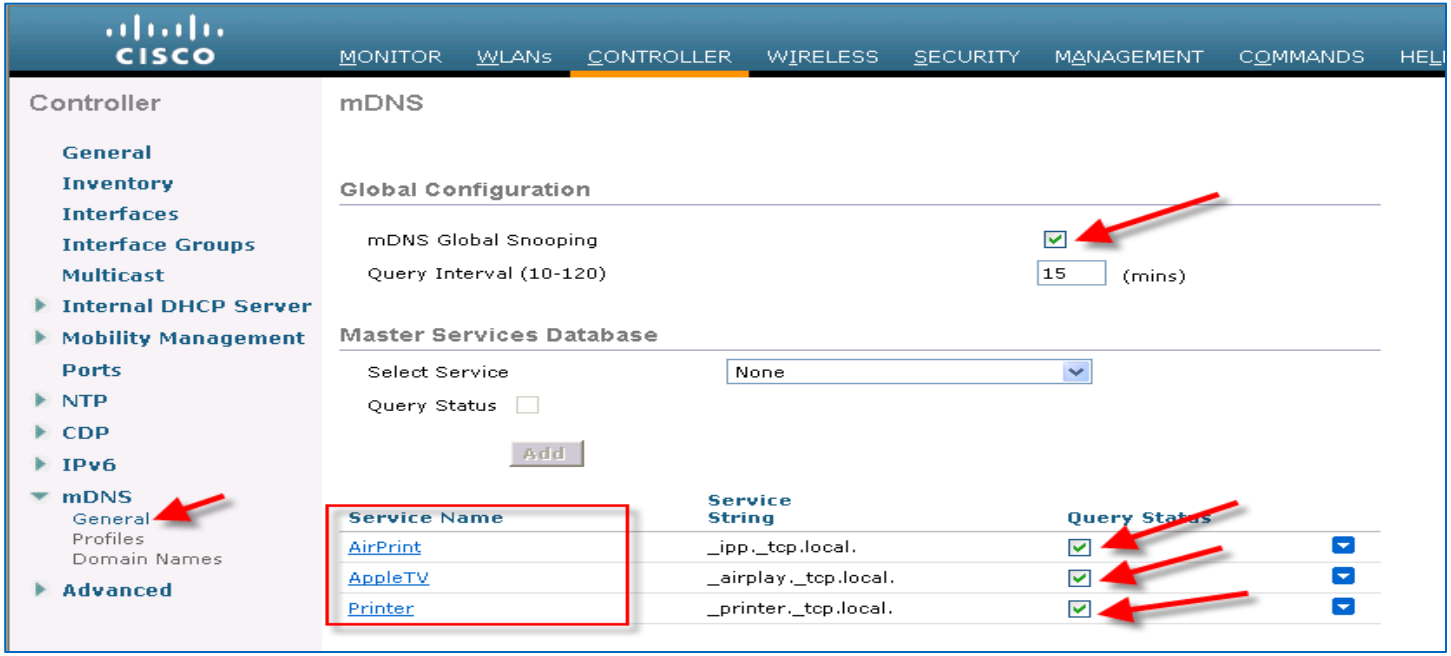
- Step 4 – Respond to Client Queries for Bonjour Services



Only Clients that require Bonjour services will receive those services

Configuring mDNS Snooping

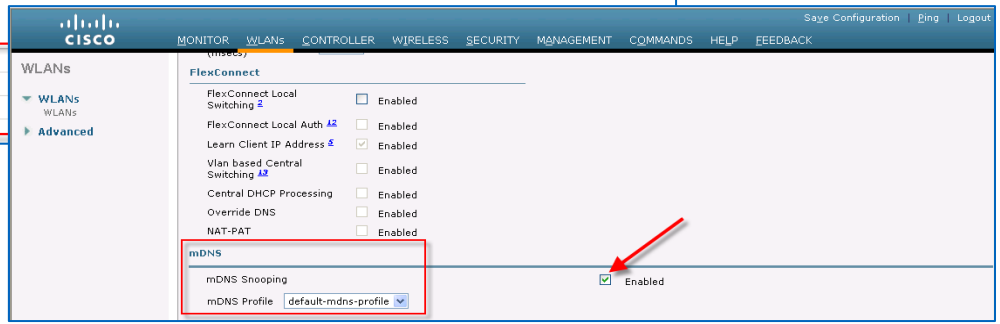
- Enable mDNS snooping globally and add services



Maximum of 100 services can be configured

Configure mDNS Profile per WLAN

- Create custom profile per WLAN

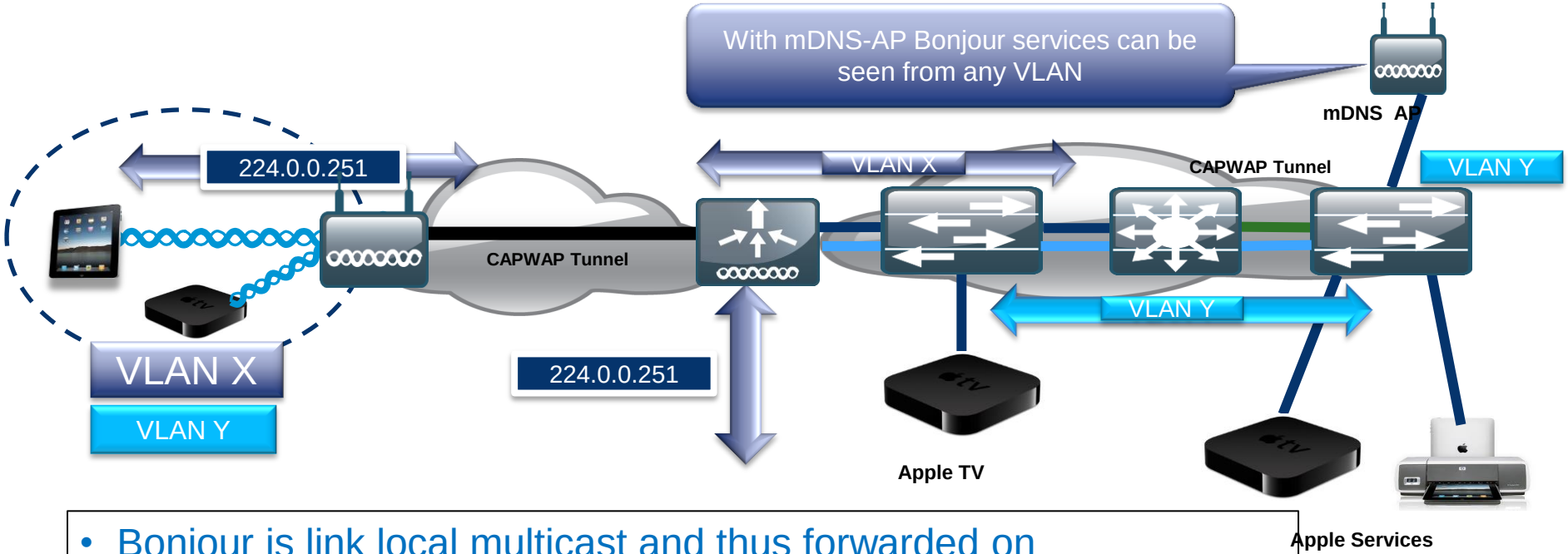


Enable mDNS snooping profile on the desired VLAN or WLAN

Bonjour Phase 2 – mDNS AP

- Given that mDNS Bonjour is a L2 multicast protocol and cannot be routed makes it enterprise unfriendly
- In rel 7.5 any of the AP's associated with the WLC as "mDNS-AP" forwards the mDNS packets received at the AP from the switch
- This enhancement allows the controller to have the visibility of wired service providers, which are on VLANs that are not visible to the controller.
- VLAN visibility at the WLC is achieved by APs forwarding the mDNS advertisements to the controller.
- The mDNS packet between AP and controller will be forwarded in CAPWAP data tunnel similar to mDNS packets from wireless client. Both capwap v4 and v6 tunnels will be supported.
- APs can be either in access mode or trunk mode to learn the mDNS packets from wired side and forward to the controller.
- The maximum number of VLANs that AP can snoop is 10
- This feature is supported on local and monitor mode AP, and not on FlexConnect Mode APs

Deployment Changes with Bonjour Services Phase 2

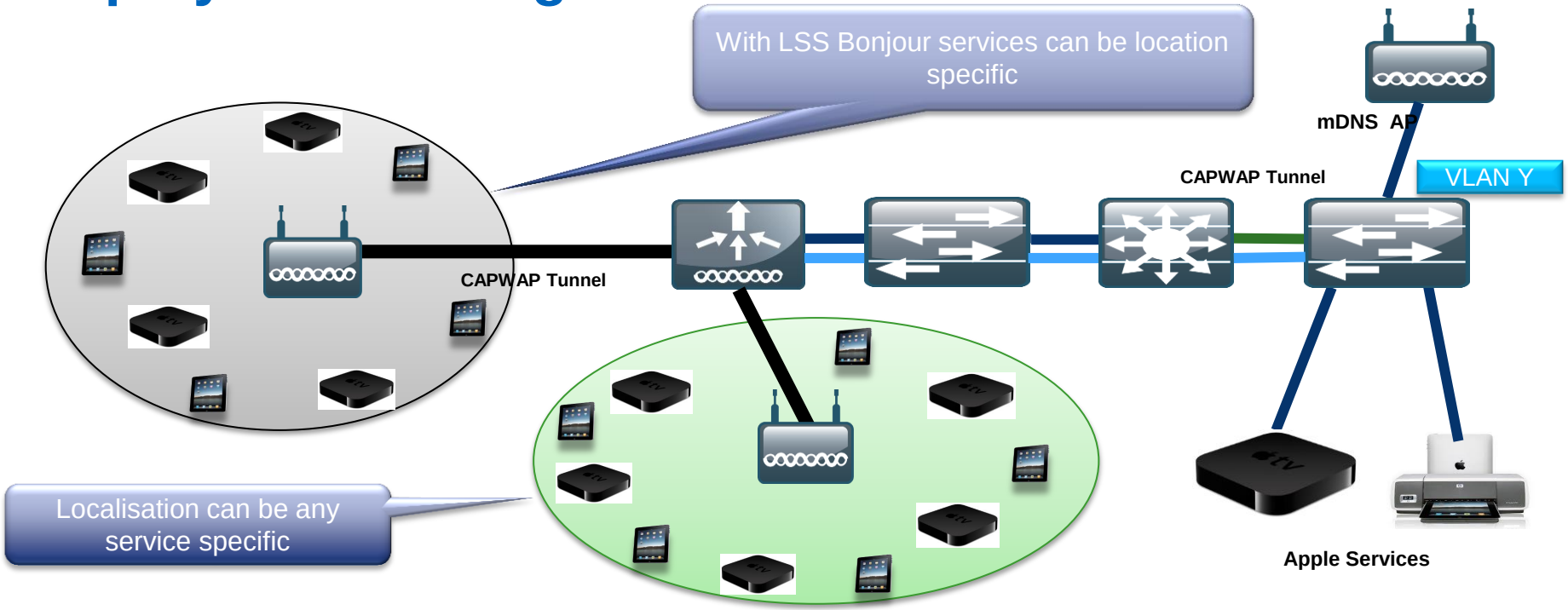


- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS AP snoop Bonjour services behind the Router or not L2 adjacent VLANs and forwards them to WLC in CAPWAP tunnel.

Bonjour Phase 2 – Location Specific Service

- Prior to rel 7.5 WLC responds with the complete SP-DB for the service being queried subject to the client profile – which could be overwhelming
- With LSS all valid wireless only mDNS service advertisements received at the WLC will be tagged with the MAC address of the AP associated with the service
- In 7.5 rel wireless entries are filtered in the SP list based on the querying client location using the RRM database and respond sent with a subset of the SP-DB
- Querying-client's AP base radio MAC address is used to query the RRM-DB to get the AP-NEIGHBOR-LIST.
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service.
- If LSS is disabled for any service then the wireless SP-DB entries will not be filtered while responding to any query from a wireless client for the said service.
- Wired SP-DB entries are never filtered.
- LSS status cannot be enabled for services with ORIGIN set to WIRED and vice-versa.

Deployment Changes with LSS



- WLC responds with the sub-set of SP-DB for the service being queried subject to the client profile
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service

Configure LSS Services From CLI

1. Once the basic bonjour gateway setup is configured the LSS can be enabled by accessing the WLC CLI, LSS is disabled by default on the

```
(Cisco Controller) >show mdns service summary
Number of Services..............................  7

Service-Name                          LSS    Origin      No SP     Service-string
--------------------------------- ----   ----------  -----    ---------------
AirPrint                              No     All           1      _ipp._tcp.local.
AirTunes                              No     All           2      _raop._tcp.local.
AppleTV                               No     All           2      _airplay._tcp.local.
HP_Photosmart_Printer_1               No     All           0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2               No     All           1      _cups._sub._ipp._tcp.local.
Printer                               No     All           0      _printer._tcp.local.
Scanner                               No     All           0      _scanner._tcp.local.
```

2. Configure LSS services from CLI:

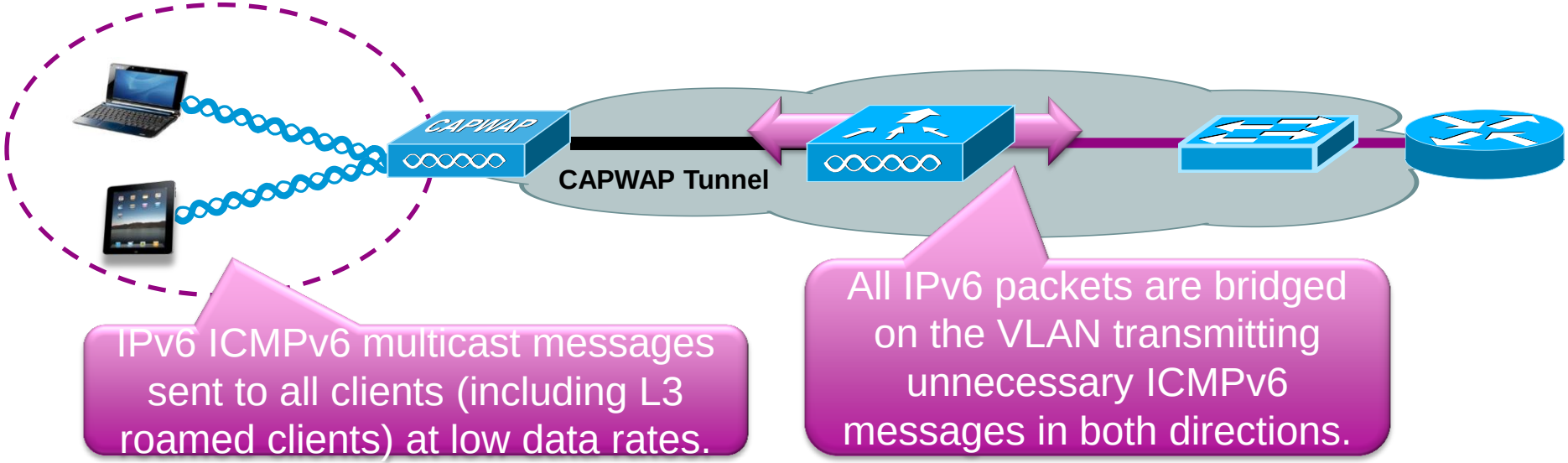
(WLC) >config mdns service lss <enable / disable> <service_name/all>

```
(Cisco Controller) >config mdns service lss enable all

(Cisco Controller) >show mdns service summary
Number of Services..............................  7

Service-Name                          LSS    Origin      No SP     Service-string
--------------------------------- ----   ----------  -----    ---------------
AirPrint                              Yes    All           1      _ipp._tcp.local.
AirTunes                              Yes    All           2      _raop._tcp.local.
AppleTV                               Yes    All           2      _airplay._tcp.local.
HP_Photosmart_Printer_1               Yes    All           0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2               Yes    All           1      _cups._sub._ipp._tcp.local.
Printer                               Yes    All           0      _printer._tcp.local.
Scanner                               Yes    All           0      _scanner._tcp.local.
```

Deploying the Cisco Unified Wireless Architecture

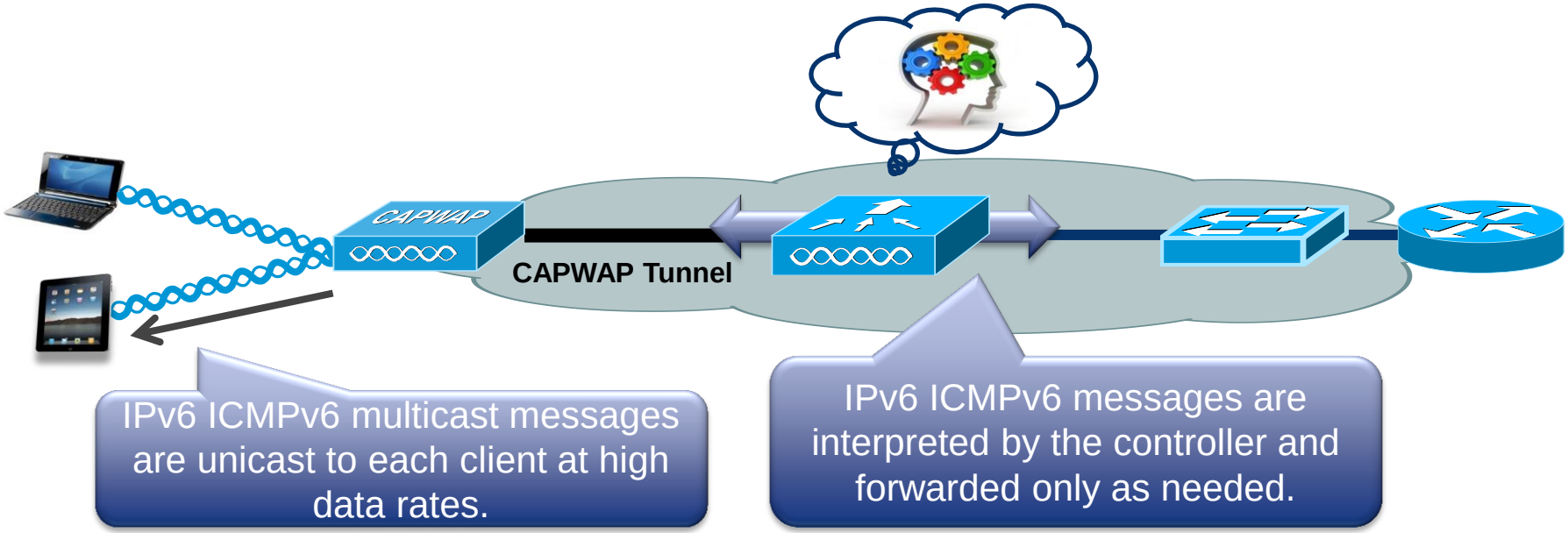
- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS Gateway
- IPv6 Deployment with Controllers
- Branch Office Designs
- Guest Access Deployment
- Home Office Design

Wireless IPv6 Support - Pre-v7.2



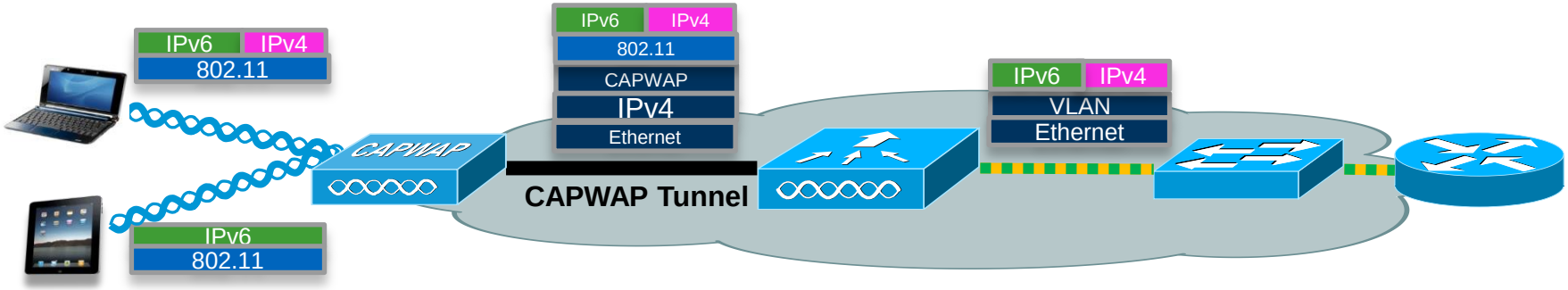
- In releases prior to 7.2, enabling IPv6 bridging provided a limited solution with no Layer 3 mobility and non-optimised delivery of essential ICMPv6 messages to clients.

Wireless IPv6 Support - Post-v7.2



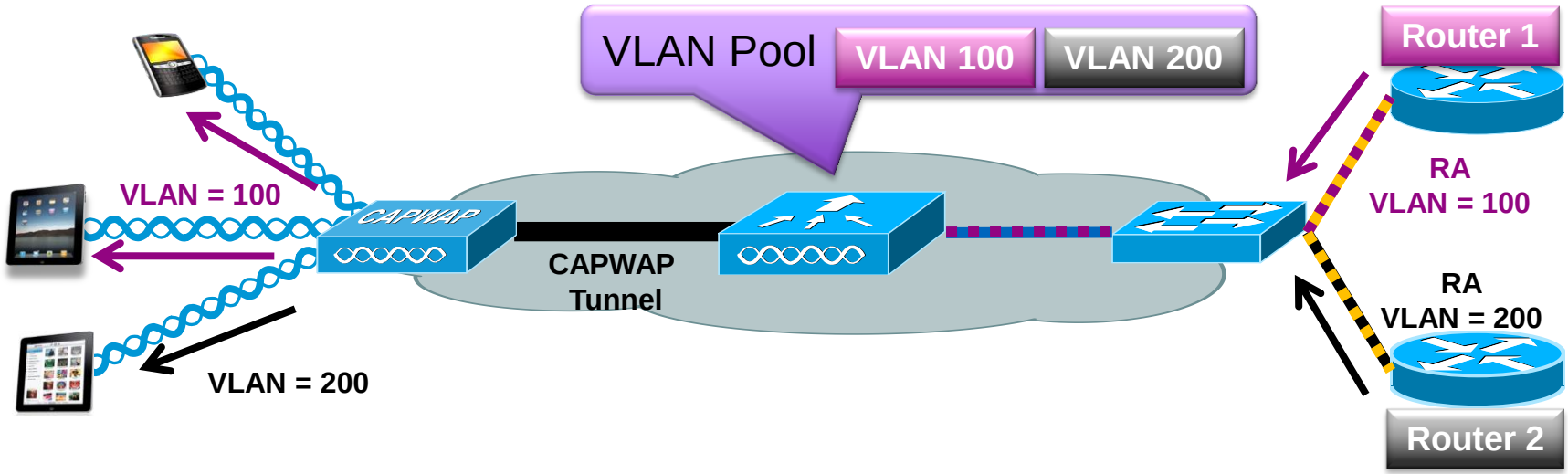
- In releases 7.2, the controller now processes ICMPv6 messages allowing for optimised delivery, Layer 3 mobility and first hop security.

Wireless IPv6 Client Support



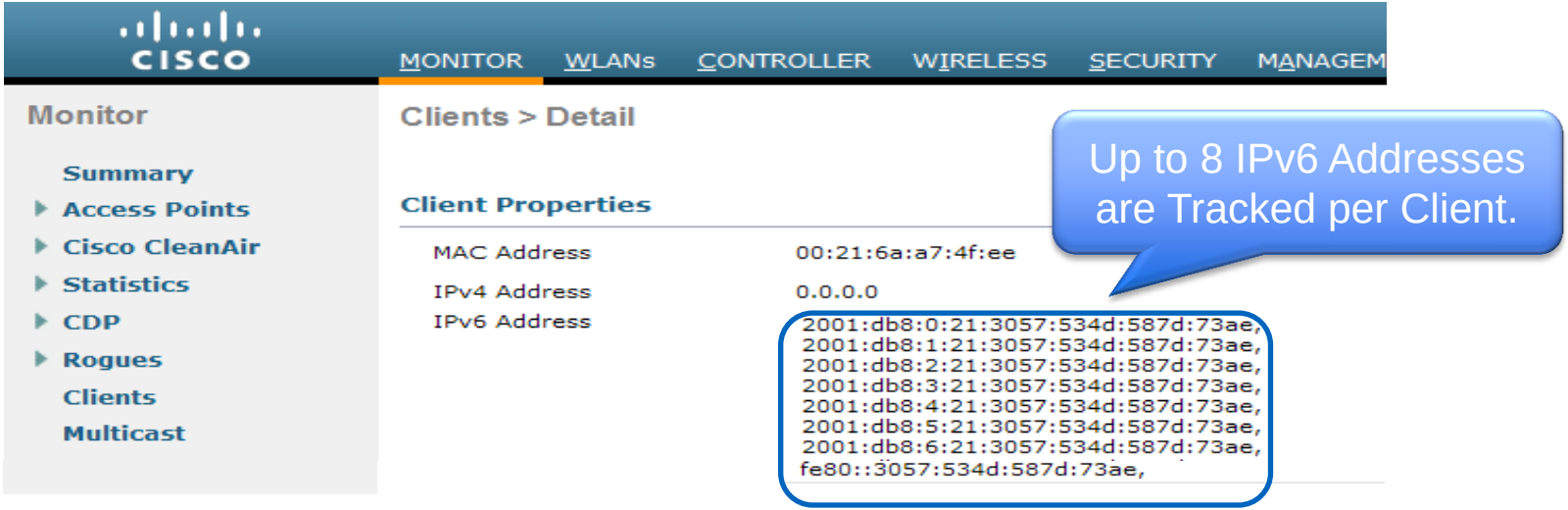
- Supports IPv4, Dual Stack and Native IPv6 clients on single WLAN simultaneously
- Supports the following IPv6 address assignment for wireless clients:
  - IPv6 Stateless Autoconfiguration [SLAAC]
  - Stateless, Stateful DHCPv6
  - Static IPv6 configuration
- Supports up to 8 IPv6 addresses per client
- 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.

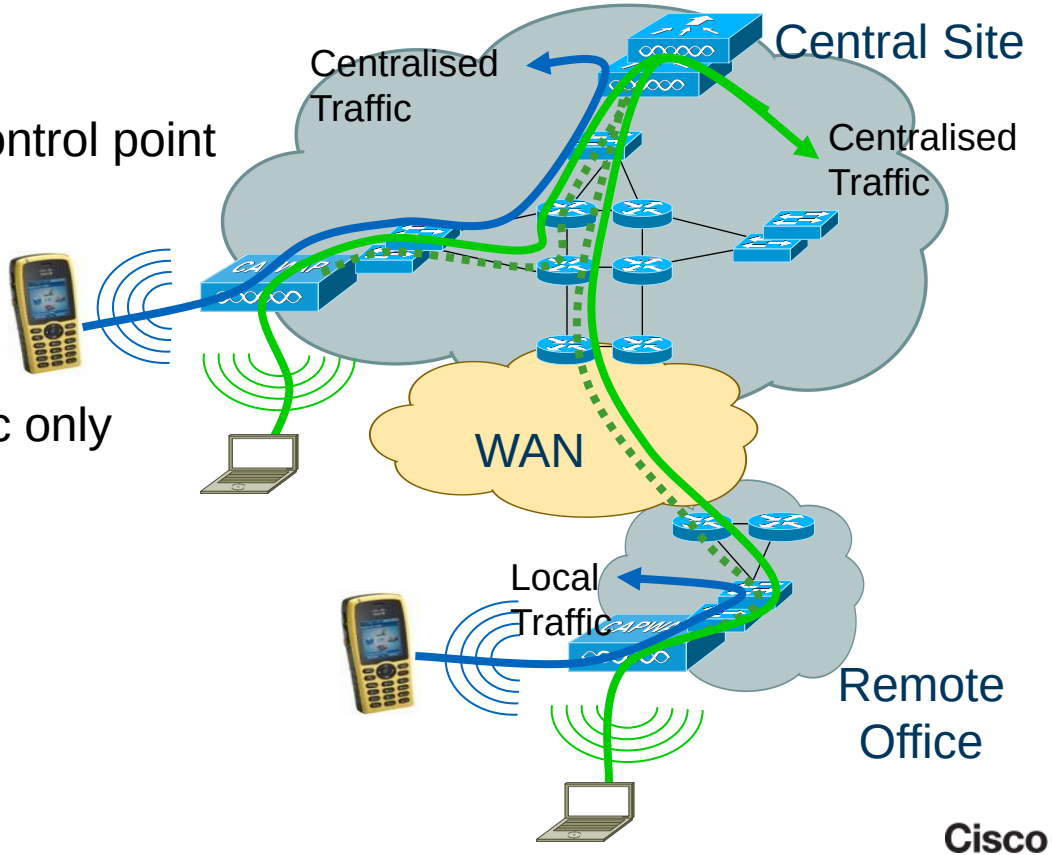
Deploying the Cisco Unified Wireless Architecture

- Client Profiling
- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS 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

WAN Limitations Apply

For Your Reference

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	1 sec	50	1000
Data+Voice	1.44 Mbps	100 ms	50	1000
Monitor	1.44 Mbps	2 sec	50	1000

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

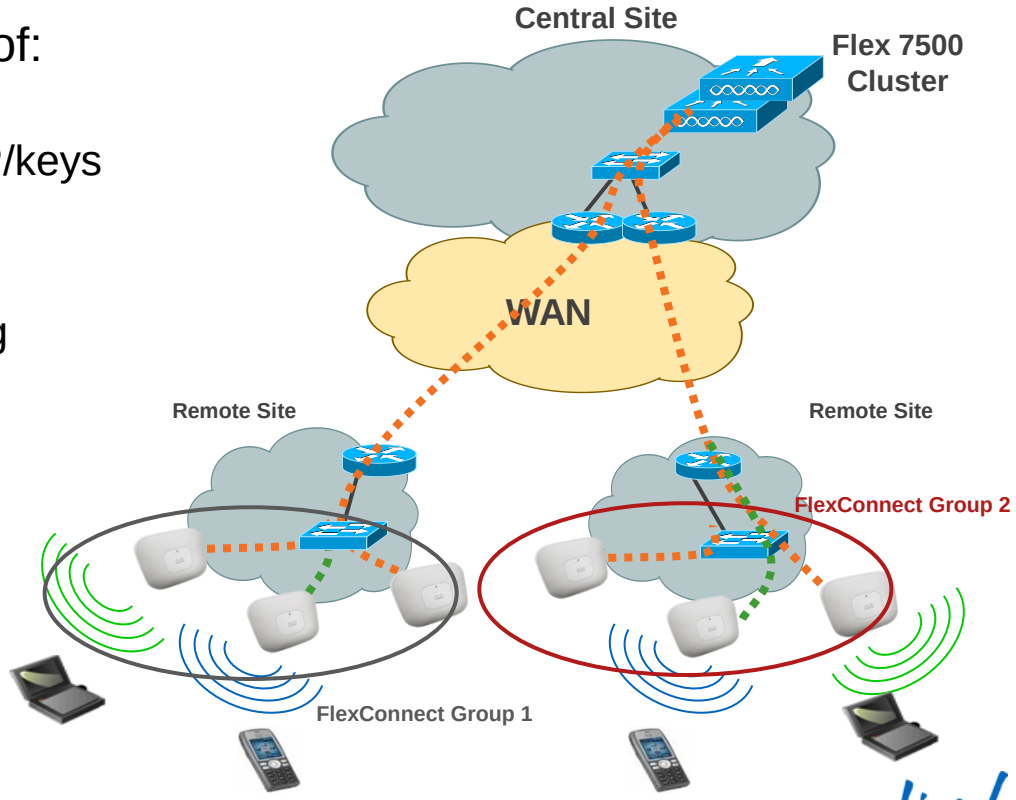
- WAN Tolerance
  - High Latency Networks
  - WAN Survivability
- Security

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

Understanding FlexConnect Groups

- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade
- Scaling information

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504
FlexConnect Groups	2000	100	100	30
AP per Group	100	25	25	25



FlexConnect Improvements in 7.2 – 7.5

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

7.3 & 7.4

- Flex 7500 Scale Update
- VLAN Based Central Switching
- Split Tunnelling
- Central DHCP Processing
- WGB/uWGB Support with local switching
- Bidirectional Rate Limiting
- Support for ISE BYOD Registration & Provisioning

7.5

- PEAP and EAP-TLS Support
- FlexConnect Group specific WLAN-VLAN mapping
- AAA Client ACL

EAP-TLS/PEAP Overview

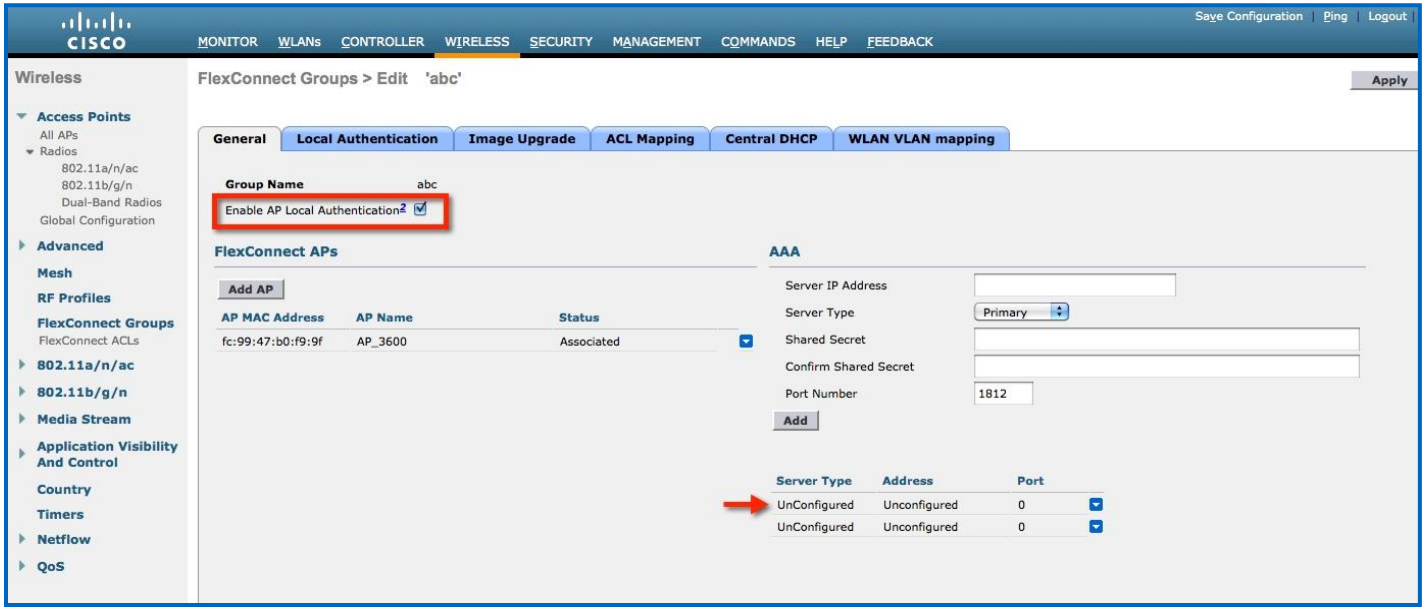
New (7.5)

- Local Authentication on FlexConnect AP
  - ➢FlexConnect AP contacting RADIUS Server
  - ➢FlexConnect AP acting as RADIUS Server
- EAP Methods when AP acting as RADIUS Server: LEAP, EAP-FAST, **PEAP, EAP-TLS**
- PEAP and EAP-TLS Support in
  - ✓Standalone Mode
  - ✓Local Authentication
- Continued support for RADIUS Servers on FlexConnect Group.
- RADIUS Server Configuration takes precedence over FlexConnect AP acting as RADIUS Server.
- Access points 1040, 1140, 1520, 1550, 1600, 3700, 3500, 3600, 2600, 1250, 1260, are supported

PEAP/EAP-TLS Web-GUI

New (7.5)

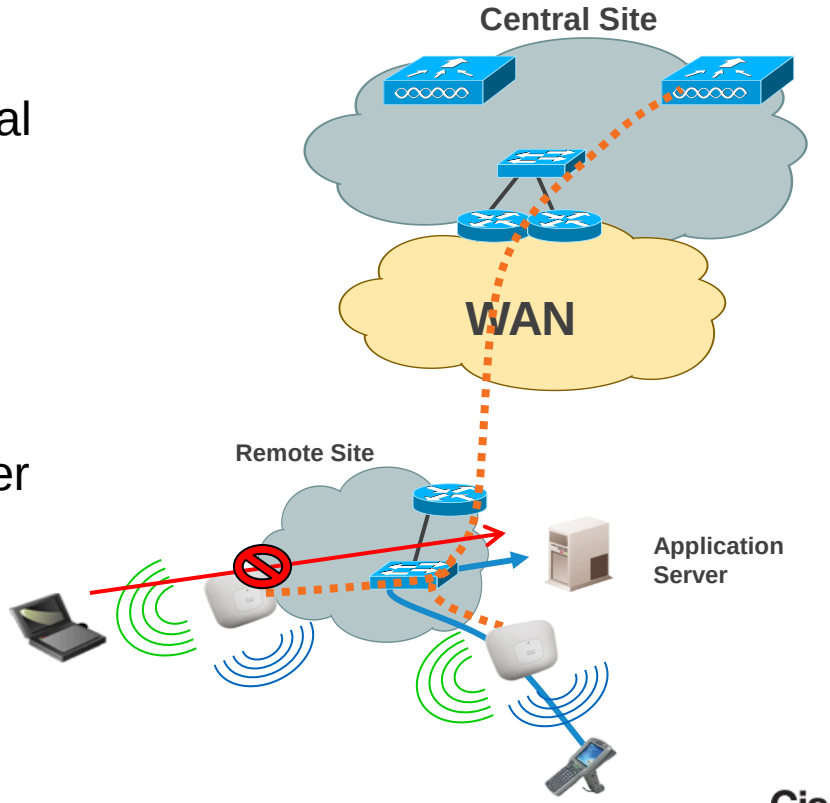
- Enable AP Local Authentication
- Radius Server configured on the FlexConnect group takes precedence over ‘AP Local Authentication’



Local Switching Access Lists (7.2)

Description

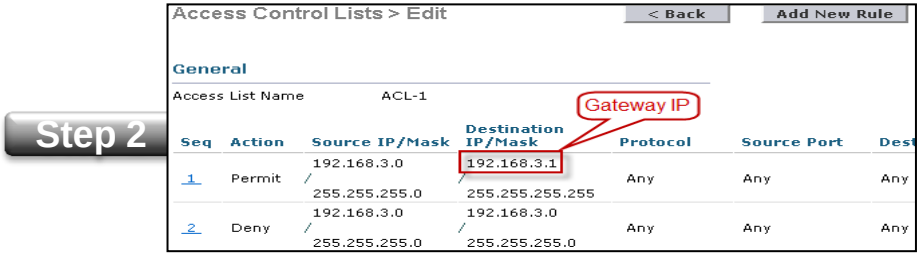
- Support for ACL in FlexConnect local switching mode
- ACL mapped to local VLAN per AP or FlexConnect Group
- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL

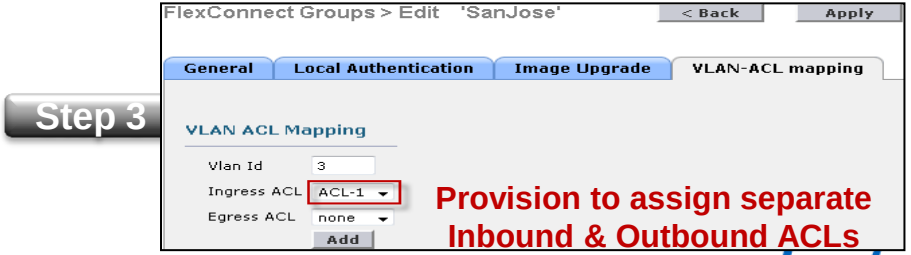


Local Switching Access Lists (7.2)

Configuration

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

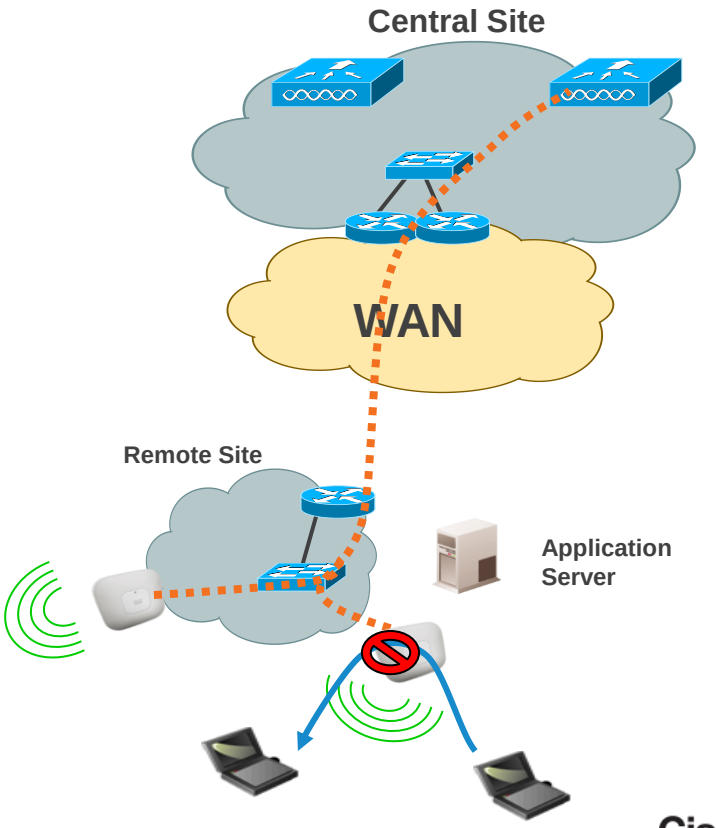




Local Switching Peer-to-Peer Blocking (7.2)

Description

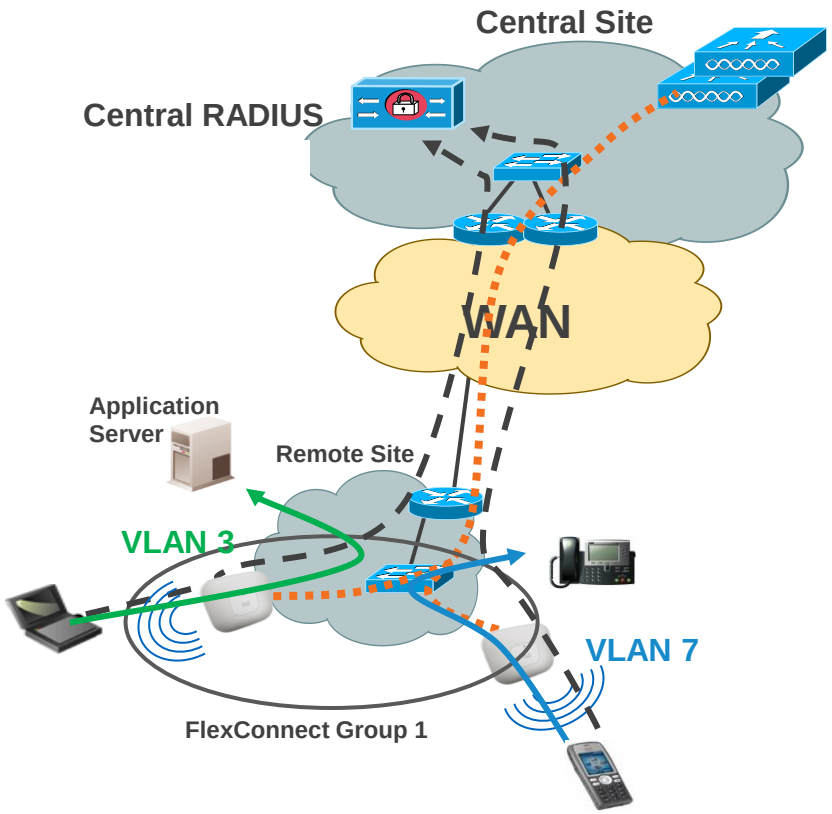
- Support for Peer-to-Peer blocking in FlexConnect AP
- Apply for clients on same FlexConnect AP
- P2P blocking modes : disable or drop
- For P2P blocking inter-AP use ACL or Private VLAN fonction



FlexConnect AAA VLAN Override (7.2)

Description

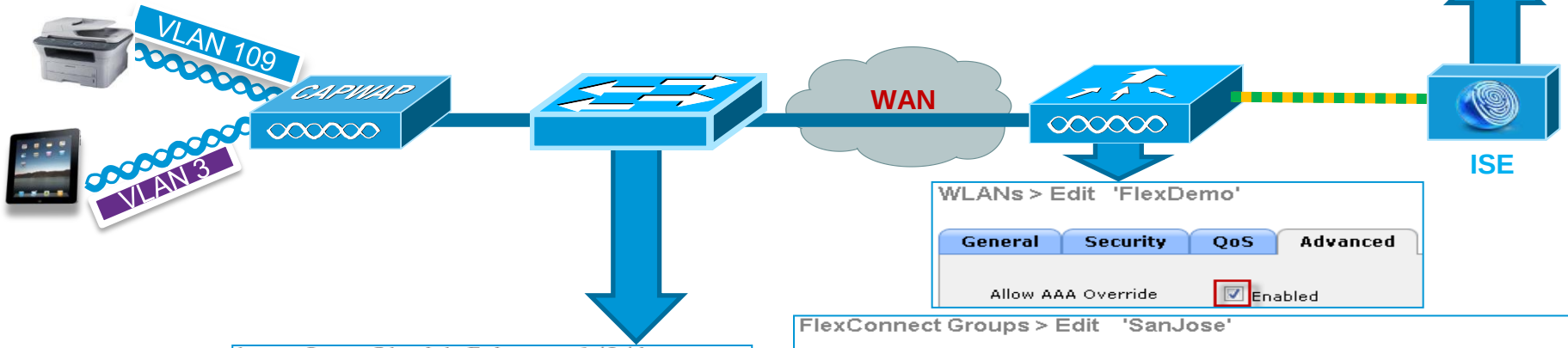
- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used
- QoS and ACL Override is not supported.



FlexConnect AAA VLAN Override (7.2)

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

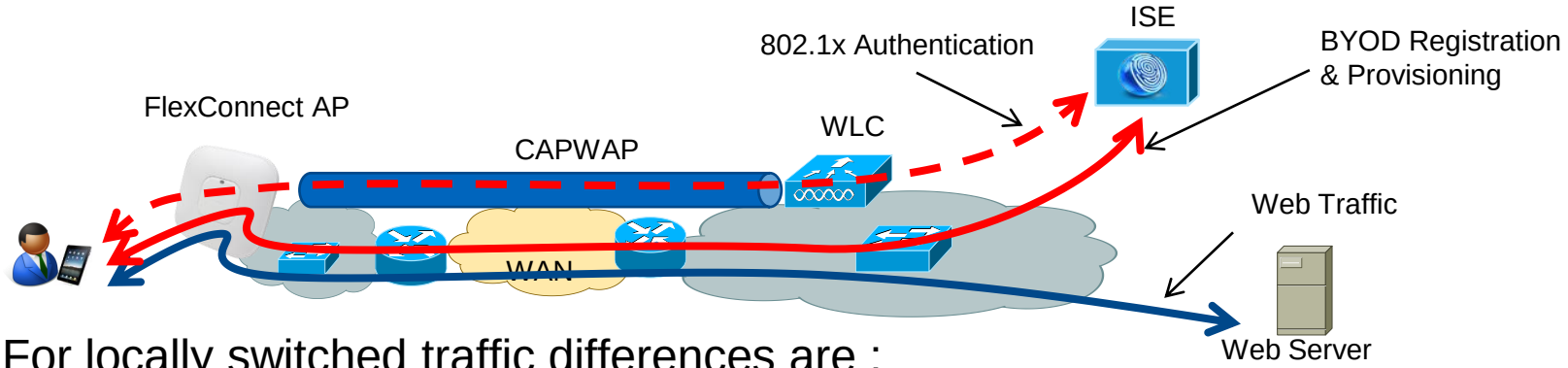
Egress ACL none

Add

Create Sub-Interface on FlexConnect AP

Deploying BYOD with FlexConnect and Local Switching

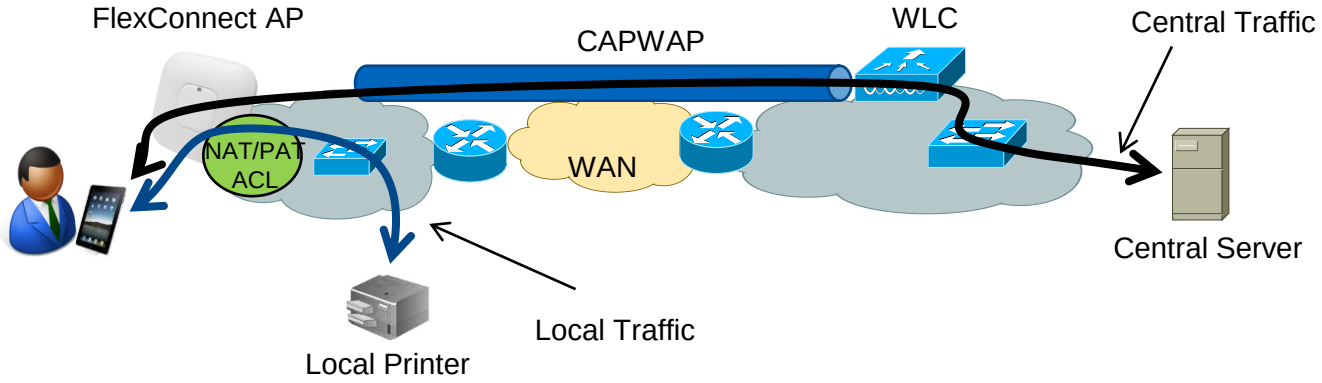
- No difference for centrally switched traffic.



- For locally switched traffic differences are :
  - No Dynamic ACL with AAA override -> Specific « Web Policies ACL » for BYOD
  - No HTTP Profiling probes (Traffic is not sent to WLC)
  - DHCP Profiling probes mandate central DHCP redirection
  - Registration & Provisioning flow will go outside the CAPWAP tunnel

FlexConnect ACL – Split Tunnelling

- Split tunnelling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunnelling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunnelling is using the AP IP@ for the NAT/PAT feature

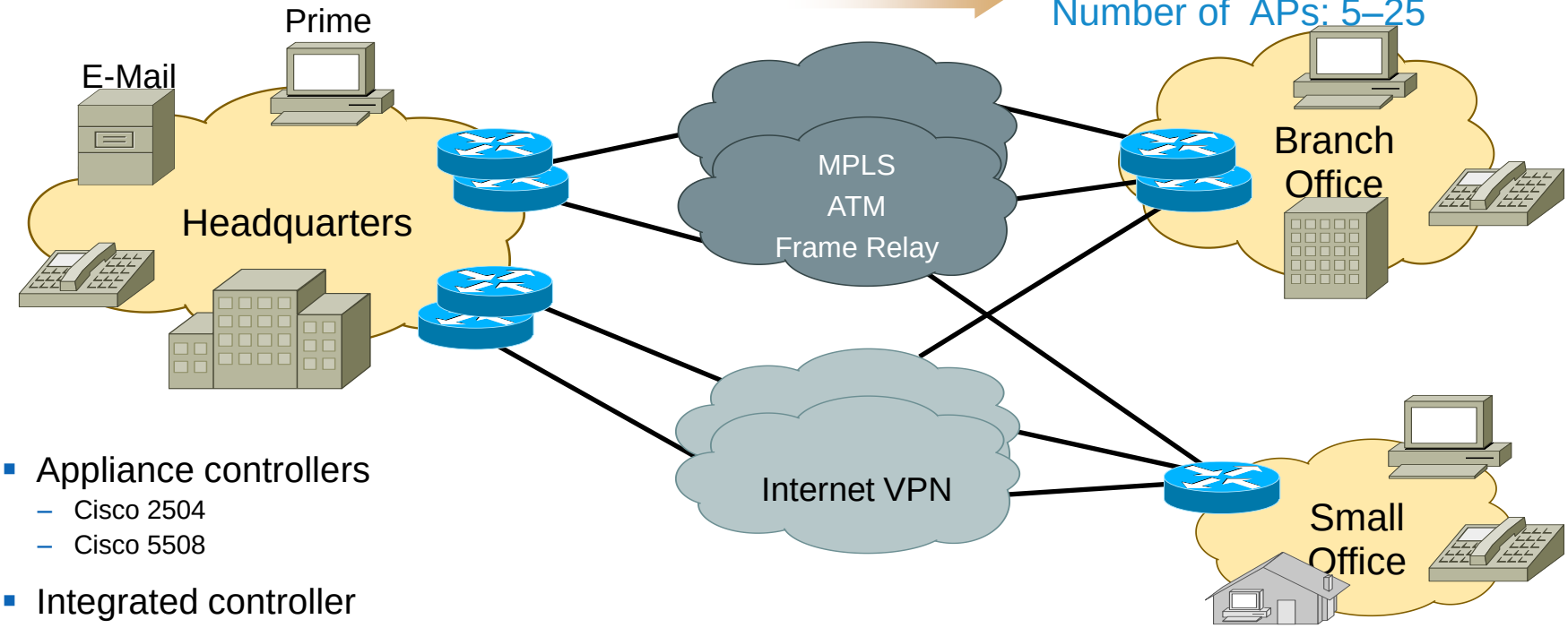


Deploying the Cisco Unified Wireless Architecture

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

Branch Office WLAN Controller Options

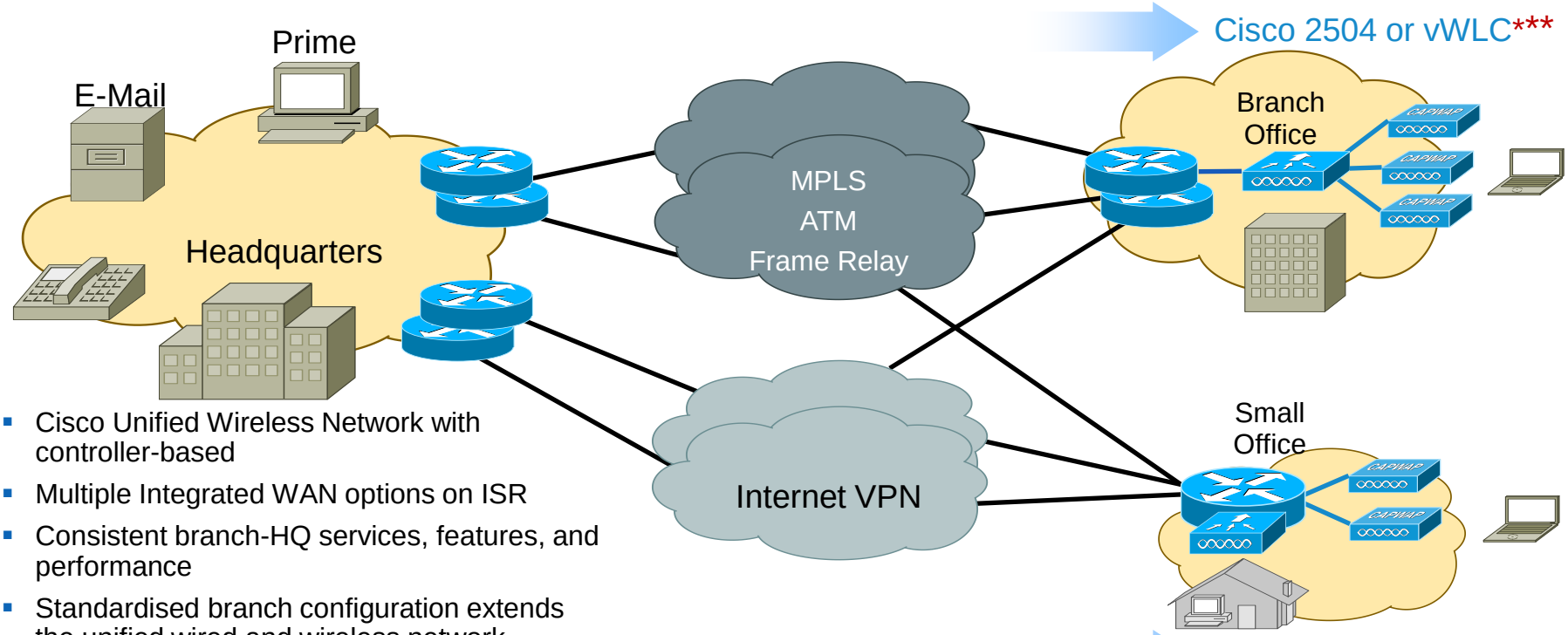
Number of Users: 100–500
Number of APs: 5–25



- Appliance controllers
  - Cisco 2504
  - Cisco 5508
- 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

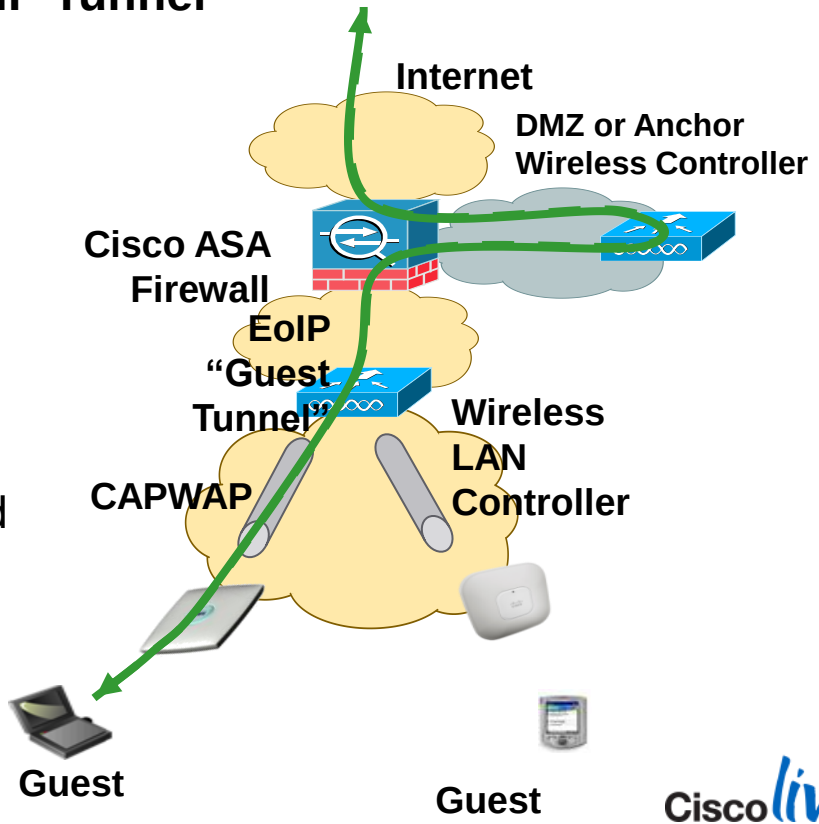
Deploying the Cisco Unified Wireless Architecture

- High Availability
- Understanding AP Groups / RF Groups
- Application Visibility
- mDNS 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
- With 7.4 release 2504 series EoIP connections can terminate 10 EoIP tunnels

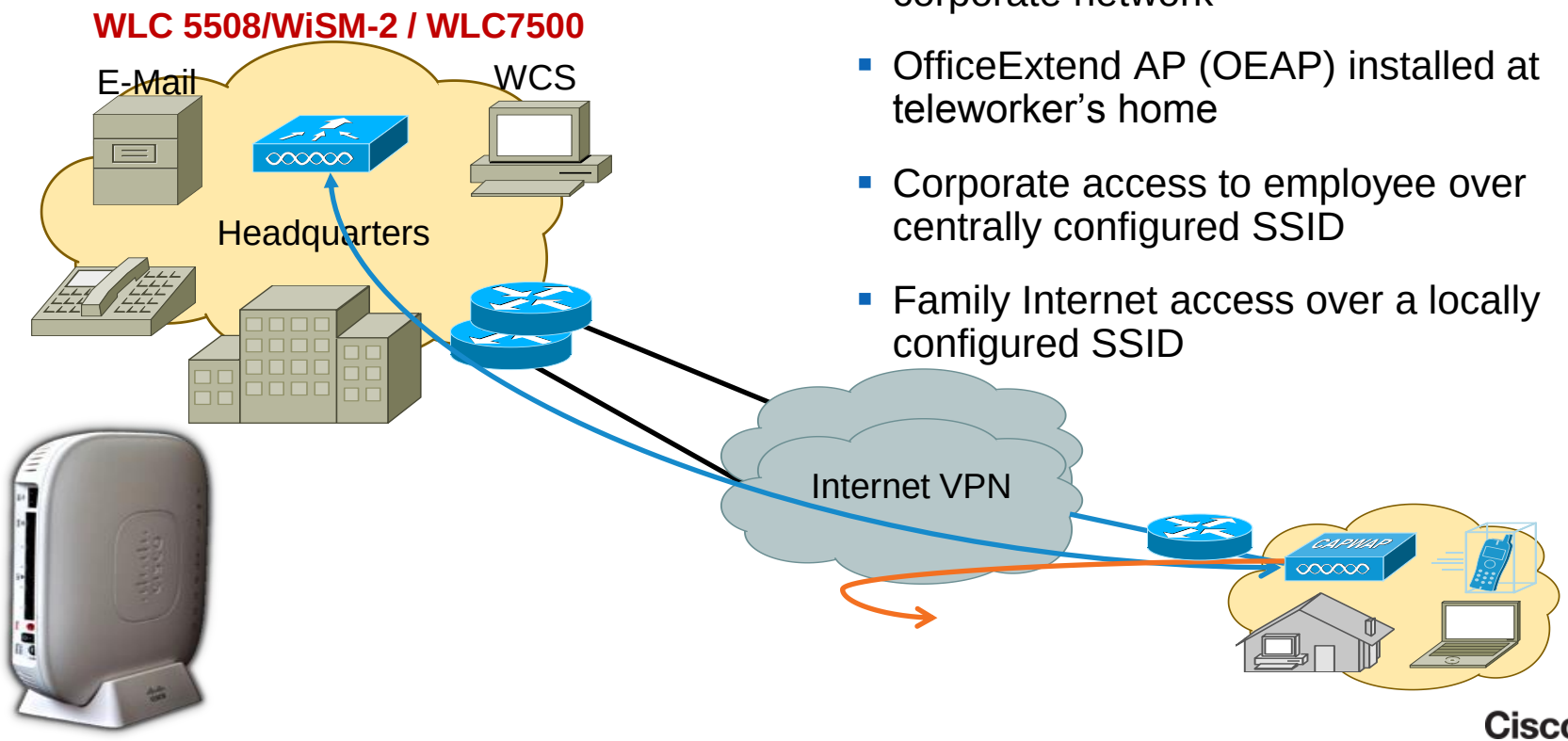


Deploying the Cisco Unified Wireless Architecture

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

Home Office Design

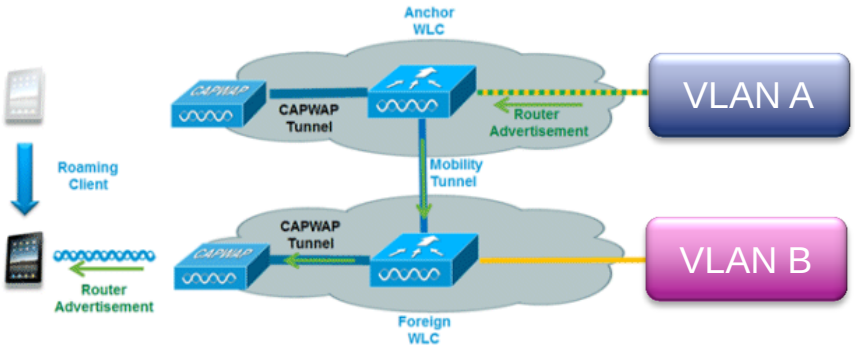
OEAP AP



- 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

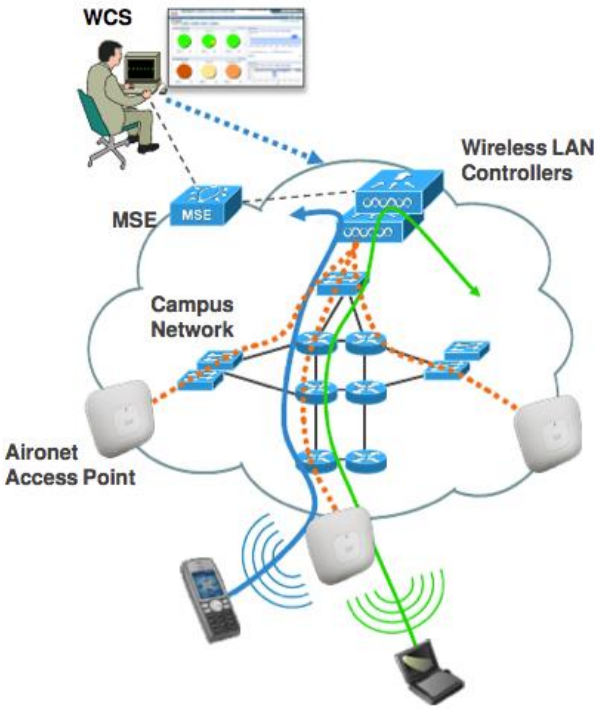
Best Practices – Campus Architecture

- ✓ Centralise traffic flow to enhance operational IP address/VLAN management
- ✓ Place all controllers in the same Mobility Domain to allow seamless mobility across L2 and L3 transitions
- ✓ Provide coverage in all possible locations leveraging mesh and outdoor Access Points.
- ✓ Use BYOD for device security and policy
- ✓ Use AP Group, Interface group and RF Profile



Best Practices – Branch Deployment

- ✓ Select correct architecture for branch office – local controller or FlexConnect
- ✓ Prioritise the right traffic over the WAN
- ✓ Have correct WAN survivability model
- ✓ Proper WAN bandwidth and Latency to support voice and multimedia applications
- ✓ Enable Enhanced Local Mode (ELM) or WiPS using WSSI module for security.
- ✓ Take advantage of latest BYOD enhancements with FlexConnect architecture



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 (11ac, CleanAir, BandSelect, ClientLink, Security, CCX, FlexConnect, etc)
- Cisco's investment into technology – Cisco Prime, ISE, New hardware, Cloud controller

Documentation

AP3700 Deployment Guide - http://www.cisco.com/en/US/partner/docs/wireless/technology/apdeploy/7.6/Cisco_Aironet_3700AP.html

AP3600, 2600, 1600 Deployment Guide : http://www.cisco.com/en/US/partner/docs/wireless/technology/apdeploy/Cisco_Aironet.html

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/partner/docs/wireless/controller/technotes/7.5/High_Availability_DG.html

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

Bonjour Deployment Guide :http://www.cisco.com/en/US/docs/wireless/technology/bonjour/7.5/Bonjour_Gateway_Phase-2_WLC_software_release_7.5.html

Wireless Device Profiling and Policy Classification Engine on WLC, Release 7.5http://www.cisco.com/en/US/docs/wireless/controller/technotes/7.5/NativeProfiling75.html

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

Enterprise Best Practices for Apple Mobile Devices on Cisco Wireless LANs – http://www.cisco.com/en/US/docs/wireless/technology/vowlan/bestpractices/EntBP-AppMobDevs-on-Wlans.html

Cisco WLAN Passpoint™ Configuration Guide : //www.cisco.com/en/US/docs/wireless/controller/technotes/7.5/Hotspot_057.html




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CISCO™