TOMORROW starts here.

cisco

Cisco live!

Converged Access Mobility Design & Architecture

BRKEWN-2022

Sujit Ghosh
Sr. Mgr. Technical Marketing
Enterprise Networking Group

Cisco live!

Converged Access Architecture Overview

Diving into the "One Network"

BRKCRS-2022 – **Session Overview and Objectives**

- **Come to this session to learn what Converged Access is – how it operates – and the features supported in the latest release.**

- Attendees at this session will gain a **greater understanding** of the design and operation of the Converged Access solution, be able to **understand** how it fits into the broader Cisco wired and wireless portfolio from both a product and a design perspective, and **recognise** the relevant benefits for their own network environments.

- In addition to introducing the terminology and platforms that make up the Cisco Converged Access system, we will look into use cases for High Availability Deployment, Application Visibility, Service Discovery Gateway protocol, 802.11ac support and TrustSec.

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Agenda

- **What is Converged Access?**
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

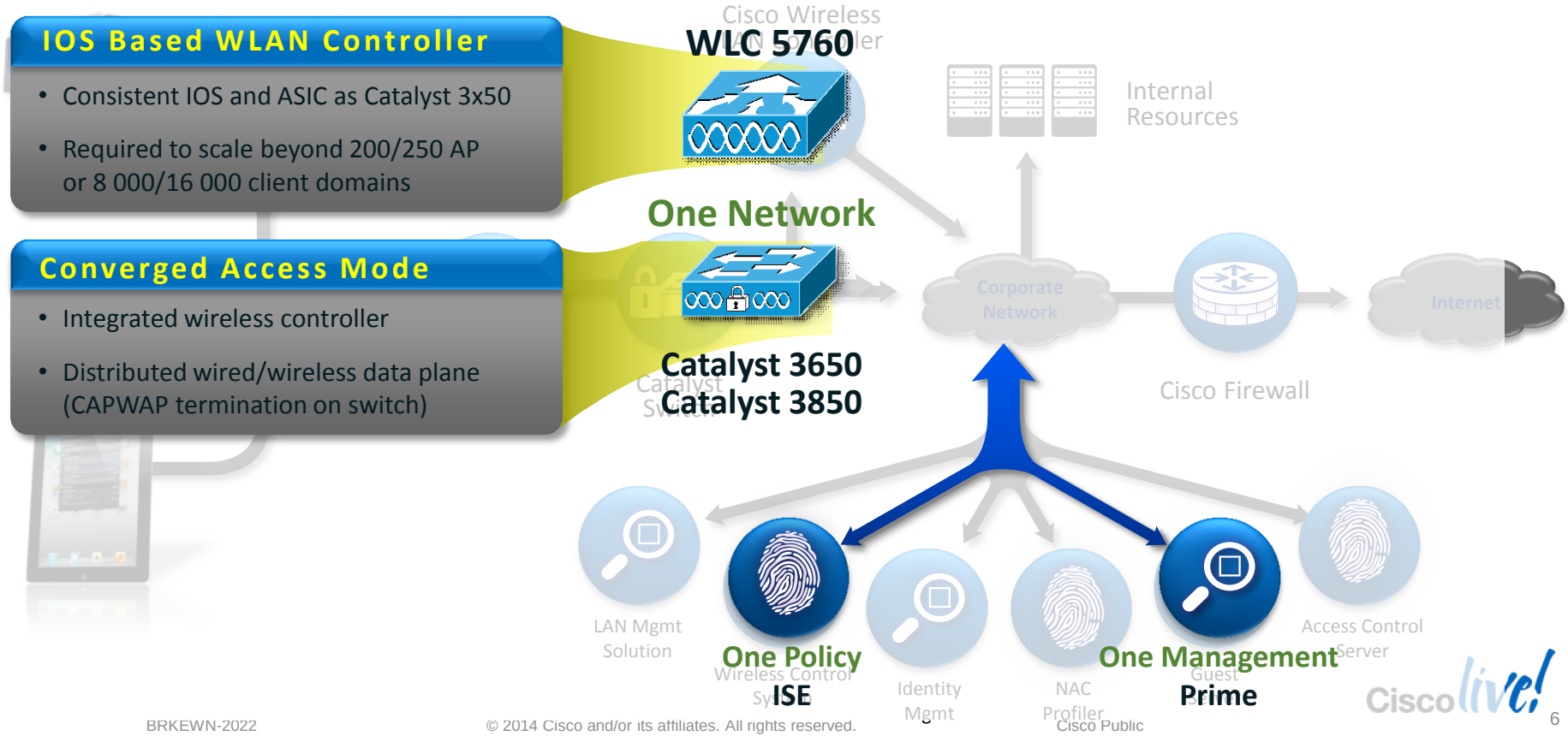
One Network with Converged Access

IOS Based WLAN Controller

- Consistent IOS and ASIC as Catalyst 3x50
- Required to scale beyond 200/250 AP or 8 000/16 000 client domains

Converged Access Mode

- Integrated wireless controller
- Distributed wired/wireless data plane (CAPWAP termination on switch)



Converged Wired/Wireless Access – Benefits

Single platform for wired and wireless

Common IOS, same administration point, one release

Network wide **visibility** for faster troubleshooting

Wired and wireless traffic visible at every hop

Consistent security and Quality of Service **control**

Hierarchical bandwidth management and distributed policy enforcement

Maximum **resiliency** with fast stateful recovery

Layered network high availability design with stateful switchover

Scale with distributed wired and wireless data plane

Large stack bandwidth; 40G wireless / switch; efficient multicast; 802.11ac optimised

Unified Access - One Policy | One Management | One Network

Agenda

- What is Converged Access?
- **Converged Access Platforms Overview**
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Unified Access Components – Complete Overview

One Policy

with Identity Services Engine (ISE)

- BYOD policy management
- Device profiling and posture
- Guest access portal

One Management

with Cisco Prime 2.0

- Full wired and wireless management
- User/device centric view
- Intuitive troubleshooting workflows

ISE

Cisco Prime

Catalyst 3850

5760 Wireless Controller

Catalyst 3850/3650

- Industry's first fully integrated wired and wireless switch
- Wireless: 480G stack, 50 APs, 2K clients, 40G
- Flexible NetFlow, Granular QoS

5760 Wireless Controller

- Consistent IOS with Catalyst 3850
- 60G, 1K APs, 12K Clients, N+1 Redundancy
- Flexible Netflow, Granular QOS

Best-in-Class Performance, Security, and Resiliency

Catalyst 3850 Switch – Platform Overview

Wireless CAPWAP Termination in HW

Up to 50 APs /2000 clients per stack, and 40G per switch

480 Gbps Stacking Bandwidth

Up to 2000 Clients per Stack

FRU Fans, Power Supplies - HA

Full POE+

Stackpower

Granular QoS / Flexible NetFlow / SGT-SGACL

Multi-Core CPU

40 Gbps Uplink Bandwidth (Modular)

Line Rate on All Ports

APs must be directly connected to Catalyst 3850

Built on Cisco's Innovative "UADP" ASIC

New Catalyst 3650 Switch – Platform Overview

APs must be directly connected to Catalyst 3650

Built on Cisco's Innovative "UADP" ASIC

Wireless LAN Controller (WLC) 5760 – Platform Overview

Centralised, or Converged Access Deployment Modes

Up to 1000 Access Points

First IOS-Based Wireless LAN Controller

Up to 12,000 Concurrent Clients

6x 1/10G SFP+ uplinks with LAG

60 Gbps Wireless Bandwidth

Granular QOS/Flexible NetFlow

FRU Fans

HA Port

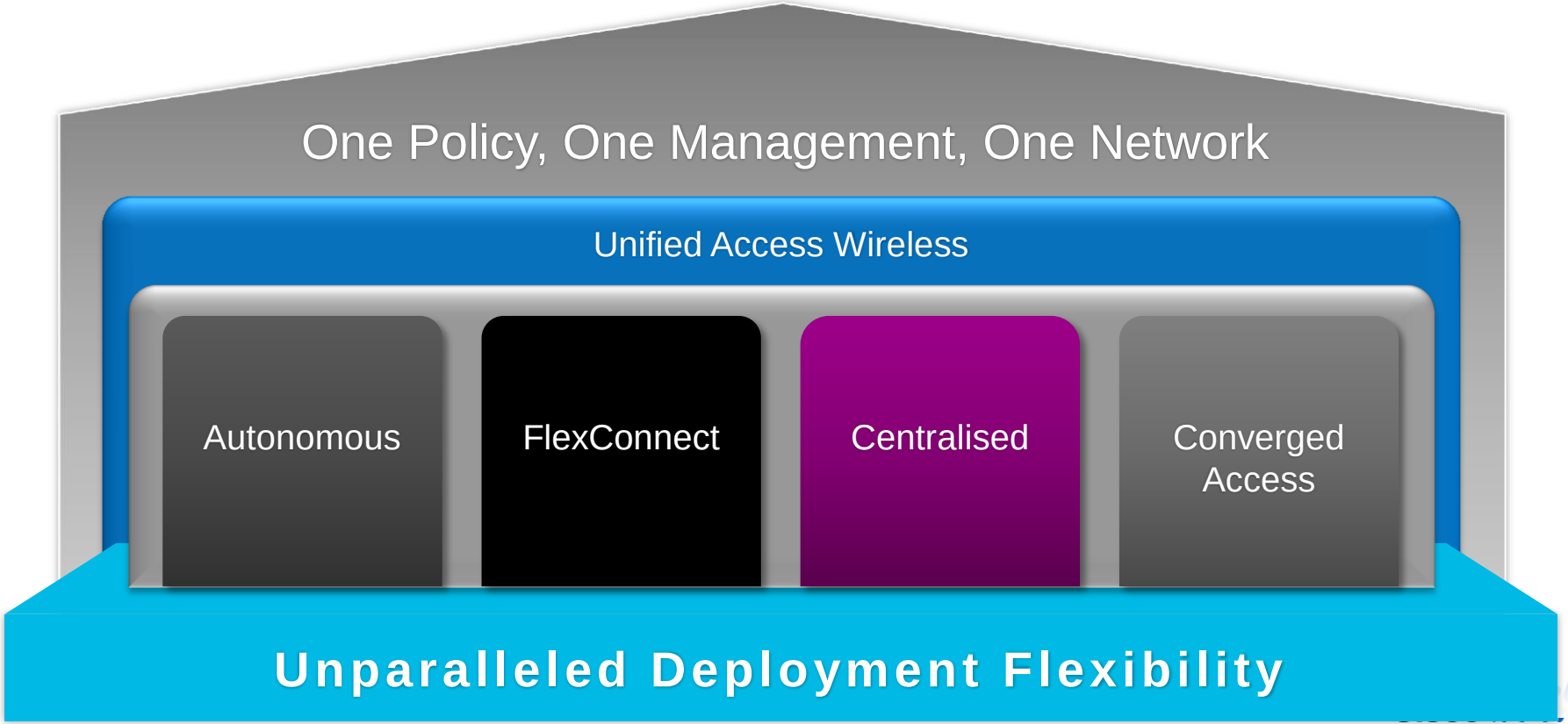
FRU Power Supplies

Built on Cisco's Innovative "UADP" ASIC

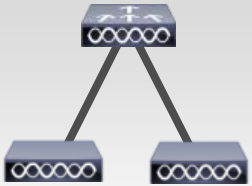
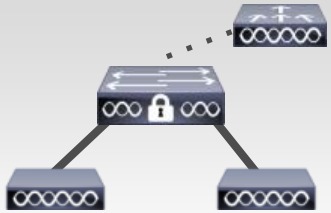
Agenda

- What is Converged Access ?
- Converged Access Platforms Overview
- **Wireless Deployment Options**
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Cisco One Network: Wireless Deployment Modes



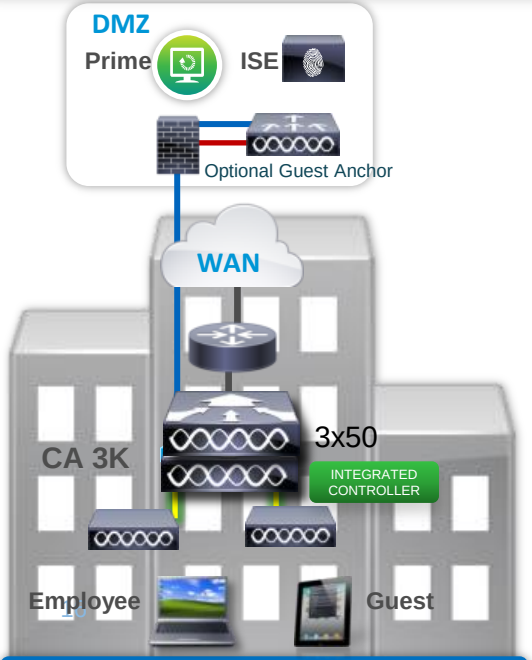
Unified Access - Wireless Deployment Modes

Autonomous	FlexConnect	Centralised	Converged Access
			
Standalone APs	Traffic Distributed at AP	Traffic Centralised at Controller	Traffic Distributed at Switch

Target Positioning	Small Wireless Network	Branch	Campus	Branch and Campus
Purchase Decision	Wireless only	Wireless only	Wireless only	Wired and Wireless
Benefits	• Simple and cost-effective for small networks	• Highly scalable for large number of remote branches • Simple wireless operations with DC hosted controller	• Simplified operations with centralised control for Wireless • Wireless Traffic visibility at the controller	• Wired and Wireless common operations • One Enforcement Point • One OS (IOS) • Traffic visibility at every network layer • Performance optimised for 11ac
Key Considerations	• Limited RRM, no Rogue detection	• L2 roaming only • WAN BW and latency requirements	• System throughput	• Catalyst 3850/3650 in the access layer

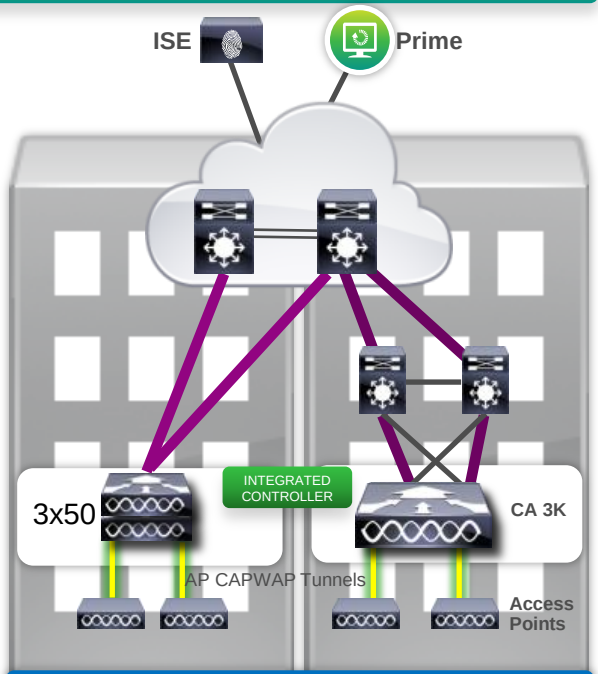
Converged Access Deployment Modes

INTEGRATED CONTROLLER OPTIONS



Controller-less BRANCH

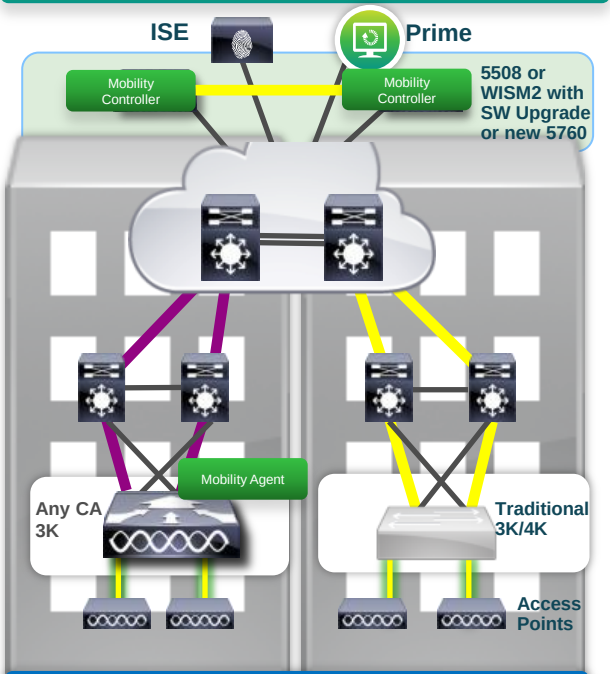
- Up to 25 Access Points with 3650 (50 w3850)
- Up to 1000 Clients per branch with 3650
- All WAN Services Available (local termination)



Controller-less SMALL/MEDIUM CAMPUS

- Up to 200 Access Points with only 3650s
- Up to 250 Access Points with 3850s
- Up to 8000 Clients with only 3650s (16k w/3850)
- Visibility, Control and resiliency

EXTERNAL MOBILITY CONTROLLER NEEDED



LARGE CAMPUS with Controllers

- Up to 72 000 Access Points (5760 or WiSM-2)
- Up to 1 080 000 clients (WiSM-2 as MCs)
- Largest Layer 3 roaming domains

Capwap Tunnel | Standard Ethernet, No Tunnels | Guest Tunnel from Switch to DMZ Controller

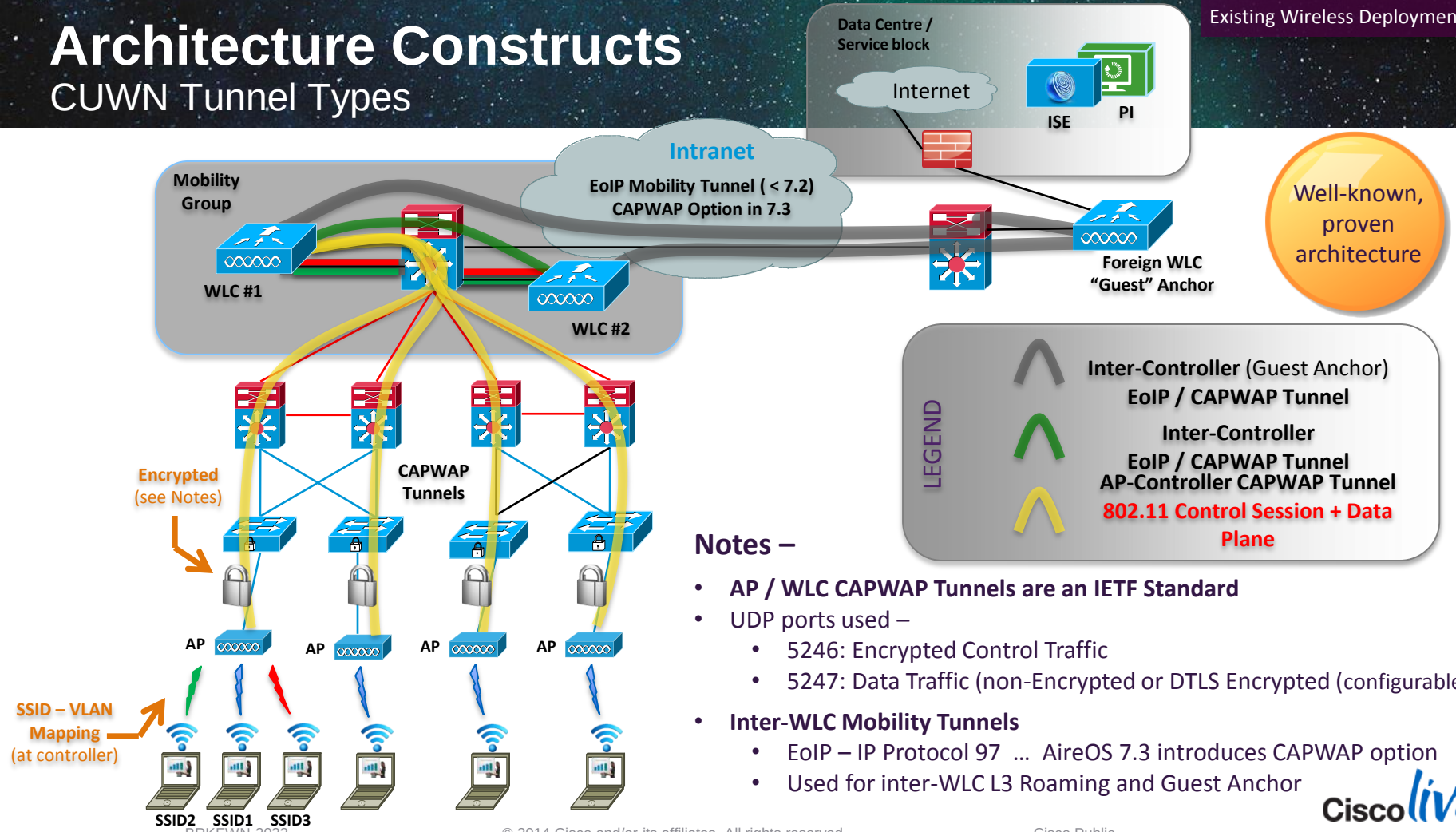
Agenda

- What is Converged Access ?
- Converged Access Platforms Overview
- Wireless Deployment Options
- **The new Converged Access Mobility Architecture**
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Architecture Constructs

CUWN Tunnel Types

Existing Wireless Deployment today



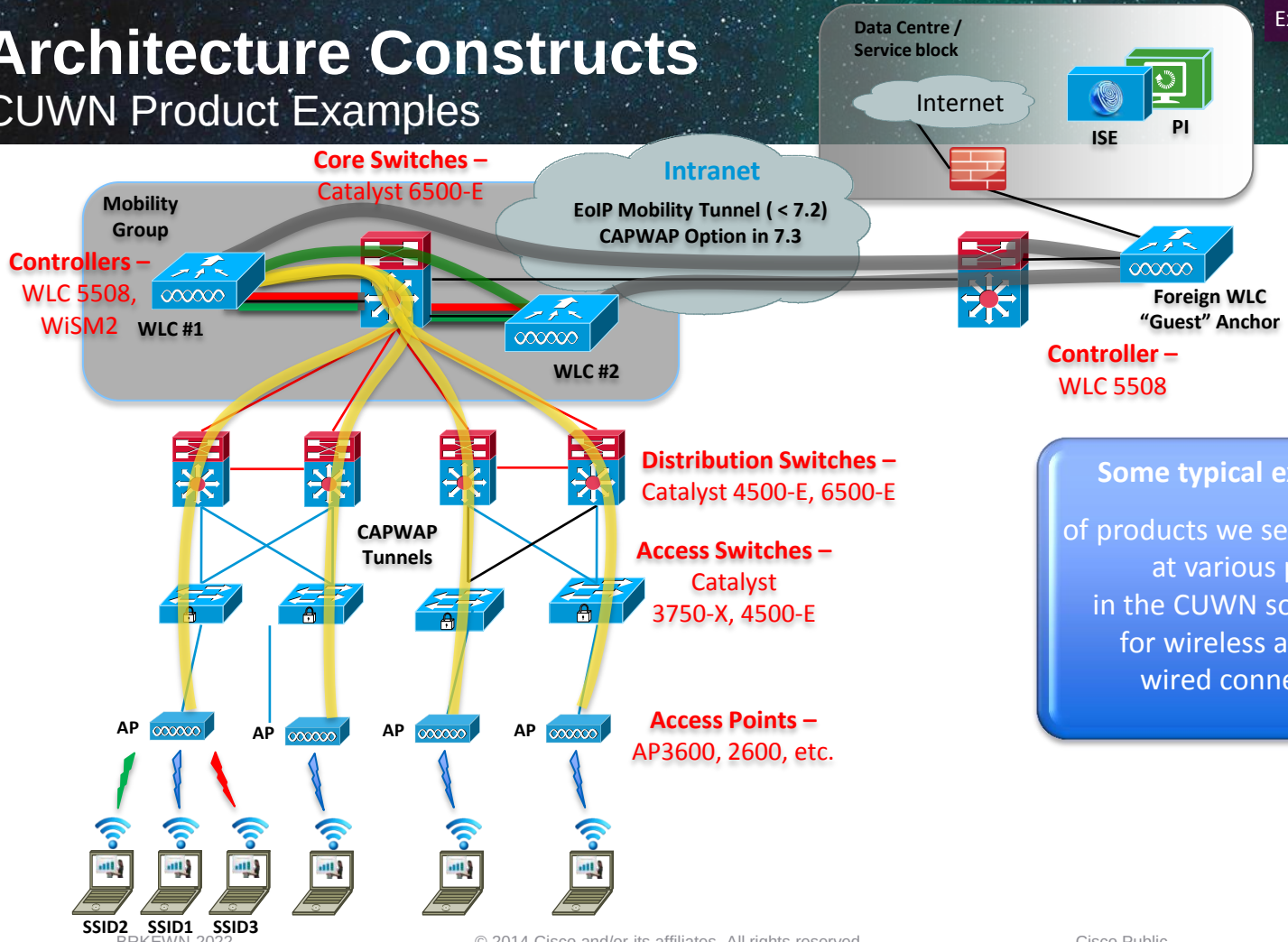
Notes –

- **AP / WLC CAPWAP Tunnels are an IETF Standard**
- UDP ports used –
  - 5246: Encrypted Control Traffic
  - 5247: Data Traffic (non-Encrypted or DTLS Encrypted (configurable))
- **Inter-WLC Mobility Tunnels**
  - EoIP – IP Protocol 97 … AireOS 7.3 introduces CAPWAP option
  - Used for inter-WLC L3 Roaming and Guest Anchor

Architecture Constructs

CUWN Product Examples

Existing Wireless Deployment today

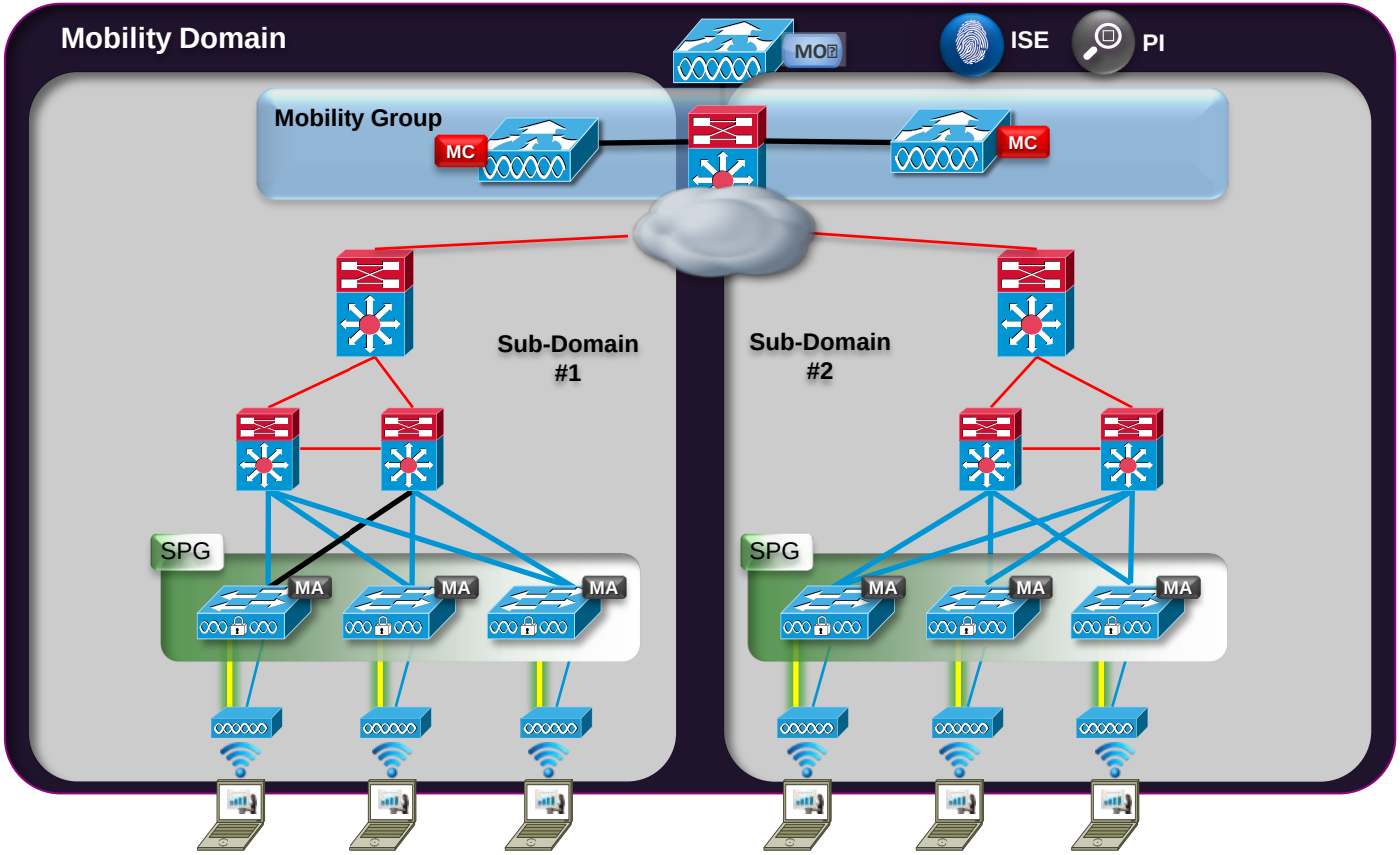


Well-known, proven architecture

Some typical examples –

of products we see used today at various points in the CUWN solution set, for wireless as well as wired connectivity

Converged Access — Deployment Overview



Converged Access
Components – Physical vs. Logical Entities

Physical Entities –

- **Mobility Agent (MA)** – Terminates CAPWAP tunnel from AP
- **Mobility Controller (MC)** – Manages mobility within and across Sub-Domains
- **Mobility Oracle (MO)** – Superset of MC,
  allows for Scalable Mobility Management within a Domain

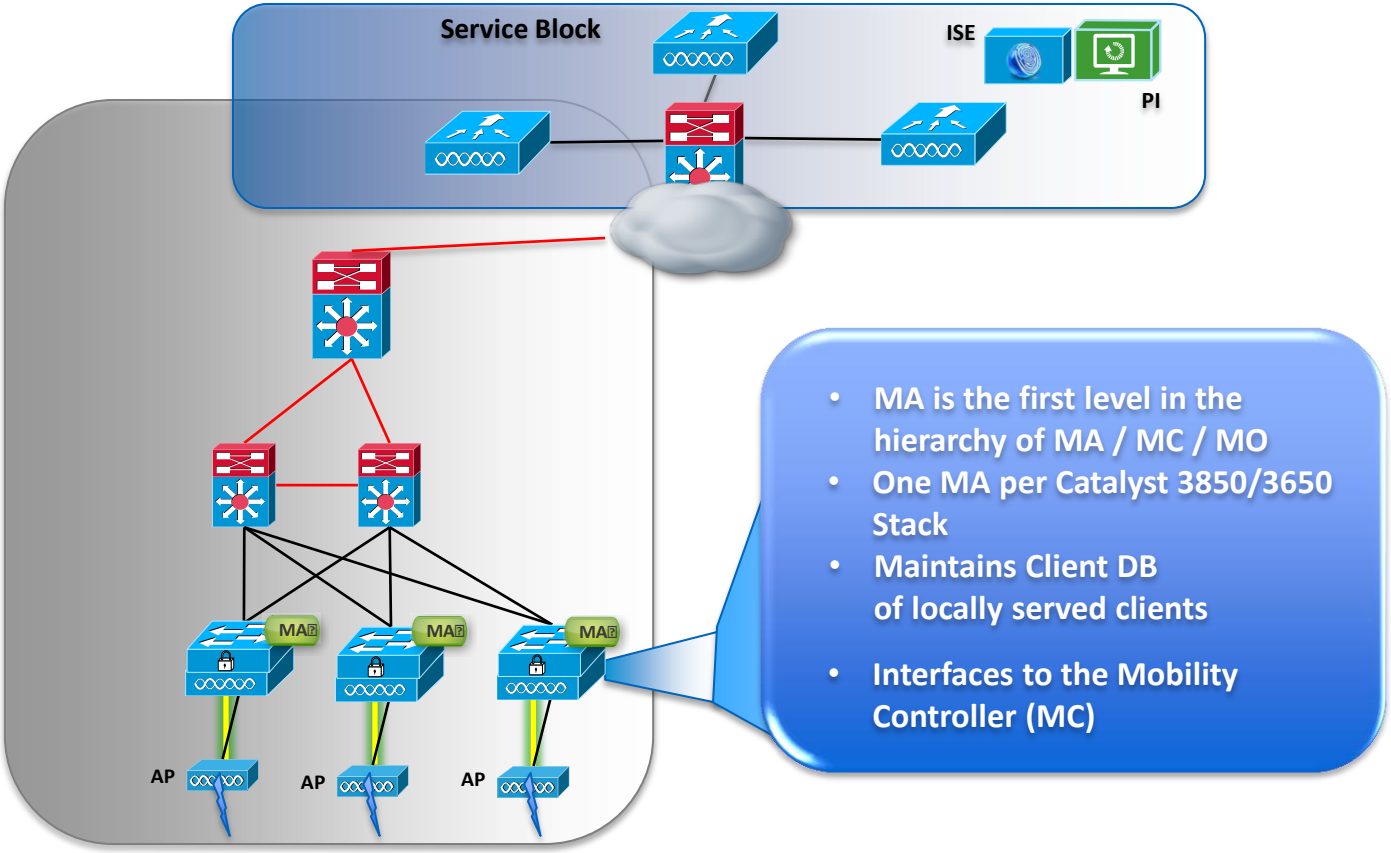
Logical Entities –

- **Mobility Groups –** Grouping of Mobility Controllers (MCs)
  to enable Fast Roaming, Radio Frequency Management, etc.
- **Switch Peer Group (SPG) –** Localises traffic for roams within its Distribution Block

MA, MC, Mobility Group functionality all exist in today's controllers (4400, 5500, WiSM2)

Converged Access

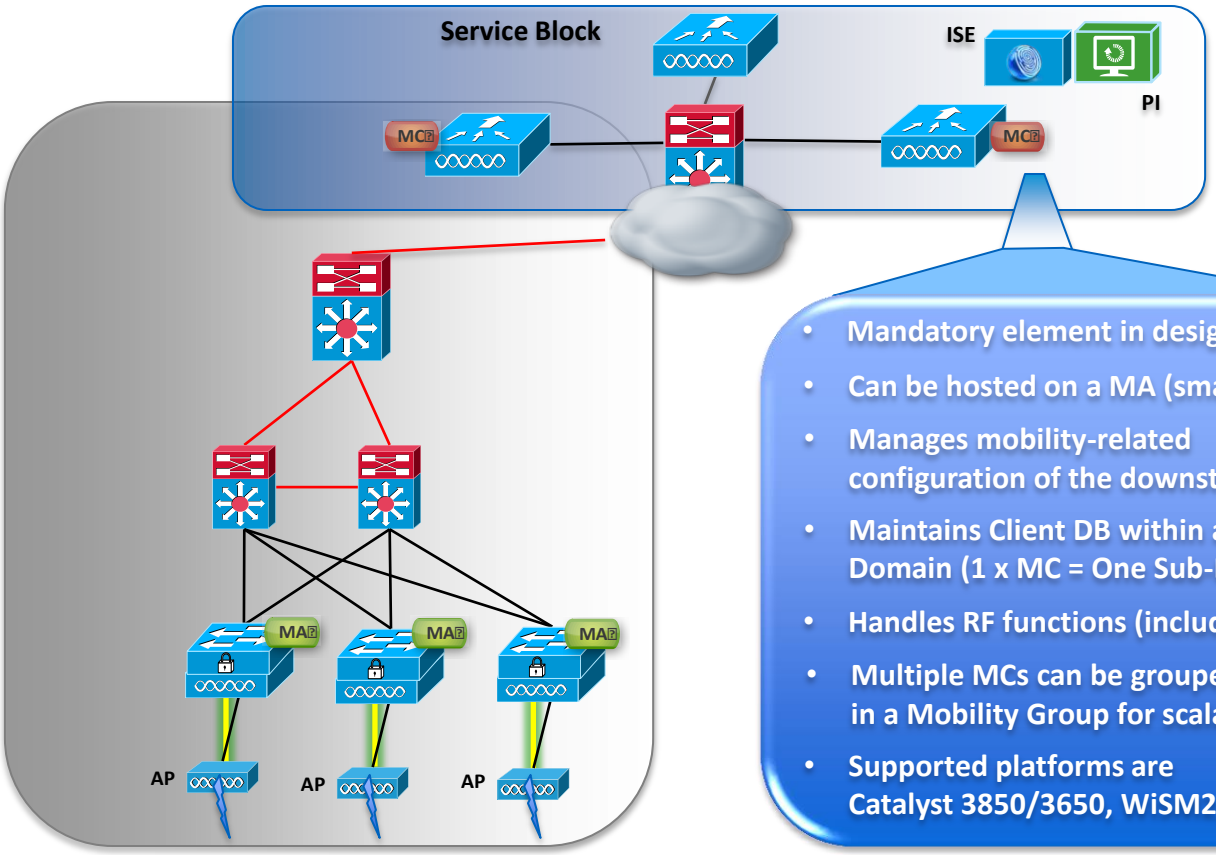
Physical Entities – Mobility Agents (MA)



- MA is the first level in the hierarchy of MA / MC / MO
- One MA per Catalyst 3850/3650 Stack
- Maintains Client DB of locally served clients
- Interfaces to the Mobility Controller (MC)

Converged Access

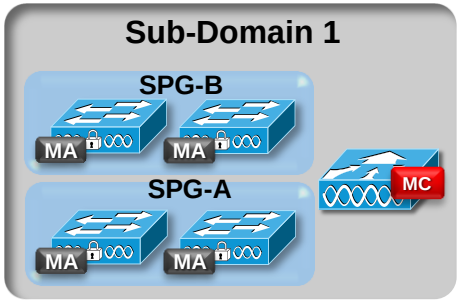
Physical Entities – Mobility Controllers (MC)



- Mandatory element in design
- Can be hosted on a MA (smaller deployments)
- Manages mobility-related configuration of the downstream MAs
- Maintains Client DB within a Sub-Domain (1 x MC = One Sub-Domain)
- Handles RF functions (including RRM)
- Multiple MCs can be grouped together in a Mobility Group for scalability
- Supported platforms are Catalyst 3850/3650, WiSM2, 5508, and 5760

Converged Access

Logical Entities – Switch Peer Groups (SPGs)



- **Made up of multiple Catalyst 3x50 switches as Mobility Agents** (MAs), **plus an MC** (on controller as shown)
- **Handles roaming across SPG** (L2 / L3)
- **MAs within an SPG are fully-meshed** (auto-created at SPG formation)
- **Fast Roaming within an SPG**
- **Multiple SPGs under the control of a single MC form a Sub-Domain**

SPGs are a logical construct, not a physical one …

SPGs can be formed across Layer 2 or Layer 3 boundaries

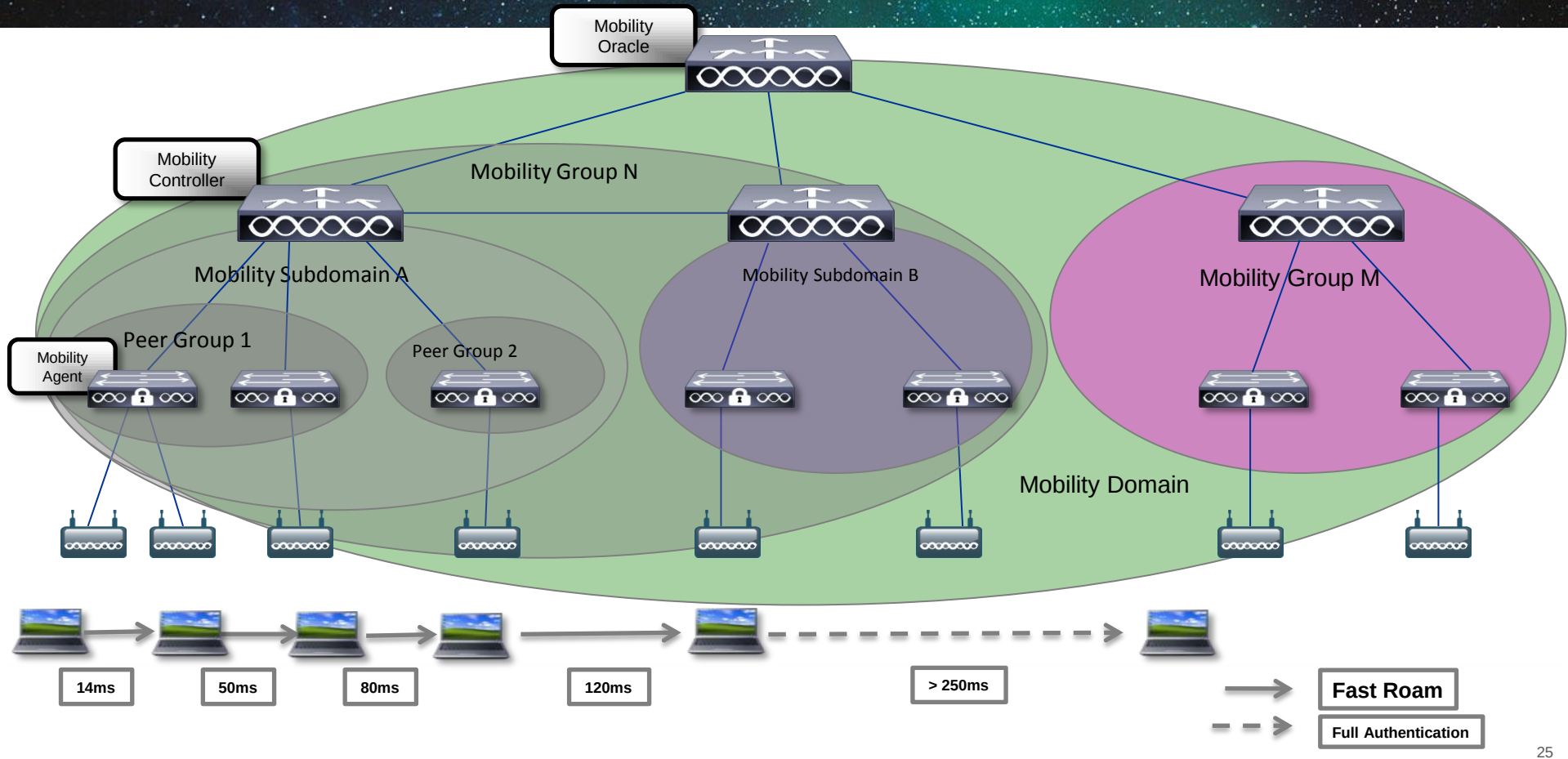
SPGs are designed to constrain roaming traffic to a smaller area, and optimise roaming capabilities and performance

Current thinking on best practices dictates that **SPGs will likely be built around buildings, around floors within a building, or other areas that users are likely to roam most within**

Roamed traffic <u>within</u> an SPG moves directly between the MAs in that SPG (CAPWAP full mesh)

Roamed traffic <u>between</u> SPGs moves via the MC(s) servicing those SPGs

Converged Access: Mobility Architecture



Converged Access – Scalability Considerations

For Your Reference

As with any solution – there are scalability constraints to be aware of …

- **These are summarised below, for quick reference**

Scalability	3650 as MC (3.3.1SE)	3850 as MC (3.3.1SE)	WLC2504 (7.6)	WLC5760 (7.6)	WLC5508 (7.6)	WiSM2 (7.6)
Max APs Supported per MC	25	50	75	1000	500	1000
Max APs Supported in overall Mobility Domain	200	250	5400	72000	36000	72000
Max Clients Supported per MC	1000	2000	1000	12000	7000	15000
Max Clients Supported in overall Mobility Domain	8000	16000	72000	864000	504000	1.08M
Max number of MC in Mobility Domain	8	8	72	72	72	72
Max number of MC in Mobility Group	8	8	24	24	24	24
Max number of MAs in Sub-domain (per MC)	16	16	350	350	350	350
Max number of SPGs in Mobility Sub-Domain (per MC)	8	8	24	24	24	24
Max number of MAs in a SPG	16	16	64	64	64	64
Max number of WLANs	64	64	16	512	512	512

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- **How to deploy a Converged Access network?**
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Converged Access Deployment

Before You Begin – How to Connect APs

- The Catalyst 3850 and 3650 support only **directly attached APs**

  APs need to be in the same VLAN as the Wireless Management interface:

```
interface GigabitEthernet1/0/1
description to_AP
switchport access vlan 31
switchport mode access
```

```
interface Vlan31
 ip address 192.168.31.42 255.255.255.0
 !
 wireless management interface Vlan31
```

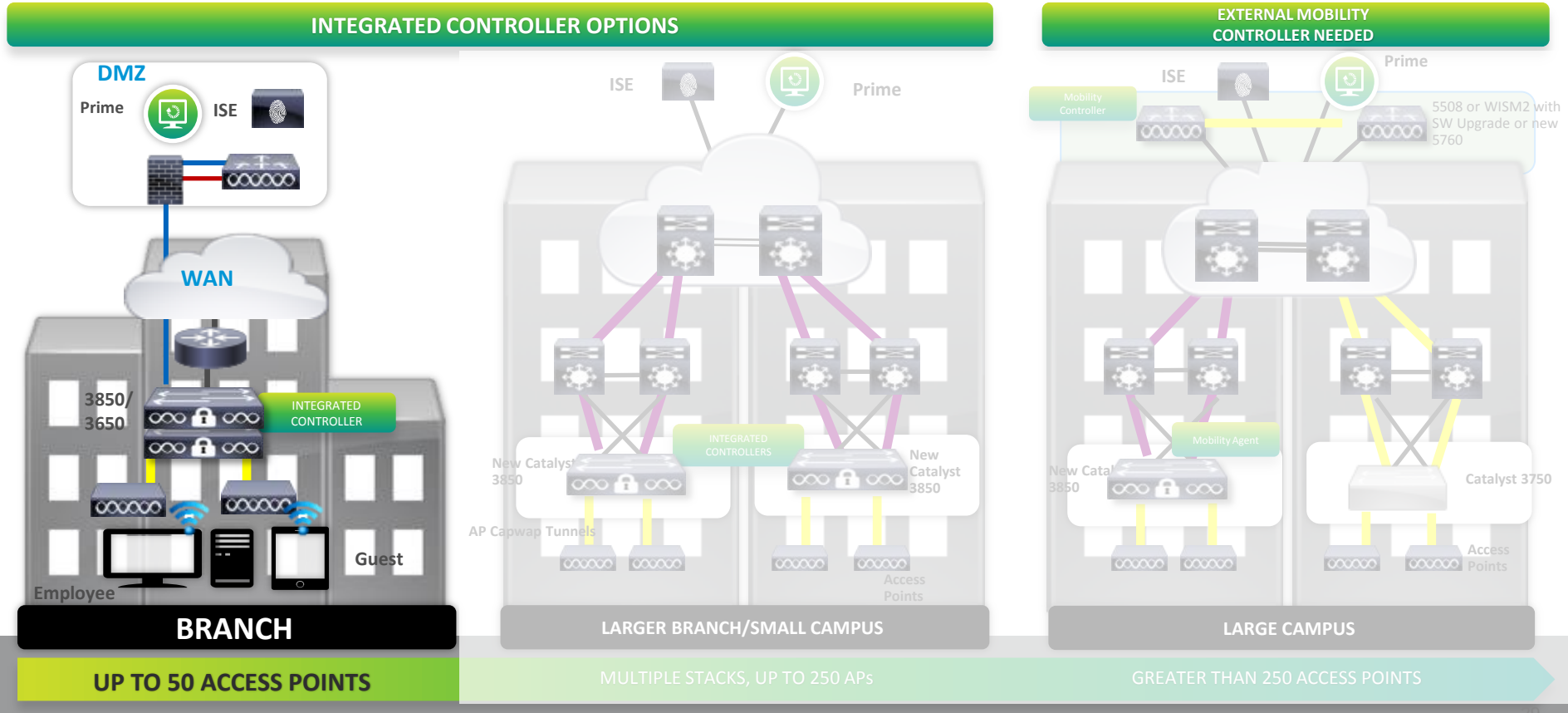
  If you do not define a wireless management VLAN on the 3x50, the switch will then be transparent to AP attachment and everything will continue to operate as it does today on a 3750-X.

  As soon as you define a «wireless management interface VLAN», the Catalyst 3x50 will intercept all incoming AP CAPWAP requests, and terminate / process them at the local ASIC.

- WLC 5760 supports only NON-directly attached APs

  Same as it works today in CUWN: AP attached to a local switch (3750-X or alike) finds the centralised controller through DHCP option 43 or other methods and registers

Converged Access Deployment – Branch Use Case



Converged Access Deployment

Branch Use Case – Mobility Configuration

- Management VLAN Configuration

```
interface Vlan31
 description MANAGEMENT VLAN
 ip address 192.168.31.42 255.255.255.0
```

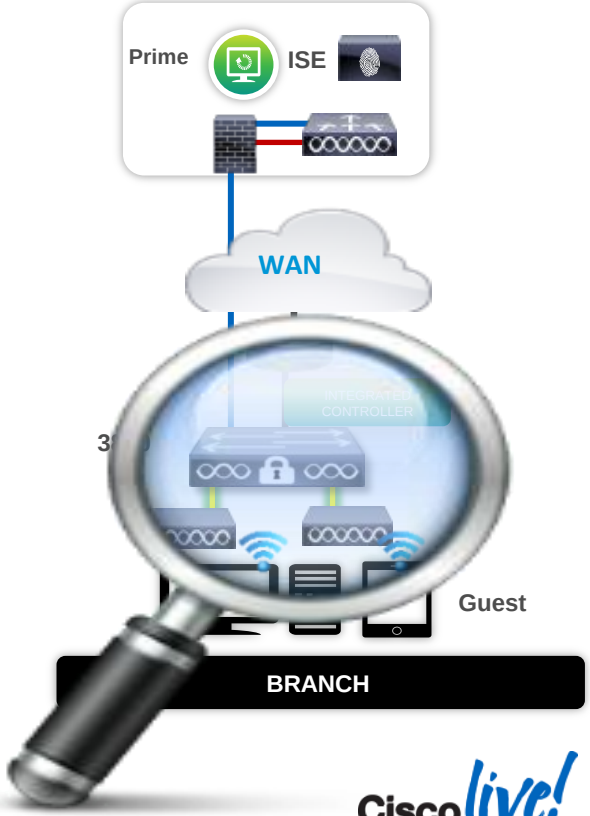
- SVIs for client VLANs defined locally on the switch

```
interface Vlan32
 description Client VLAN32
 ip address 192.168.32.2 255.255.255.0

interface Vlan33
 description Client VLAN33
 ip address 192.168.33.2 255.255.255.0
```

- Wireless Management Interface Configuration

```
3850(config)# wireless management interface VLAN31

    3850# show wireless Interface summary
    Wireless Interface Summary
    AP Manager on management Interface: Enabled
Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
-------------------------------------------------------------------------------------
Vlan31         Management     31     192.168.31.42   255.255.255.0  2037.06ce.0a55
```

This activates the MA functionality



Converged Access Deployment

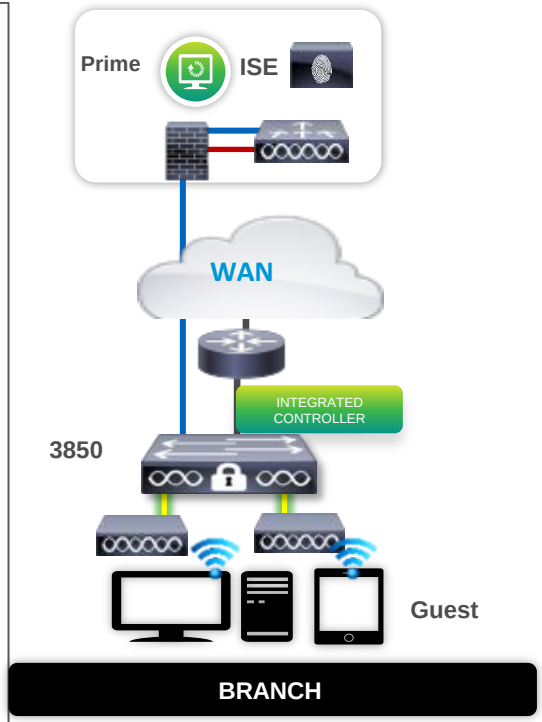
Branch Use Case – Mobility Configuration, continued

- Configuring Mobility Controller

```
3850(config)# wireless mobility controller

Mobility role changed to Mobility Controller
Please save config and reboot the whole stack

3850# sh wireless mobility summary
Mobility Controller Summary:

Mobility Role                                    : Mobility Controller
Mobility Protocol Port                           : 16666
Mobility Group Name                              : default
Mobility Oracle IP Address                       : 0.0.0.0
DTLS Mode                                        : Enabled
Mobility Domain ID for 802.11r                   : 0xac34
Mobility Keepalive Interval                      : 10
Mobility Keepalive Count                         : 3
Mobility Control Message DSCP Value              : 0
Mobility Domain Member Count                     : 1
Link Status is Control Path Status               : Data Path Status

Controllers configured in the Mobility Domain:
IP              Public IP       Group Name      Multicast IP    Link Status
-----------------------------------------------------------------------------------------
192.168.31.42   -               default         0.0.0.0         UP : UP
```

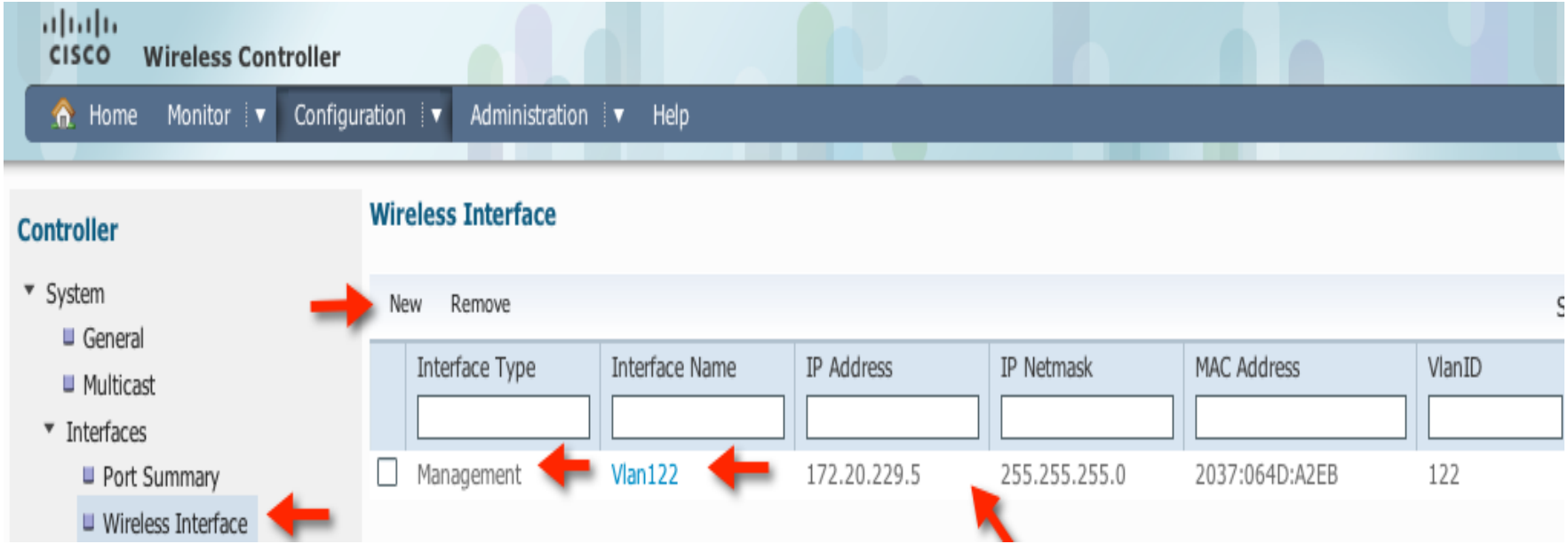
This activates the MC functionality

After reboot

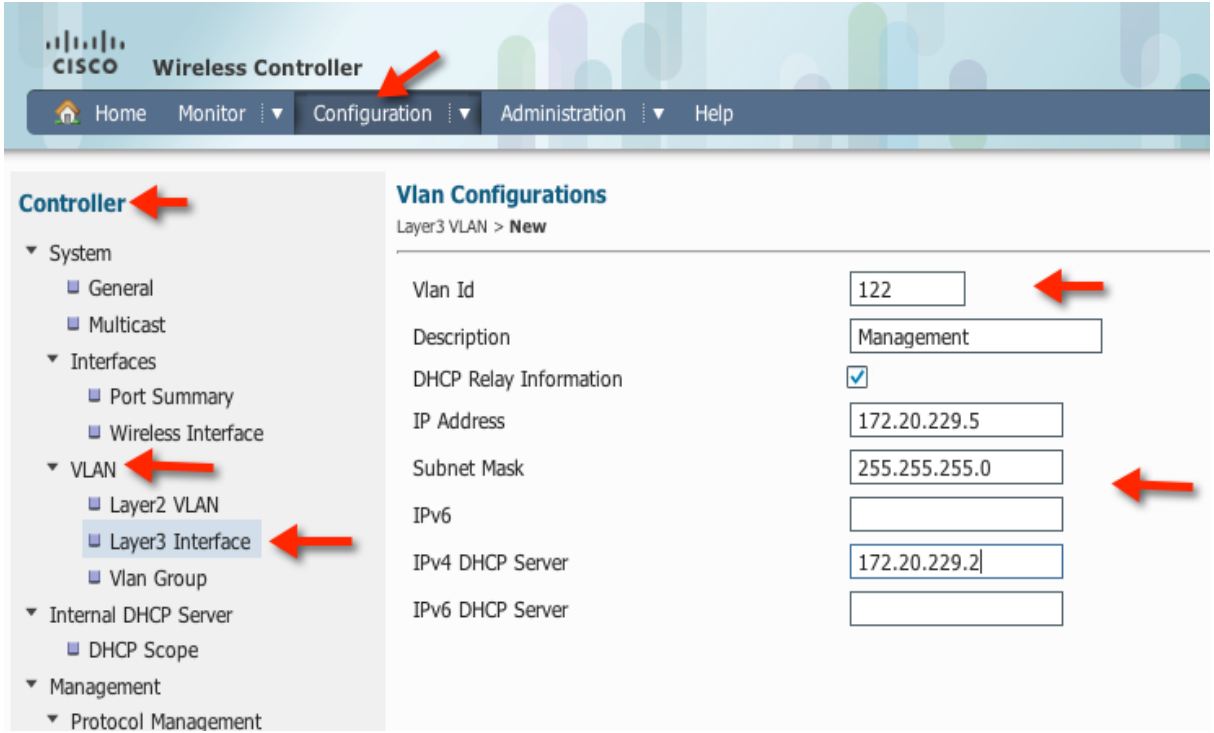


GUI: Wireless Management Configuration

IOS GUI



GUI: VLAN Interface Configuration



IOS GUI

Converged Access Deployment

Branch Use Case – AP Port and WLAN Configuration

- Access Point port configuration

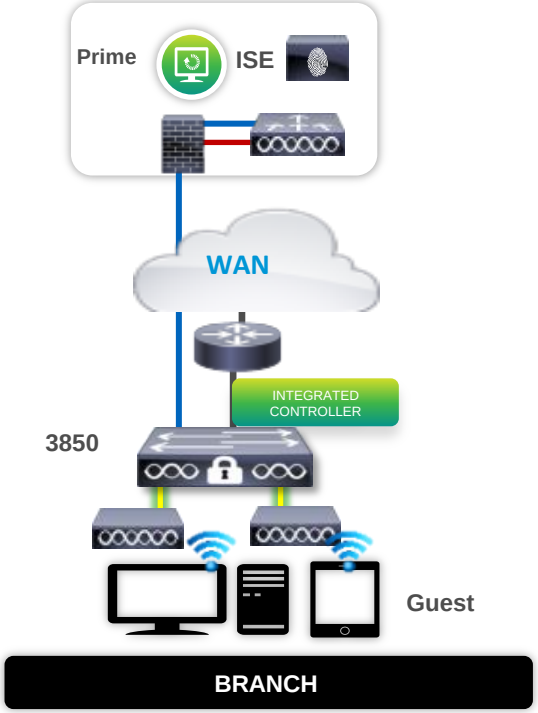
```
interface GigabitEthernet1/0/15
      description - Access port for Access points
      switchport access vlan 31
      switchport mode access

3850# show ap summary
     Number of APs: 1

     Global AP User Name: Not configured
     Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
-------------------------------------------------------------------------------------
AP3502I                          3502I     c47d.4f3a.ed80  04fe.7f49.58c0  Registered
```

Access Points need to be configured on Wireless Management VLAN

- WLAN Configuration

```
3850(config)# wlan WPA-PSK 4 wpa-psk
3850(config-wlan)# client vlan 32
3850(config-wlan)# no security wpa akm dot1x
3850(config-wlan)# security wpa akm psk set-key ascii 0 Cisco1234
3850(config-wlan)# no shut
```

WLAN sample configuration

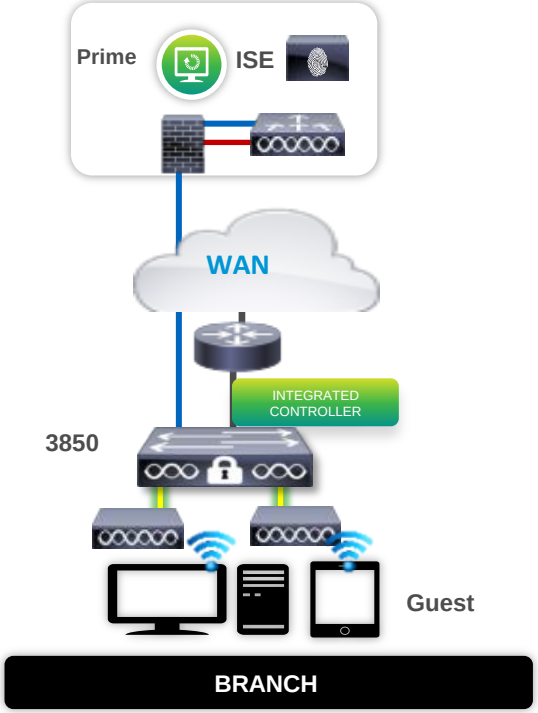


Converged Access Deployment

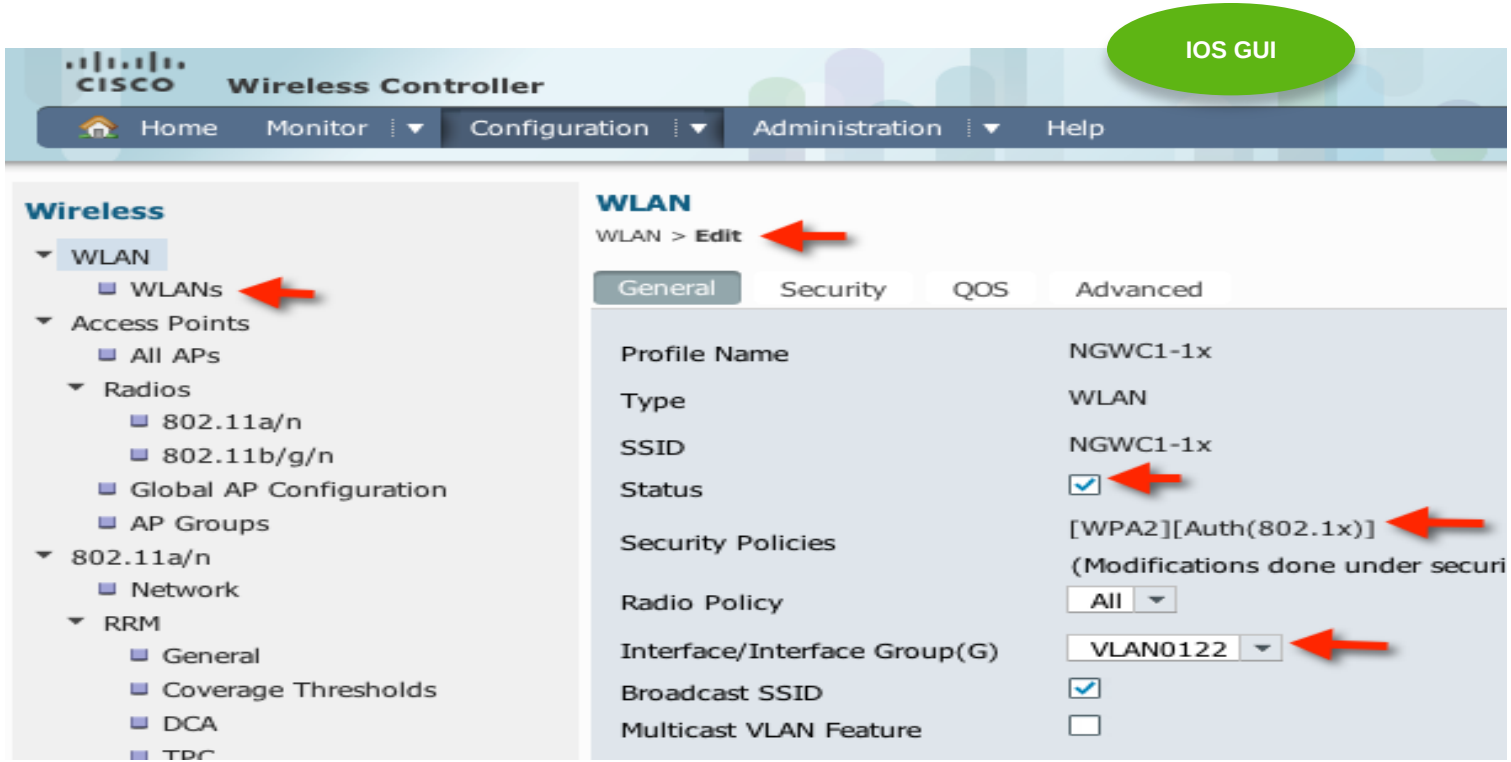
Branch Use Case – Client Connectivity

- Client Connectivity

```
3850# sh wireless client summary

Number of Local Clients : 1

MAC Address     AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
f81e.dfe2.e80e AP3502I                                4    UP              11n(5)


3850# sh wcdb database all

     Total Number of Wireless Clients          = 1
       Clients Waiting to Join        = 0
       Local Clients                  = 1
       Anchor Clients                 = 0
       Foreign Clients                = 0
       MTE Clients                    = 0

      Mac Address     VlanId  IP Address       Auth      Mob
      --------------  ------ --------------- -------  -----
      f81e.dfe2.e80e    32    192.168.32.57    RUN     LOCAL
```



GUI: WLAN Configuration

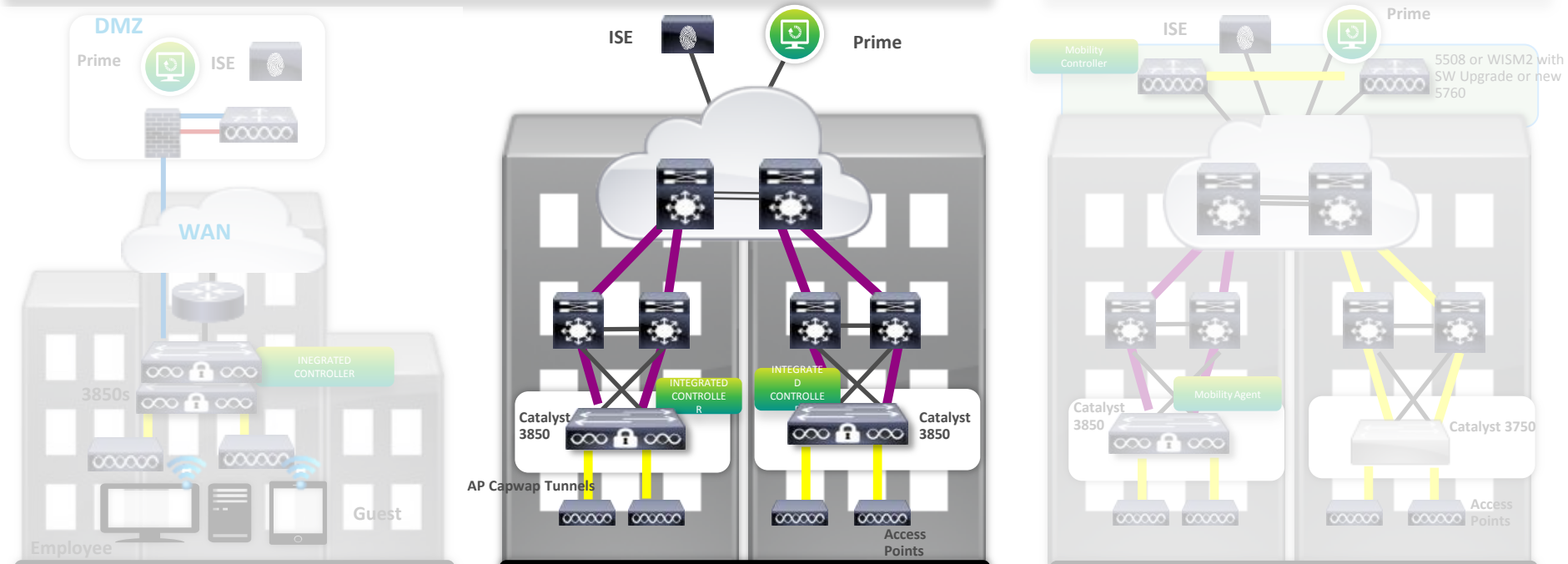


Converged Access Deployment

Larger Branch / Small Campus Use Case

INTEGRATED CONTROLLER OPTIONS

EXTERNAL MOBILITY CONTROLLER NEEDED



BRANCH

LARGER BRANCH / SMALL CAMPUS

LARGE CAMPUS

UP TO 50 ACCESS POINTS

MULTIPLE STACKS, UP TO 250 APs

GREATER THAN 250 ACCESS POINTS

Capwap Tunnel

Standard Ethernet, No Tunnels

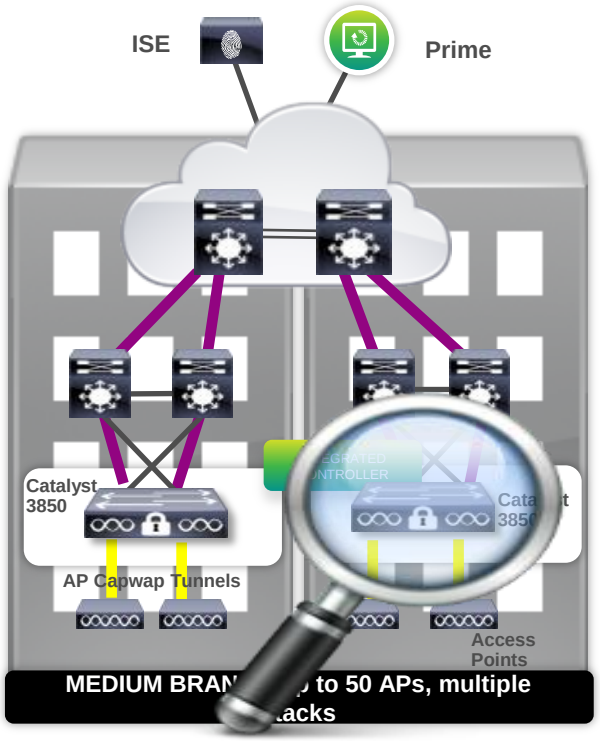
Guest Tunnel from Switch to DMZ Controller

Converged Access Deployment

Larger Branch / Small Campus Use Case – SPG Configuration

```
3850-MC1# sh wireless mobility summary

Mobility Controller Summary:

Mobility Role                              : Mobility Controller
Mobility Protocol Port                     : 16666
Mobility Group Name                        : default
Mobility Oracle IP Address                 : 0.0.0.0
DTLS Mode                                  : Enabled
Mobility Domain ID for 802.11r             : 0xac34
Mobility Keepalive Interval                : 10
Mobility Keepalive Count                   : 3
Mobility Control Message DSCP Value        : 0
Mobility Domain Member Count               : 1

Link Status is Control Path Status : Data Path Status

Controllers configured in the Mobility Domain:

IP              Public IP       Group Name      Multicast IP    Link Status
-----------------------------------------------------------------------------
192.168.31.42   -               default         0.0.0.0          UP  : UP

Switch Peer Group Name                     : GroupABC
Switch Peer Group Member Count             : 1
Bridge Domain ID                           : 0
Multicast IP Address                       : 0.0.0.0

IP              Public IP            Link Status
-------------------------------------------------
192.168.41.44   192.168.41.44        UP: UP
```

Both control and data plane need to be UP



Converged Access Deployment

Larger Branch / Small Campus Use Case – Multiple MCs

- MC configuration on the 3850 to create a Mobility Group and add the other switch as a member

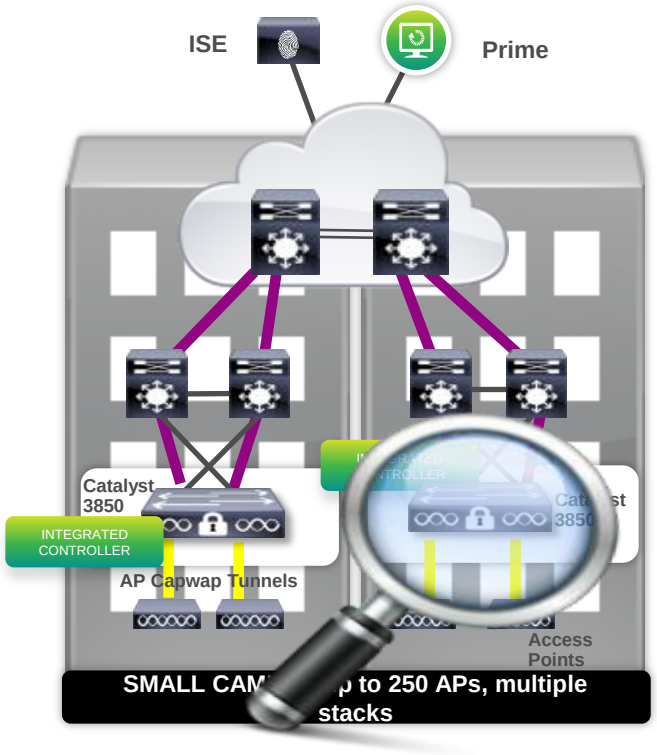
```
3850-MC1(config)# wireless mobility group name Mobility-GroupABC

3850-MC1(config)# wireless mobility group member ip 192.168.41.44 public-ip
192.168.41.44 Mobility-GroupABC
```

- MC configuration on the other 3850

```
3850-MC2(config)# wireless mobility controller

Mobility role changed to Mobility Controller
Please save config and reboot the whole stack
```

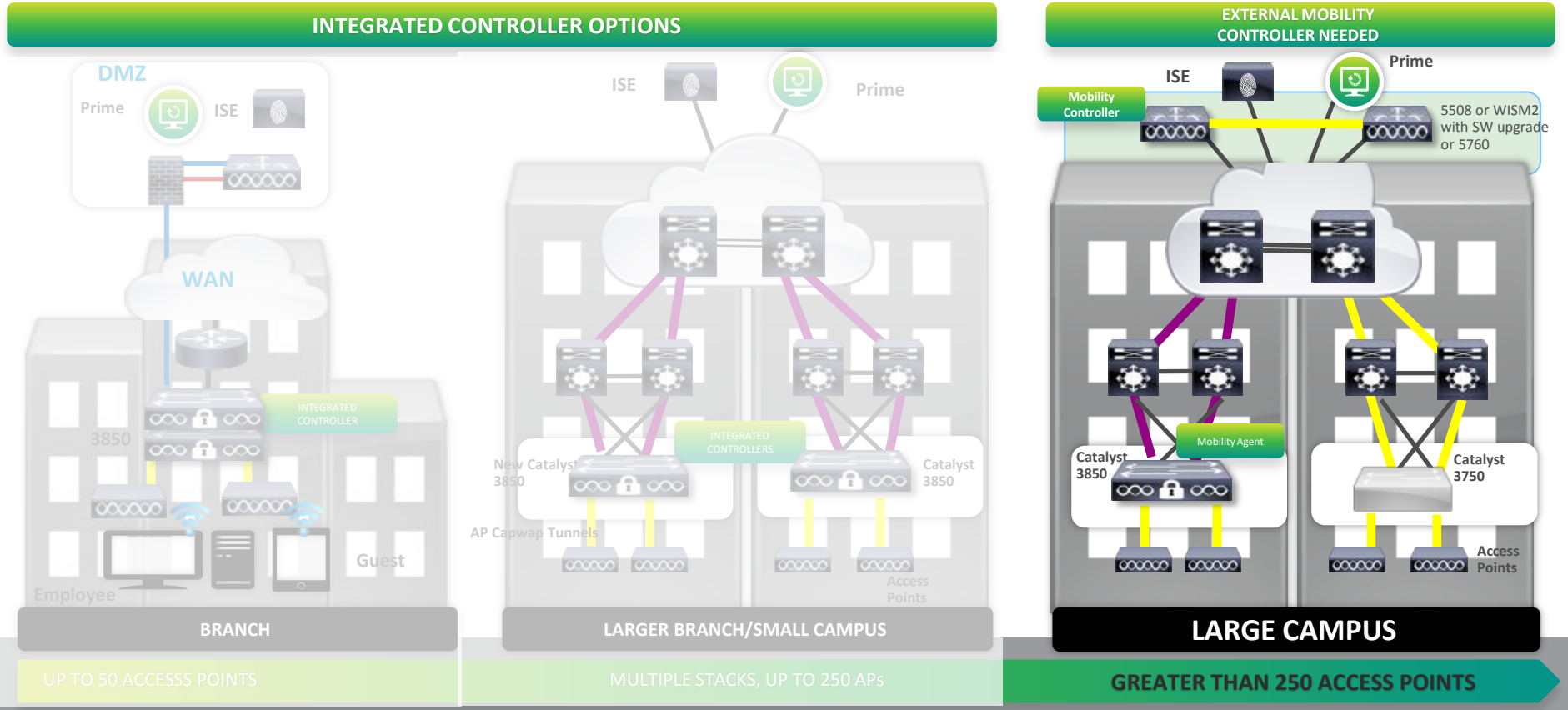
This switch is now also a Mobility Controller, not only a Mobility Agent

```
3850-MC2(config)# wireless mobility group name Mobility-GroupABC

3850-MC2(config)# wireless mobility group member ip 192.168.31.42 public-ip
192.168.31.42 Mobility-GroupABC
```



Converged Access Deployment

Large Campus Use Case



Converged Access Deployment

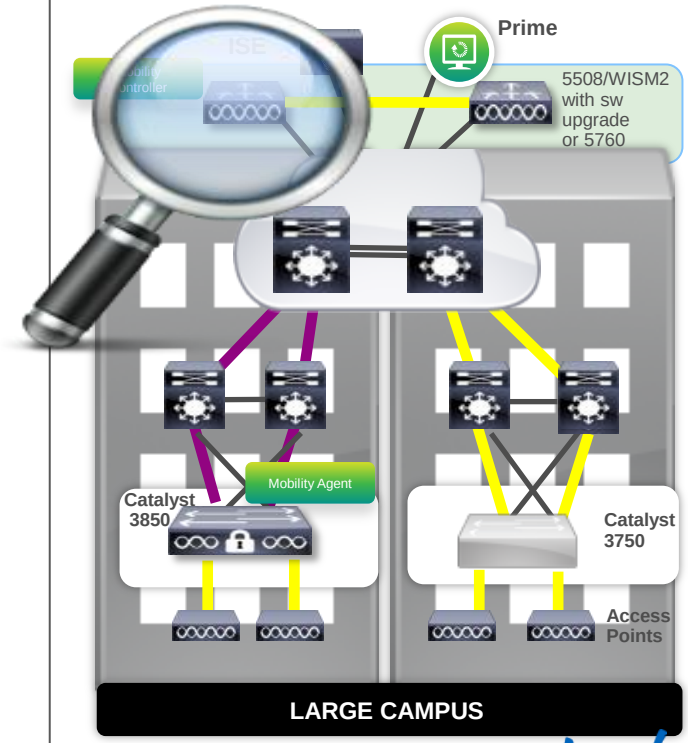
Large Campus Use Case – Mobility Configuration

- Configure 5760 as MC and member of SPG

```
interface Vlan100
 description WIRELESS MANAGEMENT VLAN
 ip address 192.168.100.42 255.255.255.0

5760(config)# wireless management interface VLAN100

5760(config)# wireless mobility controller peer-group WestBldg

5760(config)# wireless mobility controller peer-group WestBldg member ip
 10.1.1.5
```

- Configure 3850 as MA

```
interface Vlan10
 description MANAGEMENT VLAN
 ip address 10.1.1.5 255.255.255.0

3850(config)# wireless management interface VLAN10

3850(config)# wireless mobility controller ip 192.168.100.42
```



Converged Access Deployment

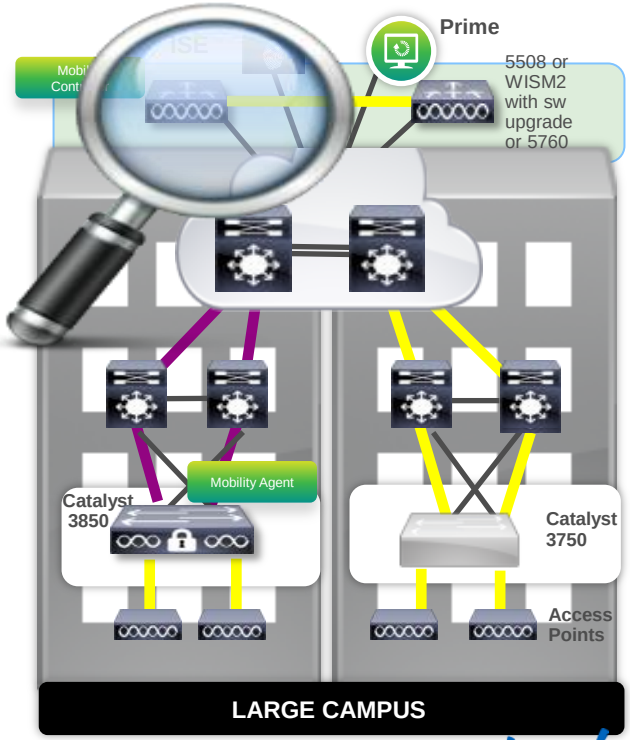
Large Campus Use Case – Mobility Configuration, continued

- Mobility Group configuration

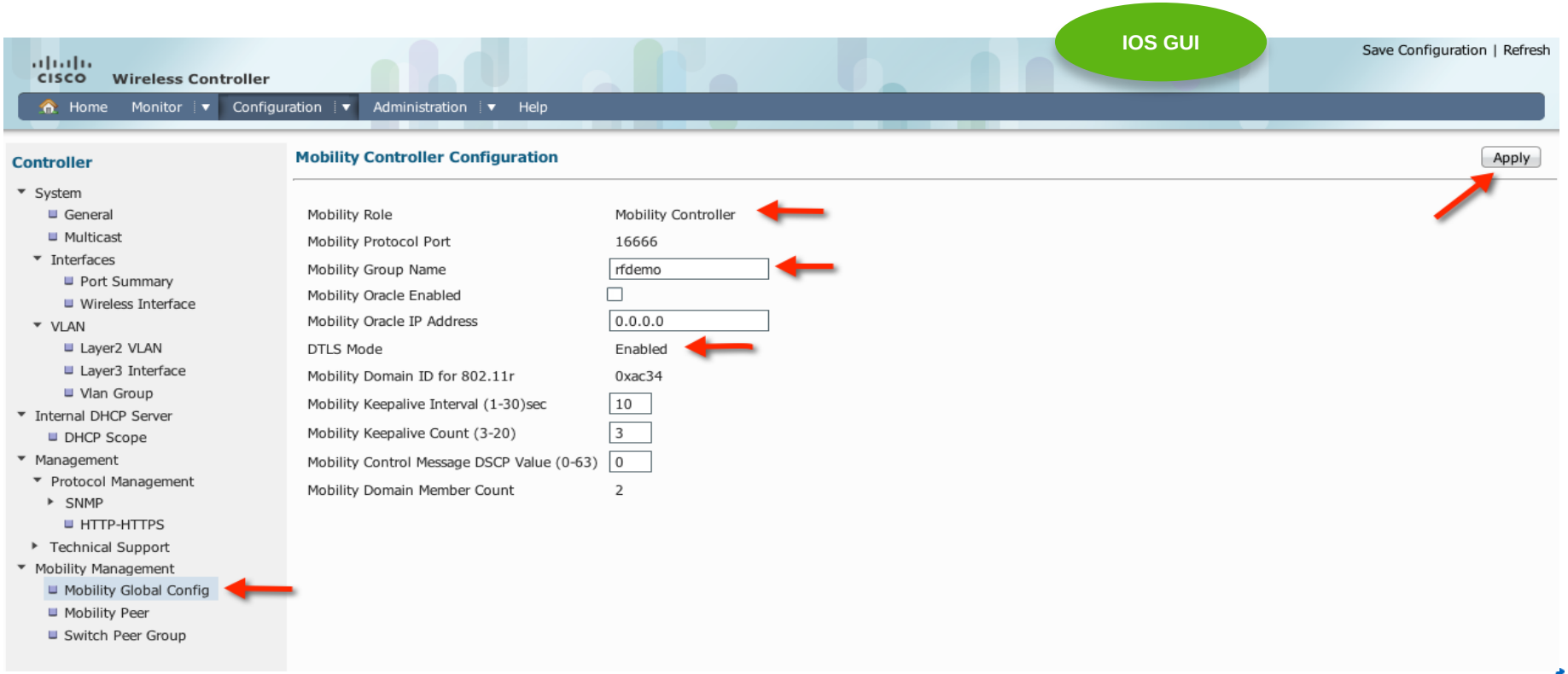
```
5760(config)# wireless mobility group name cisco-live

5760(config)# wireless mobility group member ip 10.1.1.5
```

- Verify the configuration

```
5760# sh wireless mobility summary

Mobility Controller Summary:
Mobility Role                                  : Mobility Controller
Mobility Protocol Port                         : 16666

 Controllers configured in the Mobility Domain:

 IP Address       Public IP Address     Group Name            Multicast IP     Status
 ------------------------------------------------------------------------------------
 192.168.100.42   -                     cisco-live            0.0.0.0          UP
 10.1.1.5         10.1.1.5              cisco-live            0.0.0.0          UP

 Switches configured in WestBldg switch Peer Group: 1

 IP Address       Public IP Address     Status
 ---------------------------------------------------------------
 192.168.41.44    192.168.41.44         UP
```

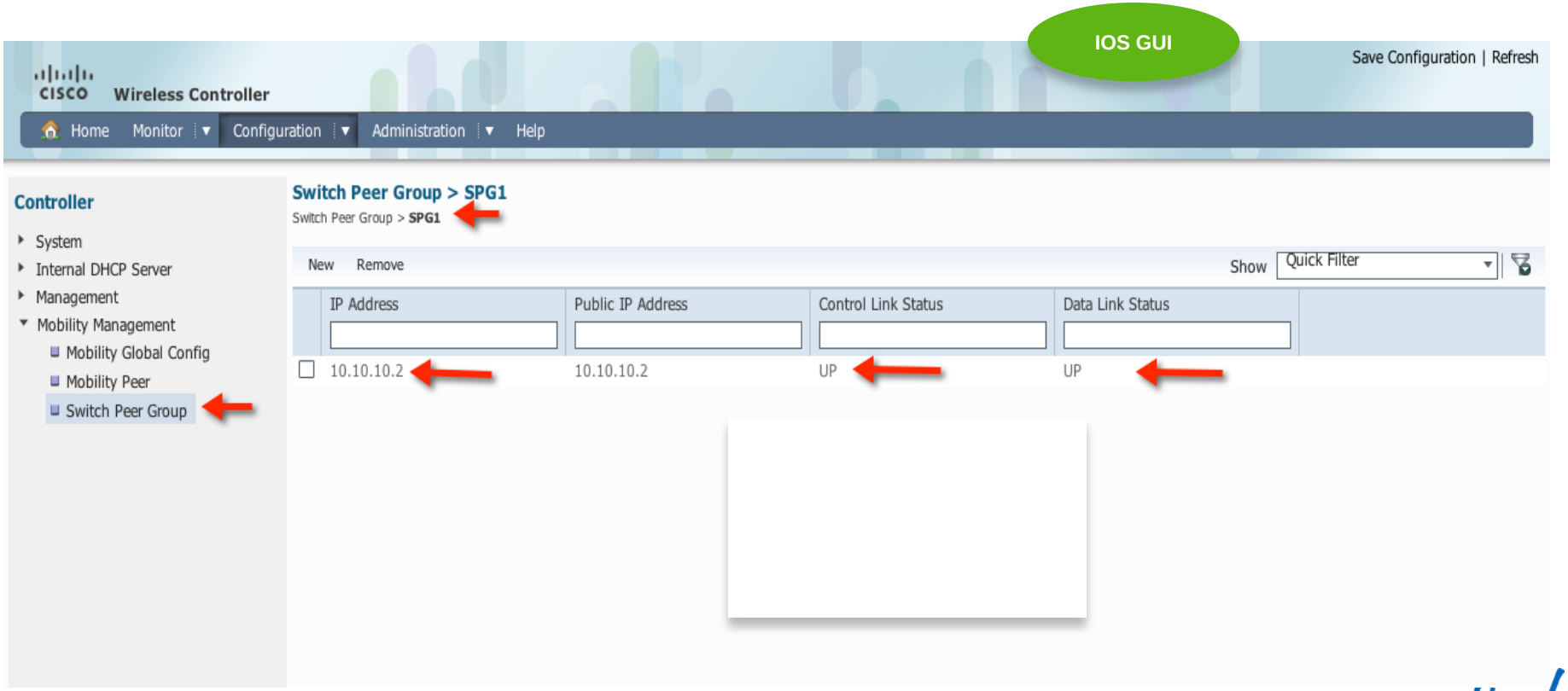


GUI: Mobility Controller Configuration-5760



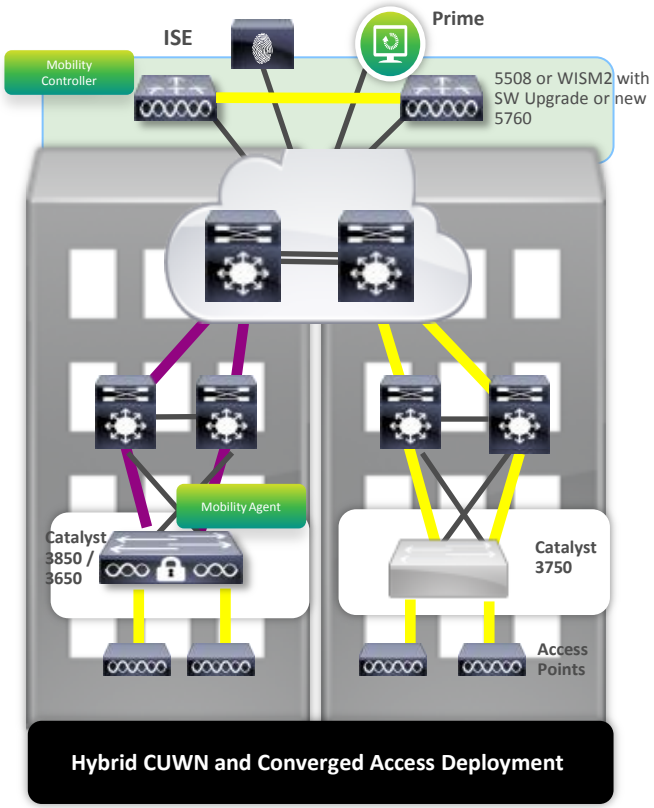
GUI: Mobility Agent Configuration CAT3850

GUI: Switch Peer Group Configuration



Converged Access Deployment

Hybrid Deployment – Key Considerations



- New Mobility is supported on 7.3.112, 7.5 and 7.6 with 5508 and WiSM2
- Only MC and MO functions are supported on the upgraded controller
  - "MA only" functionality for converged access APs is only supported on 3850
- Seamless and Fast roaming is supported between Converged Access and CUWN
  - Controllers need to be In the same Mobility Group
  - Roaming is always treated as a L3 roam
  - Traffic is anchored at the home switch/controller
- 5760 can terminate CAPWAP tunnel from APs connected to non-MA switches
- 3850 (acting as MA) will only allow APs to terminate CAPWAP locally
  - Cannot connect an AP to 3850 and have it registered to a CUWN controller

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- **IOS-XE 3.3 Release Features**
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

Converged Access Deployment

IOS-XE-based Wireless Controllers – Highlights

Differentiating capabilities

- Optimised for 802.11ac deployments
  - Distributed data forwarding & services
  - Support for latest 3700 802.11ac AP!
- Common IOS and Feature Set for Wired and Wireless
  - Granular QoS
  - Downloadable ACLs
  - EEM / TCL Scripting, Secure Copy
  - Flexible Netflow v9
- Multiple LAGs (Aggregated uplinks)
- Secure Web-auth redirection using HTTPS
- Right-To-Use license model

WLC 5760

- 60 Gbps wireless throughput
- Up to 1000 Aps
- Up to 12000 Clients

Catalyst 3850

- 40 Gbps wireless throughput
- Up to 50 directly connected APs / Stack
- Up to 2000 Clients per Switch/Stack

Catalyst 3650

- 40 Gbps wireless throughput
- Up to 25 directly connected APs / Stack
- Up to 1000 Clients per Switch/Stack

Converged Access Deployment – Software Matrix

- Software compatibility matrix for IOS based Controllers:

5760	3850	3650	5508	MSE	ISE	ACS	Prime
3.2.0SE	3.2.0SE	-	7.3.112	-	1.1.1MR	5.2	-
3.2.1SE	3.2.1SE	-	7.3.112	-	1.1.3,1.1.2	5.2, 5.3	-
3.2.2SE	3.2.2SE	-	7.3.112/7.5+	-	1.1.3,1.1.2	5.2,5.3	-
3.2.3SE	3.2.3SE	-	7.3.112/7.5+	7.4	1.1.3,1.1.2	5.2, 5.3	2.0
3.3.0SE	3.3.0SE	3.3.0SE	7.3.112/7.5+	7.5	1.2		2.0*
3.3.1SE	3.3.0SE	3.3.0SE	7.3.112/7.5+	7.5	1.2		2.0*

(*) IOS-XE 3.3 is not officially supported by PI 2.0 because it doesn't support the new features and hardware introduced in IOS-XE 3.3

Converged Access Deployment

WLC 5760 (IOS-XE 3.3) vs. WLC 5508 (AireOS 7.6)

Feature	5508	5760
Throughput	8 Gbps	60 Gbps Line-rate
Scale	500 APs, 7000 Clients	1000 APs, 12000 Clients
Data forwarding Modes	Local, *Flex, Mesh, Outdoor, OEAP*	Local Mode
Resiliency	SSO, N+1, HA SKU	AP SSO, N+1, Multiple LAG, HA SKU
QoS	Alloy (precious metal) QoS	Granular QoS (MQC), AFB
Security	Dynamic ACLs (Airspace ACL)	Downloadable and Dynamic ACLs
BYOD	ISE 1.2, CWA, Device Sensor, Policy Classification Engine	ISE 1.2, CWA
AVC	AVC phase 2, Microsoft Lynch and Jabber support	AV phase 1, without the “C”
Bonjour	Bonjour phase 2 (Location and AP detection)	Bonjour phase 1
IPv6	IPv6 Client Mobility, First Hop Security, Source Guard	IPv6 Client Mobility, First Hop Security
Management	Full featured GUI, AireOS CLI, Secure FTP	IOS CLI, EEM/TCL, Limited GUI
Licensing	License PAK based on serial number	Right to use

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - **Application Visibility**
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

How AV Solution Works

Deep Packet Inspection

DPI engine (NBAR2) identifies applications using L7 signatures

Rel 3.3 WLC/Switch

NFv9

AP

NBAR on AP

Perf. Collection & Exporting

AP collects application info and export it to controller/switch every 90 seconds

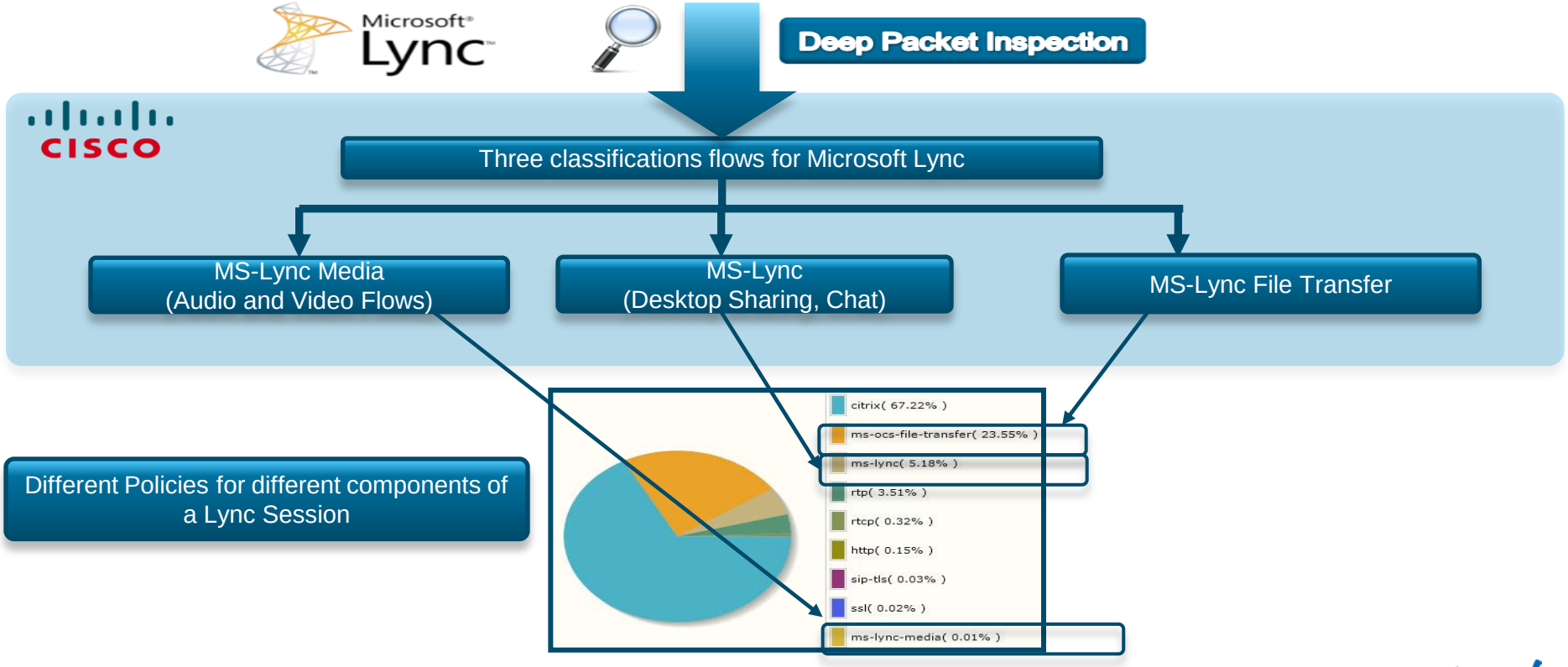
App Visibility & User Experience Report

App	BW	Transaction Time	…
WebEx	3 Mb	150 ms	…
Citrix	10 Mb	500 ms	…

Reporting Tool

Advanced reporting tool aggregates and reports application performance

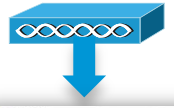
Overview: NBAR2 Classification of Microsoft Lync



In addition to detecting Microsoft Lync, AVC is able to sub-classify and prioritise Audio/Video, Desktop Sharing and File Transfer differently

Application Visibility

Flow ID	App Name	Packets
1	WebEx	2300
2	Msft-Lync	4000
3	Skype	1000
4	YouTube	3000

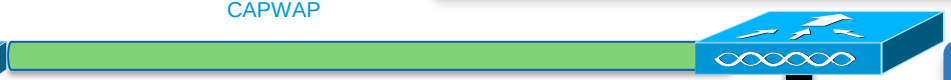


AP

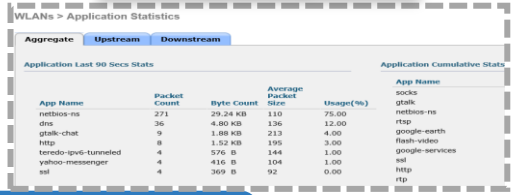
Stateful context transfer on roam

AP

CAPWAP

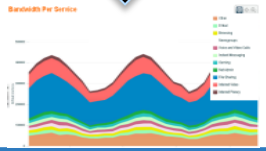


Real-time information for last 90 seconds



Netflow Export from AP to CT-5/760(Centralised) 3850 / 3650 switch(Converged Access)

FLEXIBLE NETFLOW TO CPI OR THIRD PARTY NETFLOW COLLECTOR



Flow ID	App Name	Packets
1	WebEx	1000
2	Msft-Lync	2300
3	Skype	660
4	YouTube	1000

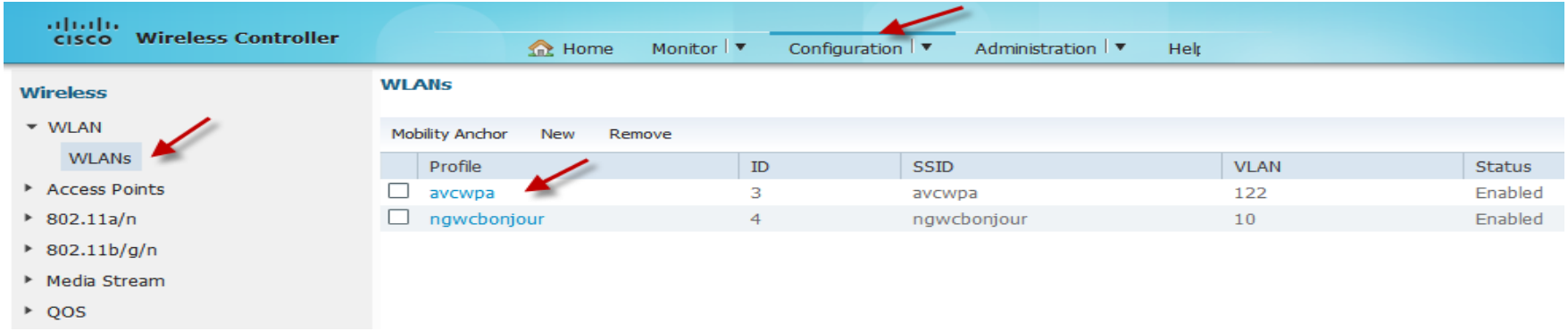
- **NBAR2 (1000+ Applications) and** Flexible Netflow **will be ported onto Access Points!**
- **Stateful context transfer is supported for inter and intra-controller roams**

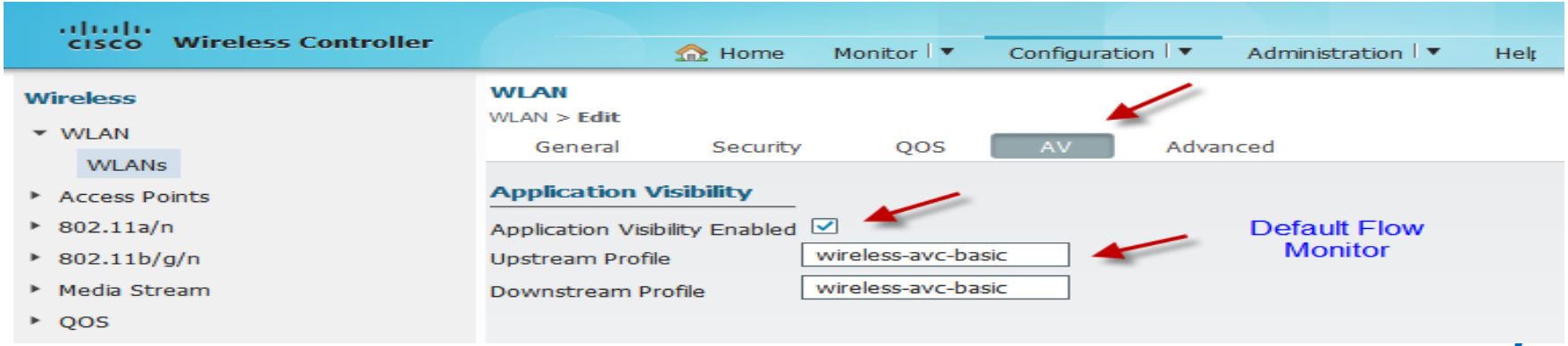
IOS XE 3.3 AV Supported Features

- Application Visibility – No Control
- Supported on IOS platforms: 5760/3850/3650
- Use NBAR2 Protocol pack 5.1
- More than 1000 Applications
- Seamless Roaming
- Supported on the following Aps: AP1600, 2600, 3600 and 3700
- Wireless Clients only
- Centralised and Converged Access
- Flexible Netflow v9 Export to PI(PAM) and external collectors(Plixir, ActionPacked, etc)

AV Configuration from GUI

AV enabled per WLAN basis





AV Monitoring and Statistics : GUI

Client AVC statistics on the WLAN

Controller

- System
- Ports
- Security
- Mobility
- Management
- Statistics
- CDP
- Application Visibility
  - WLANs
- Redundancy
- mDNS

WLANs >Application Statistics

WLANs > Application Statistics

Aggregate | UpStream | DownStream

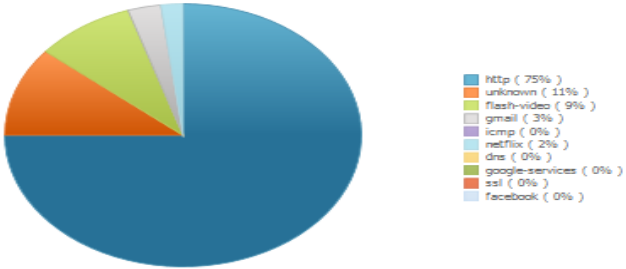
Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
http	1322	777150	587	75
unknown	578	114791	198	11
flash-video	105	95502	909	9
gmail	62	32277	520	3
icmp	33	1848	56	0
netflix	27	18705	692	2
dns	27	2786	103	0
google-services	27	1701	63	0
ssl	15	3438	229	0

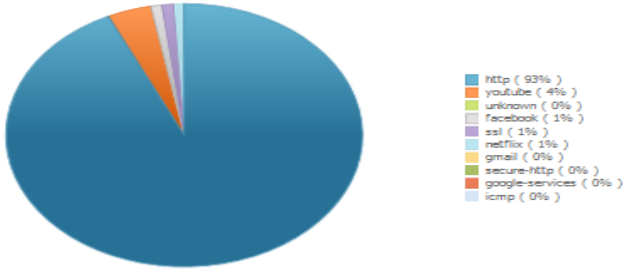
Application Cumulative Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
http	837112	879094449	1050	93
youtube	34879	36631283	1050	4
unknown	23261	3429383	147	0
facebook	8845	5165565	584	1
ssl	7831	4958526	633	1
netflix	7469	6346706	849	1
gmail	6512	4093439	628	0
secure-http	4811	2600637	540	0
google-services	4740	2474517	522	0

Application Last 90 Secs Usage(%)



Application Cumulative Usage(%)



AV Monitoring and Statistics : GUI

Client AVC statistics – Per Client

Clients

- Client Details
  - Clients

Client

Client > Detail

General | AVC Statistics

Aggregate | UpStream | DownStream

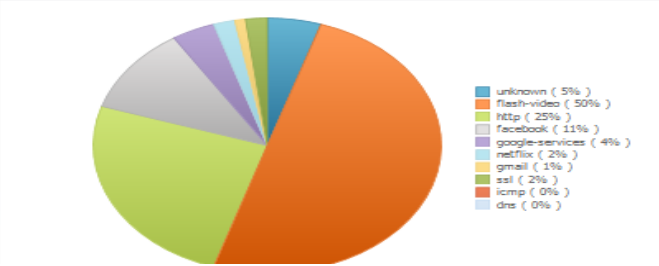
Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
unknown	907	100835	111	5
flash-video	903	945949	1047	50
http	739	476972	645	25
facebook	585	204123	348	11
google-services	188	79777	424	4
netflix	61	35263	578	2
gmail	54	13938	258	1
ssl	42	41906	997	2
icmp	35	1960	56	0

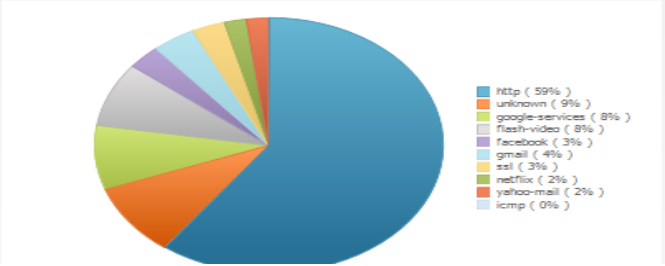
Application Cumulative Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
http	12067	8657719	717	59
unknown	8265	1421868	172	9
google-services	2470	1180363	477	8
flash-video	1243	1233548	992	8
facebook	1197	429207	358	3
gmail	1149	618036	537	4
ssl	610	410624	673	3
netflix	600	355778	592	2
yahoo-mail	470	327088	695	2

Application Last 90 Secs Usage(%)



Application Cumulative Usage(%)



NBAR/AV Facts

- Same AV profile can be mapped to multiple WLANs. But one WLAN can have only one AV profile
- Only 1 NetFlow exporter and monitor can be configured on WLC
- AV stats are displayed for top 30 applications on both GUI and CLI
- Any application, which is not supported/recognised by NBAR engine on WLC, is captured under bucket of UNCLASSFIED/Unknown traffic
- No limit on the number of AV profiles that can be created on WLC

NBAR Feature Limitations

- IPv6 traffic cannot be classified
- Multicast traffic is not supported
- No Application Control Functionality in IOS XE 3.3

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - **Service Discovery Gateway**
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

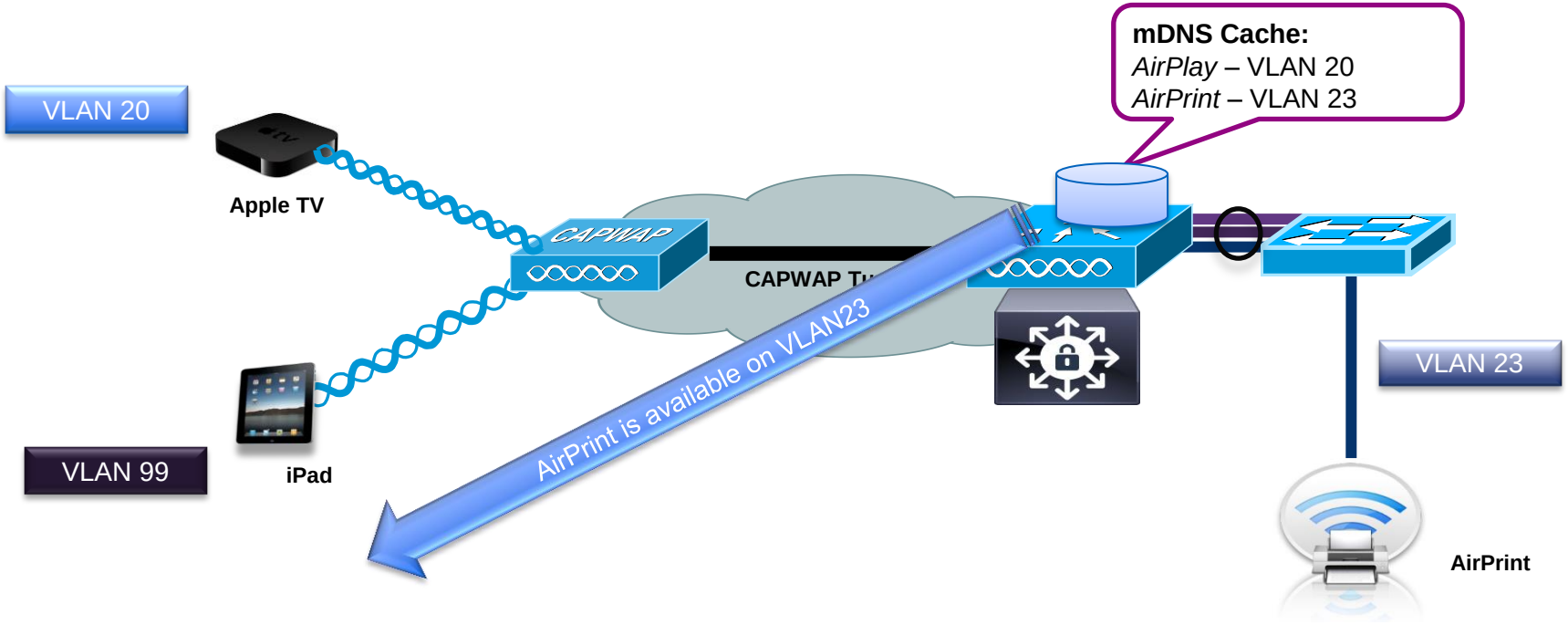
Service Discovery Gateway for Cisco IOS– Platforms

- Catalyst 3560, 3750, 4500 platforms
  - XE3.5.0E/15.2(1)E release – Available
- Catalyst 3650 and 3850
  - IOS XE 3.3.0SE release – Available
- Catalyst 5760 Wireless LAN Controller
  - IOS XE 3.3.0SE release – Available
- Catalyst 6500
  - 15.1(2)SY release – Available
- ASR1000 and ISR
  - XE 3.11 release – Available

Service Discovery Gateway

On CT-5760(Centralised), the 3850 and 3650 series switches

Both wired and wireless clients can benefit from switch or router based solution

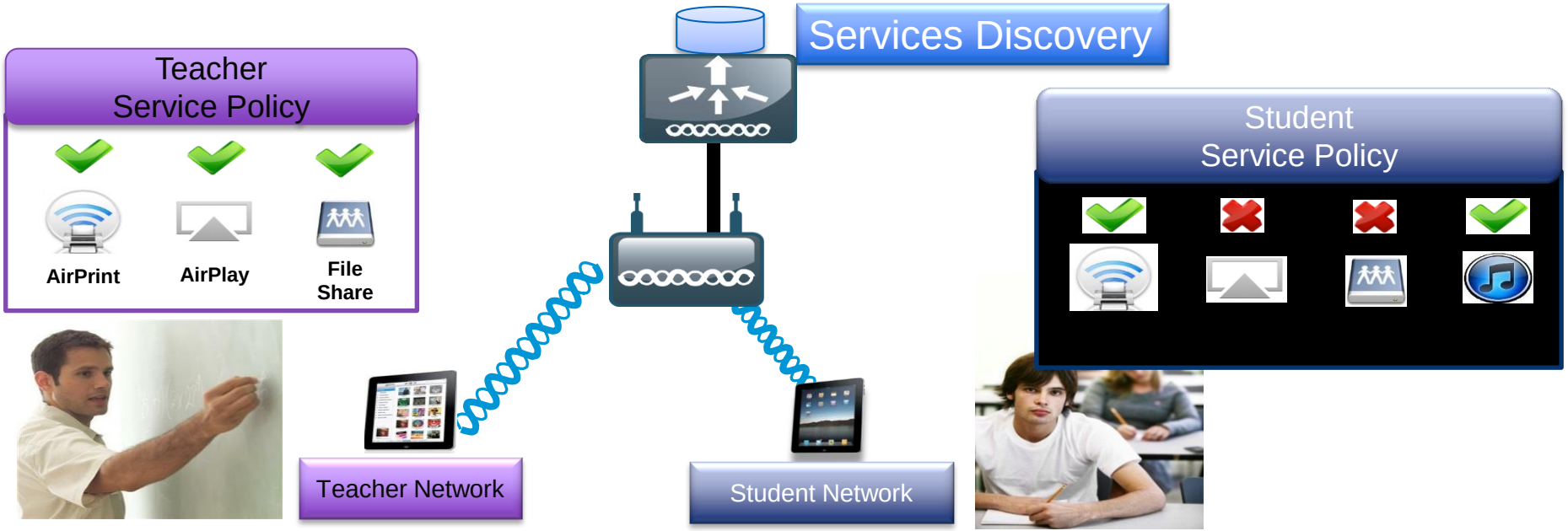


Policy Capabilities

The mDNS Policy Profile is a list of allowed network applications. (i.e. AirPlay or Printing)

- The mDNS policy profile provides filtering to allow only certain WLANs, interfaces or users to access specific service types.
- Enforced per Interface (which include WLAN and VLAN groups)
- mDNS snooping needs to be enabled globally

Service Discovery Gateway Policy Example for Education



- Teachers are allowed to print, access the Apple TV and file shares.
- Students are allowed to print and share iTunes, but not access the Apple TV, or file shares.

Configuring Service Discovery Gateway-GUI

Creating a Service List

Controller

- System
- Internal DHCP Server
- Management
- Mobility Management
- mDNS
  - Global
  - Interface
  - Service List

Create Service

Service List > **Create Service**

Service List Name: qui-permit-all

Service rule: permit

Sequence number: 10

Match Criteria

Message type: None

Service instance:

service Type

Custom: Add

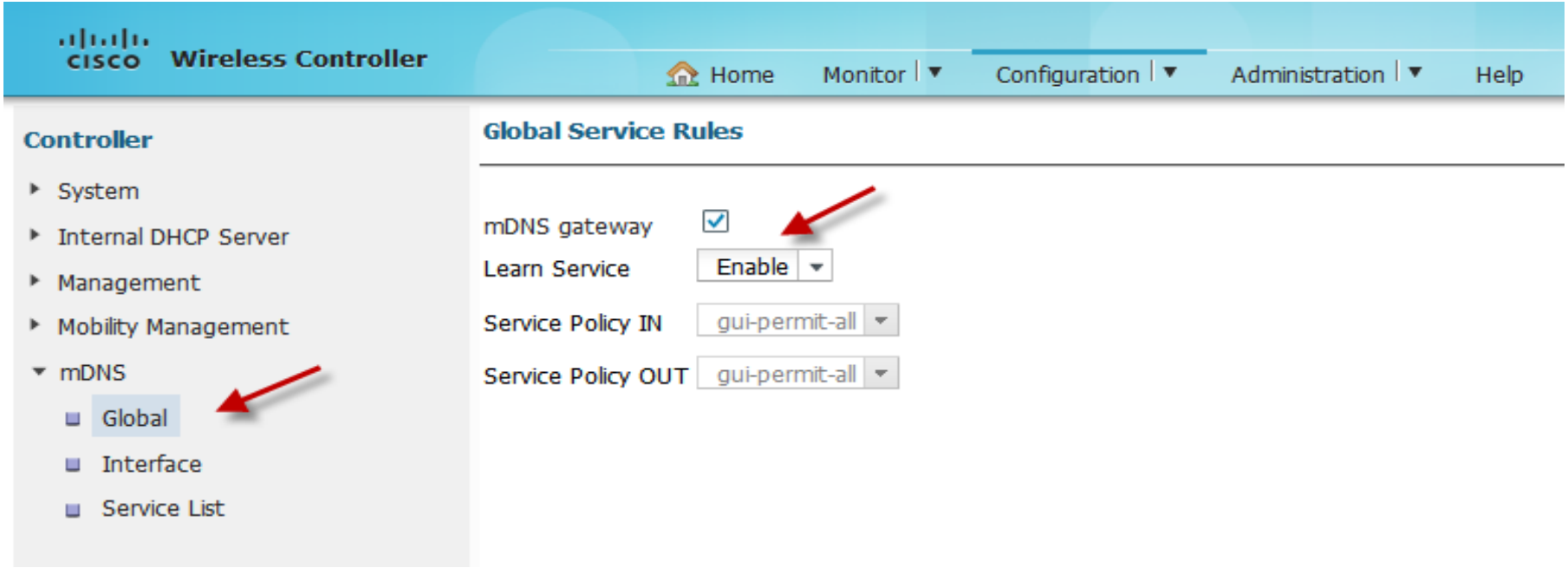
Learned Services:
_tcp.local
_airplay._tcp.local
1 Office Apple TV (2)._slee
_udp.local
_raop._tcp.local

>>
<<

Selected Service:

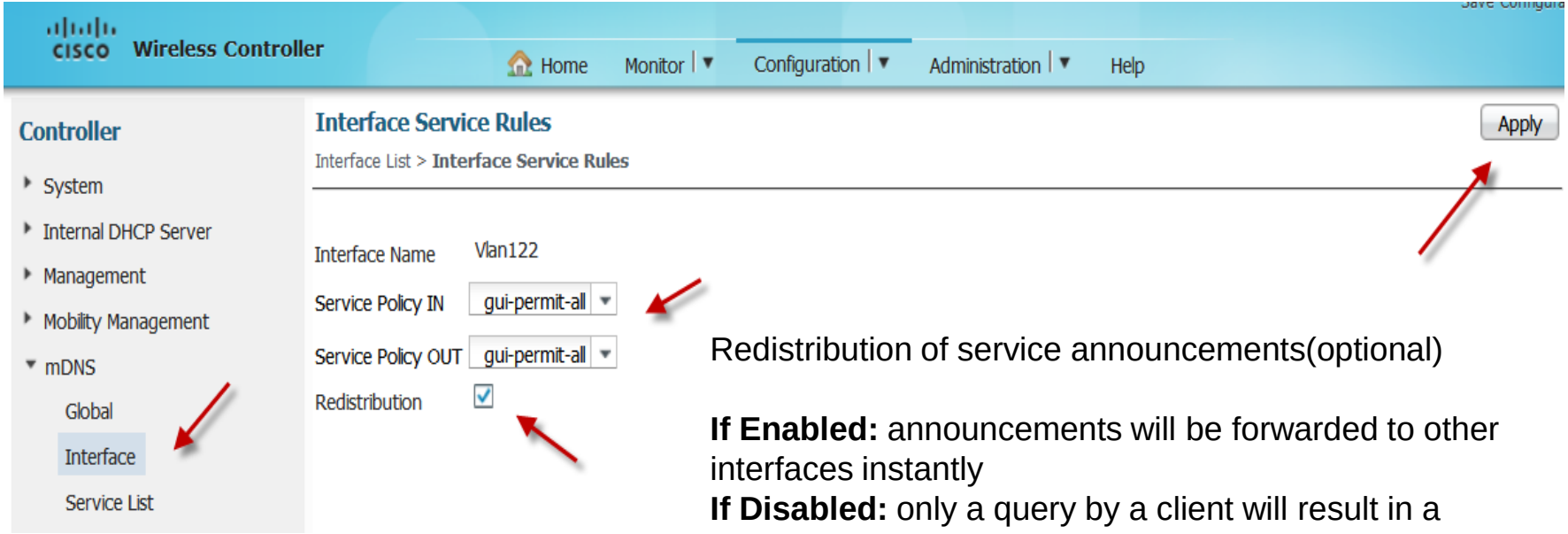
Configuring Service Discovery Gateway-GUI

Enable mDNS snooping globally



Configuring Service Discovery Gateway-GUI

Applying Services to Interface

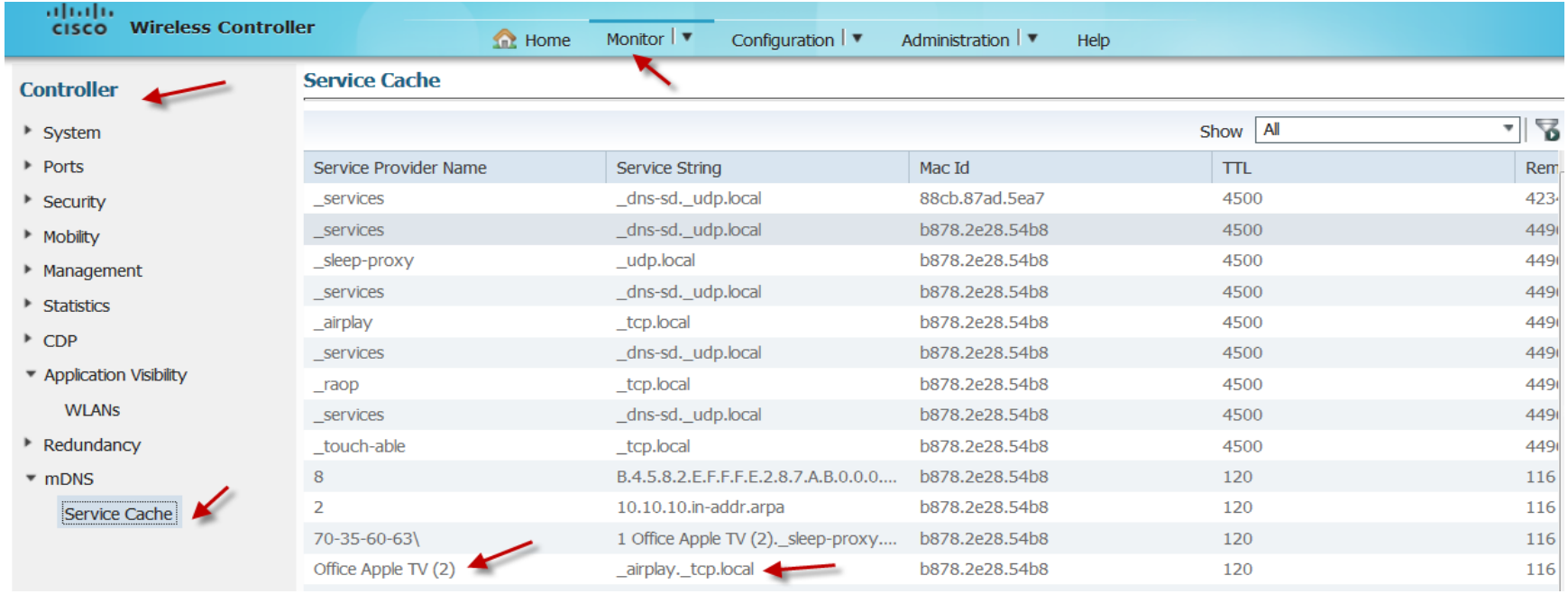


Redistribution of service announcements(optional)

If Enabled: announcements will be forwarded to other interfaces instantly
If Disabled: only a query by a client will result in a response by the cache

Monitoring of mDNS Services

List of mDNS services advertised by mDNS capable devices



Service Provider Name	Service String	Mac Id	TTL	Rem
_services	_dns-sd._udp.local	88cb.87ad.5ea7	4500	423
_services	_dns-sd._udp.local	b878.2e28.54b8	4500	449
_sleep-proxy	_udp.local	b878.2e28.54b8	4500	449
_services	_dns-sd._udp.local	b878.2e28.54b8	4500	449
_airplay	_tcp.local	b878.2e28.54b8	4500	449
_services	_dns-sd._udp.local	b878.2e28.54b8	4500	449
_raop	_tcp.local	b878.2e28.54b8	4500	449
_services	_dns-sd._udp.local	b878.2e28.54b8	4500	449
_touch-able	_tcp.local	b878.2e28.54b8	4500	449
8	B.4.5.8.2.E.F.F.F.E.2.8.7.A.B.0.0.0....	b878.2e28.54b8	120	116
2	10.10.10.in-addr.arpa	b878.2e28.54b8	120	116
70-35-60-63\	1 Office Apple TV (2)._sleep-proxy....	b878.2e28.54b8	120	116
Office Apple TV (2)	_airplay._tcp.local	b878.2e28.54b8	120	116

Service Discovery Gateway Summary

- Both wired and wireless clients are supported
- 14K services on 5760 and 2.5K on 3650/3850
- Supported with Centralised and Converged Access mode
- Roaming and Guest Anchor support
- Easy to configure and manage from both GUI and CLI

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - **TrustSec**
  - 802.11ac Support
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

TrustSec Security Group Access Overview

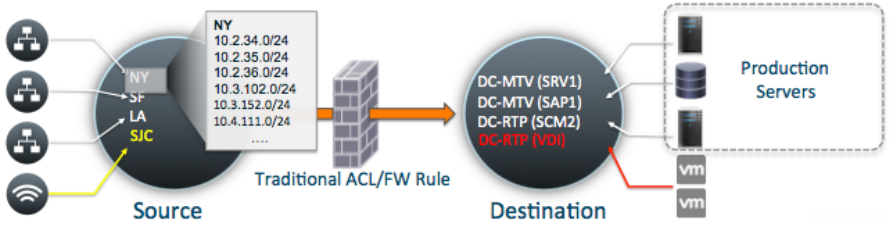
Translating Business Policy to the Network

TrustSec lets you define policy
in meaningful business terms

Business Policy

Source \ Destination	HR Database	Prod HRMS	Storage
Exec BYOD	✗	✗	✗
Exec PC	✗	✓	✗
Prod HRMS	✓	✓	✗
HR Database	✓	✓	✓

Clear ROI in OPEX




```
permit NY  to SRV1 for HTTPS
deny   NY  to SAP2 for SQL
deny   NY  to SCM2 for SSH
permit SF  to SRV1 for HTTPS
deny   SF  to SAP1 for SQL
deny   SF  to SCM2 for SSH
permit LA  to SRV1 for HTTPS
deny   LA  to SAP1 for SQL
deny   LA  to SAP  for SSH
```

ACL for 3 source objects & 3 destination objects

```
Permit SJC to SRV1 for HTTPS
deny   SJC to SAP1 for SQL
deny   SJC to SCM2 for SSH
```

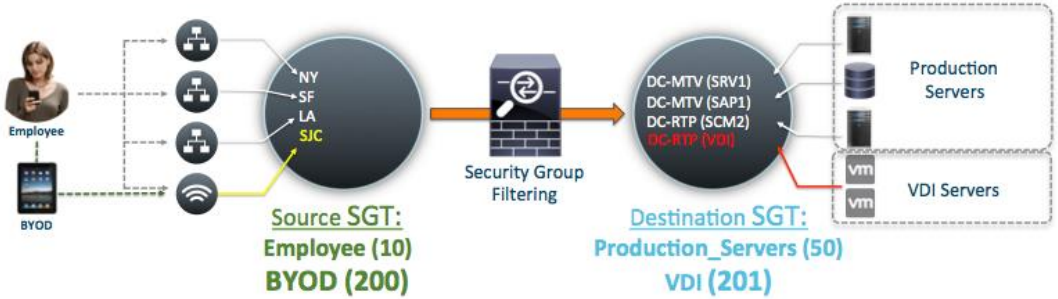
Adding source Object

```
permit NY  to VDI  for RDP
deny   SF  to VDI  for RDP
deny   LA  to VDI  for RDP
deny   SJC to VDI  for RDP
```

Adding destination Object

Traditional ACL / FW Filtering

Simplified Security Group Filtering



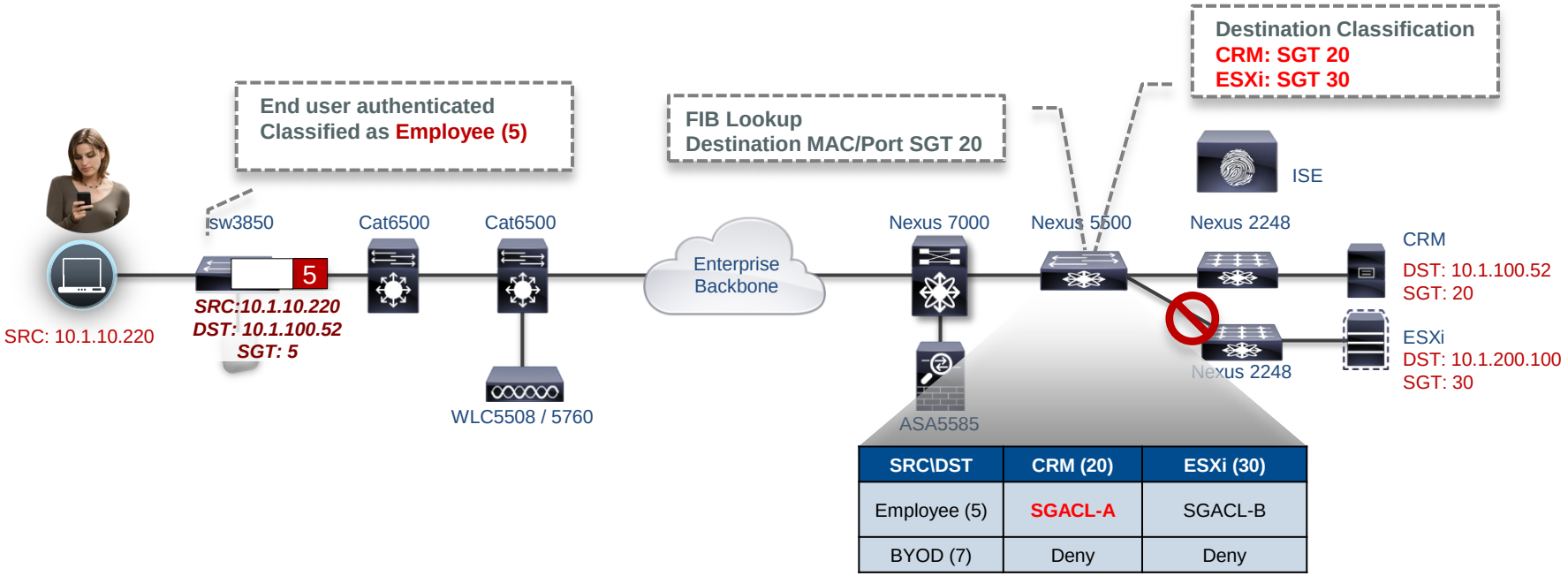

```
Permit Employee   to   Production_Servers eq HTTPS
Permit Employee   to   Production_Servers eq SQL
Permit Employee   to   Production_Servers eq SSH
Permit Employee   to   VDI                eq RDP
```

```
Deny   BYOD       to   Production_Servers
Deny   BYOD       to   VDI                eq RDP
```

SGA Policy

Destination SGT / Source SGT	Public Portal (SGT 8)	Internal Portal (SGT 9)	IT Portal (SGT 4)	Production Servers (SGT 10)
 BYOD(SGT 7)	Web	Web	No Access	Web File Share
 Corp Asset (SGT 5)	Web SSH RDP File Share	Web SSH RDP File Share	Full Access	SSH RDP File Share

SGT Assignment and Enforcement



SRC\DST	CRM (20)	ESXi (30)
Employee (5)	SGACL-A	SGACL-B
BYOD (7)	Deny	Deny

Wireless TrustSec Support for Converged Access

Deployment Mode	Controller Platforms	TrustSec Support	Authentication	Release
Unified AireOS	2504, 5508 WiSM2	SXP(speaker mode)	802.1X	7.2 and above
Converged Access IOS	3850, 3650 5760	SGT, SGACL SXP (speaker / listener)	802.1X MAB WebAuth	IOS-XE 3.3.0SE Release

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - **802.11ac Support**
  - High Availability- AP SSO
- Bringing Together Wired and Wireless

802.11ac – The Gigabit Wireless Standard

What is 802.11ac?

- Next-generation 802.11 Wi-Fi specification “gigabit” wireless
- Backwards compatible with 802.11n and 802.11a
- Most efficient Wi-Fi standard to date
- Optimised for high bandwidth applications
- WFA certification ready for Wave 1

What Are the Features?

- Specifies a data rate up to 6.9Gbps per 5 GHz radio
- Max Data rate of 1.3Gbps in Wave 1 (phase 1)
- Operates in 5 GHz band only
- Enhanced channel bonding, modulation (256 QAM) and more spatial streams than 802.11n

What Are the Benefits?

Faster Throughput
2-3x on average of 802.11n

Broader Coverage
Robust connectivity & range. Fewer dead spots

Greater Capacity
More clients utilising the resources of an AP

Longer Battery Life
On and off the Wi-Fi network faster, translates to less power draw and longer battery life

802.11ac Module for 3600 Access Point Series

- Field-upgradable 802.11ac module for the 3600 Series, enables a seamless migration to next generation wireless
  - No rip and replace of APs, power down, plug-in the module and go!
- 802.11ac Wave-1, 5 GHz Module
  - 1.3 Gbps PHY (80 MHz @ 3SS)
  - 3 Spatial Streams, 20/40/80 MHz channels, 256 QAM
  - Explicit Beam Forming support as per the 802.11ac specification
- AP3600 operates 3 active radios, 2.4 and 5 GHz integrated and the 802.11ac 5 GHz module
  - Supporting b/g/n on 2.4 GHz and a/ac/n on 5 GHz
- 18w of Power required for the 3600 with the 802.11ac Module installed
  - Power draw with 802.11ac Module exceeds 15.4 Watts (802.3af), and will require either Enhanced PoE, 802.3at PoE+, Local Supply or Power Injector 4

Next-gen AP3700 – with Modularity & Integrated 802.11ac

- 4x4:3 SU-MIMO Dual-band 2.4 and 5 GHz integrated radios with Modularity
- 802.11ac Wave 1 on the integrated 5 GHz radio
  - 1.3 Gbps PHY : 3 Spatial Streams, 20/40/80 MHz channels, 256 QAM
  - Explicit Compressed Beam Forming (ECBF) support as per the 802.11ac specification
  - 802.11a, .11n and .11ac clients supported on the integrated 5 GHz radio
- Modular architecture carried forward from the AP3600
  - WSSI Module is supported
- Requires ~15w of power at the AP – Enhanced PoE or PoE+ for full functionality
  - Fits under 15.4w 802.3af by automatically down shifting RF arch to 3x3:3 on both 2.4 and 5 GHz
- Antenna support
  - Support all the antennas available for the 3600, 2600 and 1600

Configuring 11ac : Channel Width

Wireless Controller

Home | Monitor | Configuration | Administration | Help

Wireless
- WLAN
  - WLANs
- Access Points
- 802.11a/n
  - Network
  - RRM
    - General
    - Coverage Thresholds
    - DCA
    - TPC
    - RF Grouping
  - High Throughput (802.11n/ac)
  - Media Parameters
  - Roaming Parameters
  - CleanAir
- 802.11b/g/n
- Media Stream

802.11a > RRM > Dynamic Channel Assignment (DCA)

Apply

Dynamic Channel Assignment Algorithm

Channel Assignment Method: Automatic | Interval 10 minutes | Anchortime 0

Freeze

OFF

After you apply, wait 10 min for RRM to change the channel width

Avoid Foreign AP Interference ☑

Avoid Cisco AP load ☐

Avoid Non 802.11a Noise ☑

Avoid Persistent Non-wifi Interference ☐

Channel Assignment Leader WLC5760(172.20.229.5)

Last Auto Channel Assignment 479

DCA Channel Sensitivity medium

Change the Channel Width to 80 Mhz

Channel Width 20 MHz | 40 MHz | 80 MHz

DCA Channel List

Save Configuration

Wireless Controller

Home | Monitor | Configuration | Administration | Help

Wireless
- WLAN
  - WLANs
- Access Points
  - All APs
  - Radios
    - 802.11a/n/ac
    - 802.11b/g/n

802.11a/n/ac Radios

Configure | Details | 802.11TSM

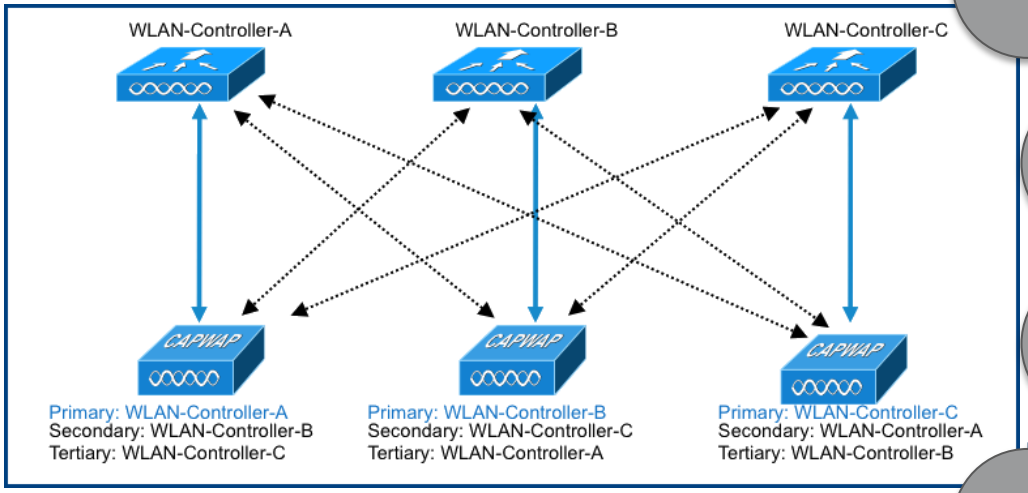
Show All

	AP Name	Base Radio MAC	operational Status	Channel	Power Level	AdminStatus	Slot No
☐	POD5-AP1	24:01:C7:14:57:10	UP	(157,161)	8(*)	Enabled	1
☑	POD5-AP1	24:01:C7:14:57:10	UP	(157,161,149,153)	8(*)	Enabled	2

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - **High Availability- AP SSO**
- Bringing Together Wired and Wireless

5760 High Availability Recap



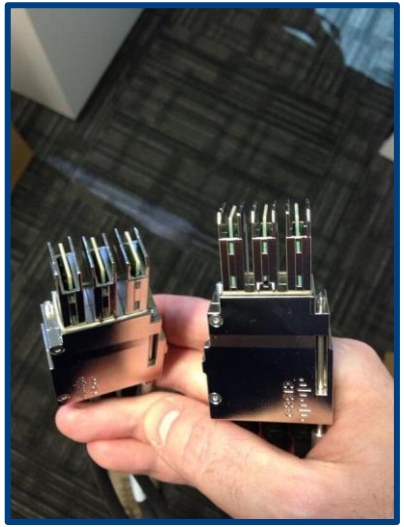
- Primary/Secondary/Tertiary WLC defined on each AP
- Primary and Secondary Backup configuration with Fast Heart Beat
- Each WLC configured separately and has unique IP Address
- With Primary Failure, AP goes in Discovery State and CAPWAP State Machine is restarted

5760 High Availability with APSSO

- Two 5760 units can be stacked for 1:1 redundancy, using stack cables
- One 5760 elected as Active and the other becomes Hot-Standby
- Bulk and Incremental Configuration sync
- Redundancy supported both at Port level and System level
- AP CAPWAP information sync. APs will not disconnect and continue to be associated to the controller
- Significantly reduces network downtime

High Availability Connectivity on 5760

High availability is enabled using Cisco StackWise-480 technology in Full Ring Setup.

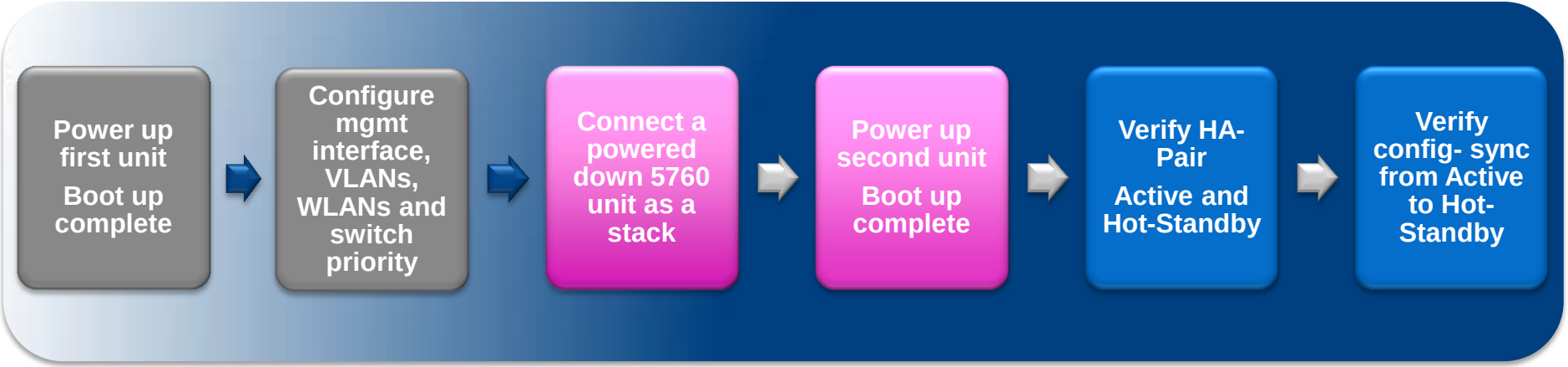


STACK-T1-50CM=	Cisco StackWise-480 50cm stacking cable spare
STACK-T1-1M=	Cisco StackWise-480 1m stacking cable spare
STACK-T1-3M=	Cisco StackWise-480 3m stacking cable spare

High Availability

WLC 5760-based MCs – How to Pair the Boxes

- Recommended: power up the second unit only after a first 5760 is deployed



- Adding powered-on 5760 Unit (merging) causes stack to reload and elect a new Active.
- Use *Controller# switch 1 Priority 15* on the first unit to prevent having the second unit become active and wipe out your config …

Active Controller Election Process

5760 that is the **current Active controller**

5760 with highest stack member **Priority Value**

5760 with **shortest Start-up Time**

5760 with **Lowest MAC Address**

```
5760#switch 2 priority ?
  <1-15>  Switch Priority
```

Verifying HA Pair Details

```
5760#show switch
Switch/Stack Mac Address : 20bb.c0a2.4d00 - Local Mac Address
Mac persistency wait time: Indefinite
                                                H/W   Current
Switch#   Role     Mac Address      Priority Version  State
-----------------------------------------------------------
*1        Active   20bb.c0a2.4d00     1       A0       Ready
 2        Standby  20bb.c0a2.4d80     1       A0       Ready
```

By Default : The 5760 stack uses the MAC address of the active 5760.

Persistent MAC address feature : time delay before the stack MAC address changes to new Active

```
5760(config)#stack-mac persistent timer ?
  <0-0>   Enter 0 to continue using current stack-mac after master switchover
  <1-60>  Interval in minutes before using the new master's mac-address
  <cr>
```

Verifying Stack Port Details

```
5760#show switch stack-ports summary

Sw#/Port#   Port Status   Neighbor   Cable Length   Link OK   Link Active   Sync OK   #Changes to LinkOK   In Lo
opback
-----------------------------------------------------------------------------------------------------------
-------
1/1         OK            2          50cm           Yes       Yes           Yes       3                    No

1/2         OK            2          50cm           Yes       Yes           Yes       2                    No

2/1         OK            1          50cm           Yes       Yes           Yes       1                    No

2/2         OK            1          50cm           Yes       Yes           Yes       2                    No
```

- No — No neighbour detected. Cannot send traffic over this link.
- Yes — Neighbour detected. Port can send traffic over this link.

nal.

port is Disabled.

Verifying Redundancy States

```
5760#show redundancy states
         my state = 13 -ACTIVE
       peer state =  8 -STANDBY HOT
             Mode = Duplex
          Unit ID = 1

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = SSO
                      Manual Swact = enabled

   Communications = Up

     client count = 78
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 0
      keep_alive threshold = 9
             RF debug mask = 0
```

```
5760-stby#show redundancy states
         my state =  8 -STANDBY HOT
       peer state = 13 -ACTIVE
             Mode = Duplex
          Unit ID = 2

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = SSO
                      Manual Swact = cannot be initiated

   Communications = Up

     client count = 78
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 1
      keep_alive threshold = 9
             RF debug mask = 0
```

APSSO Web UI

Wireless Controller

Home | Monitor | Configuration | Administration

Controller

- System
- Ports
  - General
- Security
- Mobility
  - Statistics
  - Oracle Summary
  - AP-List Summary
  - Client Summary
    - Controller
    - Agent
- Management
- Statistics
- CDP
- AVC
  - WLANs
- Redundancy
  - States
  - Switch Over History
- mDNS

Redundancy States

My State	ACTIVE
Peer State	STANDBY HOT
Mode	Duplex
Unit ID	2
Redundancy Mode (Operational)	SSO
Redundancy Mode (Configured)	SSO
Redundancy State	SSO
Manual Swact	Manual Swact = enabled

Wireless Controller

Home | Monitor | Configuration | Administration | Help

Controller

- System
  - Inventory
  - Wireless Interface
  - Multicast
- Ports
- Security

Redundancy Switch Over History

Show All

Index	Previous Active	Current Active	Switch Over Time	Switch Over Reason
1	0	2	14:51:50 EST Wed Sep 25 2013	user forced
2	0	1	15:50:37 EST Wed Sep 25 2013	active unit failed
3	0	2	15:59:00 EST Wed Sep 25 2013	active unit failed
4	0	1	14:48:02 EST Thu Sep 26 2013	user forced

APSSO Failover

```
5760#redundancy force-switchover
System configuration has been modified. Save ? [yes/no]: yes
Building configuration...
Compressed configuration from 6134 bytes to 3275 bytes[OK]This will reload the a
ctive unit and force switchover to standby[confirm]
Preparing for switchover..

*Sep 23 22:03:39.059: %RF-5-RF_RELOAD: Self Reload. Reason: Admin CLI
*Sep 23 22:03:44.298: %SYS-5-SWITCHOVER: Switchover requested by console. Reason
: Admin CLI.
<Mon Sep 23 22:03:44 2013> Message from sysmgr: Reason Code:[3] Reset Reason:Res
et/Reload requested by [console]. [Reload command]


umount: /proc/fs/nfsd: not mounted
Marconi Watchdog: device file closed unexpectedly. Will not stop the WDT!
Unmounting ng3k filesystems...
Warning! - some ng3k filesystems may not have unmounted cleanly...
Please stand by while rebooting the system...
Restarting system.
```

System Redundancy Models:

Manual Switchover

Software Failure Switchover

Power Failure Switchover

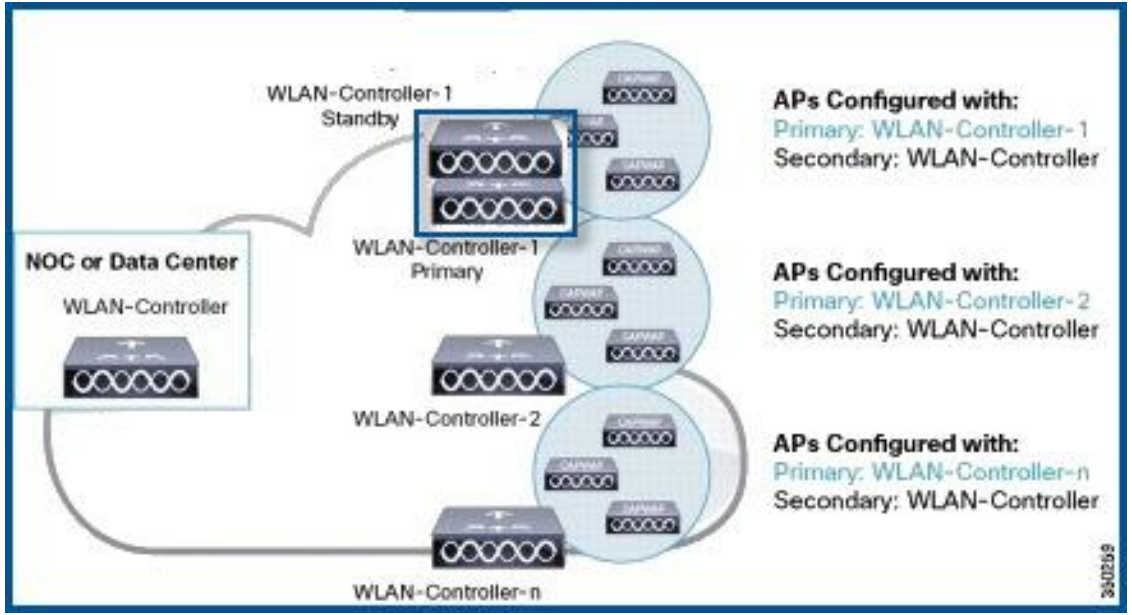
Metrics	Time
Failure Detection	In the order of 50 ms
Reconciliation Time (Standby becoming Active)	In the order of 1020 millisec

5760 APSSO Hybrid with N+1 High Availability

Both Active and Standby combined in SSO setup are configured as primary.

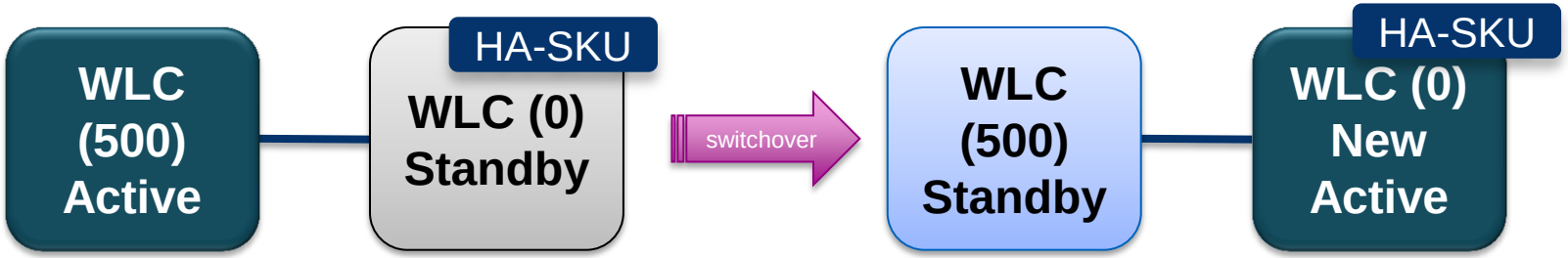
On failure of Active and Standby, APs will fall back to secondary and further to tertiary controller.

N+1 HA can be deployed with hybrid of 5760 and CUWN controllers. But APs will reload when failing over



Licensing for APSSO with HA-SKU

- Total capacity of the SSO Stack is 1000 APs
- MC keeps track of the cumulative AP Count and in-use AP licenses
- Not allow more APs than cumulative AP count licenses available in the SSO stack



Total AP Count = 500
Supported APs = 500

Total AP Count = 500
Supported APs = 500 AP failover

Agenda

- What is Converged Access?
- Converged Access Platforms Overview
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- How to deploy a Converged Access network?
- IOS-XE 3.3 Release Features
  - Application Visibility
  - Service Discovery Gateway
  - TrustSec
  - 802.11ac Support
  - High Availability- AP SSO
- **Bringing Together Wired and Wireless**

Bringing Together Wired and Wireless

How Are We Addressing This Shift?

Control plane functionality on NG Controller

(also possible on upgraded 5508s, WiSM2s for brownfield deployments, or NG Converged Access

Controller

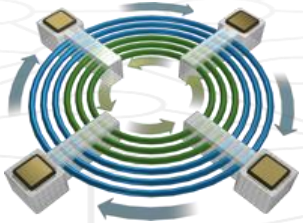
Data plane functionality on NG Switches

(also possible on NG Controllers, for deployments in which a centralised approach is preferred)

Next-Generation WLAN Controller (5760)

Next-Generation Switches (Cat 3850/3650)

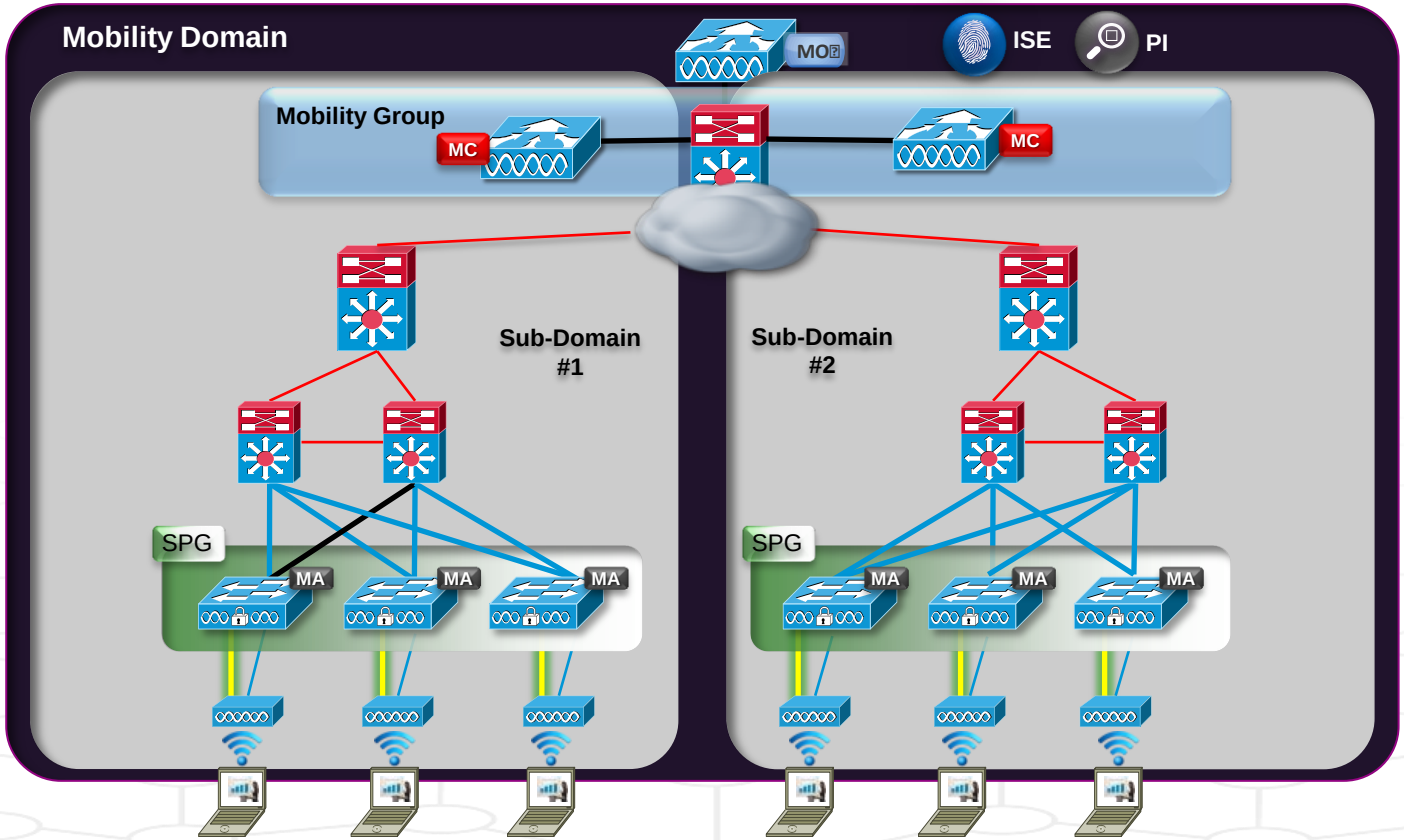
Enabled by Cisco's strength in Silicon and Systems … **UADP ASIC**



An Evolutionary Advance to Cisco's Wired + Wireless Portfolio, to address device and bandwidth scale, and services demands ….

Bringing Together Wired and Wireless

How Are We Addressing This Shift?



Cisco **Converged Access** Deployment

An Evolutionary Advance to Cisco's Wired + Wireless Portfolio, to address device and bandwidth scale, and services demands ….

Converged Access – Deployment Guides

For additional deployment information, check the deployment guides…

WLC 5760 Deployment Guide:
http://www.cisco.com/en/US/docs/wireless/technology/5760_deploy/CT5760_Controller_Deployment_Guide.html

Catalyst 3850 Deployment Guide:
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12686/deployment_guide_c07-727067.html

IOS-XE HA Deployment Guide:
http://www.cisco.com/en/US/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/5760_HA_DG_iosXE33.pdf

AVC Deployment Guide:
http://www.cisco.com/en/US/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/iosXE_3point3_AVC_DG.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™