What You Make Possible

TOMORROW
starts here.

Converged Access Campus and Branch Design Guidance

BRKARC-2666

TOMORROW starts here.

Converged Access –
Campus and Branch, Design Guidance

BRKARC-2666 – **Session Overview and Objectives**

Cisco is bringing together the best of wired and wireless networking into “One Network” with Converged Access.

This session introduces the Converged Access solution, including the next-generation Catalyst 3850 switch and how you can employ it within your network – discussing design considerations and insertion point placement within a Branch and Campus network.

You will learn how this switch works with existing Wireless Infrastructure, how roaming works seamlessly, and the QoS and Security features you need to be aware of.

This session is targeted to Network Managers, Architects and Administrators.

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – **Towards One Policy, One Management, One Network**

Converged Access – **Platform Overviews**

Converged Access – **Catalyst 3850 Platform in Detail**

Existing Wireless Deployment – **Architecture Refresher**

The Converged Access Deployment in Detail –

- Components of the Deployment – **Terminology Review**
- Converged Access Deployment – **Roaming Overview**
- Converged Access Deployment – **Quality of Service**
- Converged Access Deployment – **Security**
- Converged Access Deployment – **IP Addressing**
- Converged Access Deployment – **Deployment Options**

Summary

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Evolving User Workspace – Megatrends

BYOD

- Secure access
- Customised experience
- Guest access

Mobility

- Seamless roaming
- Optimal client performance
- Cloud access/VXI

Video

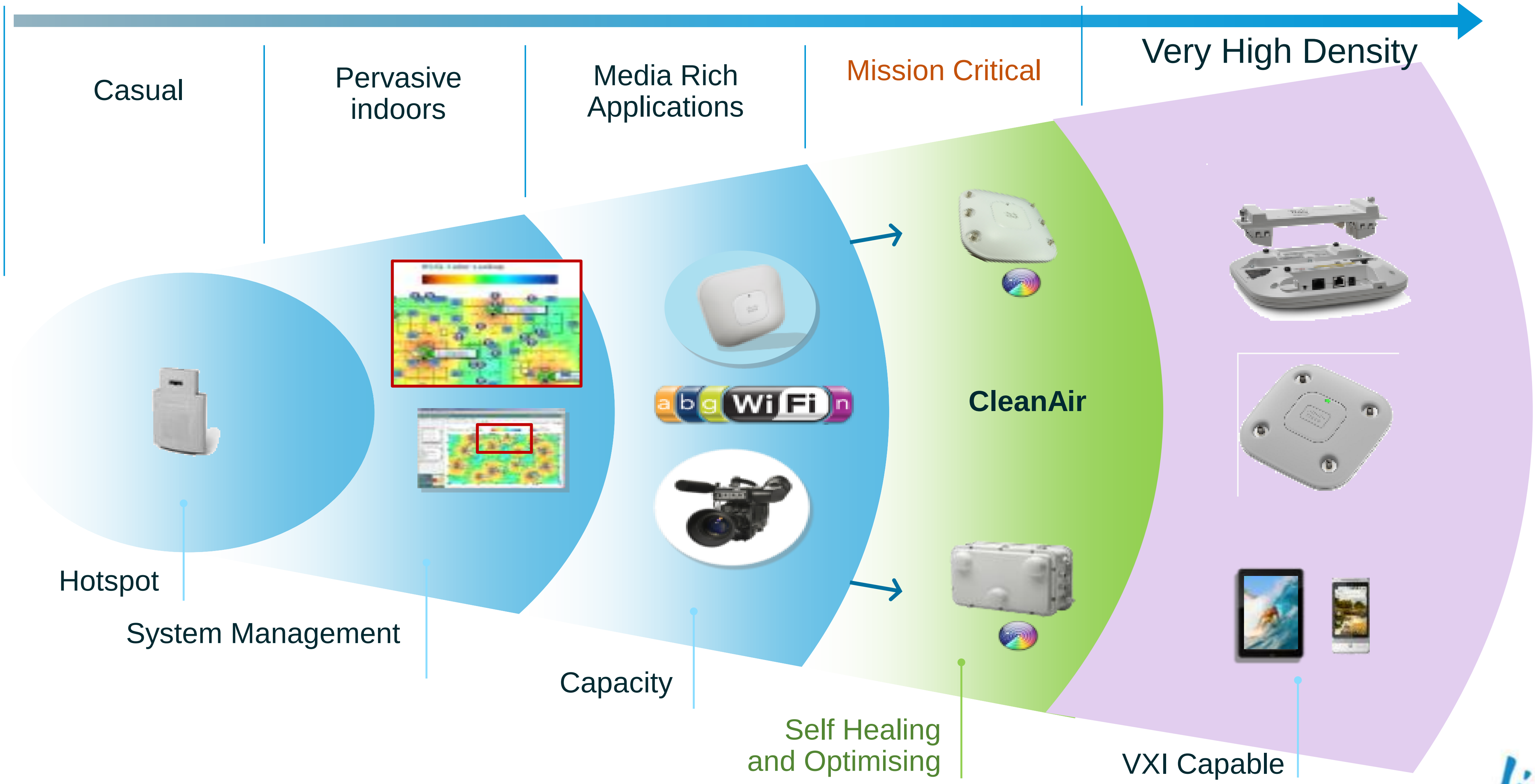
- Multicast streaming
- Video conferencing
- Reliable performance

IT Requirement

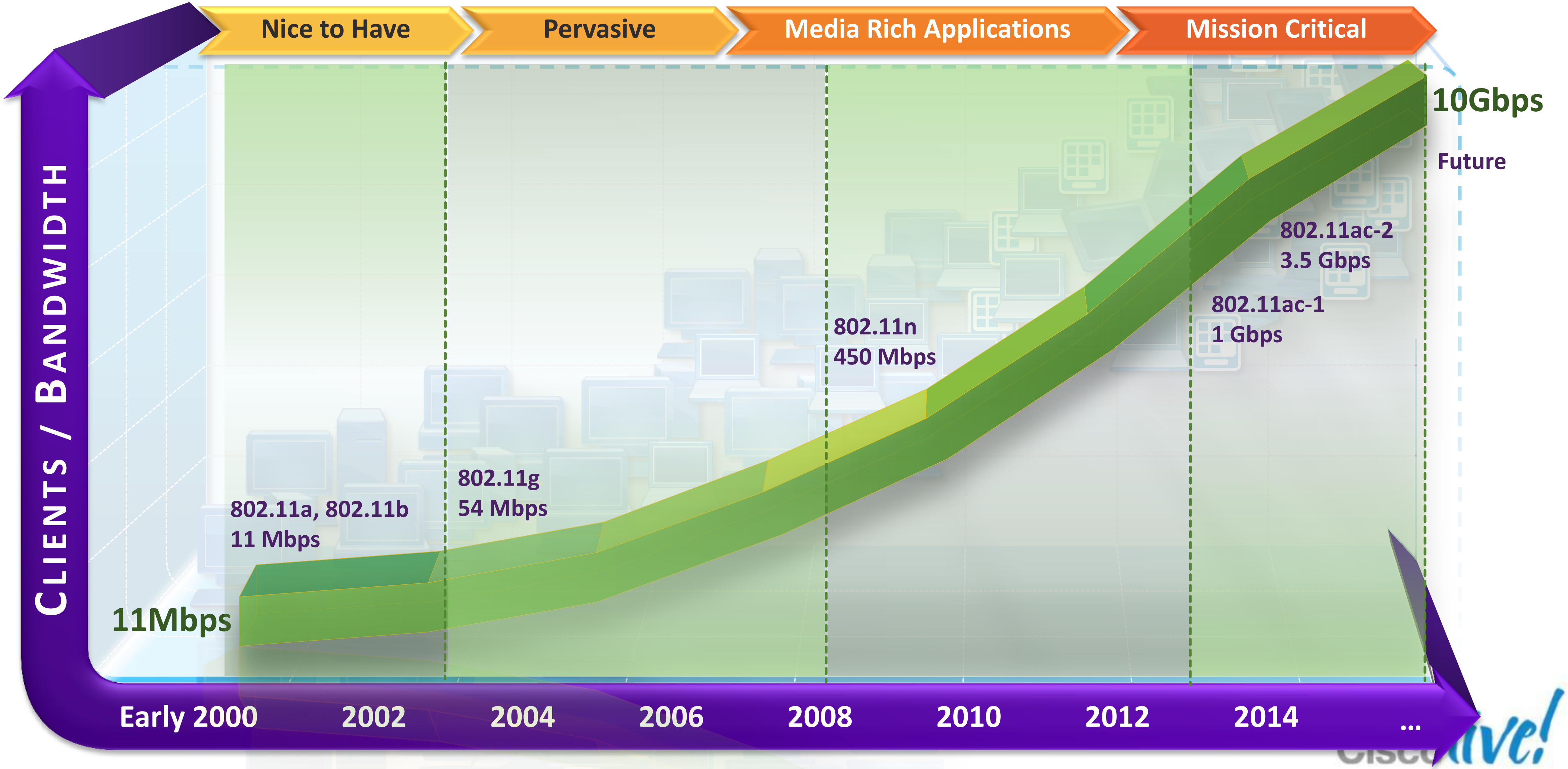
Deliver an Uncompromised User Experience on Any Workspace

Performance Protection for your 802.11 WiFi Network

Enterprise Wireless Evolution –
From Best-Effort to Mission-Critical and Very High Density



Wireless Standards –
Past, Present, and Future



How Many Mobile Data Devices –

Do You Think You Will Carry Everywhere in 2015?

Think about it, and choose the best answer

1	3	5	7

Unified Access –

Uncompromised User Experience in Any Workspace

One Network

One Management

One Policy

Unified Access

One Network, with Converged Access –

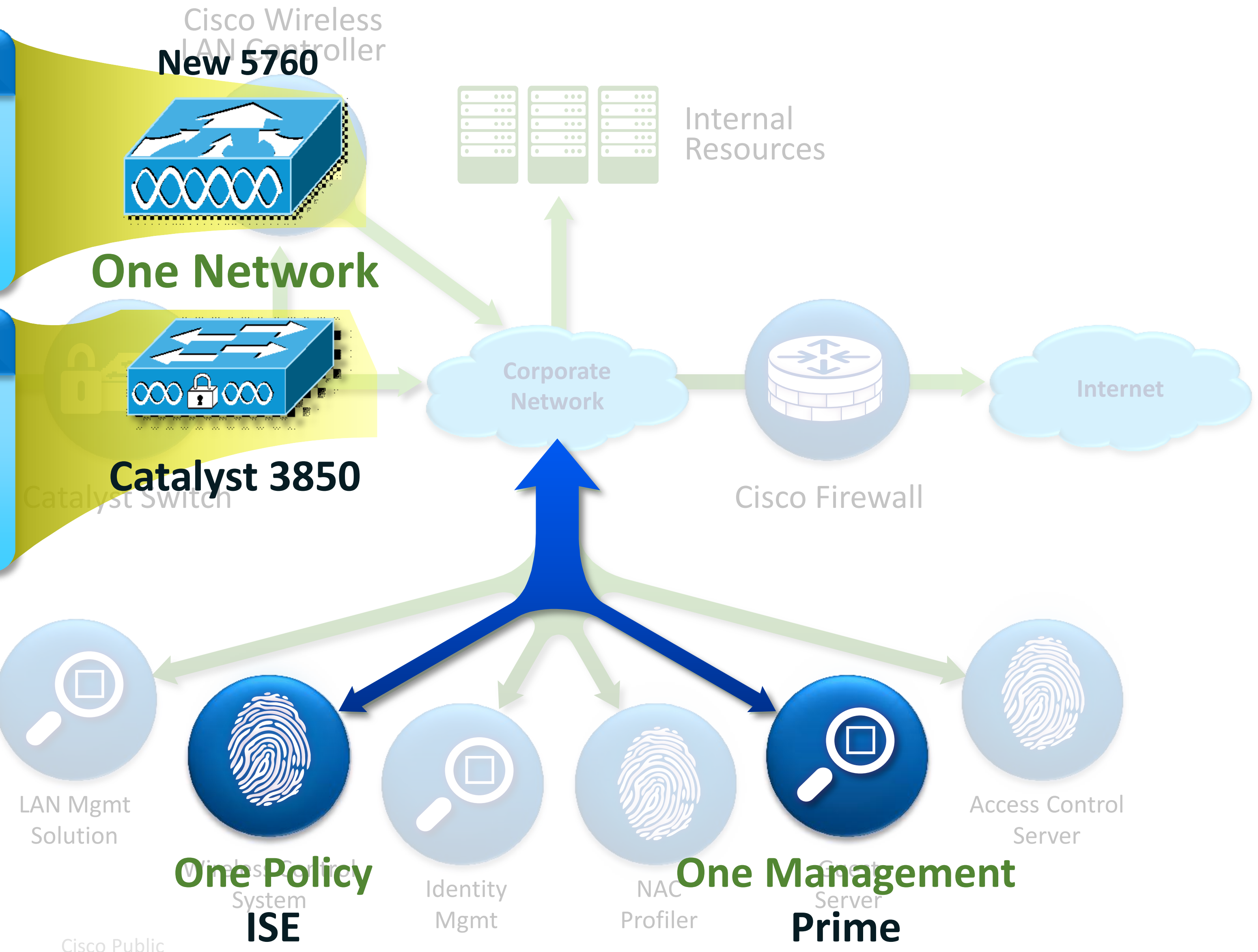
A New Deployment Option for Wired / Wireless

IOS Based WLAN Controller

- Consistent IOS and ASIC as Catalyst 3850
- Required to scale beyond 250 AP or 16K client domains

Converged Access Mode

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



Converged Wired / Wireless Access –

Benefits – Overview

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

480G stack bandwidth; 40G wireless / switch; efficient multicast; 802.11ac fully ready

Unified Access - One Policy | One Management | One Network

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

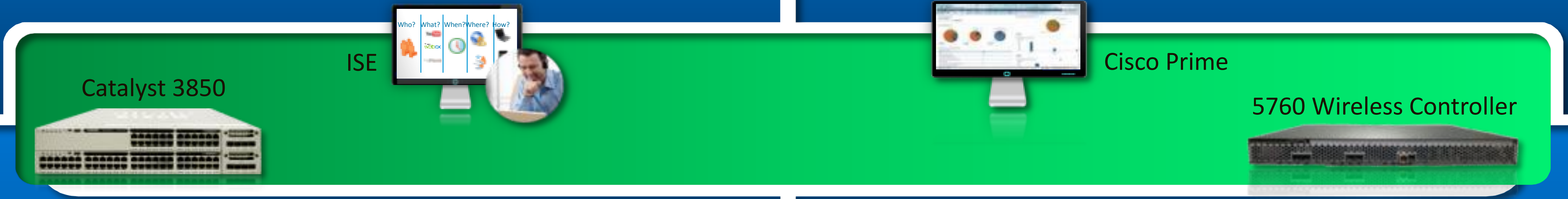
Unified Access Components –
Complete Overview

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



Catalyst 3850

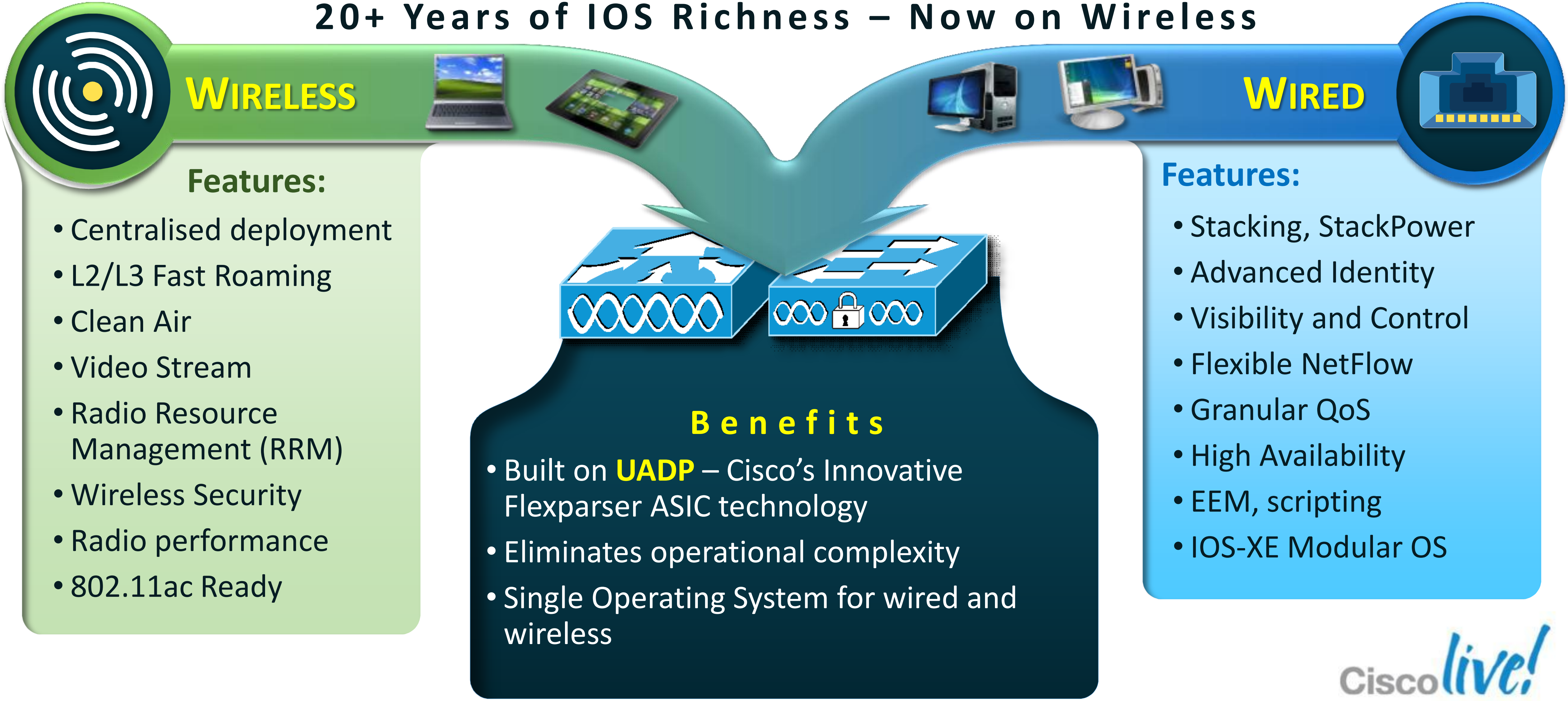
- Industry’s first fully integrated wired and wireless switch
- Wireless: 480G stack, 50 APs, 2K clients, 40G
- Flexible NetFlow, Granular QoS

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 –
Single Platform for Wired and Wireless



20+ Years of IOS Richness – Now on Wireless

WIRELESS

Features:

- Centralised deployment
- L2/L3 Fast Roaming
- Clean Air
- Video Stream
- Radio Resource Management (RRM)
- Wireless Security
- Radio performance
- 802.11ac Ready

Benefits

- Built on **UADP** – Cisco's Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

WIRED

Features:

- Stacking, StackPower
- Advanced Identity
- Visibility and Control
- Flexible NetFlow
- Granular QoS
- High Availability
- EEM, scripting
- IOS-XE Modular OS

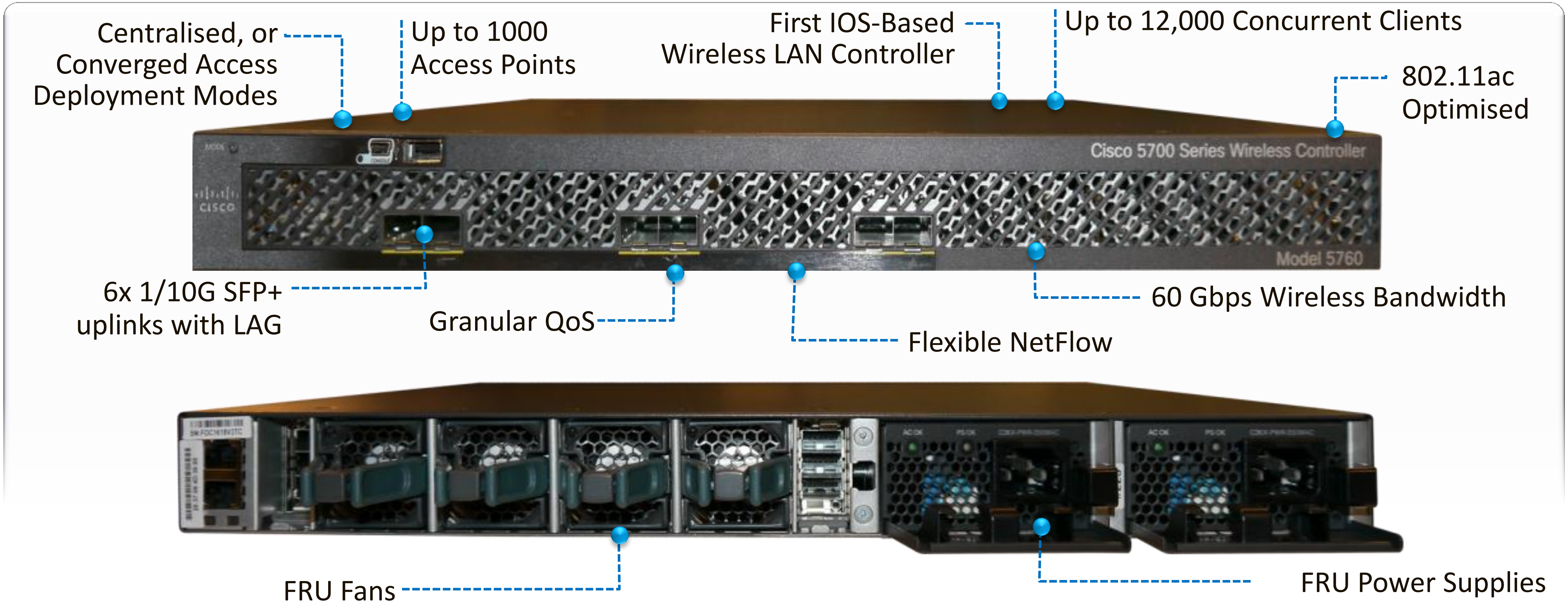
Catalyst 3850 –
Wireless Capabilities

- CAPWAP termination and DTLS in Hardware
- 40G wireless capacity per switch
  - Capacity increases with members
- 50 APs and 2000 clients per switch stack
- Wireless switch peer group support for faster roaming: latency sensitive applications
- Supports IPv4 and IPv6 client mobility

- APs must be directly connected to Catalyst 3850

Best-in-Class Wired Switch – with Integrated Wireless Mobility functionality

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

802.11ac Optimised

6x 1/10G SFP+ uplinks with LAG

Granular QoS

Flexible NetFlow

60 Gbps Wireless Bandwidth

FRU Fans

FRU Power Supplies

Built on Cisco's Innovative "UADP" ASIC

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

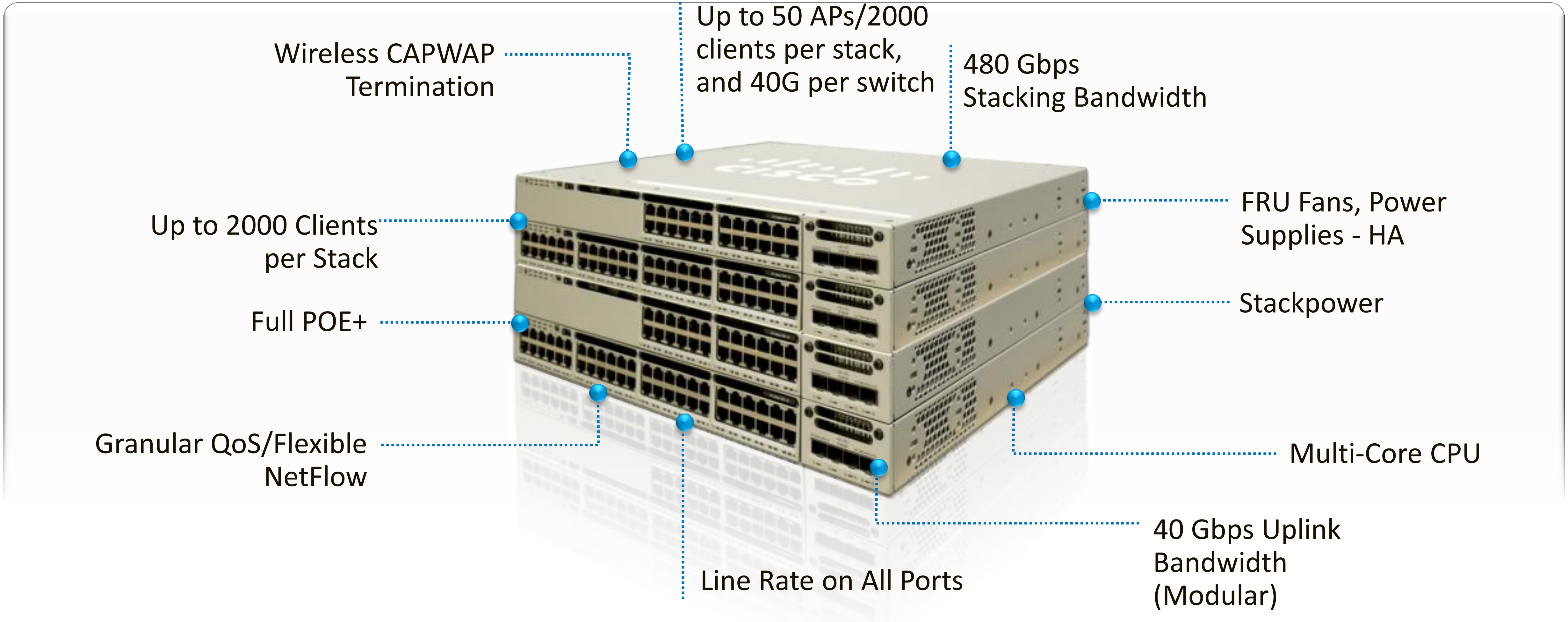
Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Catalyst 3850 – Platform Overview


Wireless CAPWAP Termination
Up to 50 APs/2000 clients per stack, and 40G per switch
480 Gbps Stacking Bandwidth
Up to 2000 Clients per Stack
Full POE+
FRU Fans, Power Supplies - HA
Stackpower
Granular QoS/Flexible NetFlow
Multi-Core CPU
Line Rate on All Ports
40 Gbps Uplink Bandwidth (Modular)

Built on Cisco’s Innovative “UADP” ASIC

Catalyst 3850 –

Network Modules

WS-C3850-NM-4-1G

- 4 x 1G
- SFP
- Supported on WS-C3850-24 & WS-C3850-48 Port

WS-C3850-NM-2-10G

- 4 x 1G OR 2 x 10G OR 2 x 1G + 1 x 10G
- SFP & SFP+
- Supported on WS-C3850-24 & WS-C3850-48 Port

WS-C3850-NM-4-10G

- Auto-sensing – All Combinations
- SFP & SFP+
- Supported on WS-C3850-48 only

Catalyst 3850 –

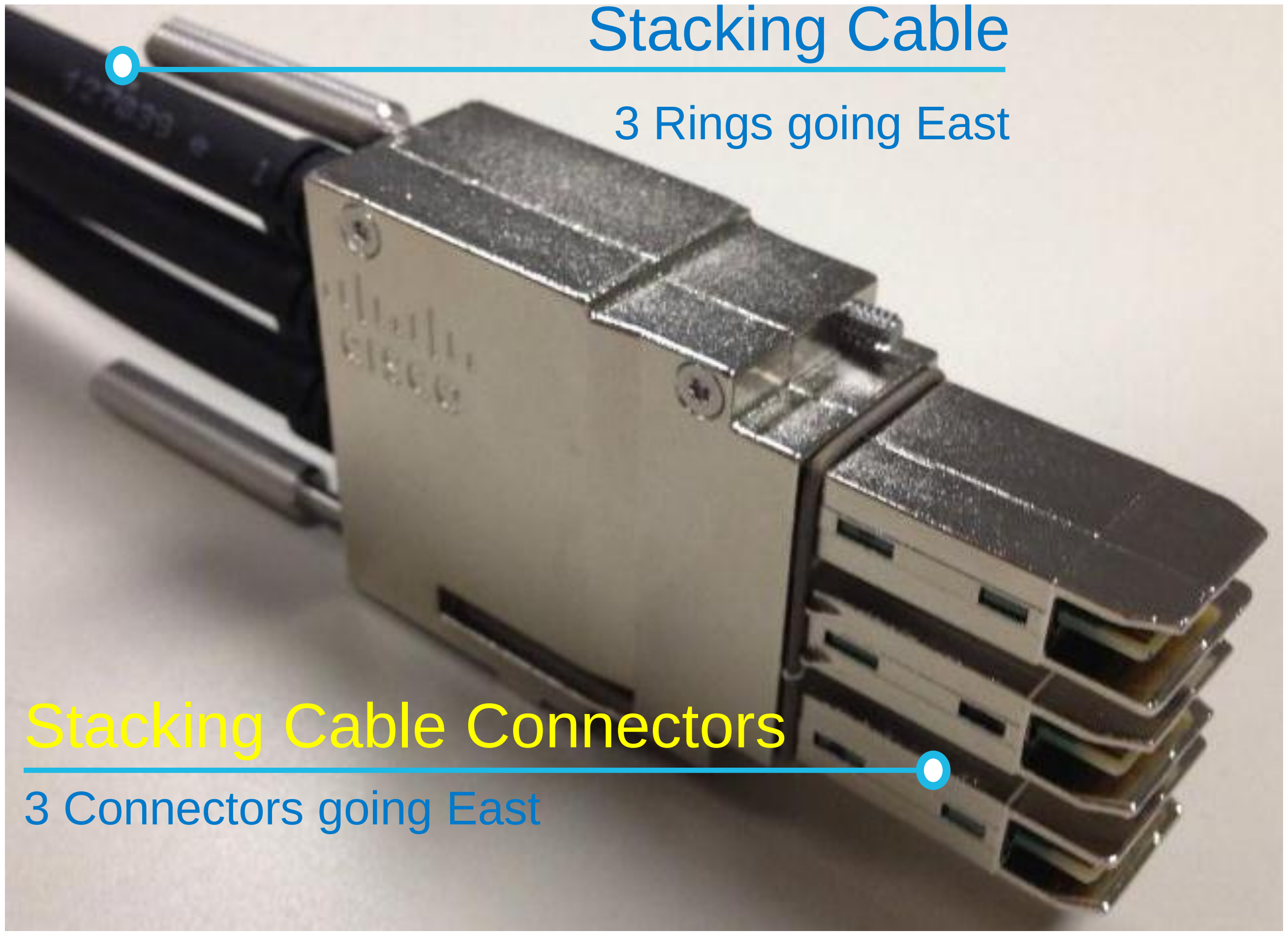
Power Modules

PWR Modules	
PWR-C1-350WAC	Same as 3K-X Series
PWR-C1-715WAC	
PWR-C1-1100WAC	
PWR-C1-440WDC	

- Power Modules is same as 3K but with a new PID
- Classic 3K Power Module can work on Catalyst 3850s
- No Interworking with classic 3Ks for StackPower

Catalyst 3850 –

Stacking Cable, Close-up

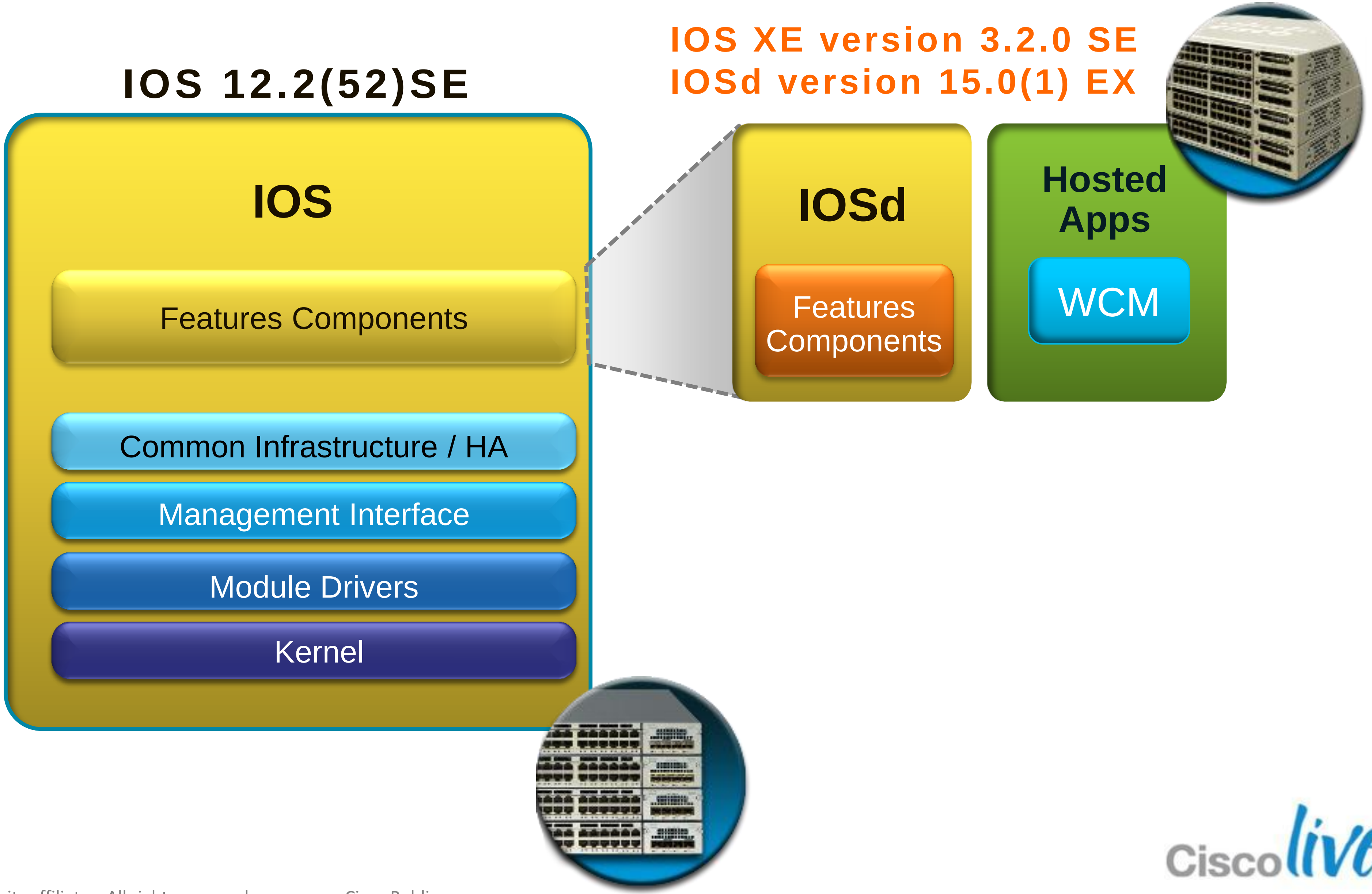


IOS-XE –

Evolution

IOS-XE

- Modern IOS to enable multi-core CPU
- Easy customer migration
- While maintaining IOS functionality and look and feel
- Allow hosted applications like Wireshark



IOS 12.2(52)SE

IOS

Features Components

Common Infrastructure / HA

Management Interface

Module Drivers

Kernel

IOS XE version 3.2.0 SE
IOSd version 15.0(1) EX

IOSd

Features Components

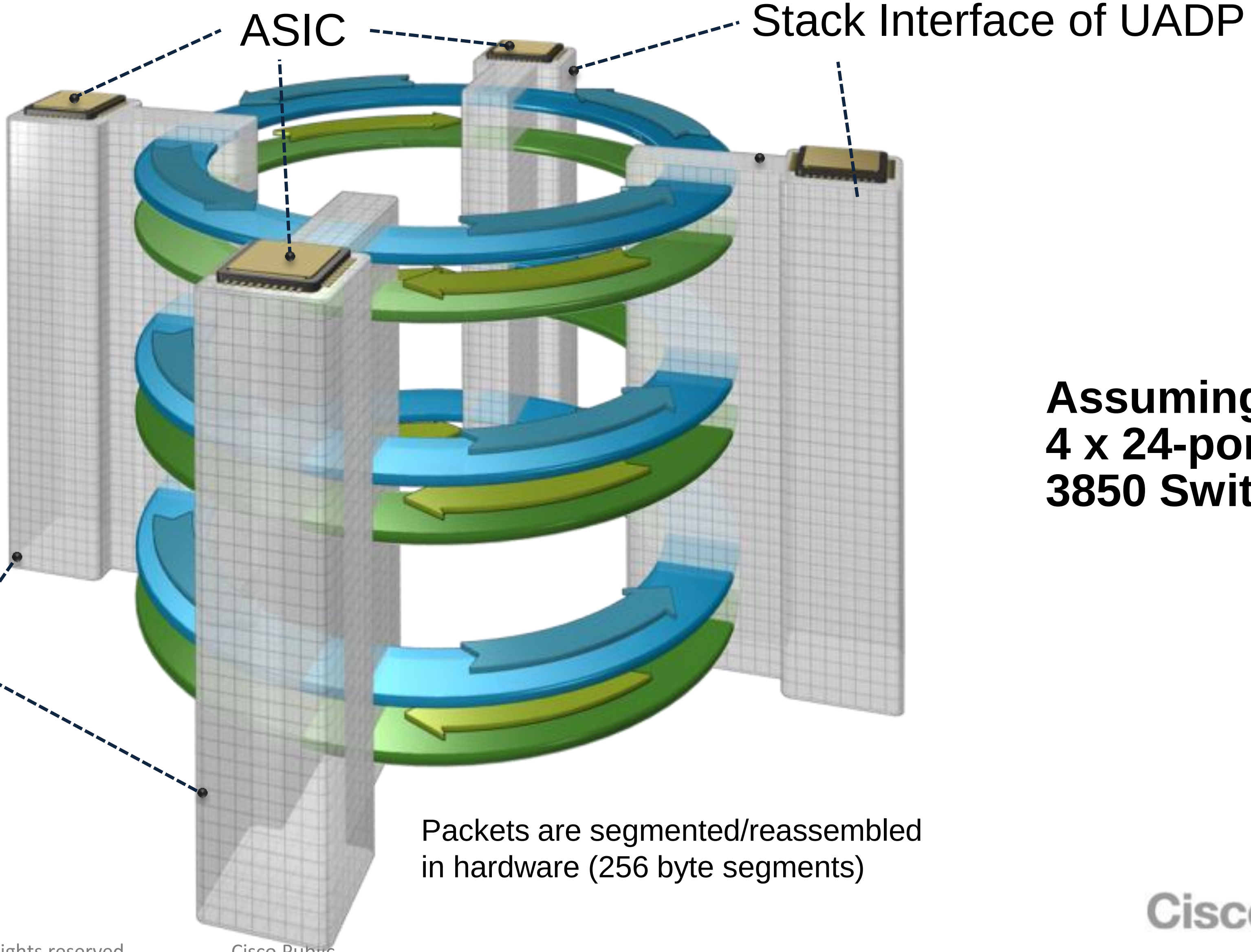
Hosted Apps

WCM

Catalyst 3850 –

Understanding the Stack Ring

- 6 rings in total
- 3 rings go East
- 3 rings go West
- Each ring is 40G
- Total Stack BW – 240G
- With Spatial Reuse= 480G

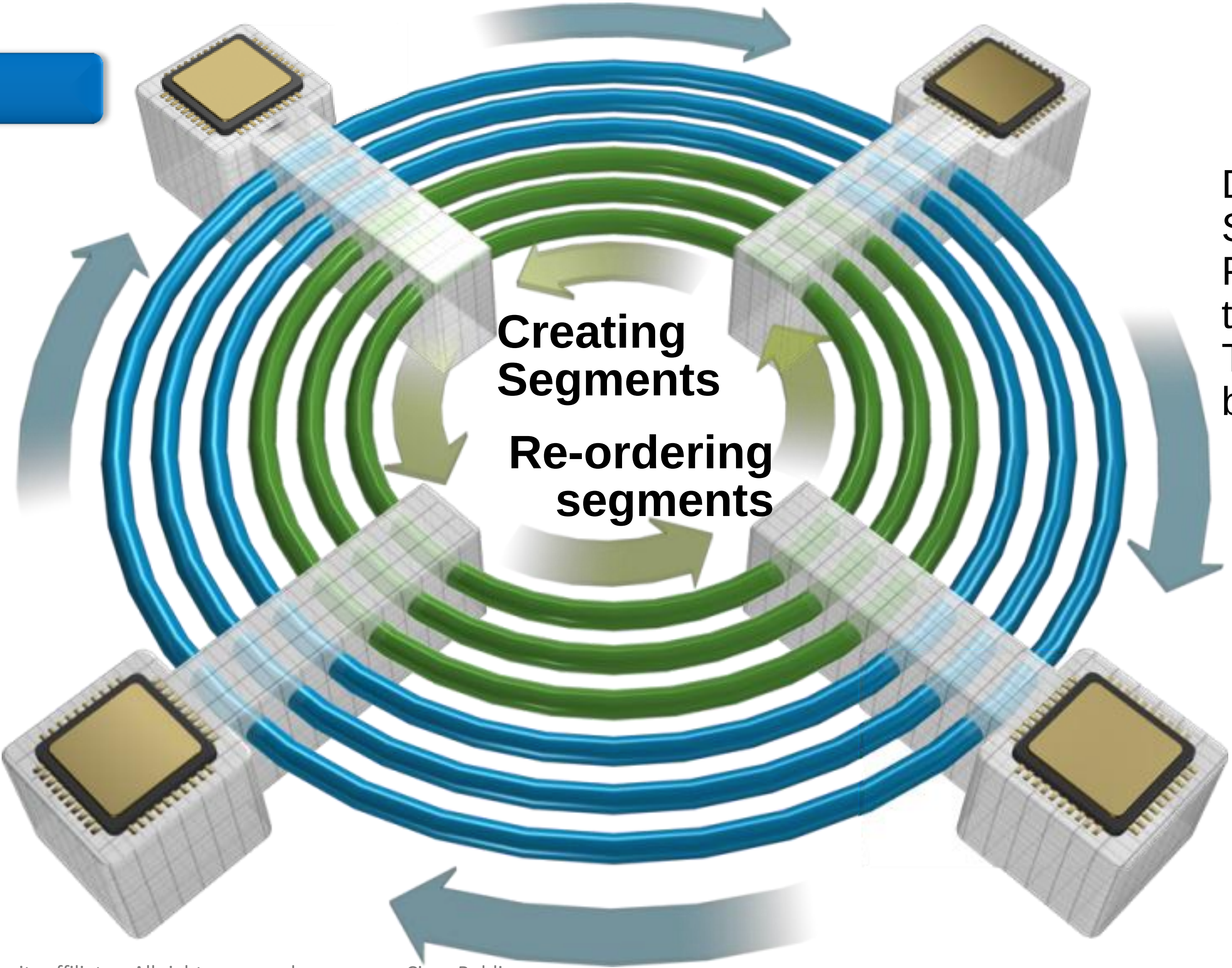


Assuming 4 x 24-port 3850 Switches

Packets are segmented/reassembled in hardware (256 byte segments)

Catalyst 3850 –
Unicast Packet Path

Assuming
4 x 24-port
3850 Switches



Creating
Segments

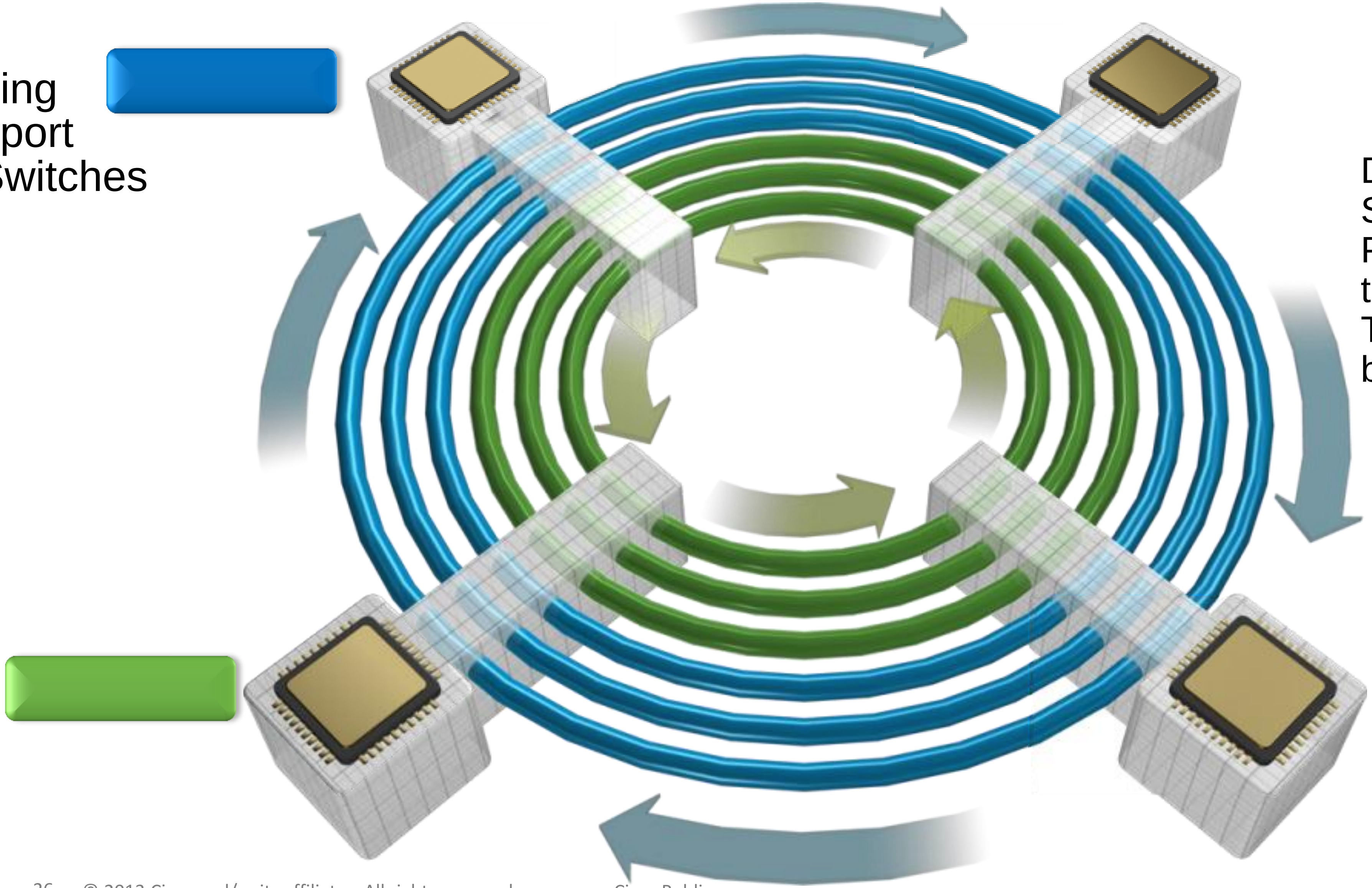
Re-ordering
segments

Destination
Stripping
Packet travels ½
the rings.
Taken out of stack
by destination

Catalyst 3850 –

Unicast Packet Path – Spatial Reuse

Assuming
4 x 24-port
3850 Switches

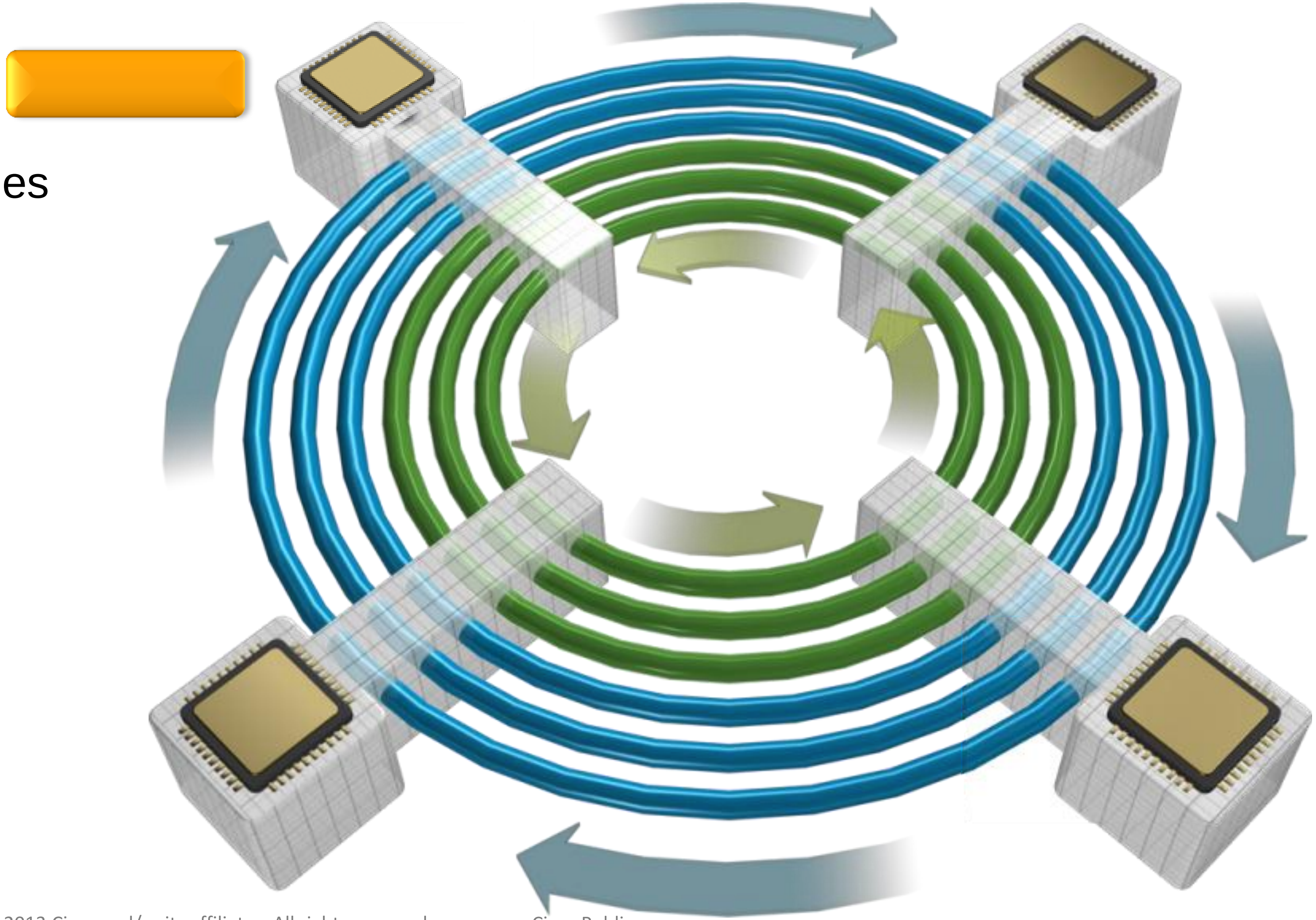


Destination
Stripping
Packet travels ½
the rings.
Taken out of stack
by destination

Catalyst 3850 –

Multicast Packet Path on the Stack Ring

Assuming
4 x 24-port
3850 Switches

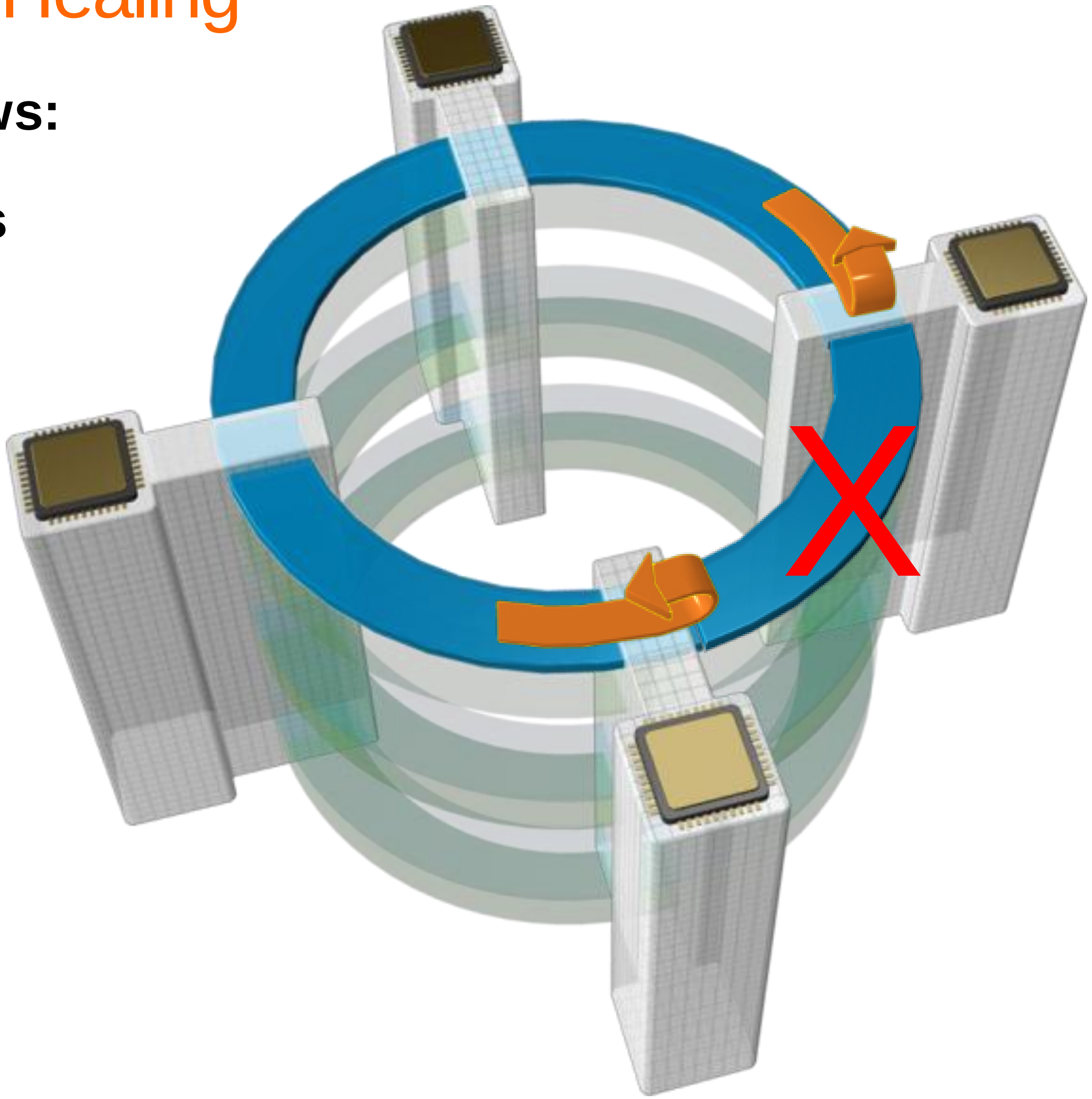


Source Stripping
Packet travels
the full rings
Taken out by
source, when packet
reach back

Catalyst 3850 –

Stack Ring Healing

Example shows:
4 x 24-port
3850 Switches



Detection is by hardware
Software is notified immediately
Ring Wrap initiated immediately > 1 ms

For Recovery –
Hardware detects other side
Software validates the link and so it brings up the connection gracefully

Unwrap is slower than Wrap

Catalyst 3850 –

HA Redundancy – Shift from 3750-X

Catalyst 3750-X – StackWise-Plus

- Hybrid control-plane processing
- N:1 stateless control-plane redundancy
- Distributed L2/L3 Forwarding Redundancy
- Stateless L3 protocol Redundancy

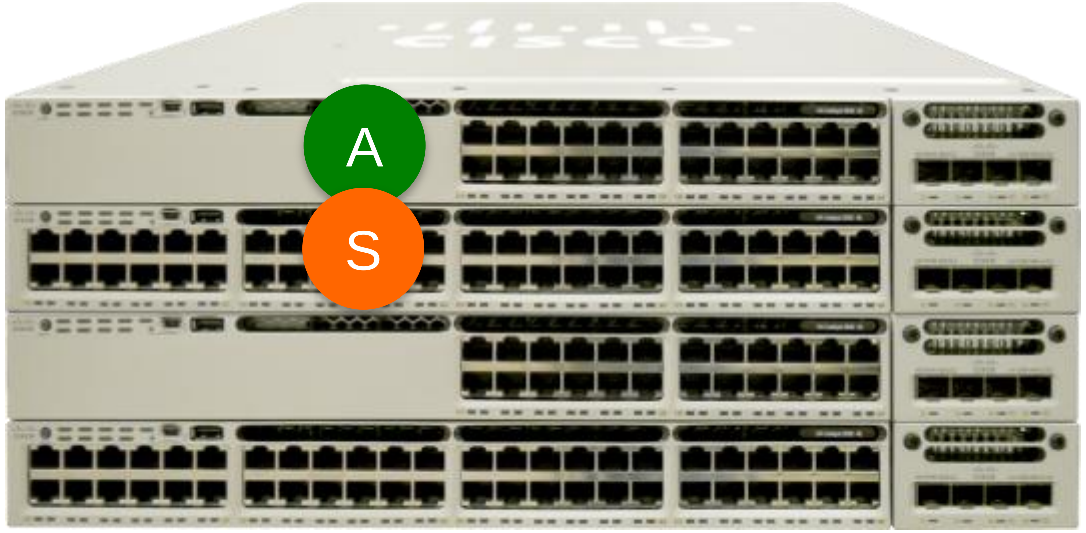
Catalyst 3850 – StackWise-480

- Centralised control-plane processing
- 1+1 Stateful redundancy (SSO)
- Distributed L2/L3 Forwarding Redundancy
- IOS HA Framework alignment for L3 protocol

Catalyst 3850 –

Stacking, vs. Catalyst 6500

Active and Standby Members run IOSd, WCM, etc.
Synchronise information
Active controls Data plane programing for all members
Member switches act as Line cards – connected via the Stack Cable



Active and Standby Supervisors
Run IOS on Supervisors
Synchronise information
Active programs all DFCs
DFCs run a subset of IOS for LCs

Catalyst 3850 –

Software HA Processes on Stack Members – Roles and Definitions

- Route Processor Domain – a set of SW processes (e.g. IOSd, WCM) that implement the centralised Active and Standby portions of the stack control plane
- Line Card Domain – a set of SW processes (e.g. FED, Platform Manager) that implement the distributed Line Card portions of the stack control plane
- Infra Domain – Support SW for the RP and LC Domains
- Active Switch – supports the Active RP Domain, a LC Domain and Infra Domain
- Standby Switch – supports the Standby RP Domain, a LC Domain and Infra Domain
- Member Switch – supports a LC Domain and Infra Domain.
- Election – assigning roles or functions within the stack

Catalyst 3850 –

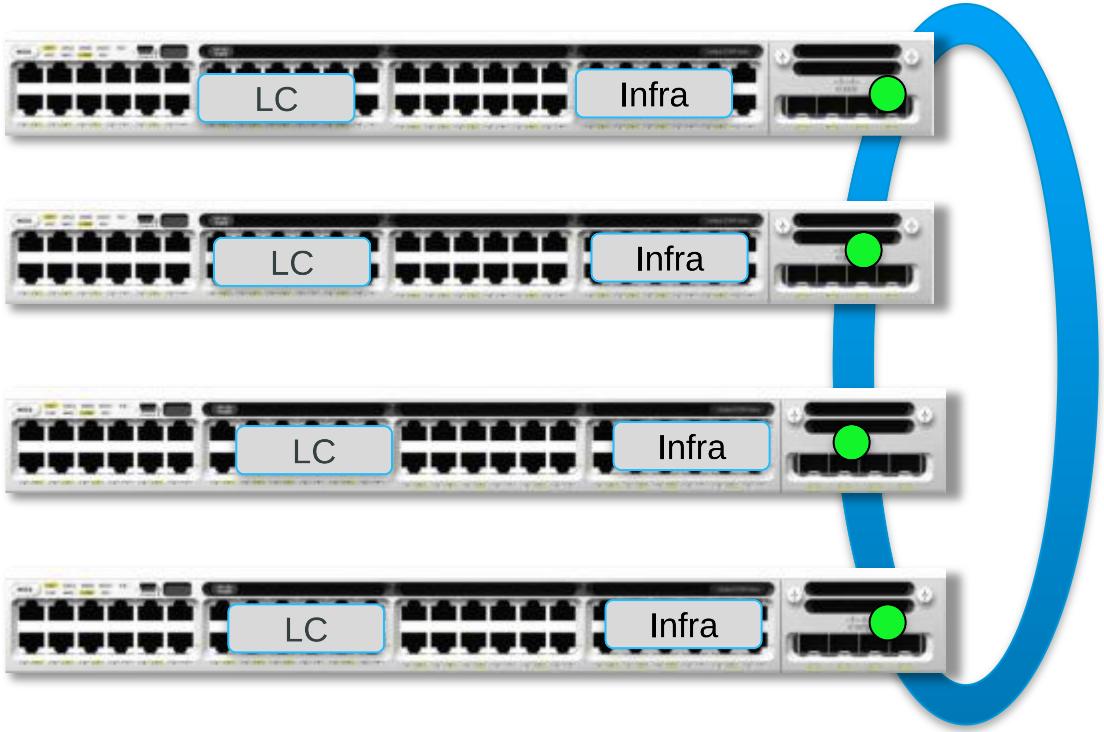
Stack Discovery

- Switches boot
- Stack Interfaces brought online
- Infra and LC Domains boot in parallel
- Stack Discovery Protocol discovers

  Stack topology – broadcast,

  followed by neighbourcast
- In full ring, discovery exits after

  all members are found
- In an incomplete ring, system waits for 2mins
- Active Election begins after Discovery exits
- Election based on Highest Priority OR Lower MAC

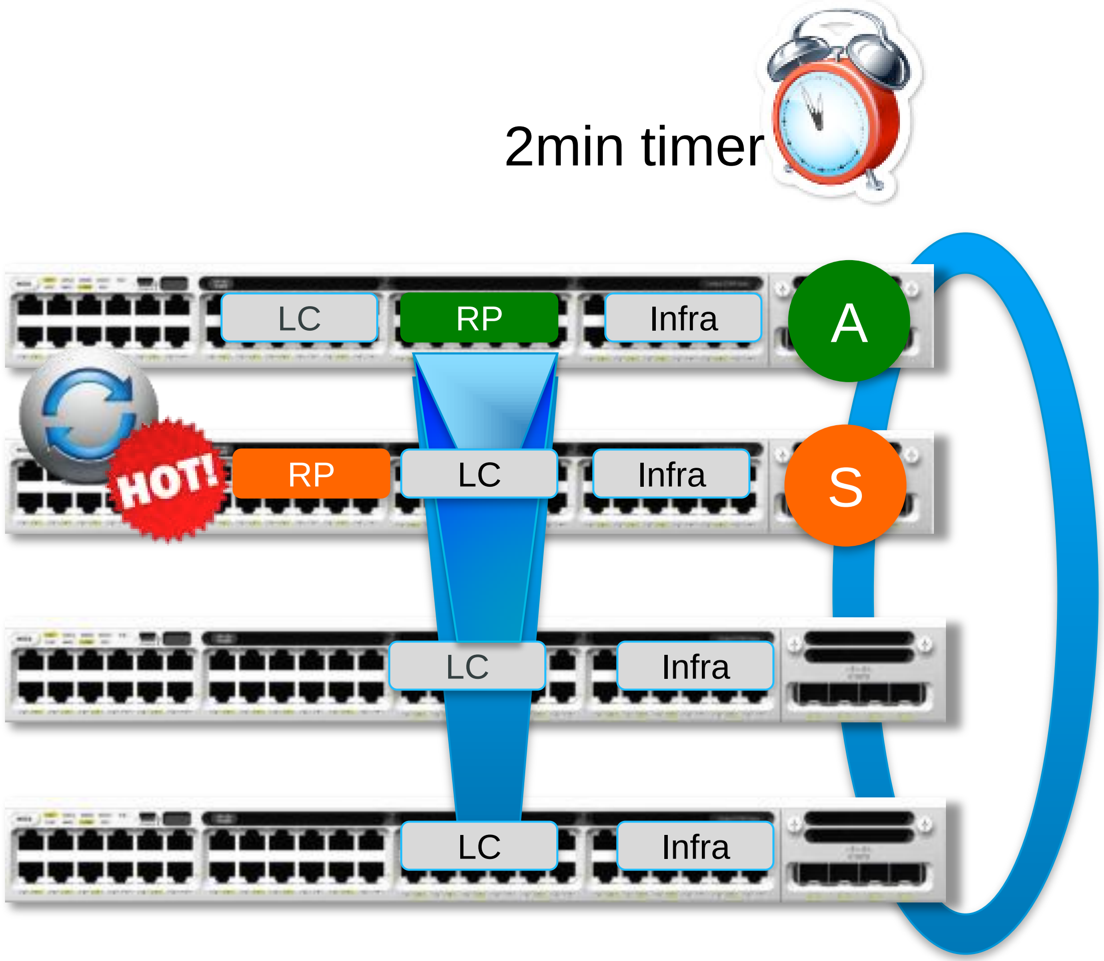


Catalyst 3850 –

Stack Formation

- Active starts RP Domain

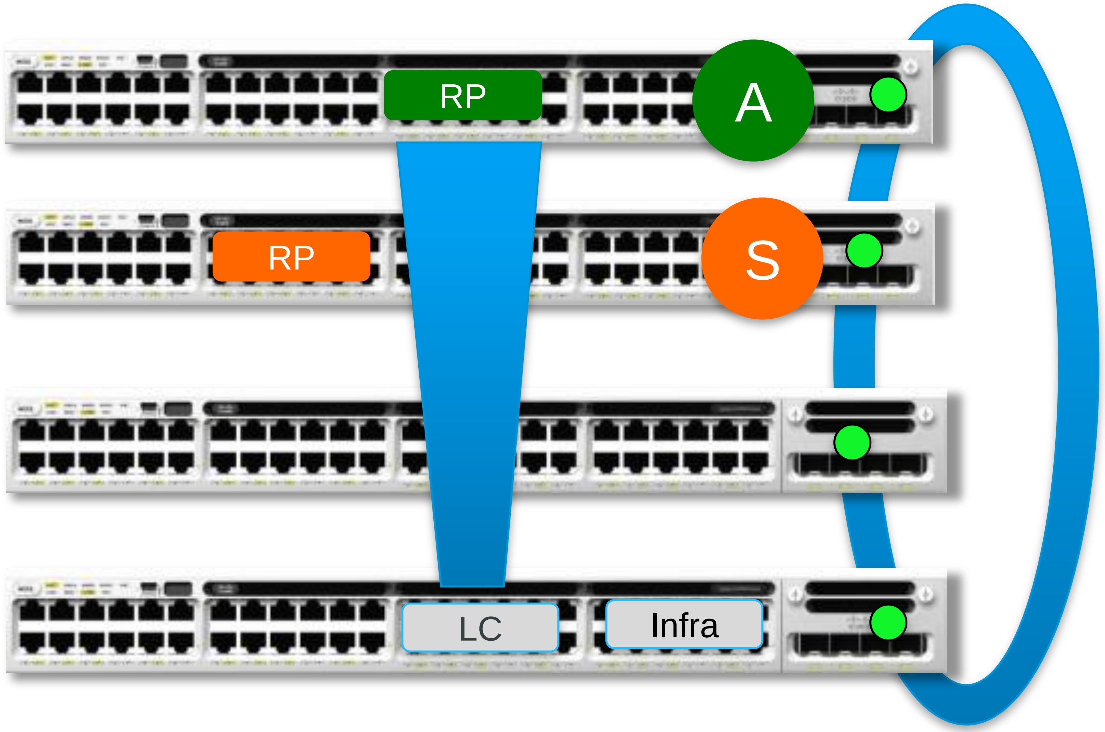
  (IOSd, WCM, etc) locally
- Programs hardware on all LC Domains
- Traffic resumes once hardware is programmed
- Starts 2min Timer to elect Standby in parallel
- Active elects Standby
- Standby starts RP Domain locally
- Starts Bulk Sync with Active RP
- Standby reaches “Standby Hot”



Catalyst 3850 –

Stack Member Addition

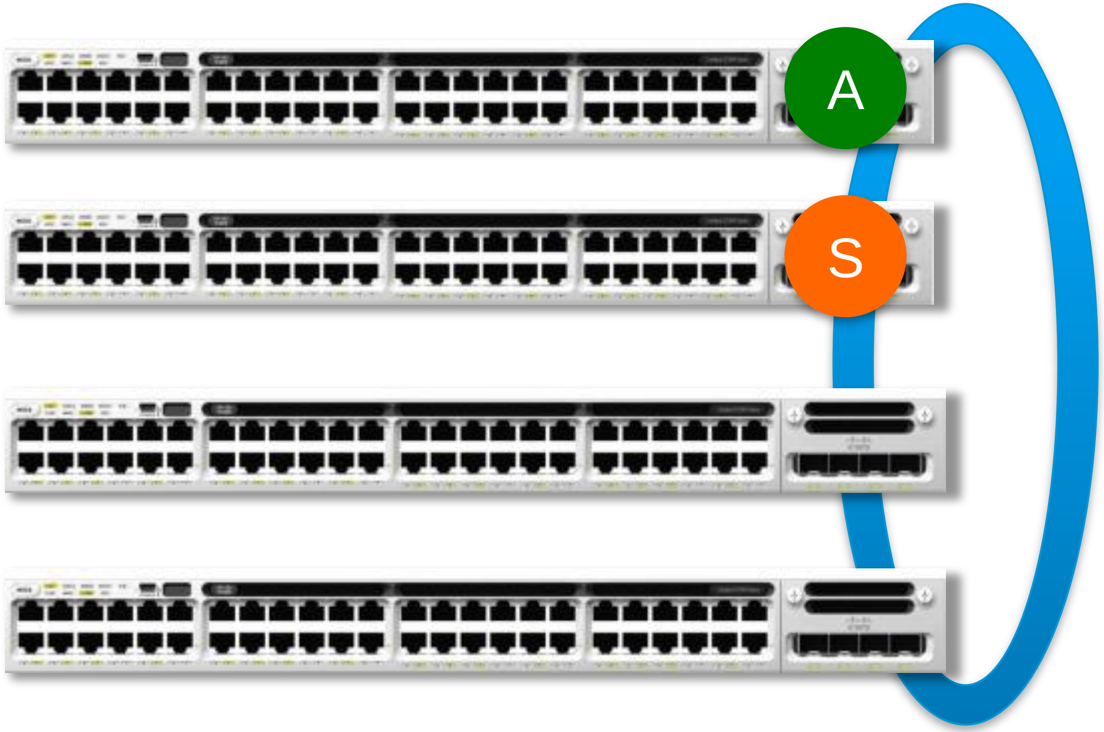
- Stack discovery initiated and completed
- Plug in the member, completing full ring
- Power up the member
- Stack Discovery process runs and completes immediately after discovery happens
- Active detects the new addition, and programs the hardware of the member
- Active is not pre-empted by powering on another member even if it was High Priority



Catalyst 3850 –

Stack Member Deletion

- Stack discovery initiated and completed
- Active detects member removal – and Clean up process is initiated
- Clean-up involves removing TCAM entries referencing removed member, MAC addresses, CDP tables – more like all ports on the member are shutdown
- Half Ring



Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

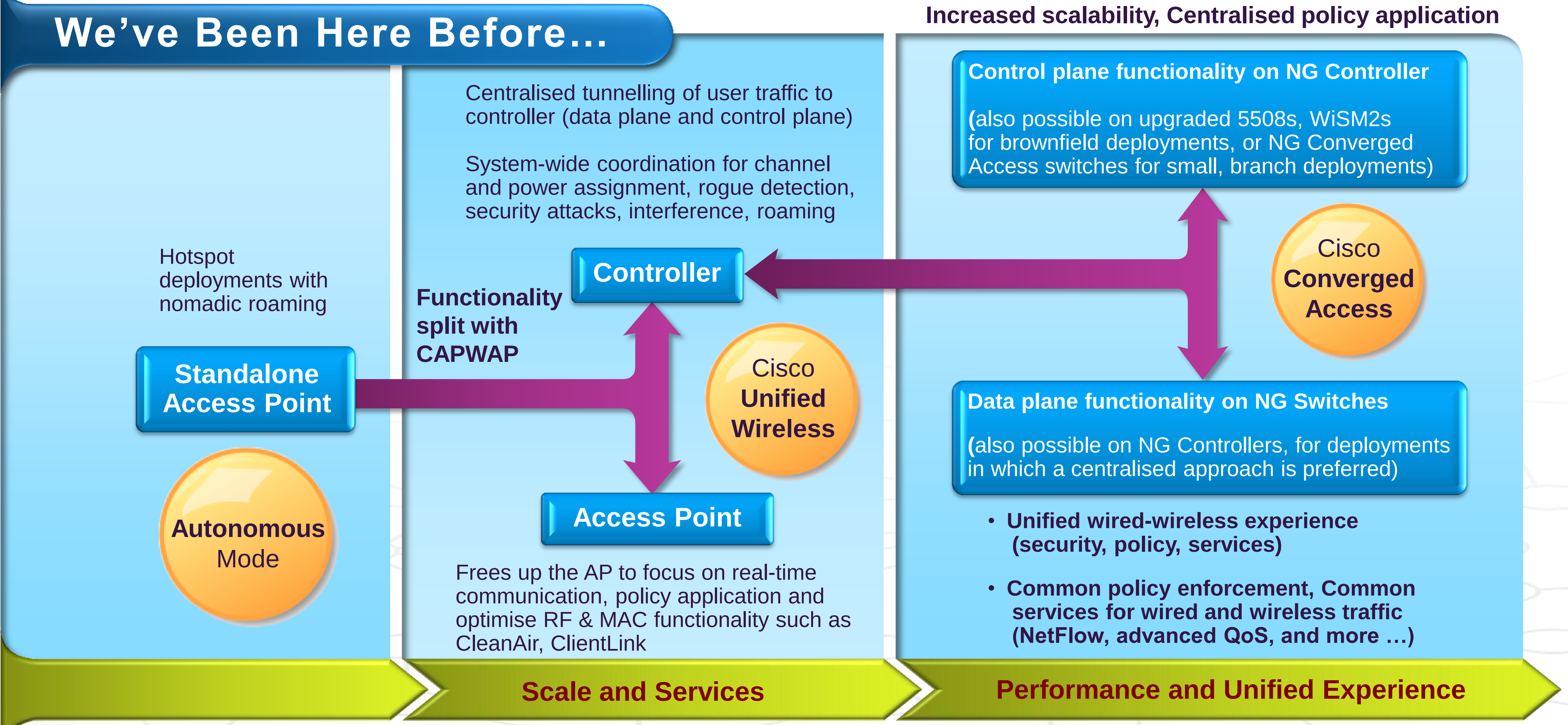
The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Cisco Converged Access –

Network Requirements Driving Wireless Evolution …



We've Been Here Before…

Increased scalability, Centralised policy application

Hotspot deployments with nomadic roaming

Standalone Access Point

Autonomous Mode

Centralised tunnelling of user traffic to controller (data plane and control plane)

System-wide coordination for channel and power assignment, rogue detection, security attacks, interference, roaming

Functionality split with CAPWAP

Controller

Cisco **Unified Wireless**

Access Point

Frees up the AP to focus on real-time communication, policy application and optimise RF & MAC functionality such as CleanAir, ClientLink

Control plane functionality on NG Controller

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

Cisco **Converged Access**

Data plane functionality on NG Switches

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

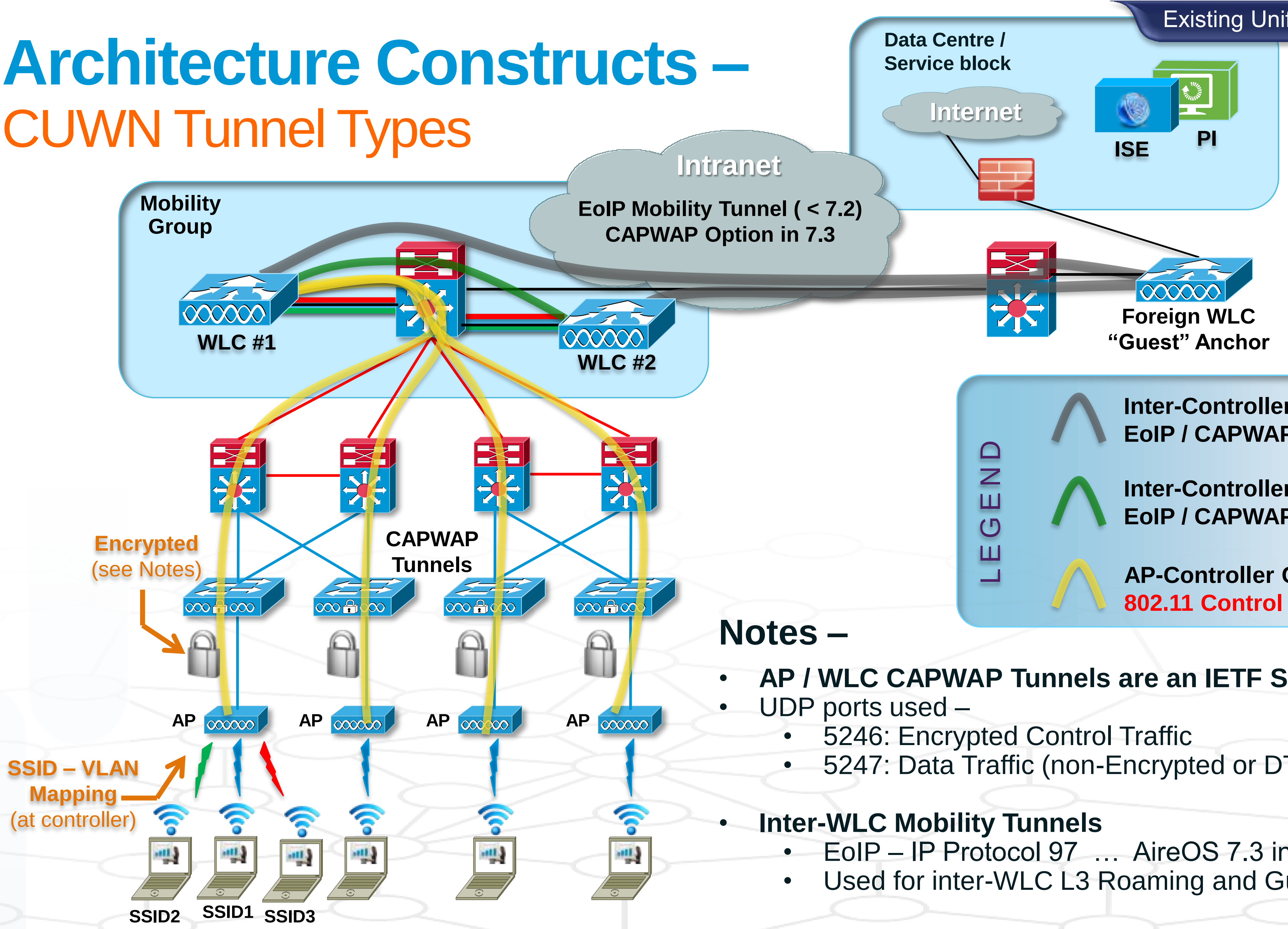
- **Unified wired-wireless experience (security, policy, services)**
- **Common policy enforcement, Common services for wired and wireless traffic (NetFlow, advanced QoS, and more …)**

Scale and Services

Performance and Unified Experience

Existing Unified Wireless Deployment today …

Architecture Constructs –
CUWN Tunnel Types



Well-known, proven architecture

LEGEND

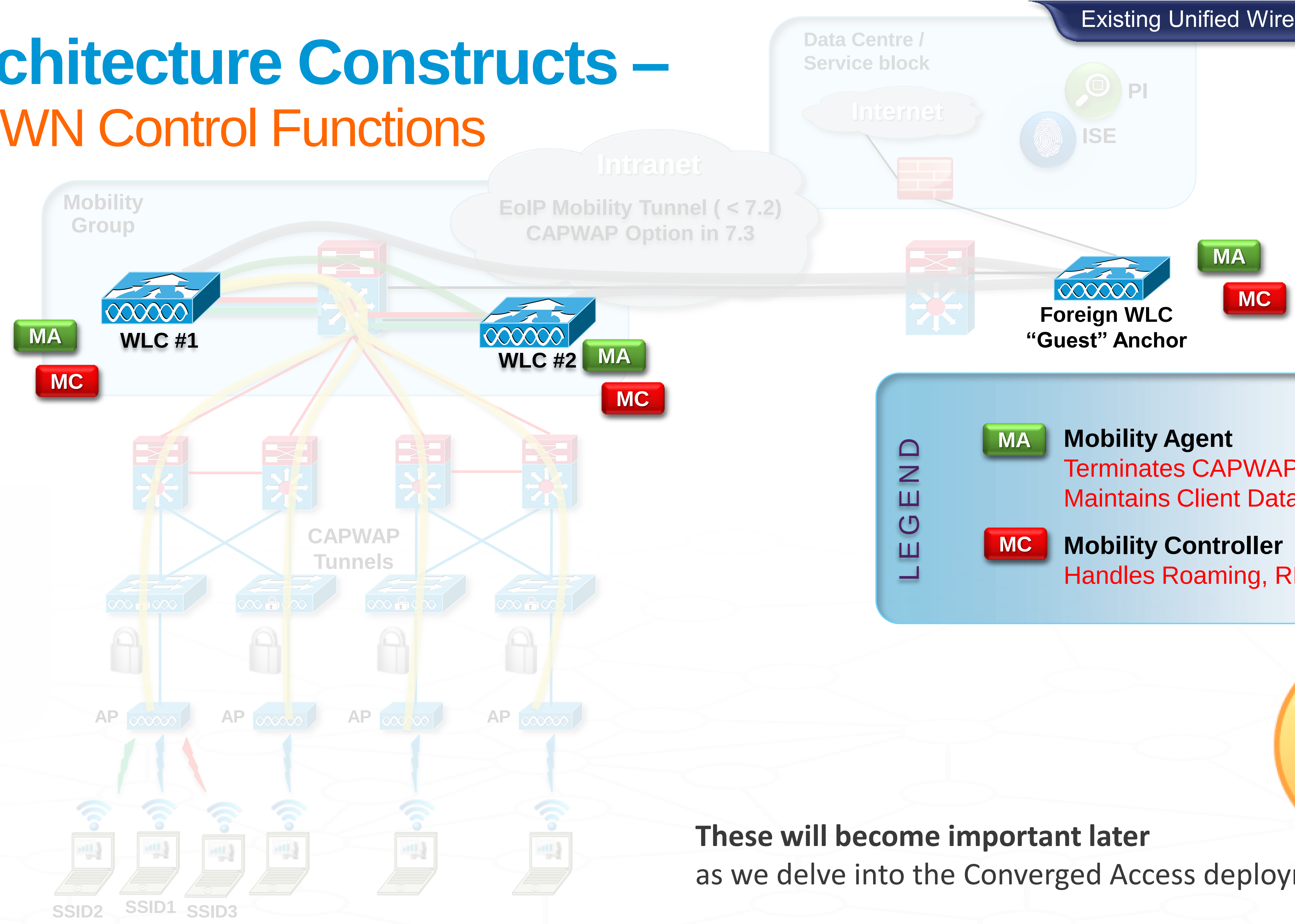
- **Inter-Controller** (Guest Anchor) **EoIP / CAPWAP Tunnel**
- **Inter-Controller EoIP / CAPWAP Tunnel**
- **AP-Controller CAPWAP Tunnel** **802.11 Control Session + Data Plane**

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

Existing Unified Wireless Deployment today …

Architecture Constructs –
CUWN Control Functions



LEGEND

MA **Mobility Agent**
Terminates CAPWAP Tunnels,
Maintains Client Database

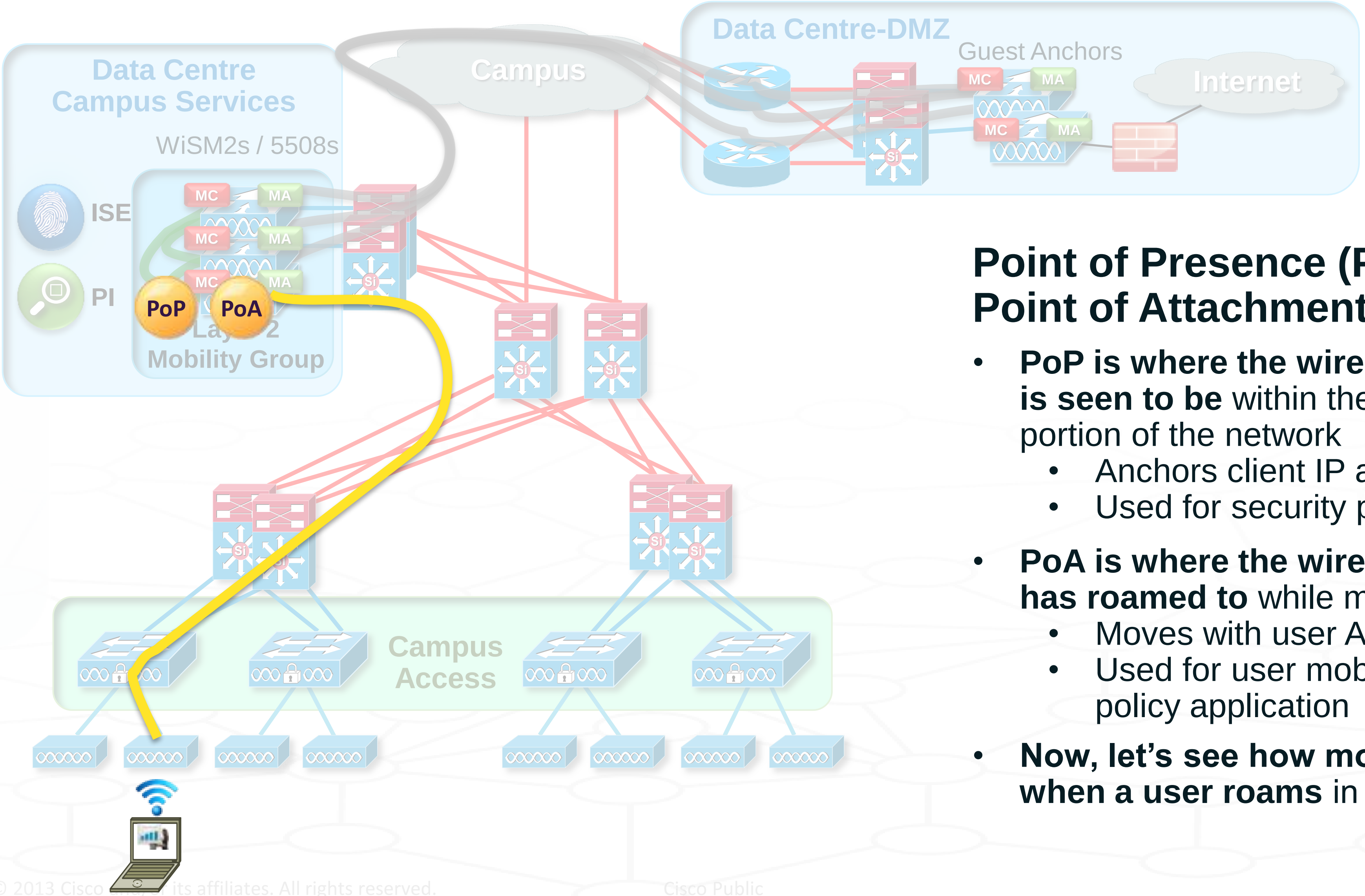
MC **Mobility Controller**
Handles Roaming, RRM, WIPS, etc.

Additional details on controller functionality

These will become important later
as we delve into the Converged Access deployment …

Architecture Constructs –

Point of Presence (PoP), Point of Attachment (PoA)

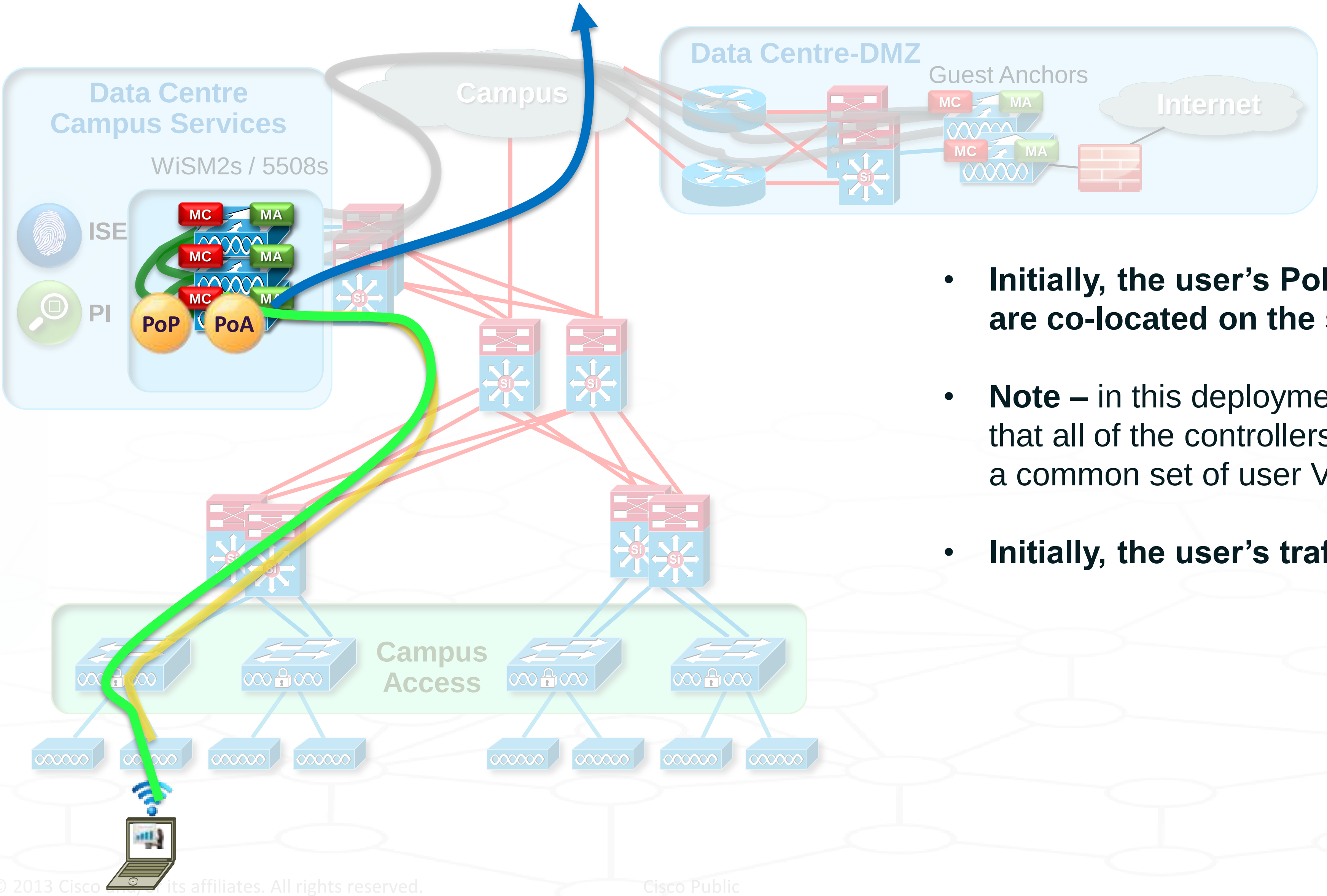


Point of Presence (PoP) vs. Point of Attachment (PoA) –

- **PoP is where the wireless user is seen to be** within the wired portion of the network
  - Anchors client IP address
  - Used for security policy application
- **PoA is where the wireless user has roamed to** while mobile
  - Moves with user AP connectivity
  - Used for user mobility and QoS policy application
- **Now, let's see how mobility works when a user roams** in this deployment model …

Architecture Constructs –

Layer 2 Roaming (Campus Deployment)

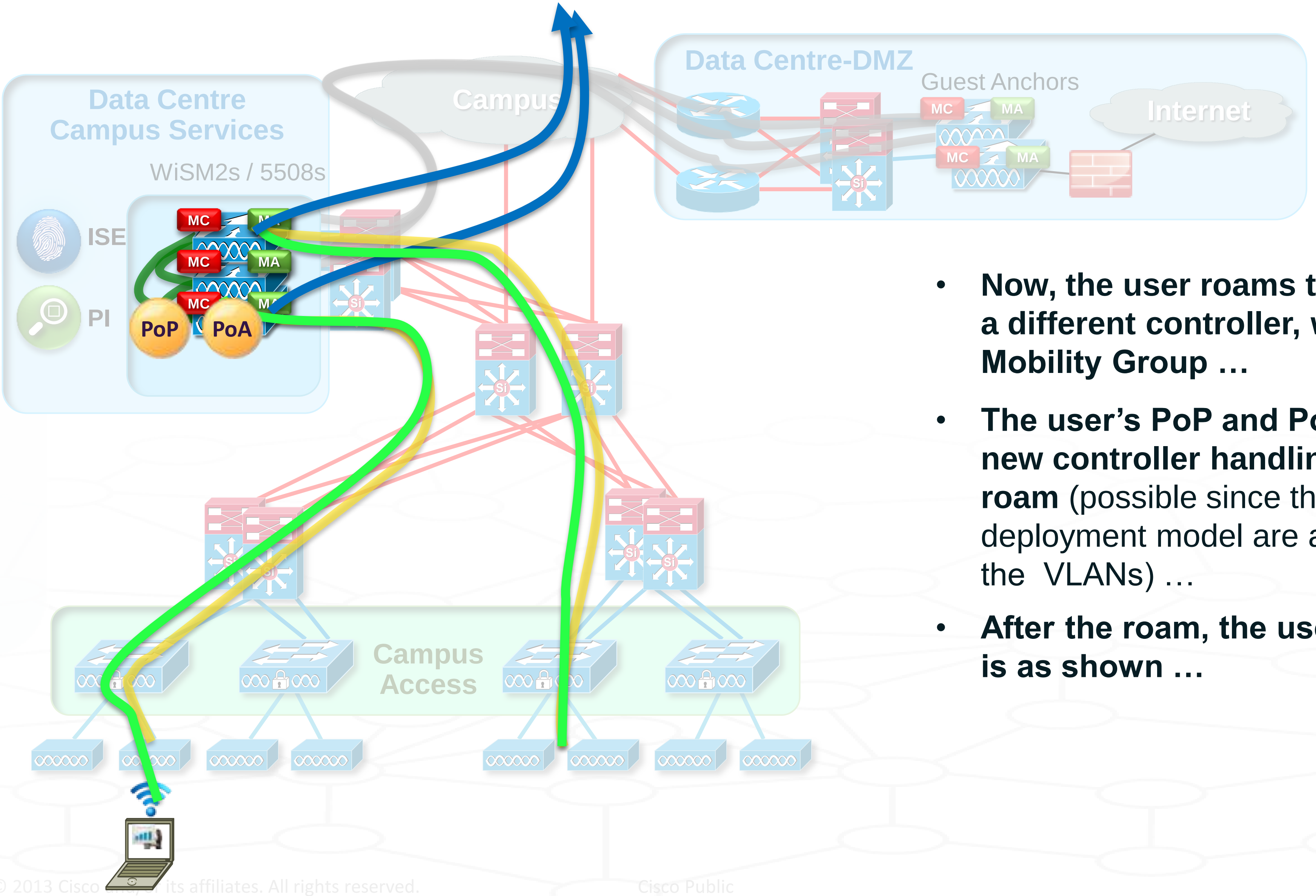


- **Initially, the user's PoP and PoA are co-located on the same controller**
- **Note –** in this deployment model, it is assumed that all of the controllers within the DC share a common set of user VLANs at Layer 2
- **Initially, the user's traffic flow is as shown …**

Architecture Constructs –

Layer 2 Roaming (Campus Deployment)

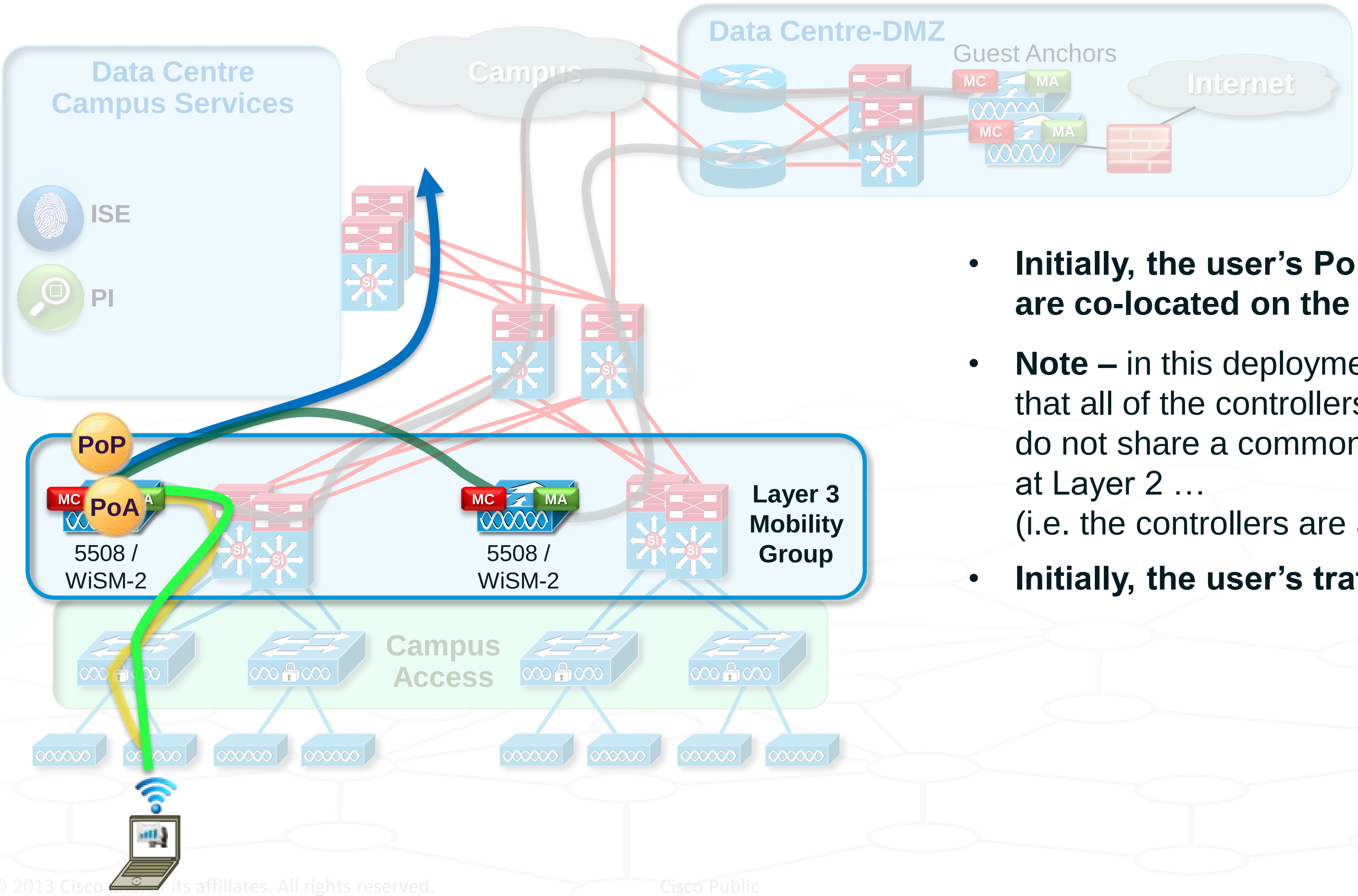
Move of the user's entire Mobility Context



- **Now, the user roams to an AP handled by a different controller, within the same Mobility Group …**
- **The user's PoP and PoA both move to the new controller handling that user after the roam** (possible since the controllers in this deployment model are all L2-adjacent within the VLANs) …
- **After the roam, the user's traffic flow is as shown …**

Architecture Constructs –

Layer 3 Roaming (Campus Deployment)

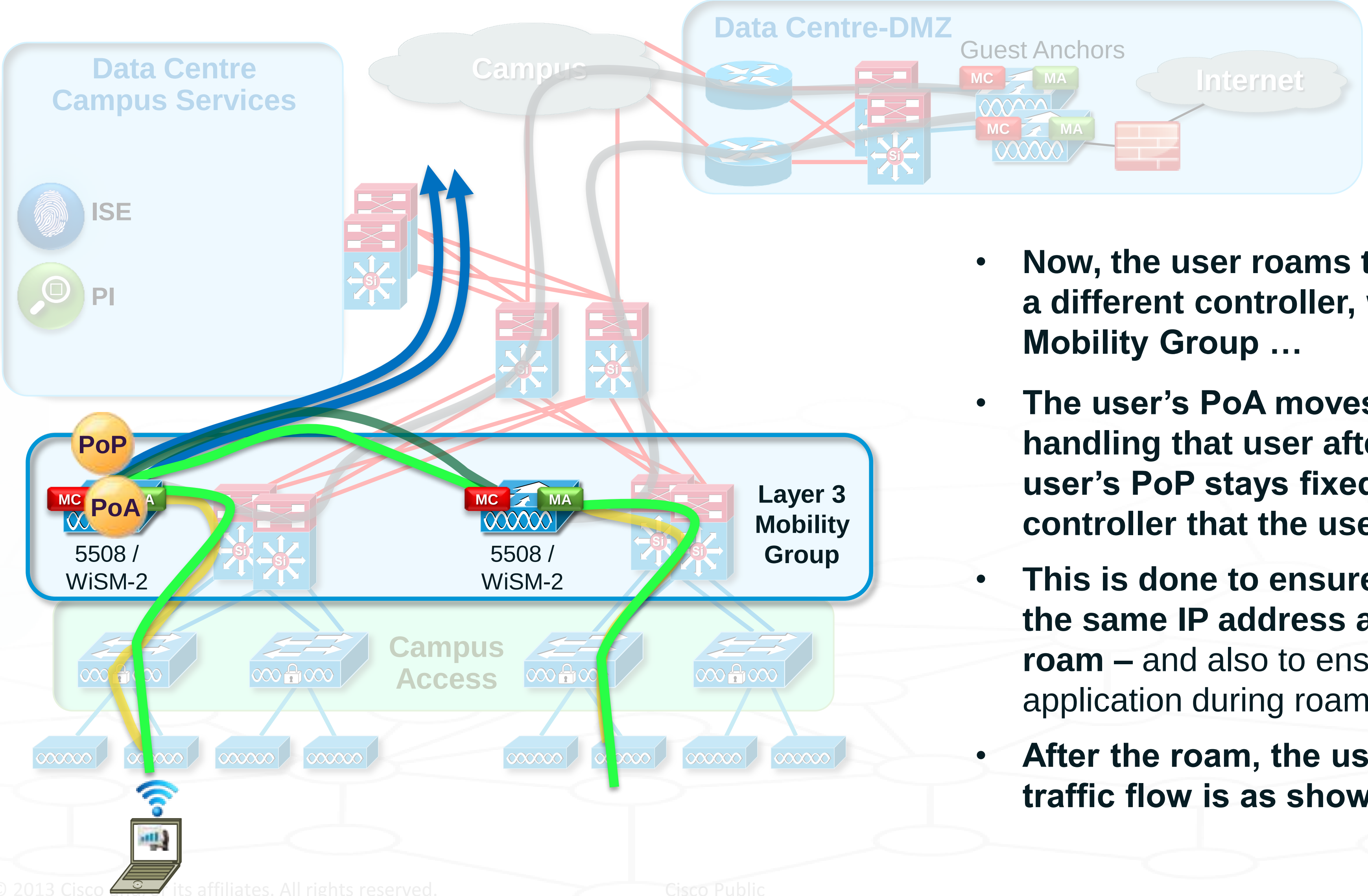


- **Initially, the user's PoP and PoA are co-located on the same controller**
- **Note –** in this deployment model, it is assumed that all of the controllers across the Campus do not share a common set of user VLANs at Layer 2 …
(i.e. the controllers are all L3-separated)
- **Initially, the user's traffic flow is as shown …**

Architecture Constructs –

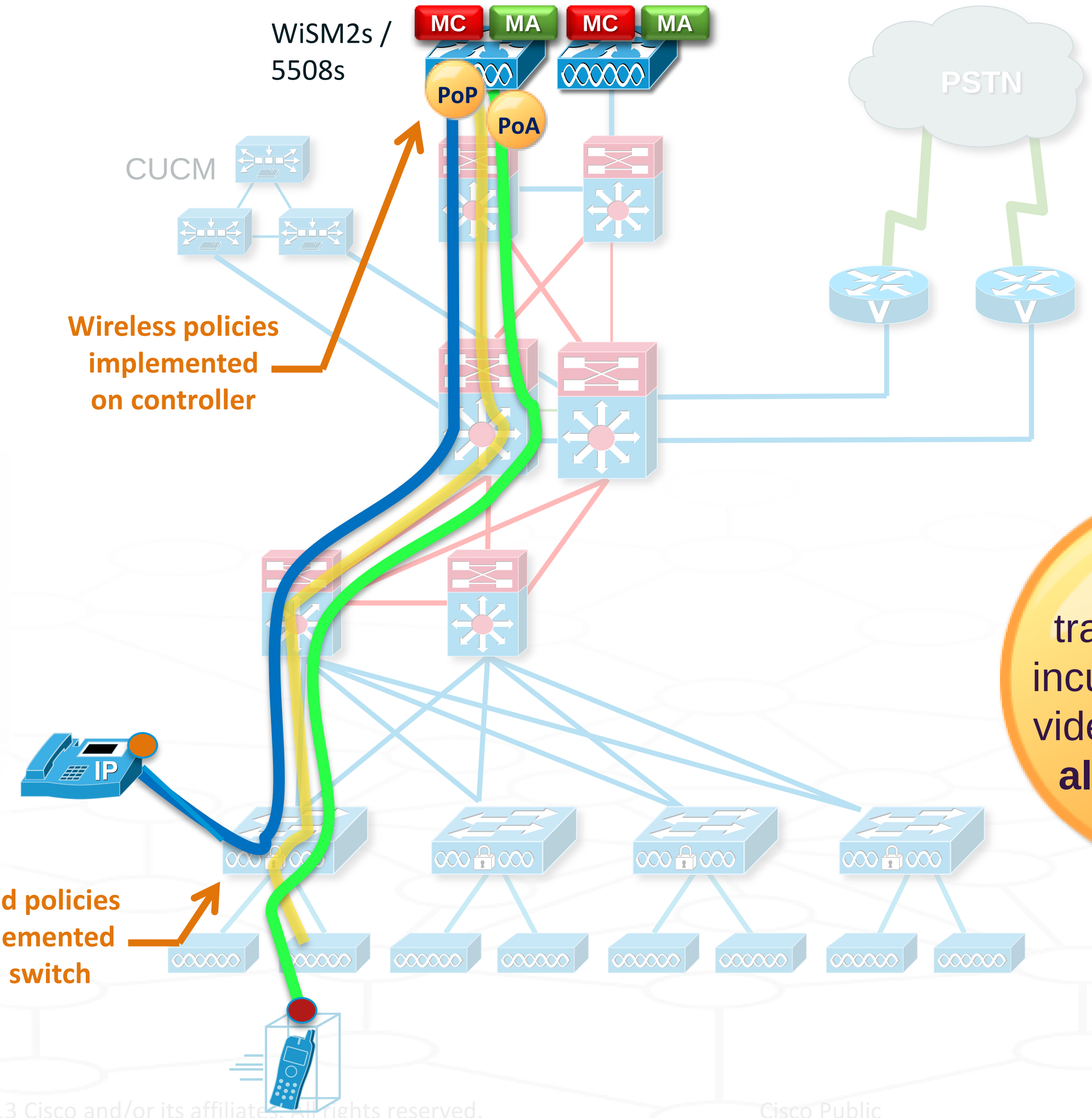
Layer 3 Roaming (Campus Deployment)

Symmetric Mobility Tunnelling



- **Now, the user roams to an AP handled by a different controller, within the same Mobility Group …**
- **The user's PoA moves to the new controller handling that user after the roam – but the user's PoP stays fixed on the original controller that the user associated to**
- **This is done to ensure that the user retains the same IP address across an L3 boundary roam –** and also to ensure continuity of policy application during roaming
- **After the roam, the user's traffic flow is as shown …**

Unified Wireless –
Traffic Flow



Wireless policies implemented on controller

Wired policies implemented on switch

Separate policies and services for wired and wireless users

The same traffic paths are incurred for voice, video, data, etc. – **all centralised**

Traffic Flows, Unified Wireless –

- In this example, a VoIP user is on today's CUWN network, and is making a call from a wireless handset to a wired handset …
- **We can see that all of the user's traffic needs to be hairpinned back through the centralised controller,** in both directions …

In this example, a total of **9 hops** are incurred for each direction of the traffic path (including the controllers – Layer 3 roaming might add more hops) …

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

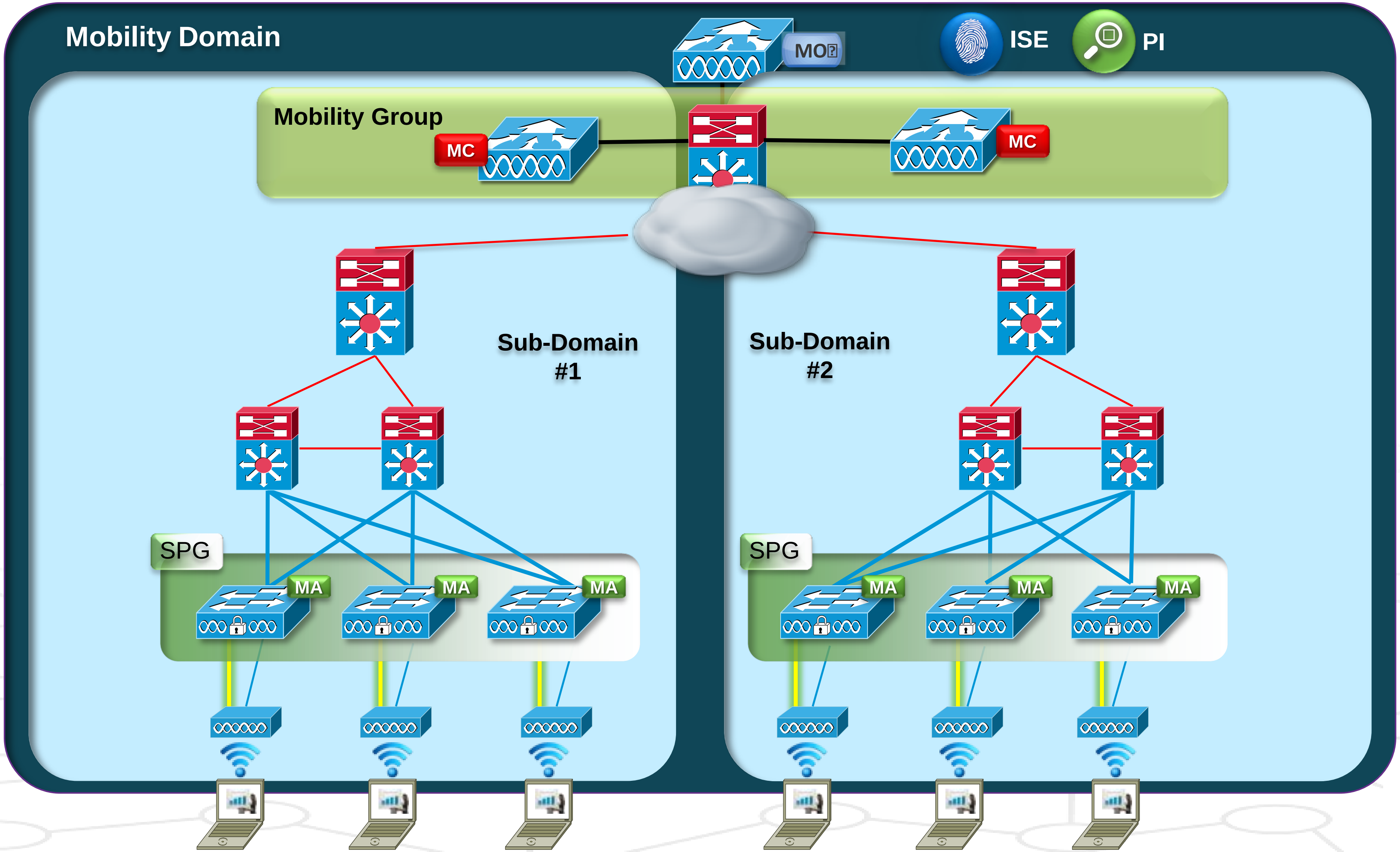
Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- **Components of the Deployment – Terminology Review**
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

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.
- **Mobility Domain** – Grouping of MCs to support seamless roaming
- **Switch Peer Group (SPG) –** Localises traffic for roams within Distribution Block

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

Converged Access –

Physical Entities – Catalyst 3850 Switch Stack

Best-in-Class Wired Switch – with Integrated Wireless Mobility functionality

MA

- Can act as a **Mobility Agent** (MA)
  for terminating CAPWAP tunnels for locally connected APs …

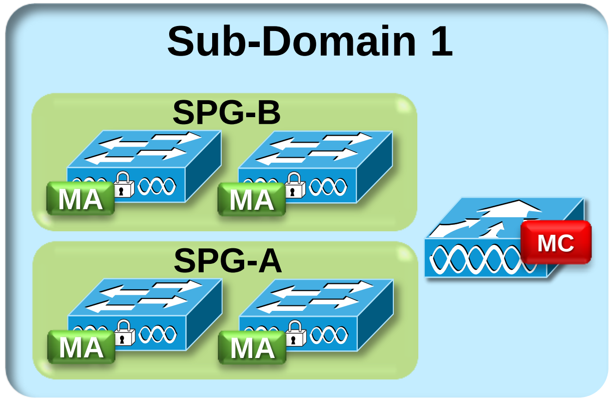
MC

- as well as a **Mobility Controller** (MC)
  for other Mobility Agent (MA) switches, in small deployments

  - MA/MC functionality works on a Stack of Catalyst 3850 Switches
  - MA/MC functionality runs on Stack Master
  - Stack Standby synchronises some information (useful for intra-stack HA)

Converged Access –

Logical Entities – Switch Peer Groups



- **Made up of multiple Catalyst 3850 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**

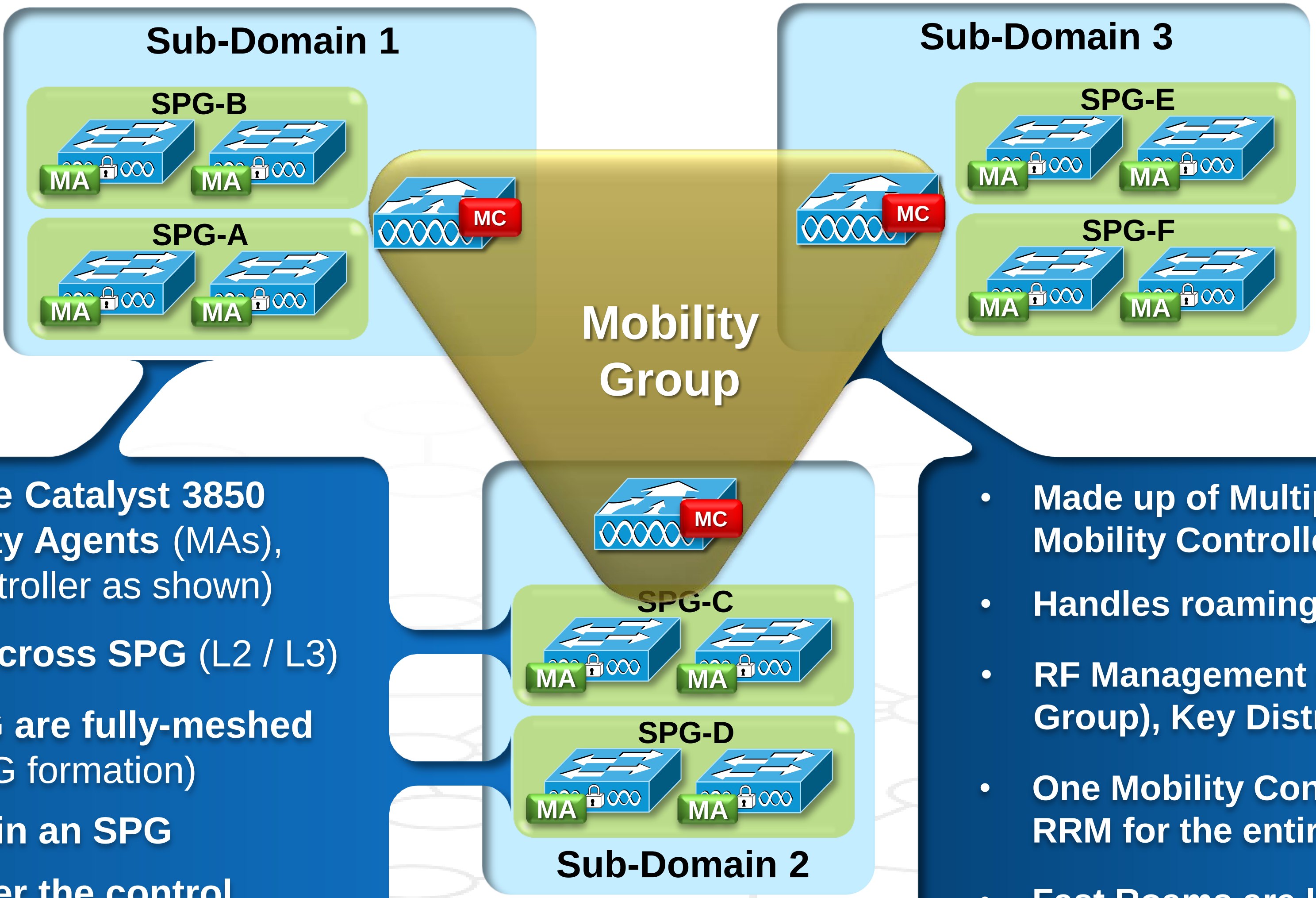
Roamed traffic within an SPG moves directly between the MAs in that SPG (CAPWAP full mesh)

Roamed traffic between SPGs moves via the MC(s) servicing those SPGs

Hierarchical architecture is optimised for scalability and roaming

Converged Access –

Logical Entities – Switch Peer Groups and Mobility Group



- **Made up of multiple Catalyst 3850 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**

- **Made up of Multiple Mobility Controllers (MCs)**
- **Handles roaming across MG** (L2 / L3)
- **RF Management (RRM, handled by RF Group), Key Distribution for Fast Roaming**
- **One Mobility Controller** (MC) **manages RRM for the entire RF Group**
- **Fast Roams are limited to Mobility Group member MCs**

Converged Access –

Scalability Considerations

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

- **These are summarised below, for quick reference**
- **Full details on scalability – for both CUWN as well as Converged Access deployments – is located in the Reference section at the end of this slide deck**

Scalability	3850 as MC	5760	5508	WiSM2
Max number of MCs in a Mobility Domain	8	72	72	72
Max number of MCs in a Mobility Group	8	24	24	24
Max number of MAs in a Sub-domain (per MC)	16	350	350	350
Max number of SPGs in a Mobility Sub-Domain (per MC)	8	24	24	24
Max number of MAs in a SPG	16	64	64	64
Max number of WLANs	64	512	512	512

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

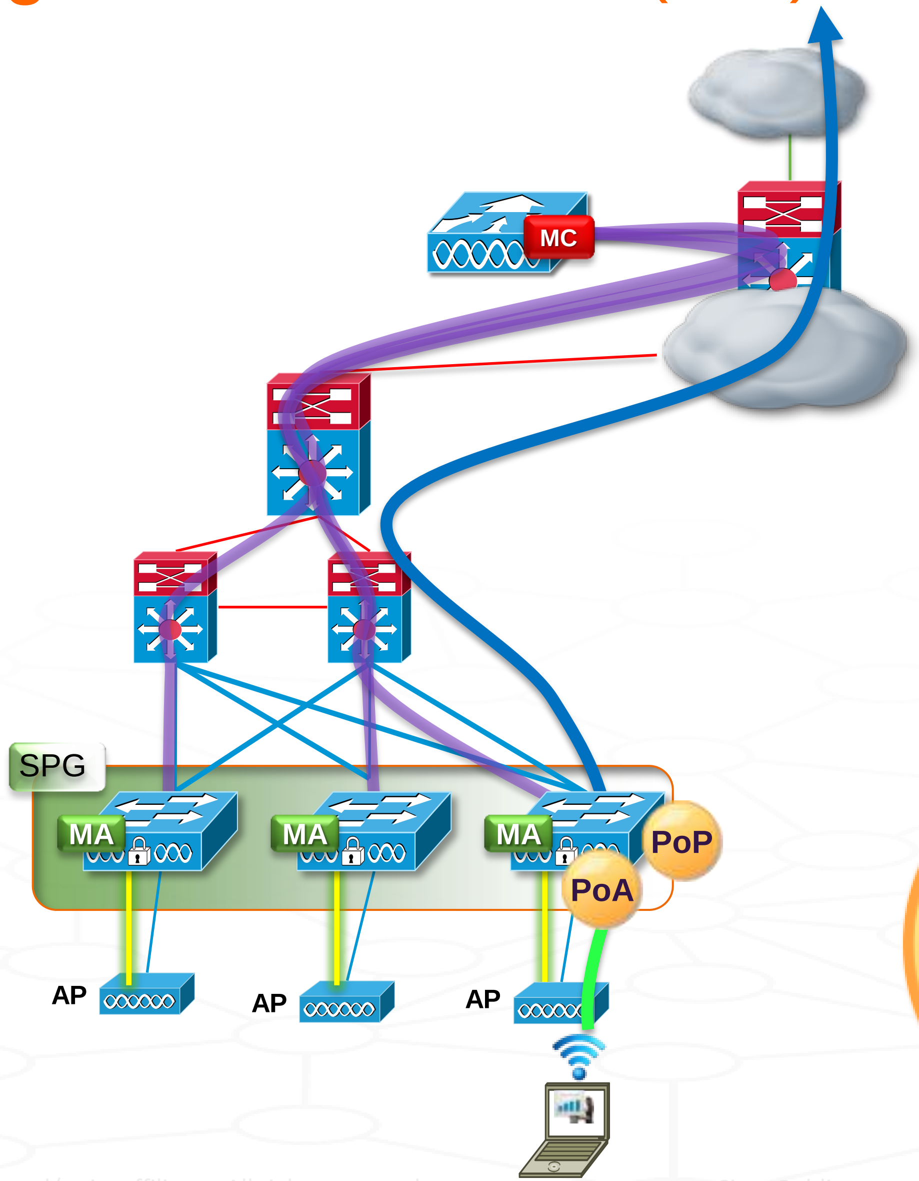
The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- **Converged Access Deployment – Roaming Overview**
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Converged Access –

Roaming – Point of Presence (PoP), Point of Attachment (PoA)



If users associate and remain stationary, this is their traffic flow

Point of Presence (PoP) vs. Point of Attachment (PoA) –

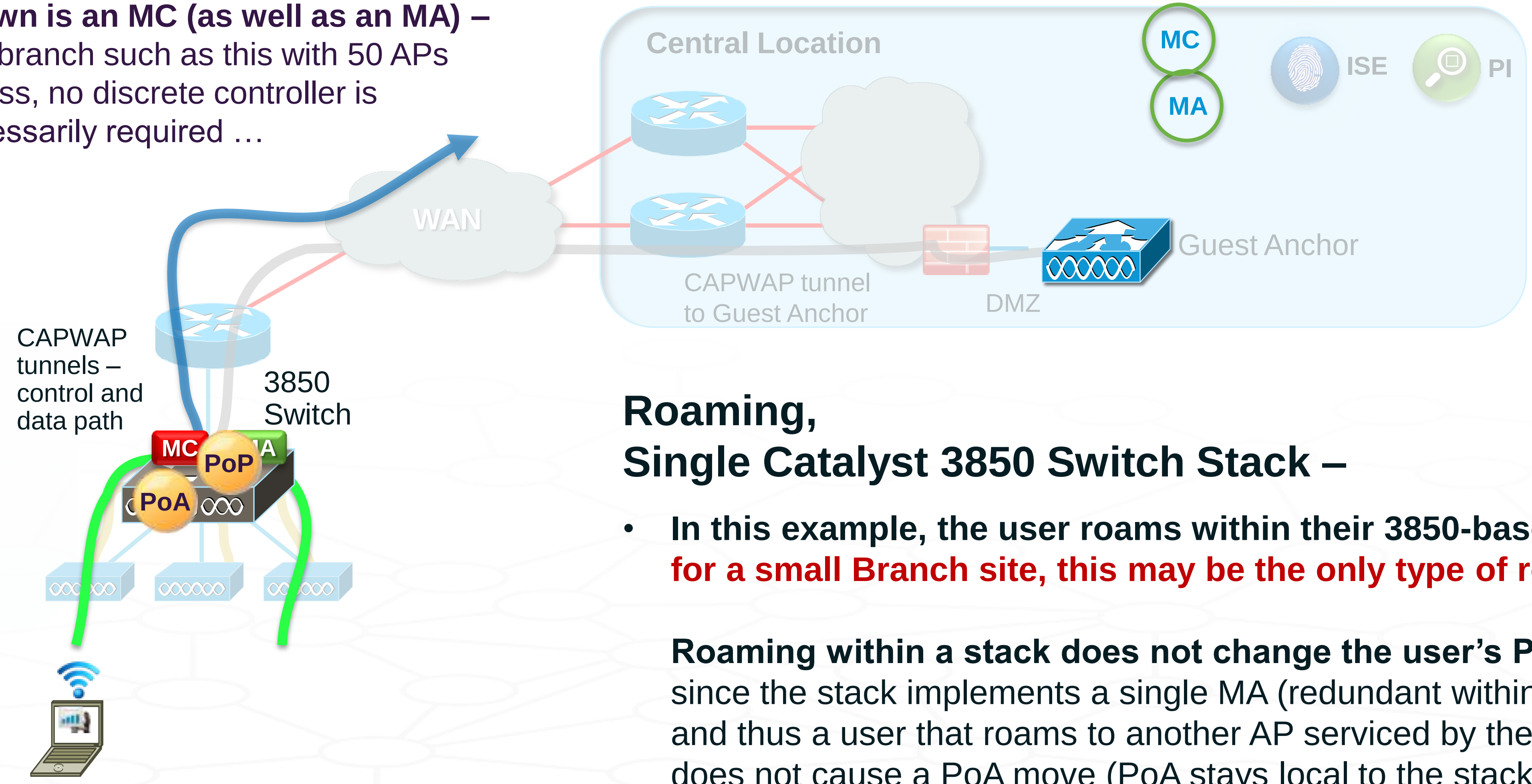
- **PoP is where the wireless user is seen to be** within the wired portion of the network
- **PoA is where the wireless user has roamed to** while mobile
- **Before a user roams, PoP and PoA are in the same place**

Note – for the purposes of illustrating roaming, we are showing the purple connections herein that indicate the connections between the MAs and their corresponding MC for the Switch Peer Group (or Groups) involved on each slide … notice that, in this example, **the traffic does NOT flow through the MC …**

Converged Access –

Traffic Flow and Roaming – Branch, Single Catalyst 3850 Stack

Notice how the 3850 switch stack shown is an MC (as well as an MA) – in a branch such as this with 50 APs or less, no discrete controller is necessarily required …


Central Location
MC
MA
ISE
PI
WAN
Guest Anchor
CAPWAP tunnel to Guest Anchor
DMZ
CAPWAP tunnels – control and data path
3850 Switch
MC
MA
PoP
PoA

Roaming across Stack (small branch)

Roaming, Single Catalyst 3850 Switch Stack –

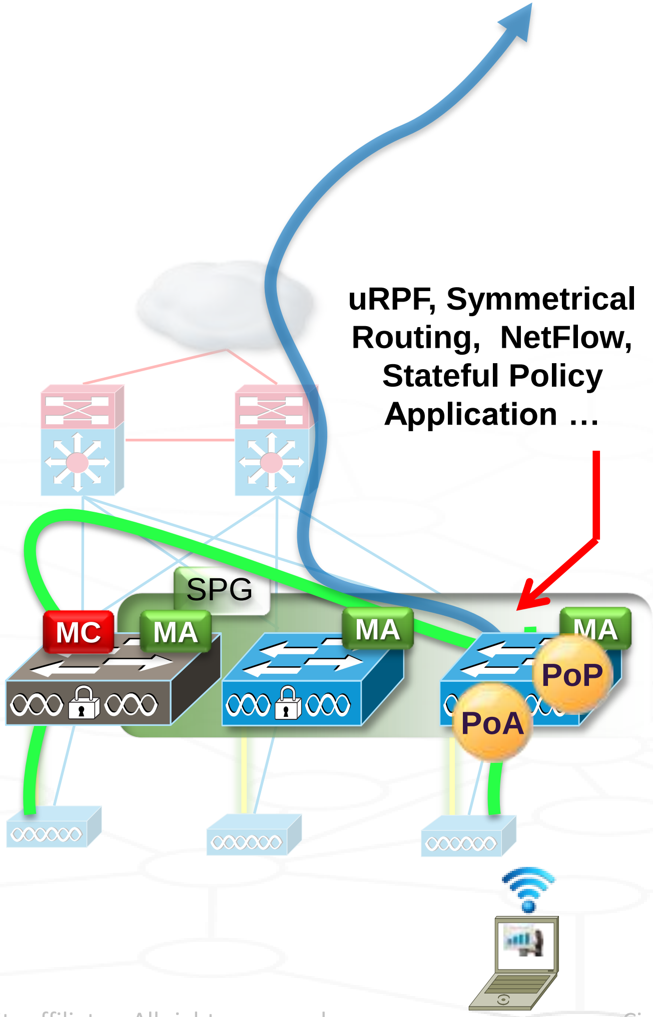
- **In this example, the user roams within their 3850-based switch stack – for a small Branch site, this may be the only type of roam**

  Roaming within a stack does not change the user's PoP or PoA – since the stack implements a single MA (redundant within the stack), and thus a user that roams to another AP serviced by the same stack does not cause a PoA move (PoA stays local to the stack)

Converged Access –

Traffic Flow and Roaming – Branch, L2 / L3 Roam (within SPG)

Roaming across Stacks (larger branch)



uRPF, Symmetrical Routing, NetFlow, Stateful Policy Application …

Roaming, Within a Switch Peer Group (Branch) –

- Now, let’s examine a roam at a larger branch, with multiple 3850-based switch stacks joined together via a distribution layer
- **In this example, the larger Branch site consists of a single Switch Peer Group – and the user roams within that SPG – again, at a larger Branch such as this, this may be the only type of roam**

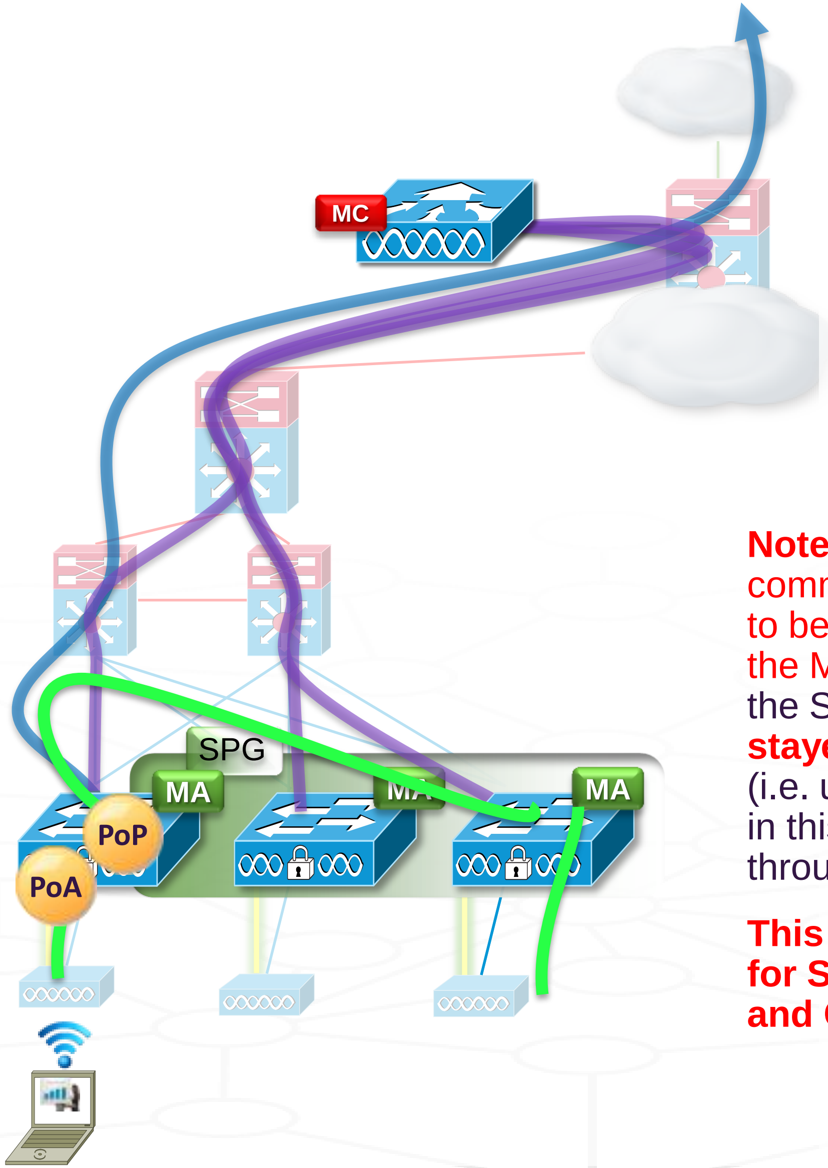
  The user may or may not have roamed across an L3 boundary (depends on wired setup) – **however, users are always* taken back to their PoP** for policy application

Again, notice how the 3850 switch stack on the left is an MC (as well as an MA) in this picture – in a larger branch such as this with 50 APs or less, no discrete controller is necessarily required …

* Adjustable via setting, may be useful for L2 roams (detailed on slides in following section of this slide deck)

Converged Access –

Traffic Flow and Roaming – Campus L2 / L3 Roam (within SPG)



Roaming within an SPG

(L3 behaviour and default L2 behaviour)

Note – the traffic in this most common type of roam did **not** have to be transported back to, or via, the MC (controller) servicing the Switch Peer Group – **traffic stayed local to the SPG only** (i.e. under the distribution layer in this example – not back through the core).

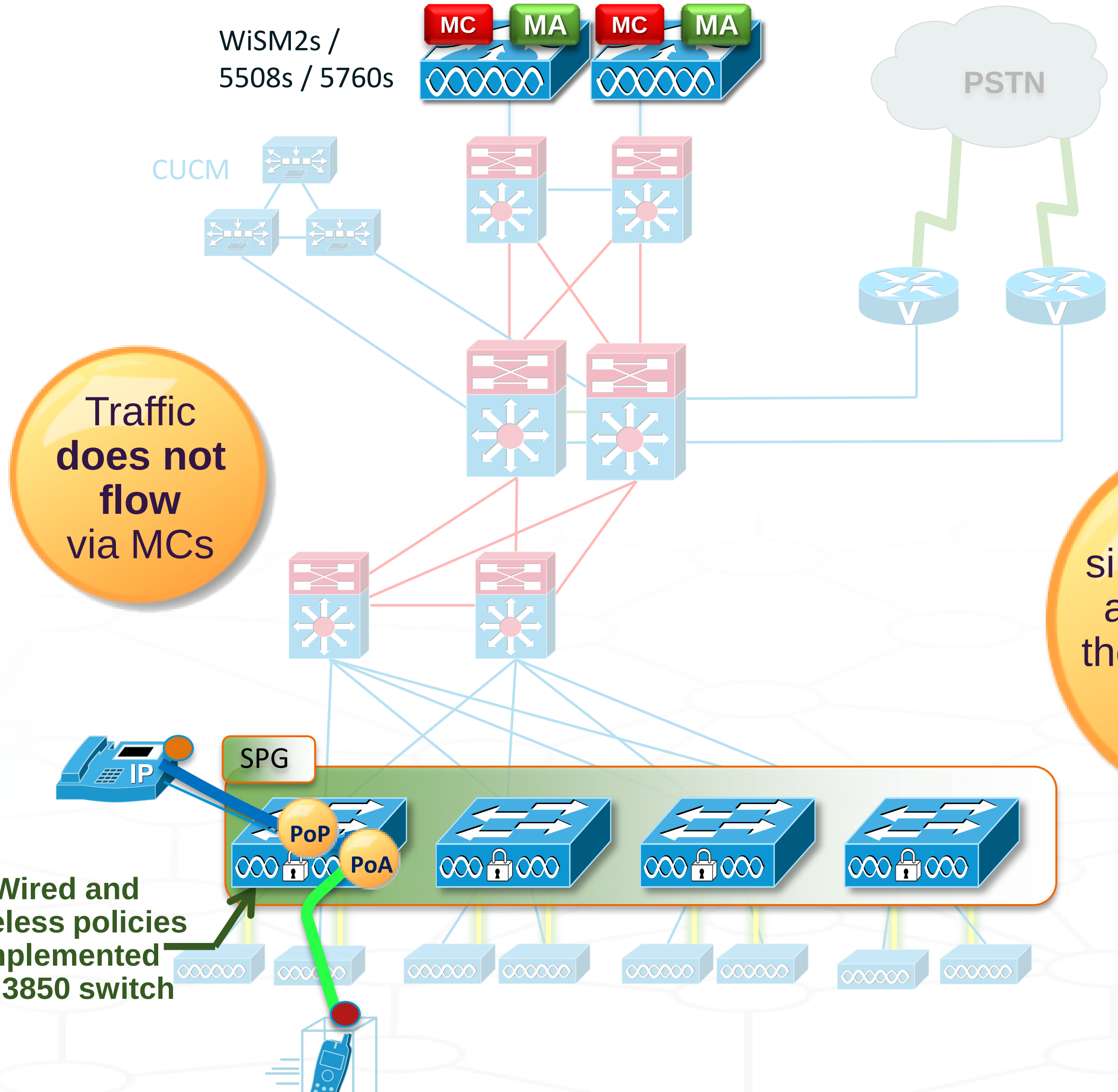
This is an important consideration for Switch Peer Group, traffic flow, and Controller scalability.

Roaming, Within an SPG (Campus) –

- Now, let's examine a few more types of user roams
- **In this example, the user roams within their Switch Peer Group –** since SPGs are typically formed around floors or other geographically-close areas, **this is the most likely and most common type of roam**

  The user may or may not have roamed across an L3 boundary (depends on wired setup) – **however, users are always* taken back to their PoP** for policy application

Converged Access – Traffic Flow



Traffic **does not flow** via MCs

Wired and wireless policies implemented on 3850 switch

More efficient since traffic flows are localised to the 3850 switch – **Performance Increase**

Converged policies and services for wired and wireless users

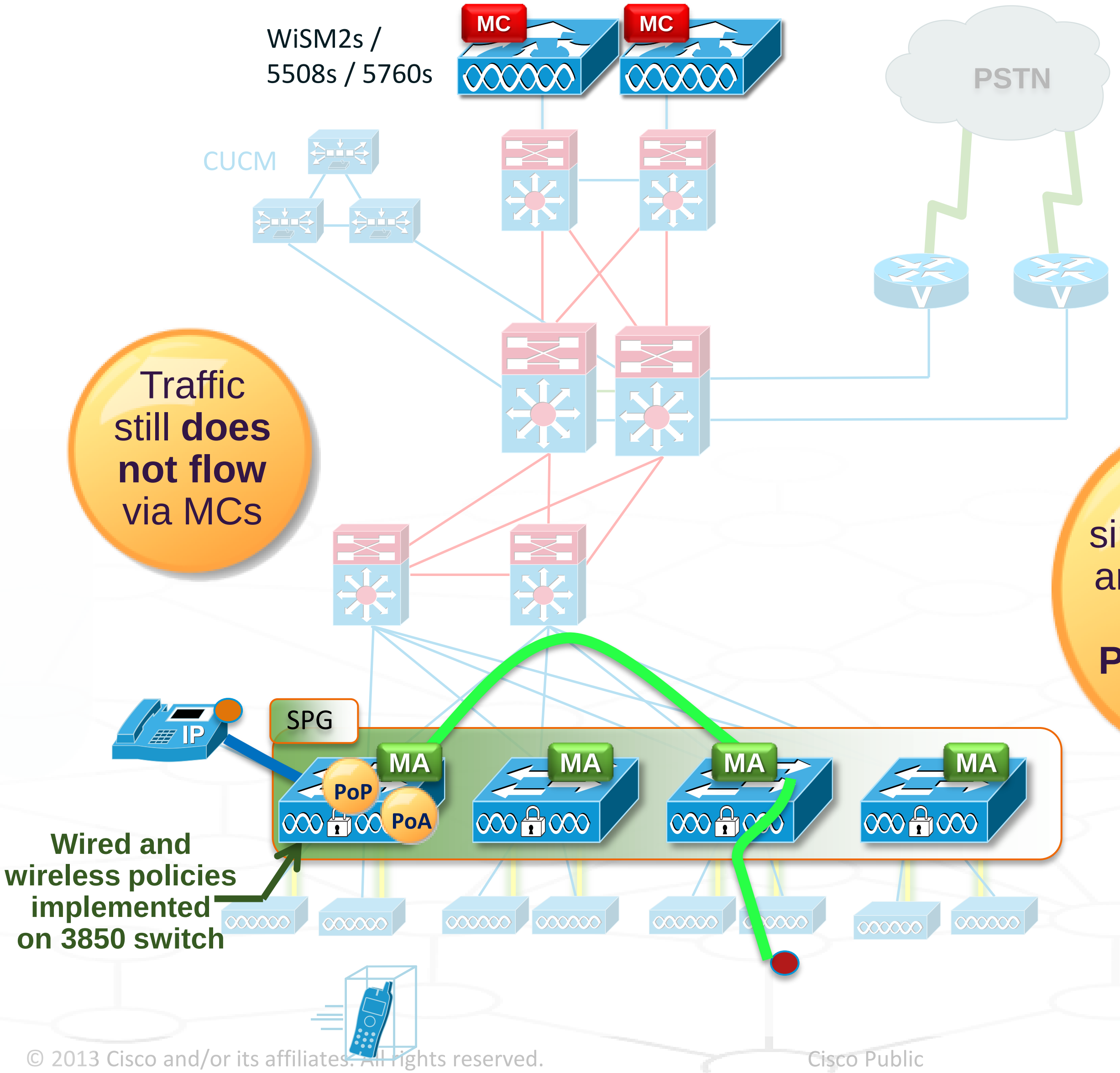
Traffic Flows, Comparison (Converged Access) –

- Now, our VoIP user is on a Cisco Converged Access network, and is again making a call from a wireless handset to a wired handset …
- **We can see that all of the user's traffic is localised to their Peer Group, below the distribution layer,** in both directions …

In this example, a total of **1 hop** is incurred for each direction of the traffic path (assuming no roaming) … two additional hops may be incurred for routing …

Converged Access –

Traffic Flow – with Intra-SPG Roam



Traffic still **does not flow** via MCs

Wired and wireless policies implemented on 3850 switch

Converged policies and services for wired and wireless users

More efficient since traffic flows are still localised to the SPG – **Performance & Scalability**

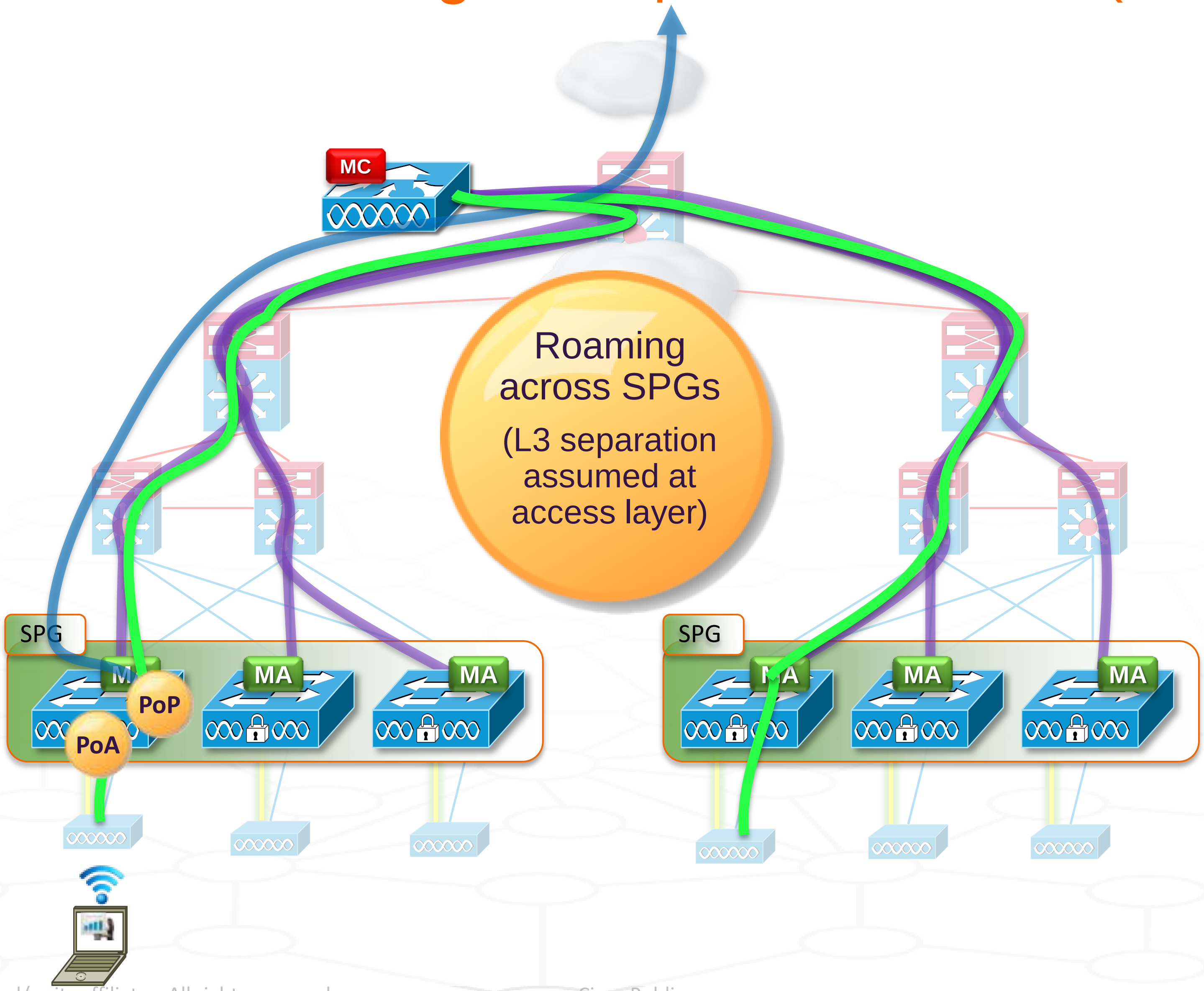
Traffic Flows, Comparison (Converged Access) –

- Now, our VoIP user on the Cisco Converged Access network roams, while a call is in progress between the wireless and wired handsets …
- **We can see that all of the user's traffic is still localised to their Switch Peer Group, below the distribution layer,** in both directions …

In this example, a total of **3 hops** is incurred for each direction of the traffic path (assuming intra-SPG roaming) … two additional hops may be incurred for routing …

Converged Access –

Traffic Flow and Roaming – Campus, L2 / L3 Roam (across Switch Peer Groups)



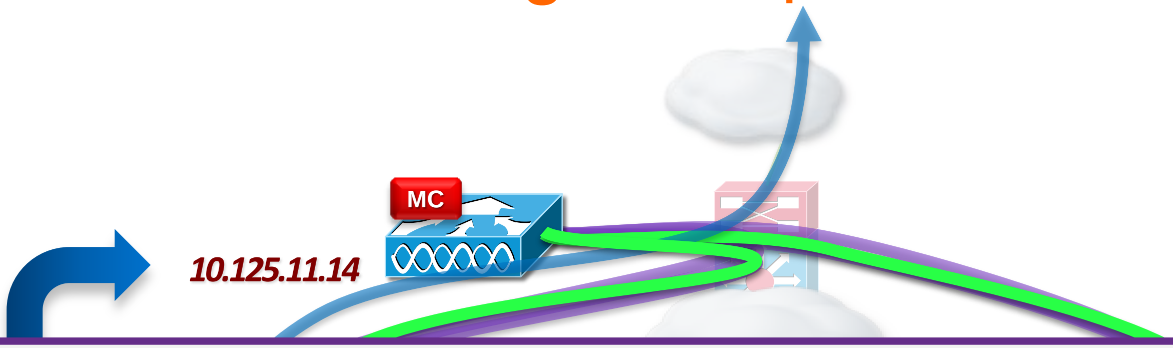
Roaming, Across SPGs (Campus) –

- Now, let's examine a few more types of user roams
- **In this example, the user roams across Switch Peer Groups –** since SPGs are typically formed around floors or other geographically-close areas, **this type of roam is possible, but less likely than roaming within an SPG**

Typically, this type of roam will take place across an L3 boundary (depends on wired setup) – **however, users are always* taken back to their PoP** for policy application

Converged Access –

Traffic Flow and Roaming – Campus, L2 / L3 Roam (across Switch Peer Groups)



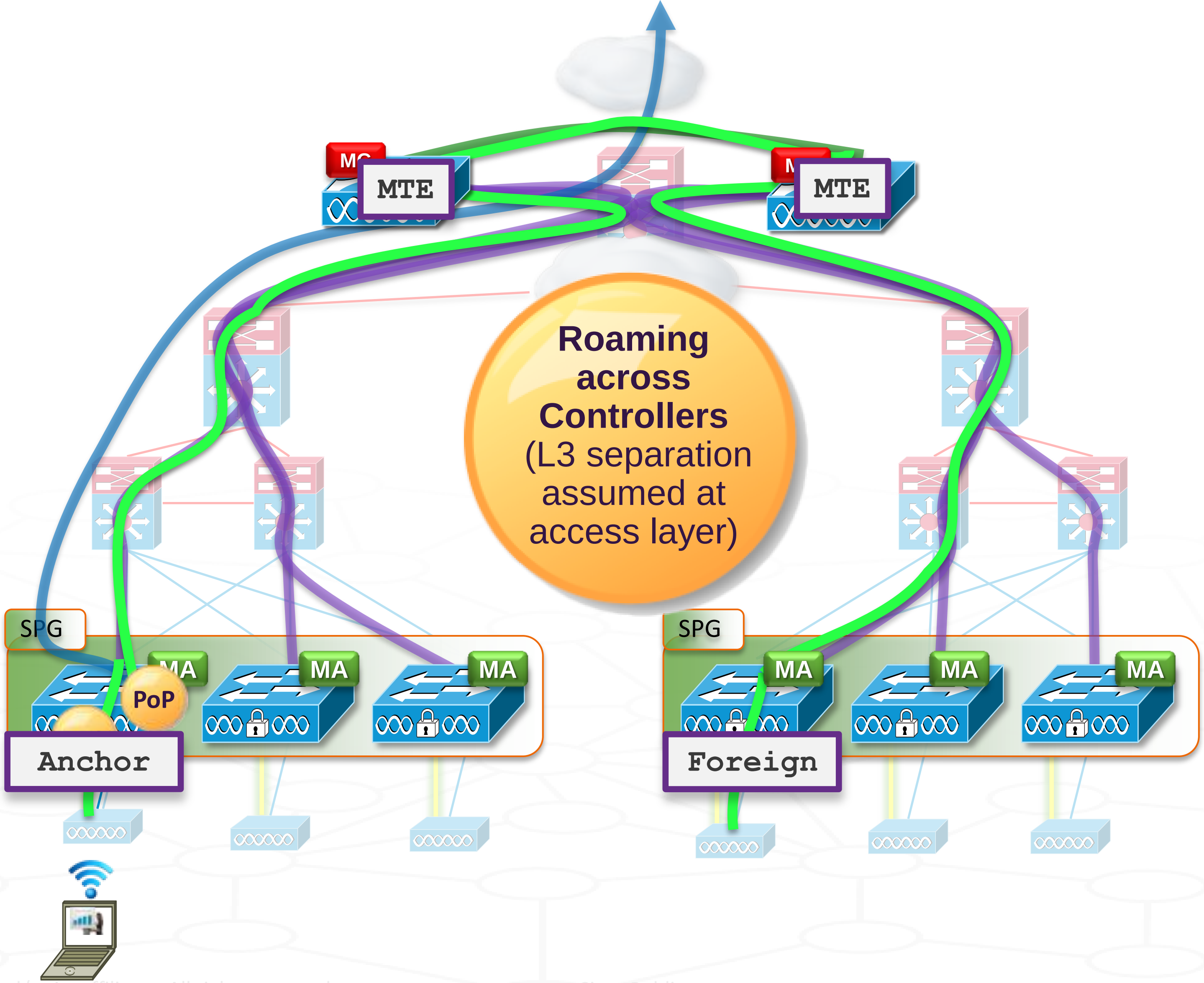
Overall view – across the entire Sub-Domain controlled by the MC

```
L09-5760-1# show wireless mobility controller client summary
Number of Clients : 5

State is the Sub-Domain state of the client.
* indicates IP of the associated Sub-domain
Associated Time in hours:minutes:seconds

MAC Address     State       Anchor IP           Associated IP    Associated Time
------------------------------------------------------------------------------
001e.65b7.7d1a  Local       10.101.1.109        10.101.6.109     00:04:36
b817.c2f0.61b2  Local       0.0.0.0             10.101.7.109     00:21:07
74e1.b65a.a8f3  Local       10.101.3.109        10.101.1.109     00:03:27
cc08.e028.6fdd  Local       0.0.0.0             10.101.1.109     00:04:57
a467.06e2.813d  Local       0.0.0.0             10.101.3.109     00:02:56
```

Roamed client, Switch 1 to Switch 6 (inter-SPG)
Stationary client, Switch 7
Roamed client, Switch 3 to Switch 1 (intra-SPG)
Stationary client, Switch 1
Stationary client, Switch 3

Converged Access –

Traffic Flow and Roaming – Campus, L2 / L3 Roam (across SPGs and MCs)


MC
MTE
MC
MTE
Roaming across Controllers (L3 separation assumed at access layer)
SPG
MA
PoP
MA
MA
Anchor
SPG
MA
MA
MA
Foreign

Roaming, Across SPGs and MCs (Campus) –

- Now, let's examine a few more types of user roams

- **In this example, the user roams across Switch Peer Groups and Controllers –** (within the same Mobility Group) … again, **this type of roam is possible, but less likely than intra-SPG roaming**

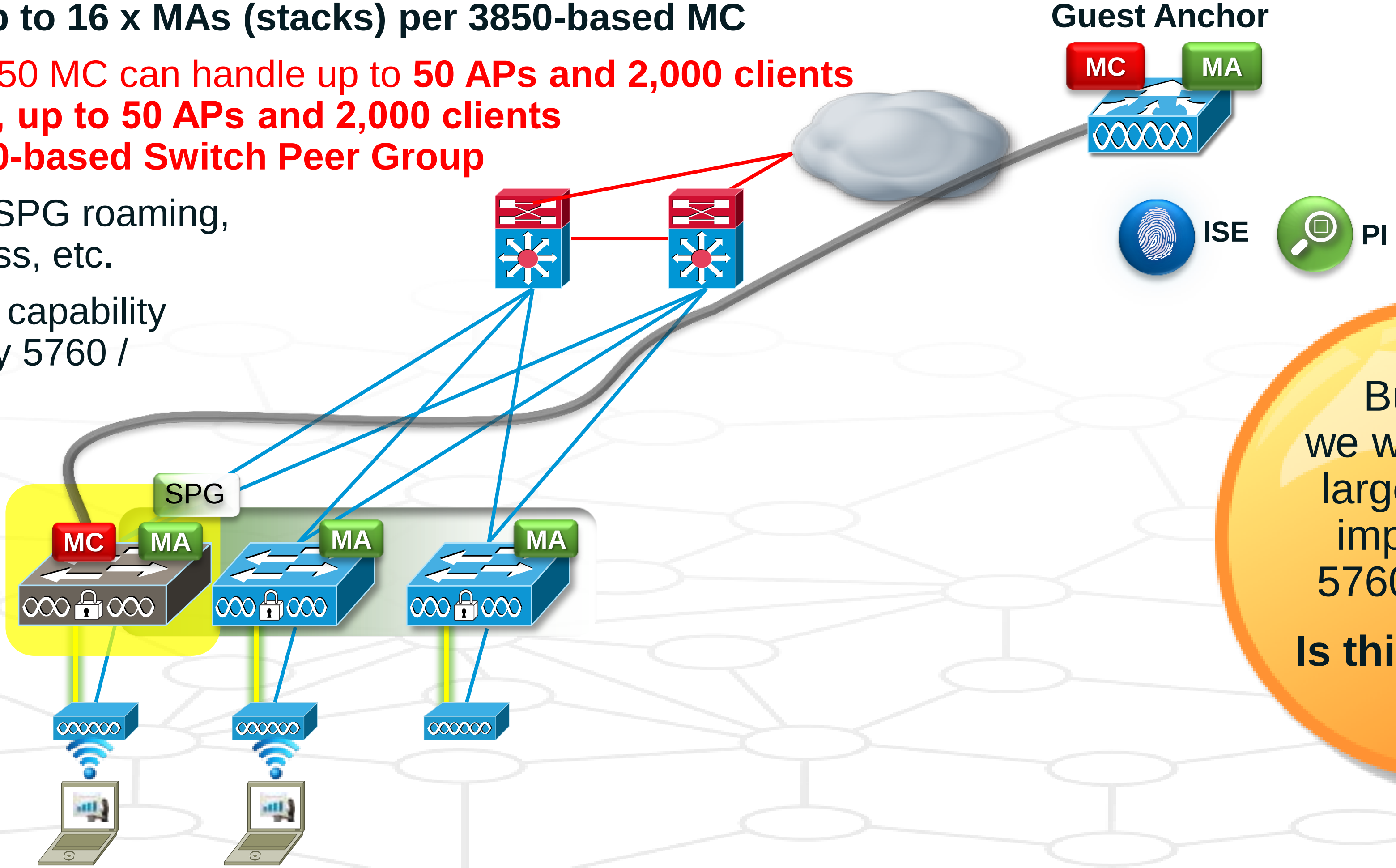
Typically, this type of roam will take place across an L3 boundary (depends on wired setup) – **however, users are always* taken back to their PoP** for policy application

Converged Access –

Catalyst 3850-based MCs – Functionality

As we saw previously, we can also optionally use a Catalyst 3850 switch as an MC + co-located MA for a Switch Peer Group **…** let's explore this in more detail –

- **Single Catalyst 3850 MC** supported per Switch Peer Group …
- which can have **up to 16 x MAs (stacks) per 3850-based MC**
- Single Catalyst 3850 MC can handle up to **50 APs and 2,000 clients total … therefore, up to 50 APs and 2,000 clients in a Catalyst 3850-based Switch Peer Group**
- MC handles inter-SPG roaming, RRM, Guest Access, etc.
- More scalable MC capability can be provided by 5760 / WiSM2



But what if we want to scale larger, **without** implementing 5760 / WiSM2?

Is this possible?

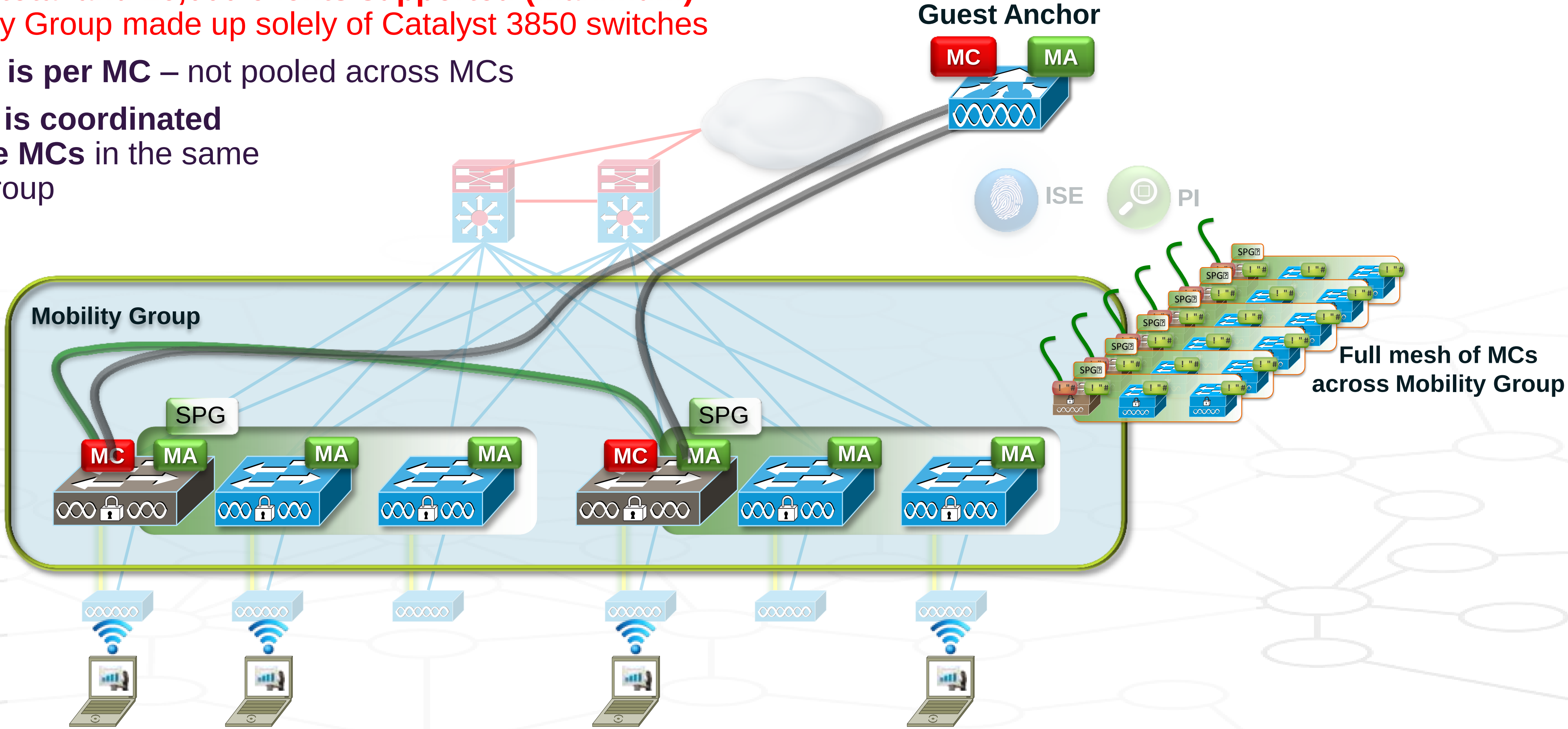
Converged Access –

Catalyst 3850-based MCs – Scaling

Switch Peer Group / Mobility Group Scaling with Catalyst 3850 –

- **Up to 8 x Catalyst 3850 MCs** can be formed into a Mobility Group
- **Up to 250 APs total and 16,000 clients supported (maximum)** across a Mobility Group made up solely of Catalyst 3850 switches
  - **Licensing is per MC** – not pooled across MCs
  - **RRM, etc. is coordinated across the MCs** in the same Mobility Group

- **Guest tunnelling is per MC** – to Guest Anchor controller

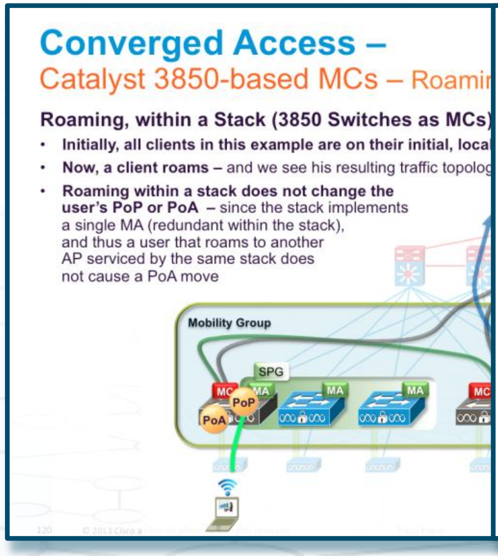


Converged Access –

Catalyst 3850-based MCs – Roaming

There are multiple roaming scenarios with Catalyst 3850-based MCs –

- **These replicate the traffic flow expectations seen elsewhere with Converged Access**
- **Traffic within an SPG flows directly between MAs – traffic between SPGs flows via MCs**
  - **Which, in this case,** are Catalyst 3850 switches operating as MCs
  - **Catalyst 3850-based MC deployments are likely to be common in branches and even possibly smaller Campuses**
  - **Larger deployments are likely to use discrete controllers**
    (5760, 5508, WiSM2s) as MCs, for **scalability and simplicity**
  - **Rather than detail every roaming case here, these are summarised below –**
    Full details are given in the Reference section at the end of this slide deck …

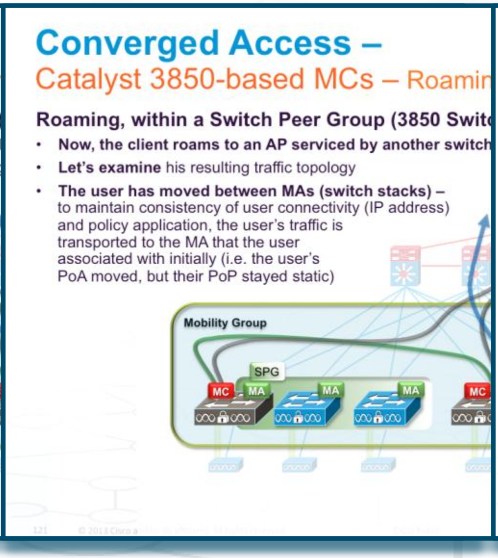


Converged Access –

Catalyst 3850-based MCs – Roamin

Roaming, within a Stack (3850 Switches as MCs)

- **Initially, all clients in this example are on their initial, local**
- **Now, a client roams –** and we see his resulting traffic topolog
- **Roaming within a stack does not change the user's PoP or PoA** – since the stack implements a single MA (redundant within the stack), and thus a user that roams to another AP serviced by the same stack does not cause a PoA move

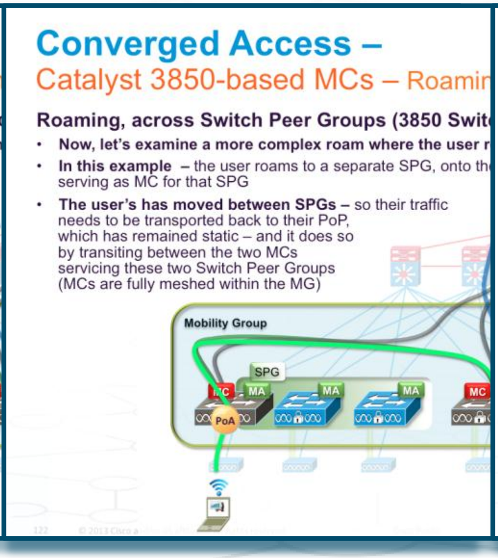


Converged Access –

Catalyst 3850-based MCs – Roamin

Roaming, within a Switch Peer Group (3850 Swit

- **Now, the client roams to an AP serviced by another switch**
- **Let's examine** his resulting traffic topology
- **The user has moved between MAs (switch stacks) –** to maintain consistency of user connectivity (IP address) and policy application, the user's traffic is transported to the MA that the user associated with initially (i.e. the user's PoA moved, but their PoP stayed static)

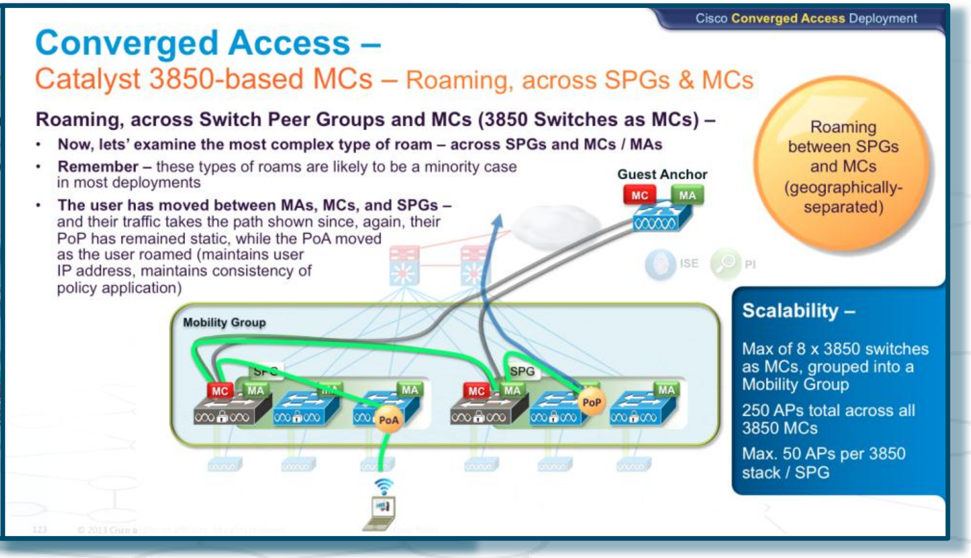


Converged Access –

Catalyst 3850-based MCs – Roamin

Roaming, across Switch Peer Groups (3850 Swit

- **Now, let's examine a more complex roam where the user r**
- **In this example** – the user roams to a separate SPG, onto th serving as MC for that SPG
- **The user's has moved between SPGs –** so their traffic needs to be transported back to their PoP, which has remained static – and it does so by transiting between the two MCs servicing these two Switch Peer Groups (MCs are fully meshed within the MG)



Cisco Converged Access Deployment

Converged Access –

Catalyst 3850-based MCs – Roaming, across SPGs & MCs

Roaming, across Switch Peer Groups and MCs (3850 Switches as MCs) –

- **Now, lets' examine the most complex type of roam – across SPGs and MCs / MAs**
- **Remember –** these types of roams are likely to be a minority case in most deployments
- **The user has moved between MAs, MCs, and SPGs –** and their traffic takes the path shown since, again, their PoP has remained static, while the PoA moved as the user roamed (maintains user IP address, maintains consistency of policy application)

Roaming between SPGs and MCs (geographically-separated)

Scalability –

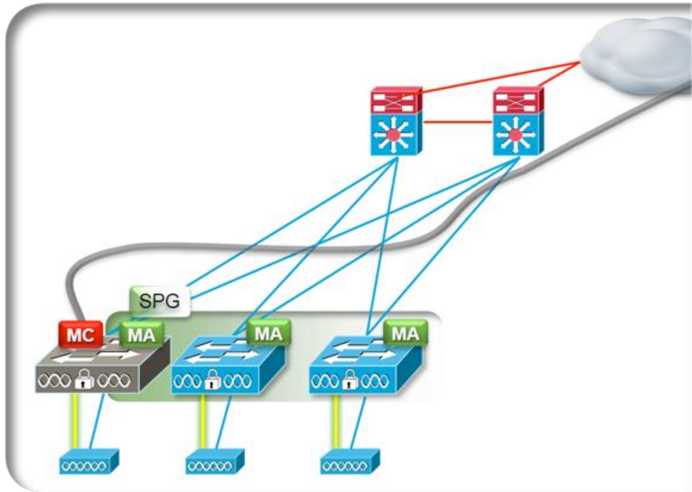
Max of 8 x 3850 switches as MCs, grouped into a Mobility Group

250 APs total across all 3850 MCs

Max. 50 APs per 3850 stack / SPG

Converged Access –

Catalyst 3850-based MCs – When to Use



Considerations –

- **Many larger designs (such as most Campuses) will likely utilise a discrete controller, or group of controllers, as MCs.** Combined with Catalyst 3850 switches as MAs, this likely provides the most scalable design option for a larger network build.
- **However, if using 3850 switches as MCs for smaller builds – and with the scaling limits detailed on the previous slide in mind – we need to determine where to best use this capability.**

- **Pros –**
  - **CapEx cost savings** – via the elimination of a discrete-controller-as-MC in some designs (typically, smaller use cases and deployments) … cost also needs to take into consideration licensing on the Catalyst 3850 switches.
- **Cons –**
  - **OpEx complexity** – due to some additional complexity that comes into roaming situations when using multiple 3850 switch-based MCs (as detailed in the preceding slide). While not insurmountable, this does need to be factored in as part of the decision process.

Roaming details provided on Reference slides

Conclusion –

In smaller designs (such as branches), the use of Catalyst 3850 switches as MCs is likely workable. In mid-sised designs, this may also be workable, but does lead to some additional roaming considerations (as detailed on the following slides). In large campus deployments, the use of controllers as MCs is more likely, due to economies of scale.

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

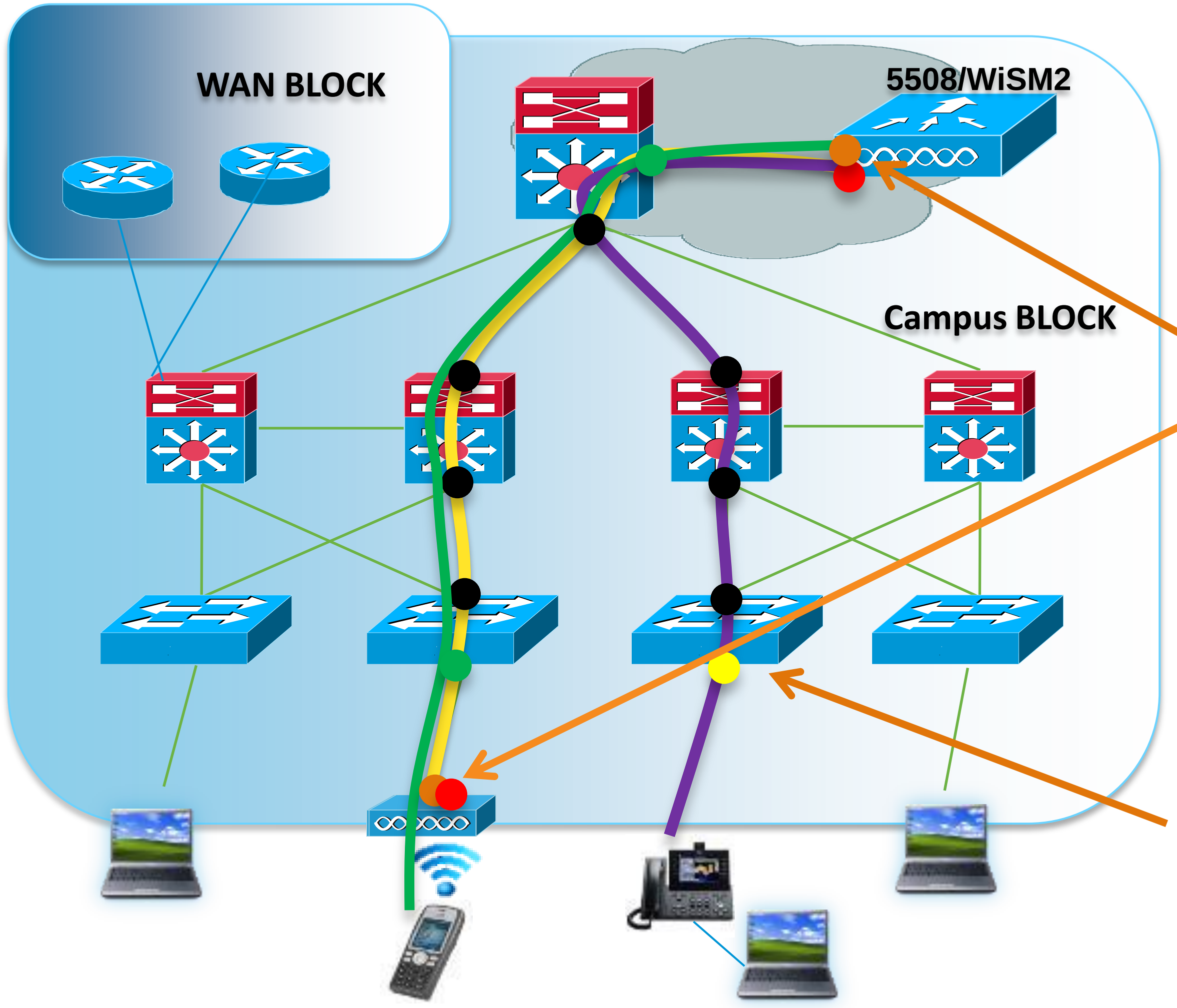
- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- **Converged Access Deployment – Quality of Service**
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Existing QoS Deployments–

How We Overlay QoS Policies Today

Current QoS Architecture



Distributed Management Configuration and Deployment

Separate policies and services for wired and wireless users

Wireless policies implemented on controller pushed to AP

Wired policies implemented on switch

● Marking ● Policing

● Queuing

QoS – What's New with Converged Access

Wired (Cat 3850)

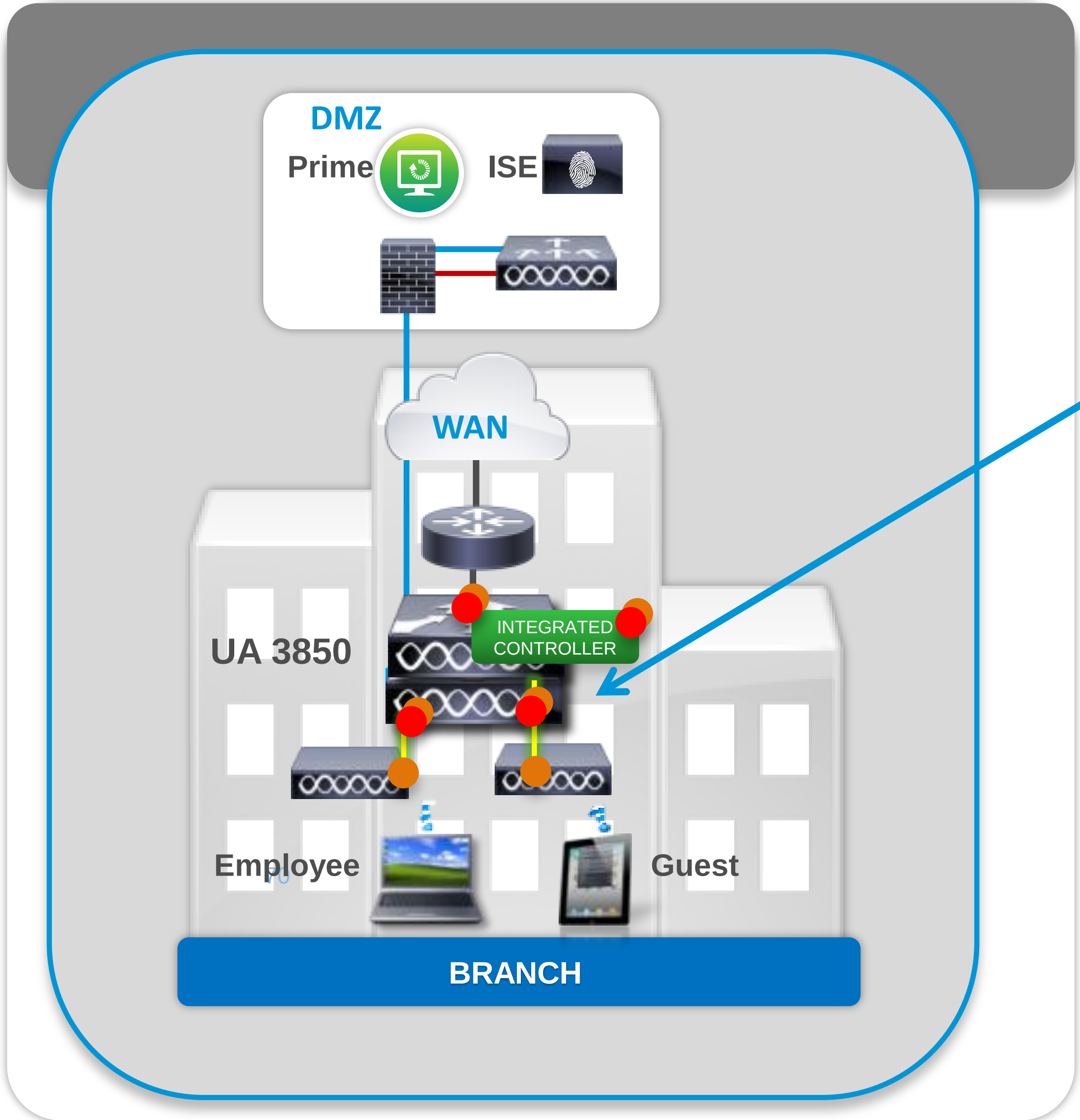
- Modular QoS based CLI (MQC)
  - Alignment with 4500E series (Sup6, Sup7)
  - Class-based Queueing, Policing, Shaping, Marking
- More Queues
  - Up to 2P6Q3T queuing capabilities
  - Standard 3750 provides 1P3Q3T
  - Not limited to 2 queue-sets
  - Flexible MQC Provisioning abstracts queuing hardware

Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge
  - Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network
- Enhanced Bandwidth Management
  - Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic
- Wireless Specific Interface Control
  - Policing capabilities Per-SSID, Per-Client upstream*** and downstream
  - AAA support for dynamic Client based QoS and Security policies
- Per SSID Bandwidth Management

*** **NOT** available on CT 5760 at FCS

QoS – What's New with Converged Access



● Marking ● Policing

Wireless(Cat 3850 & CT 5760)

- **Granular QoS control at the wireless edge**

  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- Enhanced Bandwidth Management

  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- Wireless Specific Interface Control

  Policing capabilities Per-SSID, Per-Client upstream*** and downstream

  AAA support for dynamic Client based QoS and Security policies

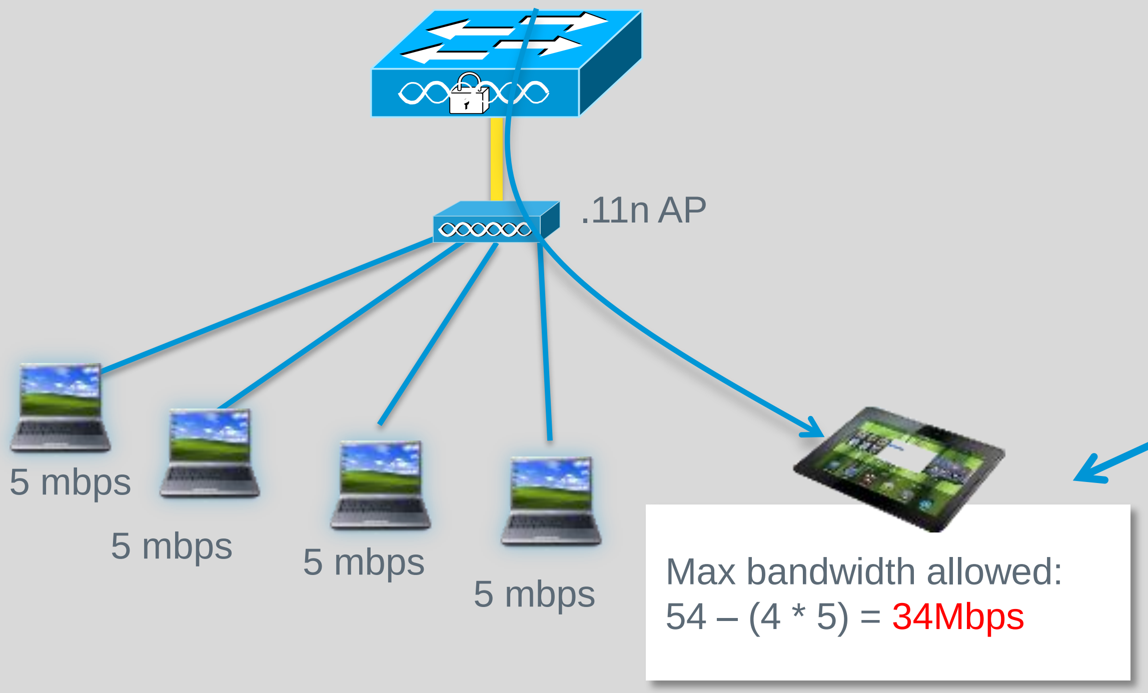
- Per SSID Bandwidth Management

*** **NOT** available on CT 5760 at FCS

QoS – What's New with Converged Access

With the CT 5760 or CAT 3850

Usage based fair allocation without configuration



Max bandwidth allowed:
54 – (4 * 5) = 34Mbps

Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge

  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- **Enhanced Bandwidth Management**

  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- Wireless Specific Interface Control

  Policing capabilities Per-SSID, Per-Client upstream*** and downstream

  AAA support for dynamic Client based QoS and Security policies

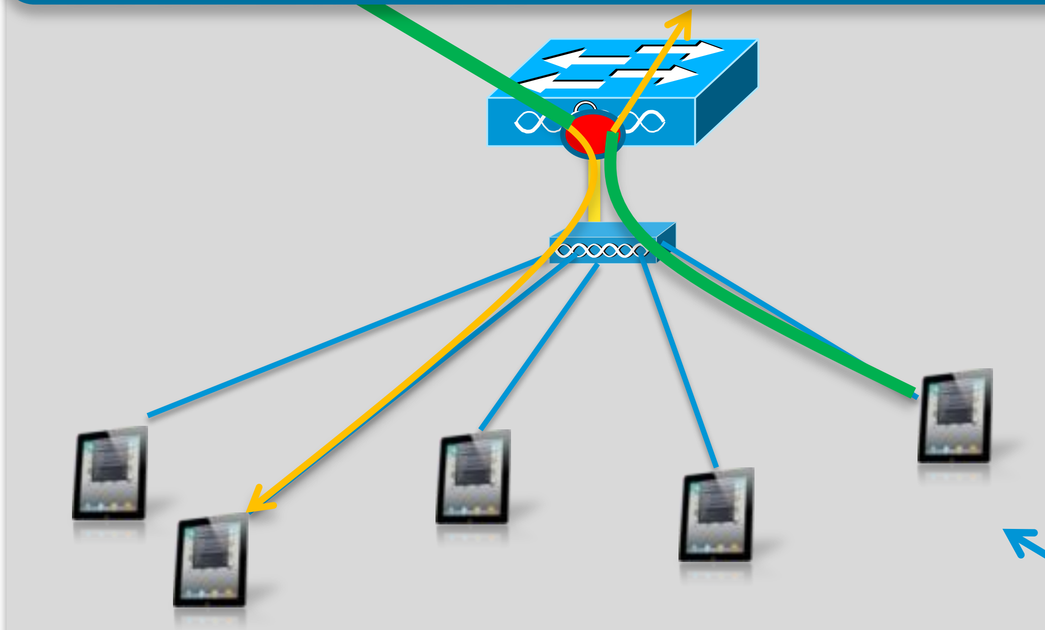
- Per SSID Bandwidth Management

*** **NOT** available on CT 5760 at FCS

QoS – What's New with Converged Access

With the 3850

Bidirectional policing at the edge per- user , per-SSID and in Hardware



- SSID: BYOD
- QoS policy on 3850 used to police each client bidirectionally
- Policy can be sent via AAA to provide specific per-client policy
- Allocate Bandwidth or police/shape SSID as a whole

Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge

  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- Enhanced Bandwidth Management

  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- Wireless Specific Interface Control

  Policing capabilities Per-SSID, Per-Client upstream*** and downstream

  AAA support for dynamic Client based QoS and Security policies

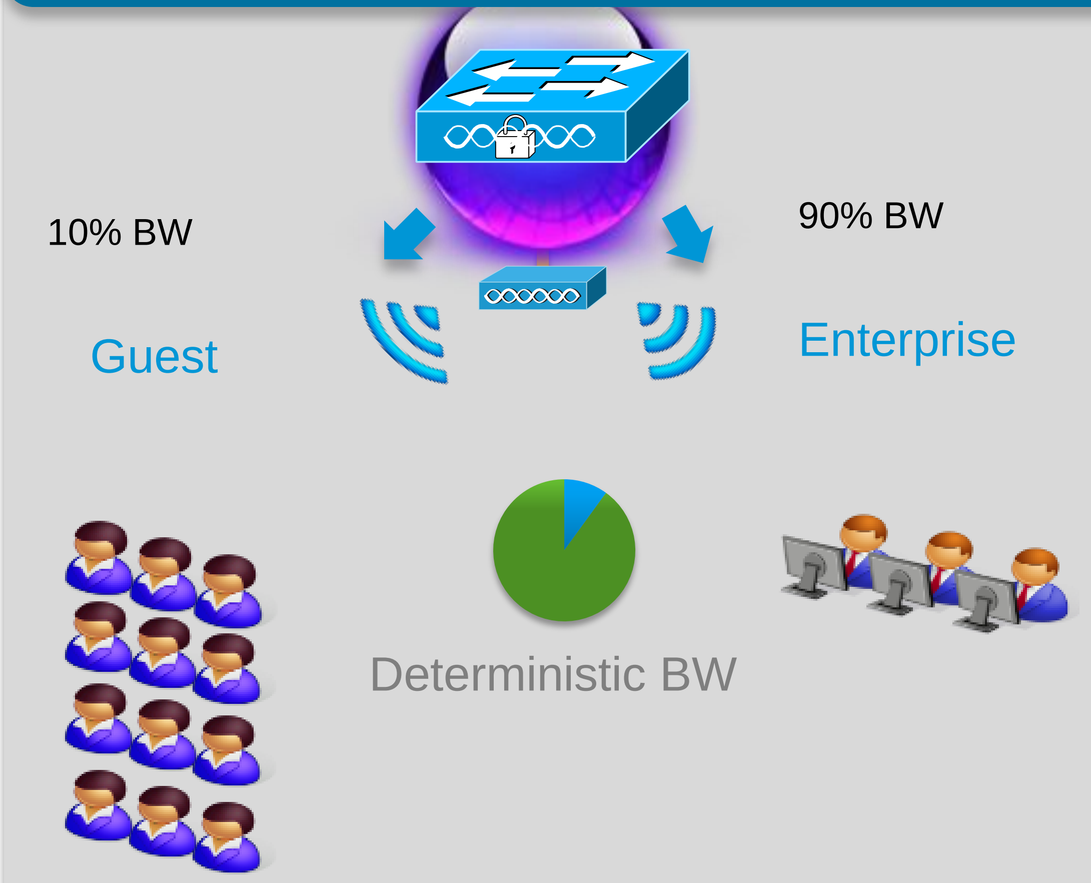
- Per SSID Bandwidth Management

*** **NOT** available on CT 5760 at FCS

QoS – What's New with Converged Access

With the CT 5760 or CAT 3850

Deterministic bandwidth is allocated per SSID



Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge

  Tunnel termination allows customers to provide QoS treatment per SSIDs, per-Clients and common treatment of wired and wireless traffic throughout the network

- Enhanced Bandwidth Management

  Approximate Fair Drop (AFD) Bandwidth Management ensures fairness at Client, SSID and Radio levels for NRT traffic

- Wireless Specific Interface Control

  Policing capabilities Per-SSID, Per-Client upstream*** and downstream

  AAA support for dynamic Client based QoS and Security policies

- **Per SSID Bandwidth Management**

*** **NOT** available on CT 5760 at FCS

QoS – What's New with Converged Access

Wired (Cat 3850)

- **Modular QoS based CLI (MQC)**

  Alignment with 4500E series (Sup6, Sup7)

  Class-based Queueing, Policing, Shaping, Marking

- More Queues

  Up to 2P6Q3T queuing capabilities

  Standard 3750 provides 1P3Q3T

  Not limited to 2 queue-sets

  Flexible MQC Provisioning abstracts queuing hardware

```
Policy-map PER-PORT-POLICING
 Class VOIP
   set dscp ef
    police 128000 conform-action transmit exceed-action drop
 Class VIDEO
   set dscp CS4
    police 384000 conform-action transmit exceed-action drop
 Class SIGNALING
   set dscp cs3
    police 32000 conform-action transmit exceed-action drop
 Class TRANSACTIONAL-DATA
   set dscp af21
 Class class-default
   set dscp default
```

Wireless(Cat 3850 & CT 5760)

- Granular QoS control at the wireless edge

  rs to per-

- jement

  ures levels

- ontrol

  r-Client upstream and downstream

  AAA support for dynamic Client based QoS and Security policies

- Per SSID bandwidth allocation

*** **NOT** available on CT 5760 at FCS

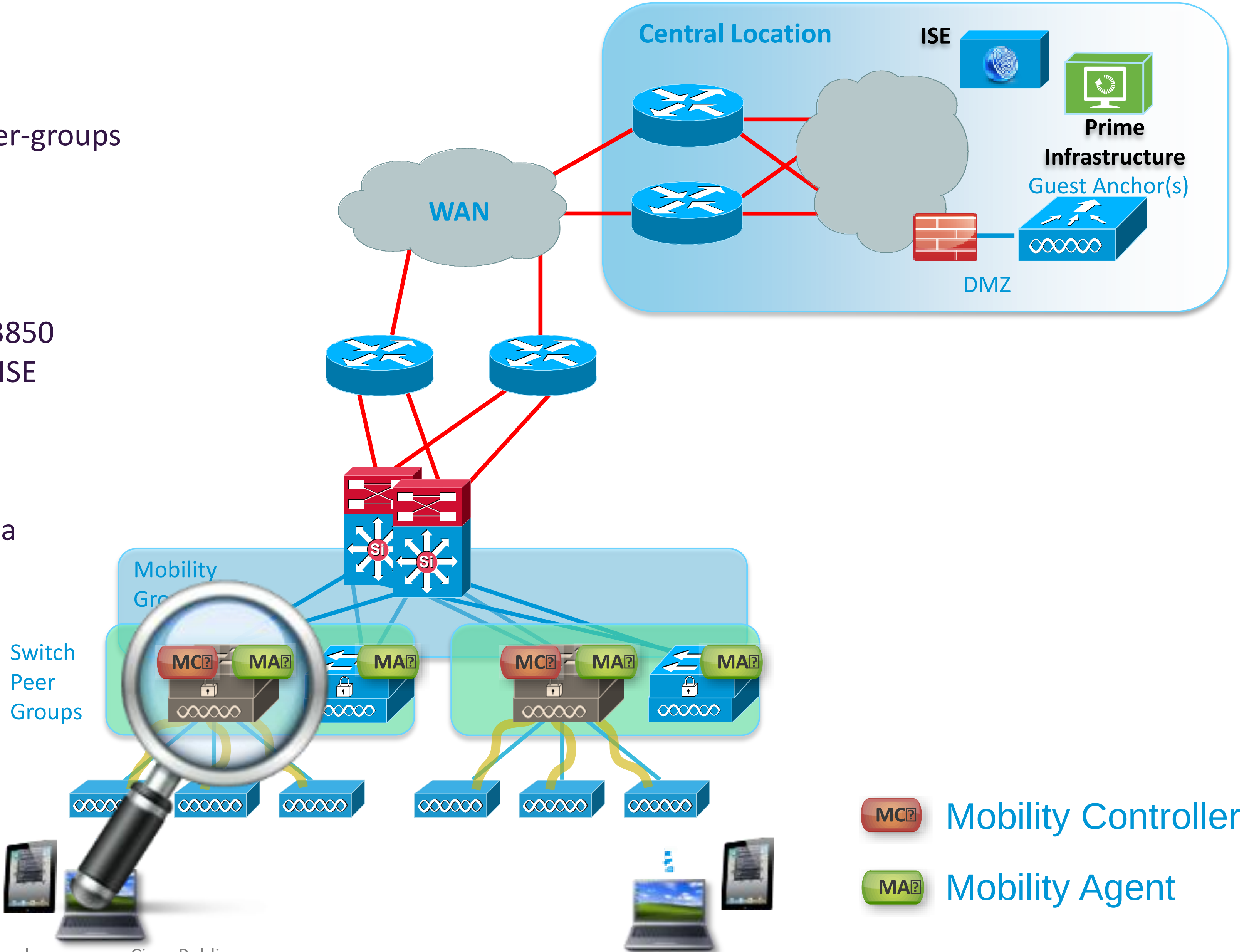
Converged Access, Deployment –

Goals:

- Simplify transition to MQC
- Use ISE to incrementally add new users/user-groups
- Limit management of QoS policies

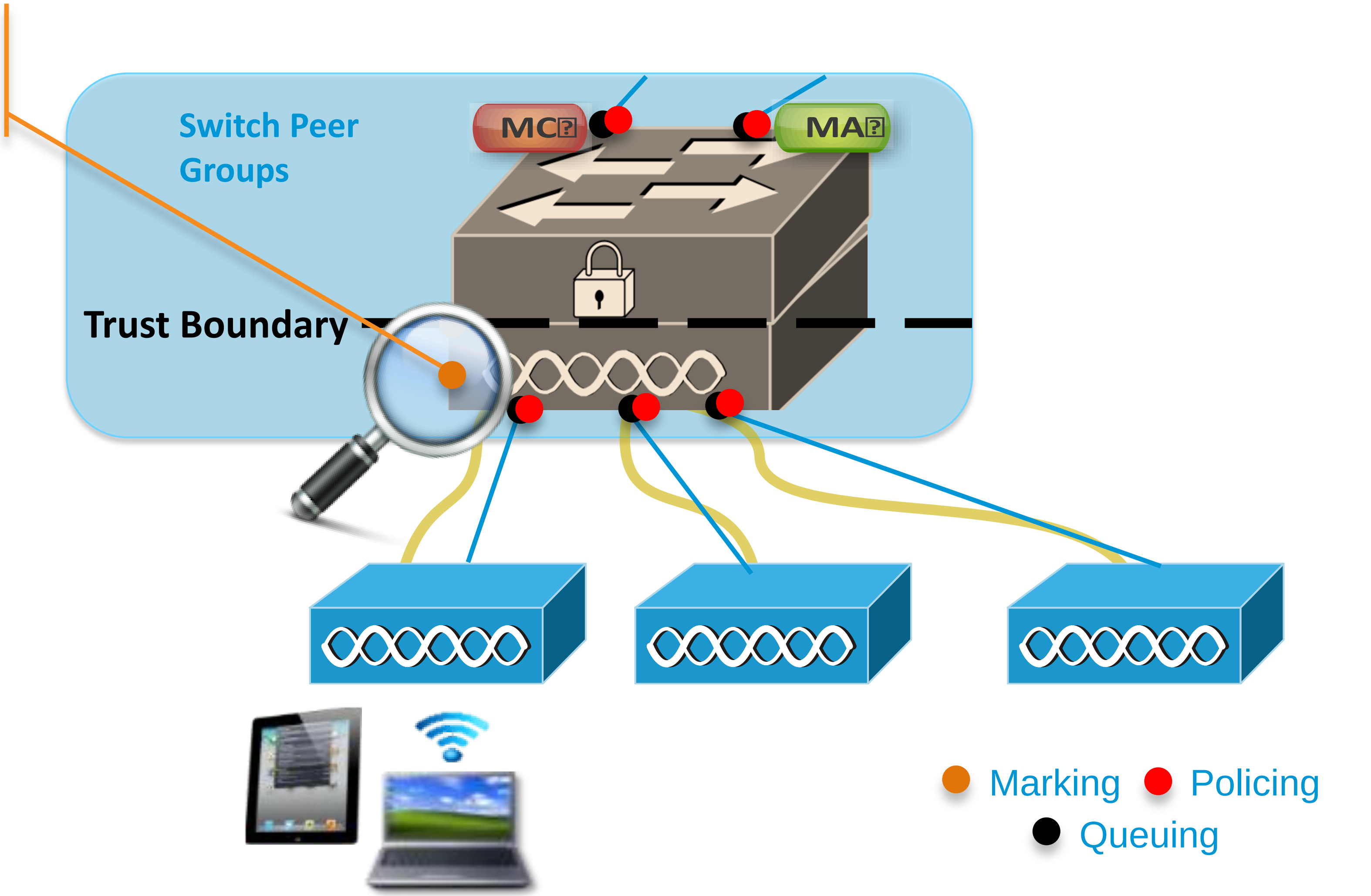
Details of Deployment:

- Provision a default policy for all clients on 3850
- Manage new users based on exception via ISE
- ISE provisioned policy overrides default
- Deploy 2 SSIDs – FACULTY, STUDENT
- Faculty and Students are authenticated
- Both groups provided Voice, Video and Data guarantees
- Each group is given a bandwidth guarantee



Converged Access, Deployment – Classification and Marking

```
Policy-map client-default
  class class-default
    set dscp 0
```



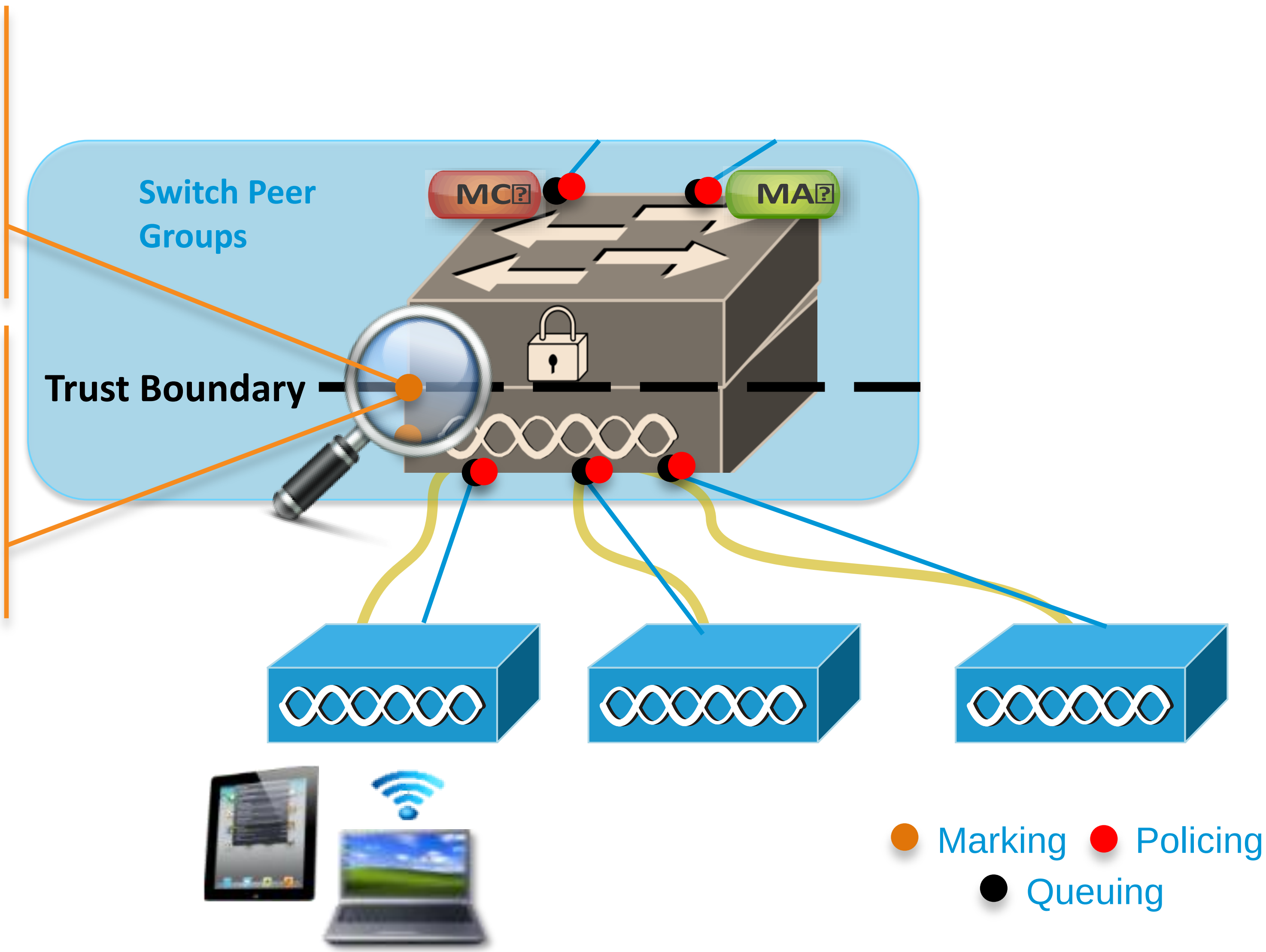
Interface Configuration:

```
wlan FACULTY 3 FACULTY
 aaa-override
 client vlan 67
 …
service-policy client in client-default
service-policy client out client-default

wlan STUDENT 4 STUDENT
 aaa-override
 client vlan 68
 …
service-policy client in client-default
service-policy client out client-default
```

Converged Access, Deployment –
Bandwidth Unfairness

```
table-map dscp2dscp
default copy

Policy-map TRUST-BW-FACULTY
Class class-default
  set dscp dscp table dscp2dscp
  set wlan user-priority dscp table dscp2up
   bandwidth remaining ratio 90
```

```
table-map dscp2dscp
default copy

Policy-map TRUST-BW-STUDENTS
Class class-default
  set dscp dscp table dscp2dscp
  set wlan user-priority dscp table dscp2up
   bandwidth remaining ratio 10
```



Interface Configuration:

```
wlan FACULTY 3 FACULTY
 aaa-override
 client vlan 67
 …
service-policy out TRUST-BW-FACULTY
```

Converged Access, Deployment – Classification and Marking

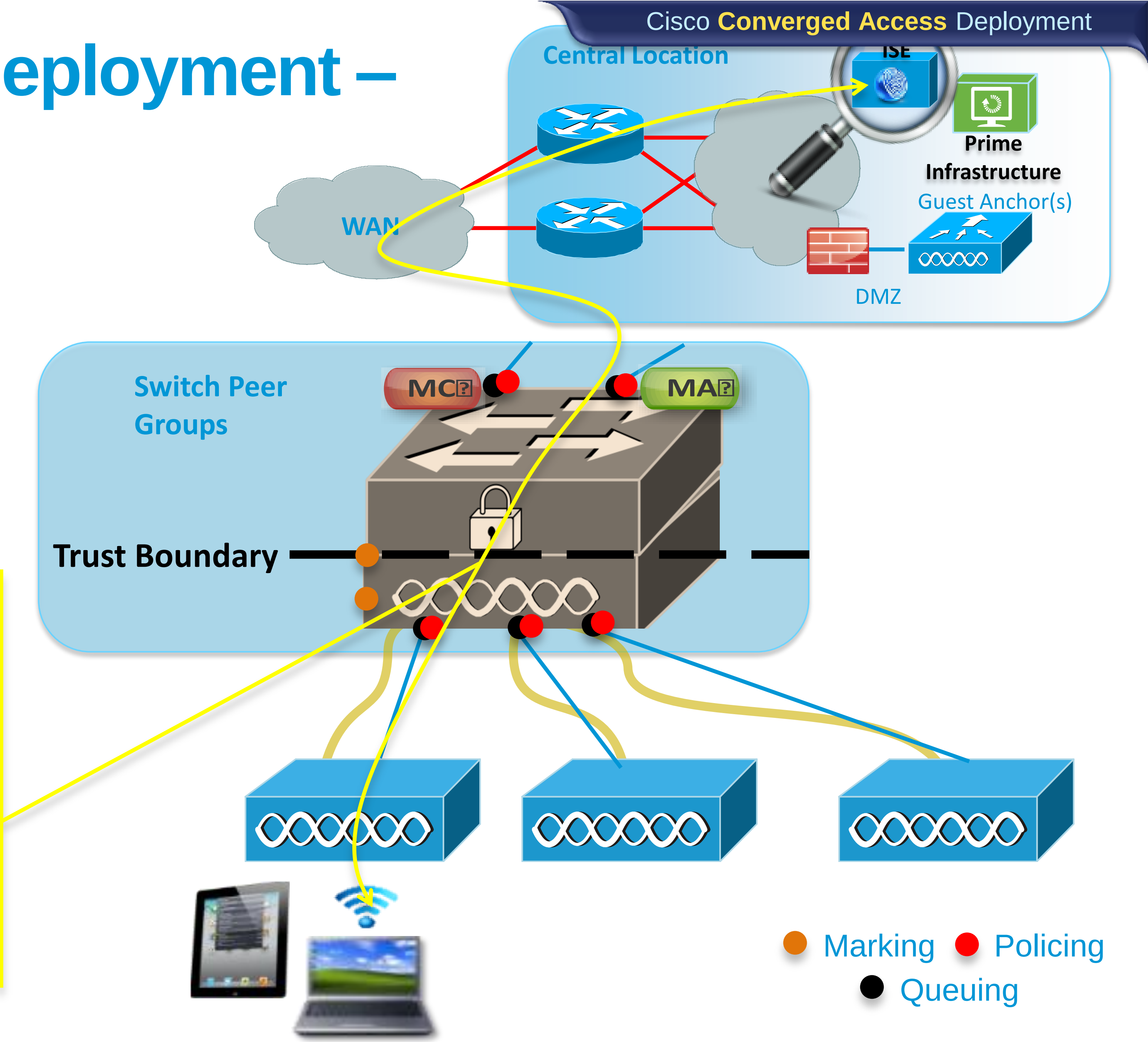
Cisco Identity Services Engine (ISE)

- Group configured for FACULTY
- Group configured for FACULTY via ISE or AD
- QoS policy name provided per Group
- QoS policy name pushed to 3850 from ISE

Per user MQC policy

- QoS Policy pre-configured on 3850
- After client authentication, policy applied to client on ingress

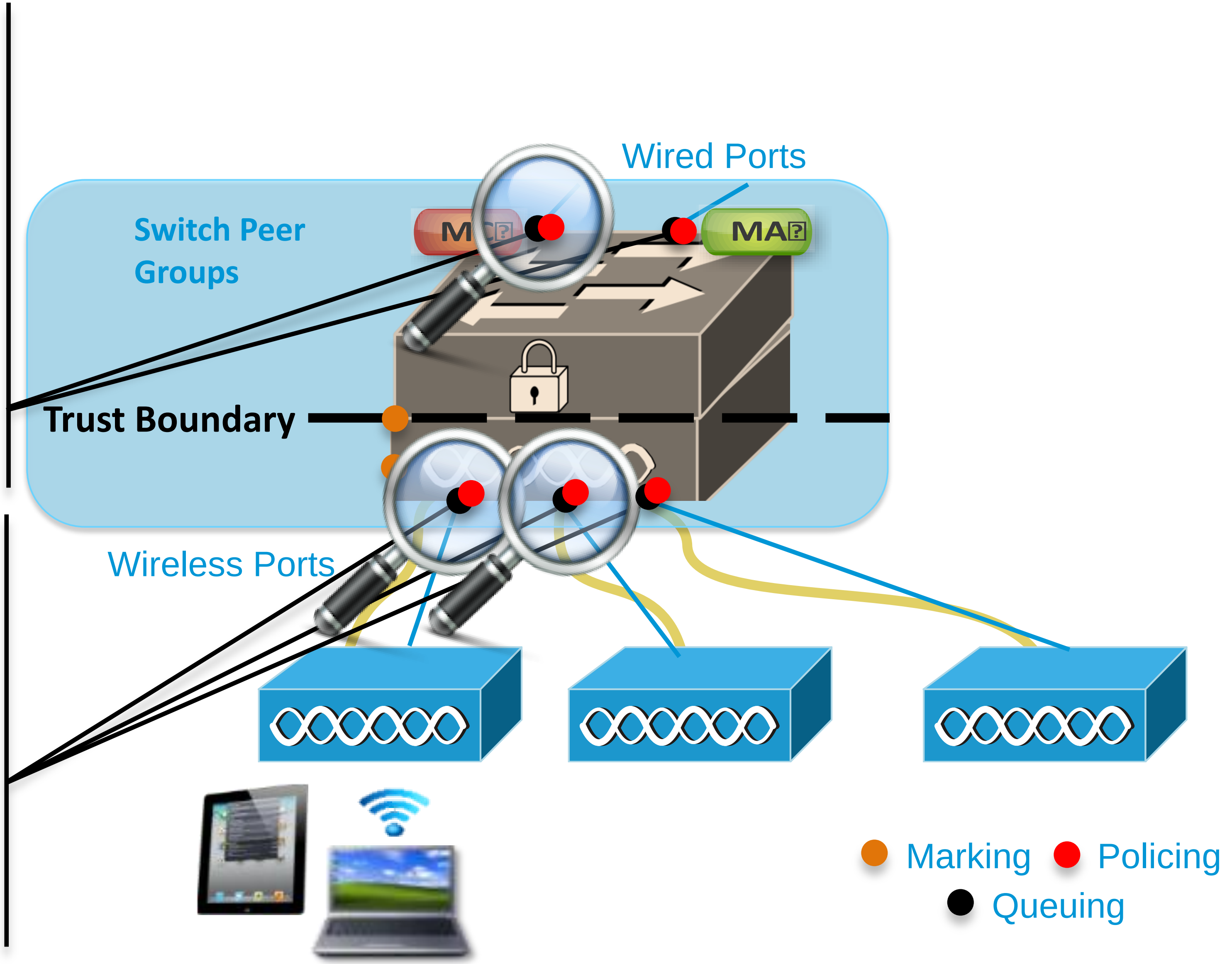
```
policy-map FACULTY
 class VOIP
   set dscp ef
   police 128000 conf transmit exceed drop
 class VIDEO
   set dscp AF41
   police 384000 conf transmit exceed drop
 class SIGNALING
   set dscp cs3
   police 32000 conf transmit exceed drop
 class TRANSACTIONAL-DATA
   set dscp af21
 class class-default
   set dscp default
```



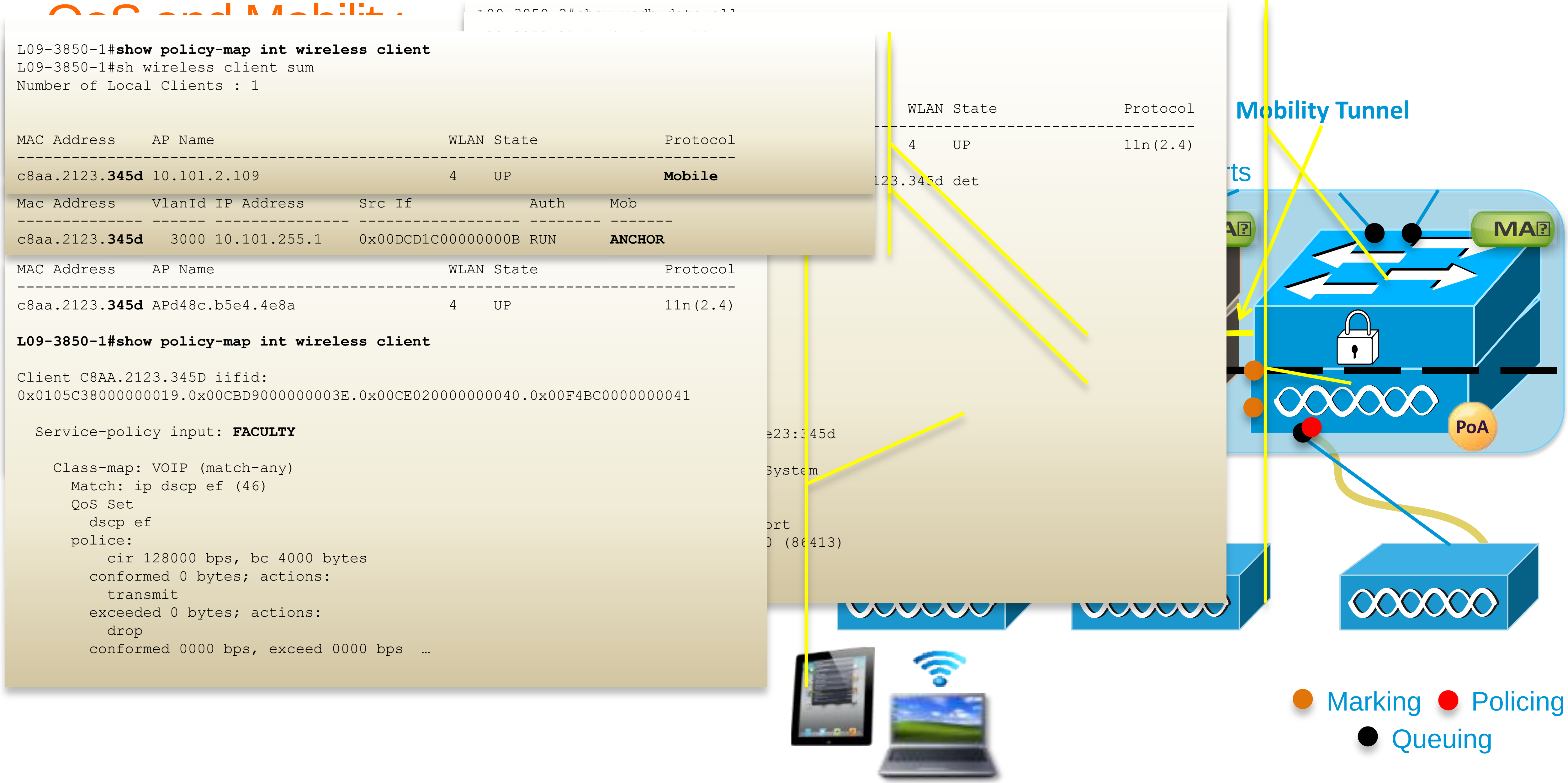
Converged Access, Deployment – Queuing

```
policy-map 2P6Q3T
 class PRIORITY-QUEUE-1
   priority level 1
    police rate per 10 conf tran exceed drop
 class PRIORITY-QUEUE-2
   priority level 2
    police rate per 20 conf tran exceed drop
 class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 20
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 20
 class SCAVENGER
    bandwidth remaining percent 5
 class class-default
    bandwidth remaining percent 25
```

```
policy-map port_child_policy
 class RT1
   priority level 1
    police 500000 conf tran exceed drop
 class RT2
   priority level 2
    police 500000 conf tran exceed drop
 class non-client-nrt-class
    bandwidth remaining ratio 7
 class class-default
    bandwidth remaining ratio 63
```



Converged Access, Deployment – QoS and Mobility



```
L09-3850-1#show policy-map int wireless client
L09-3850-1#sh wireless client sum
Number of Local Clients : 1


MAC Address    AP Name                          WLAN State              Protocol
--------------------------------------------------------------------------------
c8aa.2123.345d 10.101.2.109                     4    UP                 Mobile
```

```
Mac Address    VlanId IP Address      Src If              Auth     Mob
-------------- ------ --------------- ------------------- -------- -------
c8aa.2123.345d   3000 10.101.255.1    0x00DCD1C00000000B  RUN      ANCHOR
```

```
MAC Address    AP Name                          WLAN State              Protocol
--------------------------------------------------------------------------------
c8aa.2123.345d APd48c.b5e4.4e8a                 4    UP                 11n(2.4)

L09-3850-1#show policy-map int wireless client

Client C8AA.2123.345D iifid:
0x0105C38000000019.0x00CBD9000000003E.0x00CE020000000040.0x00F4BC0000000041

  Service-policy input: FACULTY

    Class-map: VOIP (match-any)
      Match: ip dscp ef (46)
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 4000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps  …
```

```
L09-3850-2#show wcdb data all

WLAN State              Protocol
---------------------------------
4    UP                 11n(2.4)

123.345d det

e23:345d

System

ort
0 (86413)
```

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

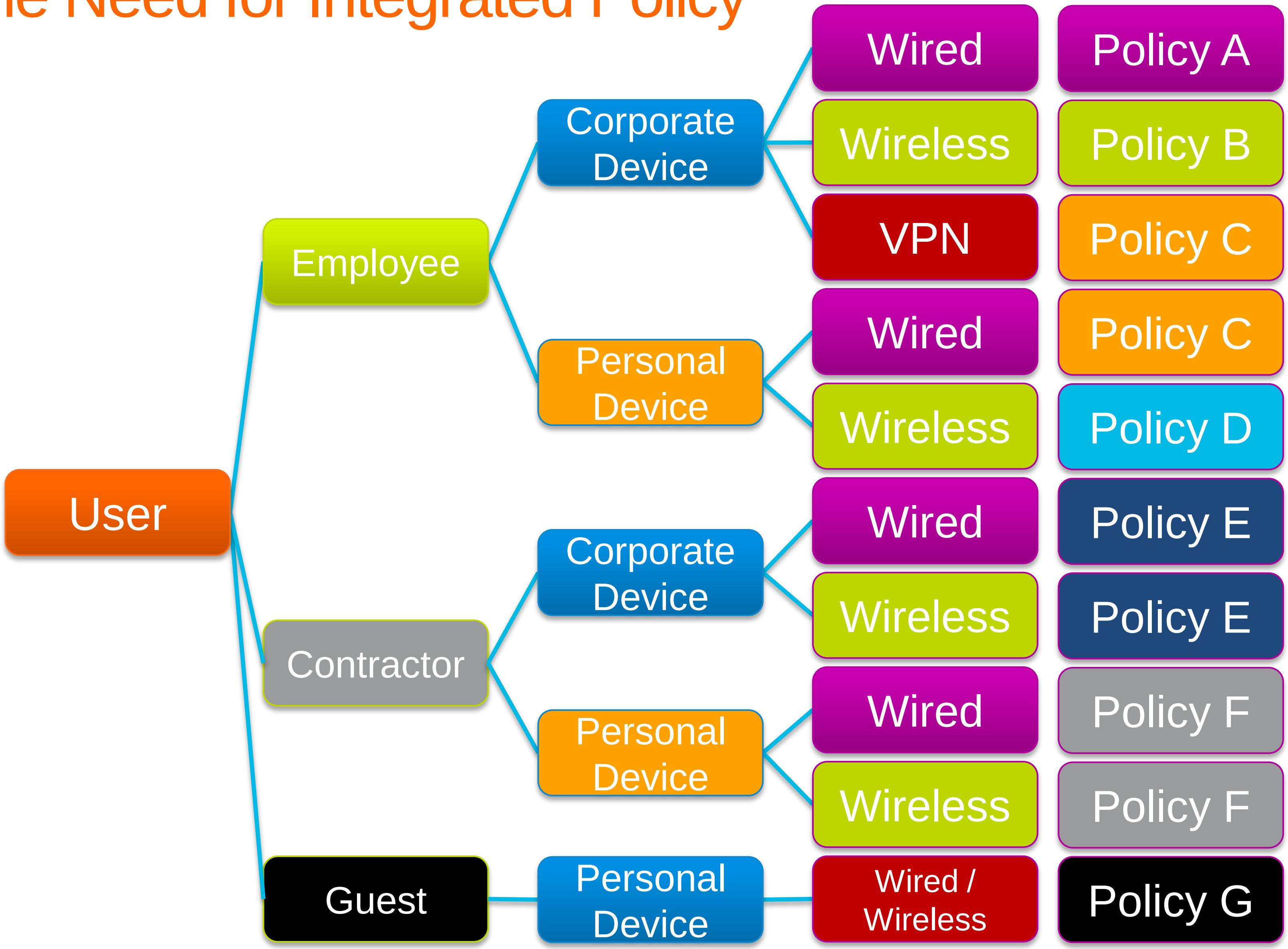
The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- **Converged Access Deployment – Security**
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Converged Access –

The Need for Integrated Policy



How to **define and apply** security policy **consistently** across every device on the network?

Policy Definition – Where?

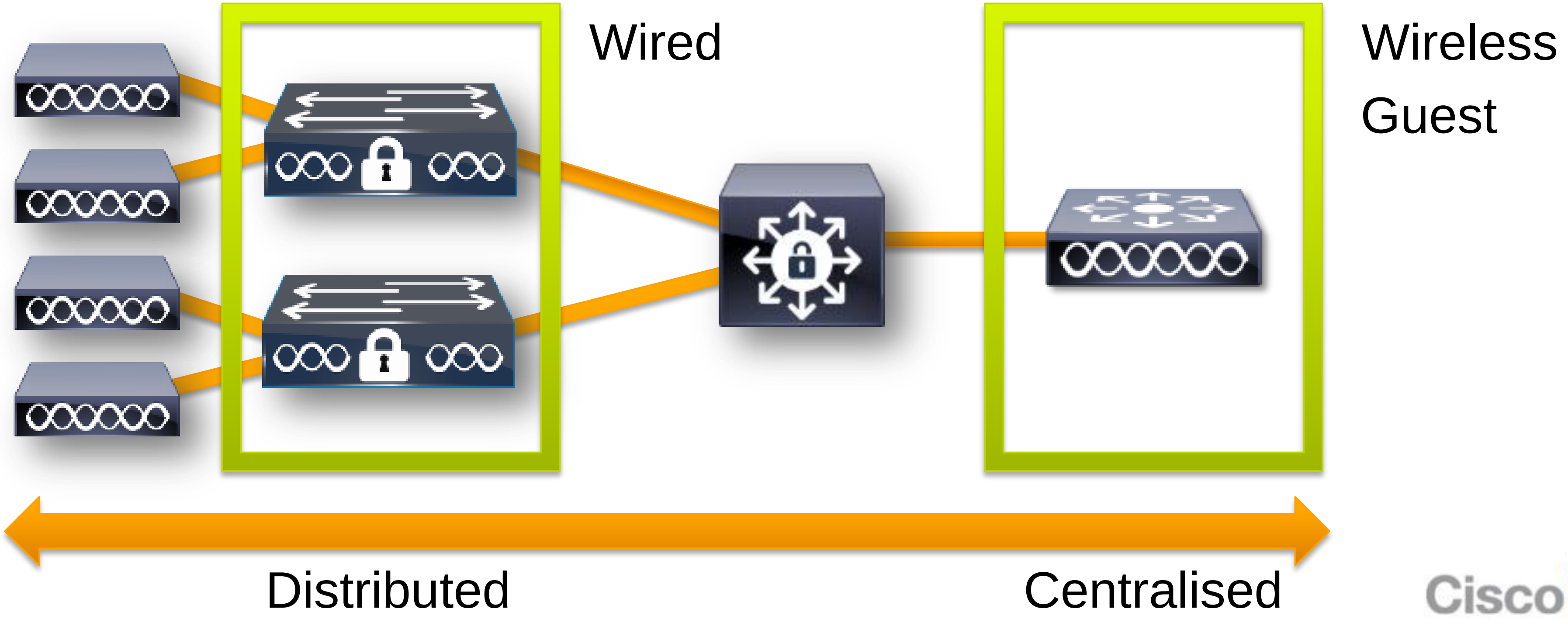
Distributed and/or Centralised

- On-Device Policy
  - AAA services (mandatory)
  - Local Policy Objects
  - Local Policy
  - Users
- Central Policy
  - Users / External Databases
  - Central Policy Objects
  - Central Policy and Control
  - Profiling
- Typically a Combination of both

Policy Application – Where?

Distributed and/or Centralised

- Prior to Converged Access, policy application was **applied at different places** for wired, wireless and guests
- With Converged Access, policy application is **distributed**, allowing for **better scalability**



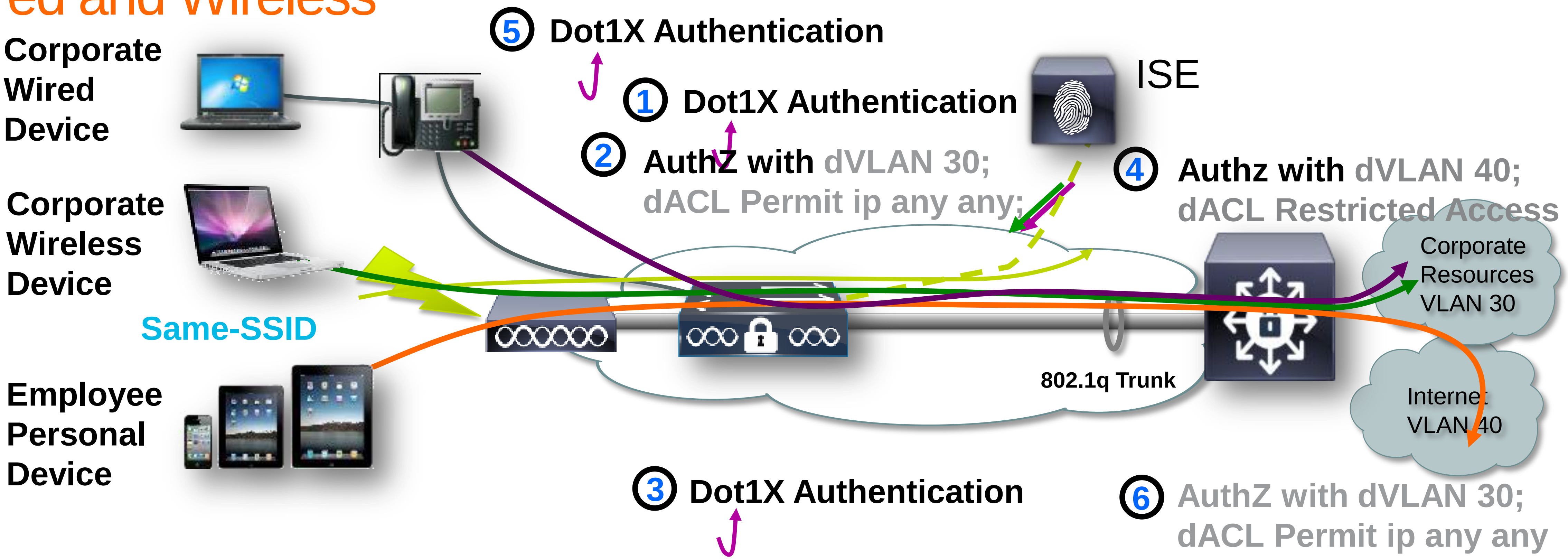
Today – Inconsistent Central Policy Definition

One Policy to the Rescue!

Feature		
ACL Application	dACL, Filter-ID, per-User ACL	Airespace-ACL-Name
VLAN Assignment	Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-ID	As with wired but **PLUS** Airespace-Interface-name
QoS	Platform dependent ☹ (C3PL, MQC, …)	Airespace-QoS-Level, Airespace-DSCP

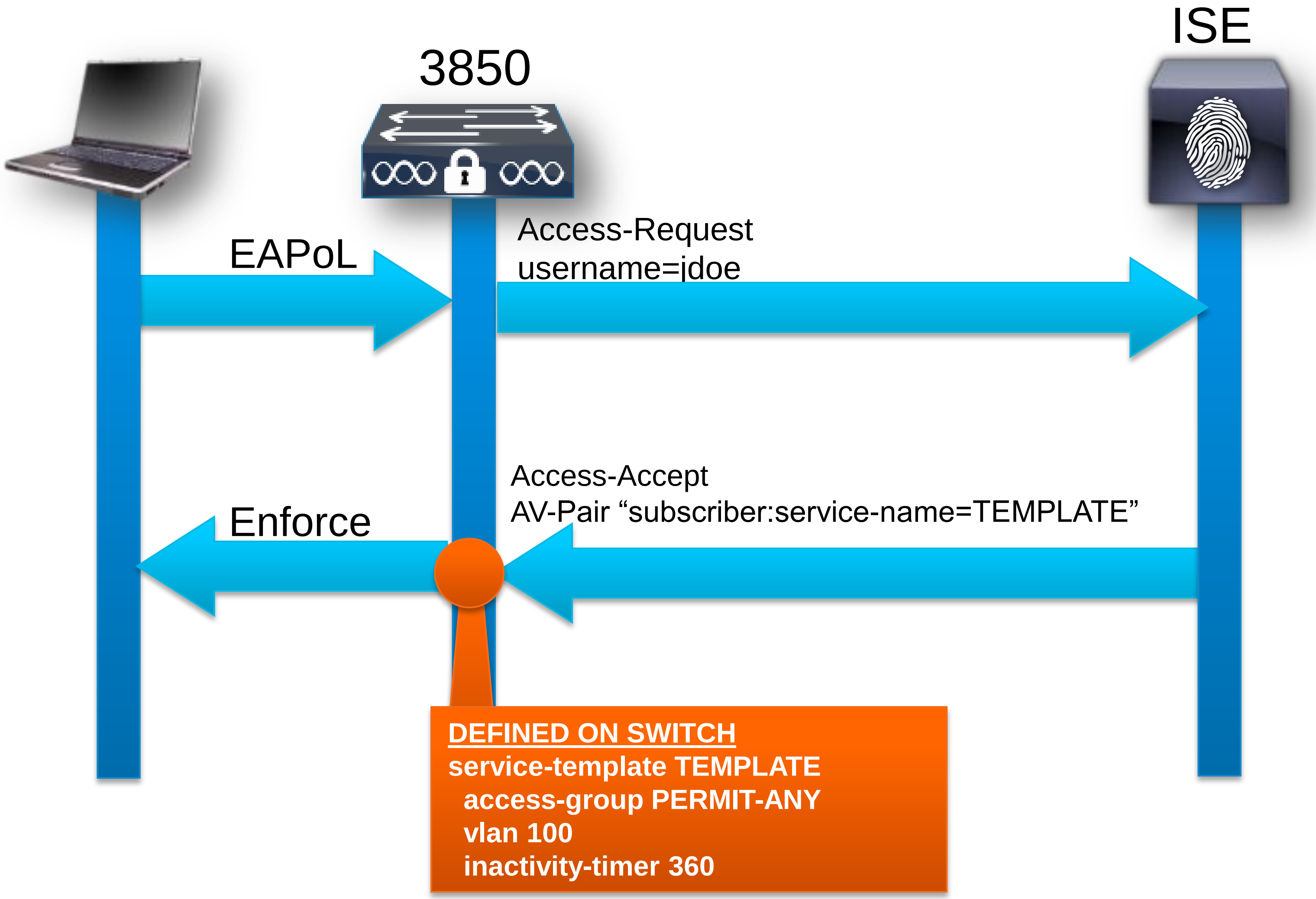
C3PL: Cisco Classification Configuration Policy Language
MQC: Modular QoS CLI

One Policy – Wired and Wireless


Corporate Wired Device
5 Dot1X Authentication
1 Dot1X Authentication
ISE
2 AuthZ with dVLAN 30; dACL Permit ip any any;
4 Authz with dVLAN 40; dACL Restricted Access
Corporate Wireless Device
Same-SSID
Corporate Resources VLAN 30
Internet VLAN 40
802.1q Trunk
Employee Personal Device
3 Dot1X Authentication
6 AuthZ with dVLAN 30; dACL Permit ip any any

- Employee using the same SSID, can be associated to different VLAN interfaces and policy after EAP authentication
- Employee using corporate wired and wireless device with their AD user id can be assigned to same VLAN 30 to have full access to the network
- Employee using personal iDevice with their AD user id can be assigned to VLAN 40 and policy to access internet only

Applying a Template –
Similar to Applying a Port ACL via *filter-id*

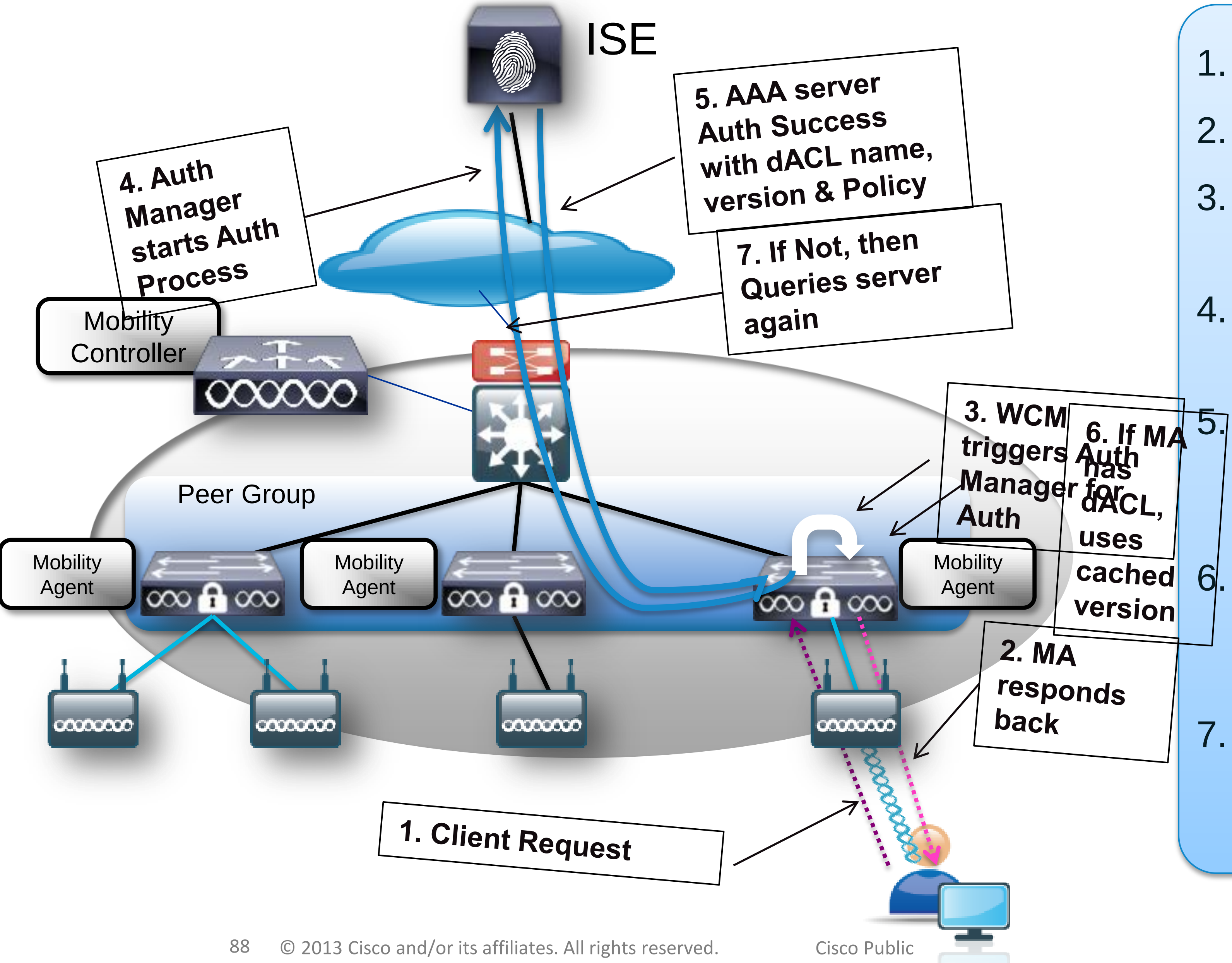


DEFINED ON SWITCH

```
service-template TEMPLATE
  access-group PERMIT-ANY
  vlan 100
  inactivity-timer 360
```

- Media Independent
- Can also be triggered via RADIUS CoA
- Service-Templates activation can be a local Control Policy action
- If it doesn’t exist, it can be downloaded similar to a dACL

Downloadable ACL



4. Auth Manager starts Auth Process

5. AAA server Auth Success with dACL name, version & Policy

7. If Not, then Queries server again

3. WCM triggers Auth Manager for Auth

6. If MA has dACL, uses cached version

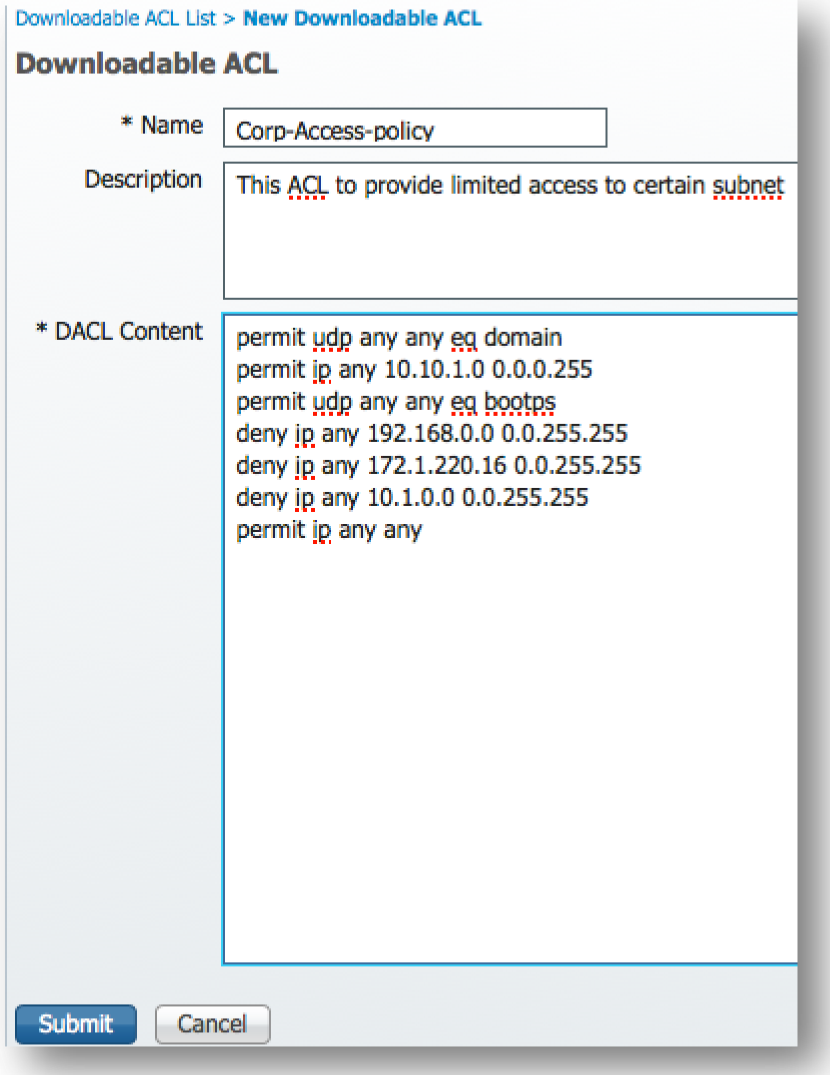
2. MA responds back

1. Client Request

1. Wireless Client request Association
2. MA respond back with Association
3. WCM triggers IOS module to do authentication
4. IOS starts authentication process for client with AAA server
5. AAA server responds with ‘access accept’ including dACL name and version number in policy attributes
6. If switch has downloaded this dACL previously and has current version it uses the cached version
7. If switch does not have current version then it queries the server for latest dACL version

Downloadable ACL (continued)

- Downloadable ACLs can be defined **identical** for both Wired and Wireless clients
- They provide network policy enforcement based on a user / device authorisation profile
- Policy can be changed on the fly and it will be pushed on-demand (NAD keeps track of version)



Downloadable ACL List > **New Downloadable ACL**

Downloadable ACL

* Name: Corp-Access-policy

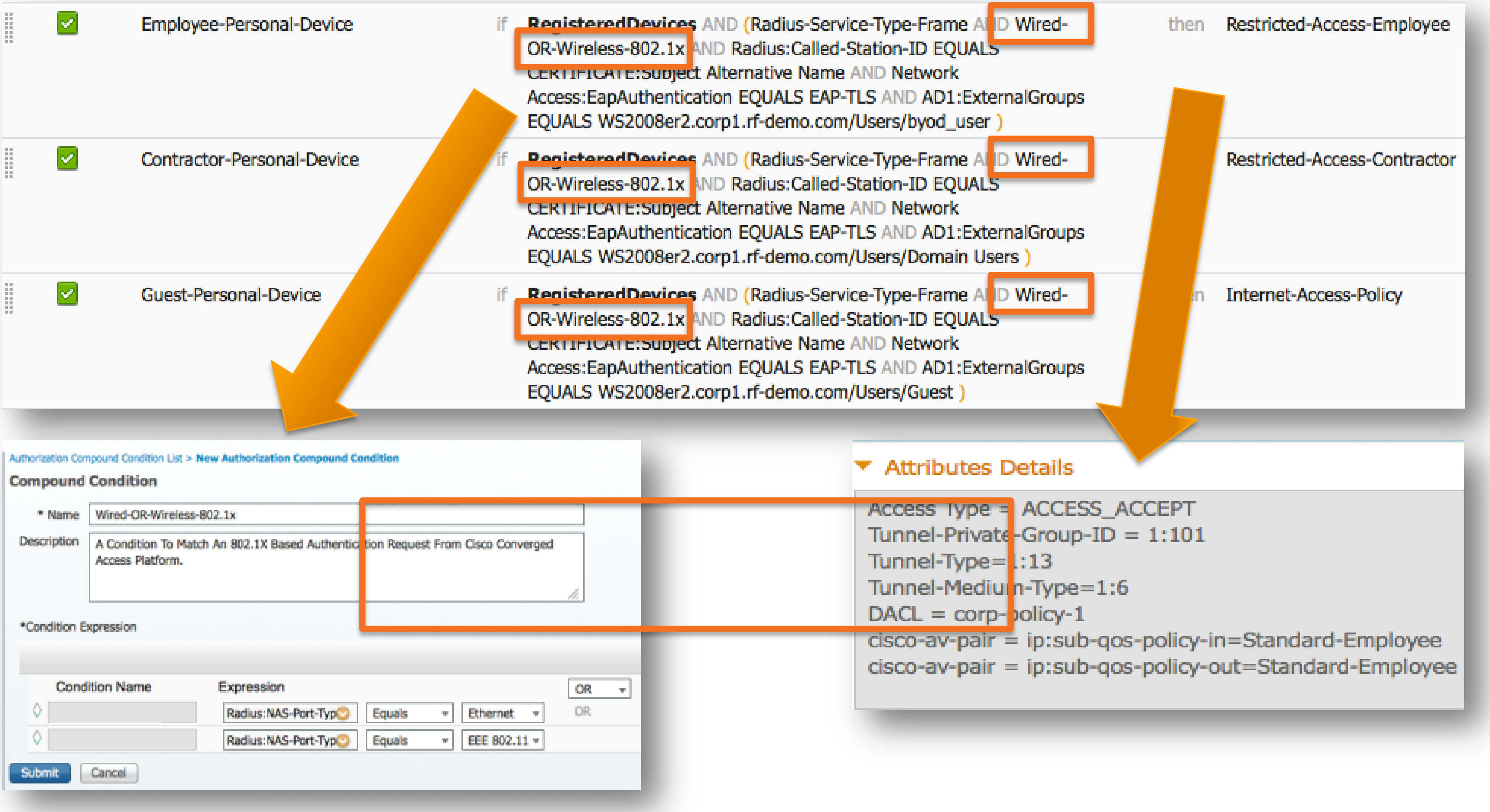
Description: This ACL to provide limited access to certain subnet

* DACL Content:

```
permit udp any any eq domain
permit ip any 10.10.1.0 0.0.0.255
permit udp any any eq bootps
deny ip any 192.168.0.0 0.0.255.255
deny ip any 172.1.220.16 0.0.255.255
deny ip any 10.1.0.0 0.0.255.255
permit ip any any
```

ISE Policy Definition Example –

Same Authorisation Policy for Wired AND Wireless



☑	Employee-Personal-Device	if	RegisteredDevices AND (Radius-Service-Type-Frame AND Wired-OR-Wireless-802.1x AND Radius:Called-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS WS2008er2.corp1.rf-demo.com/Users/byod_user)	then	Restricted-Access-Employee
☑	Contractor-Personal-Device	if	RegisteredDevices AND (Radius-Service-Type-Frame AND Wired-OR-Wireless-802.1x AND Radius:Called-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS WS2008er2.corp1.rf-demo.com/Users/Domain Users)	then	Restricted-Access-Contractor
☑	Guest-Personal-Device	if	RegisteredDevices AND (Radius-Service-Type-Frame AND Wired-OR-Wireless-802.1x AND Radius:Called-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS WS2008er2.corp1.rf-demo.com/Users/Guest)	then	Internet-Access-Policy

Authorization Compound Condition List > **New Authorization Compound Condition**

Compound Condition

* Name: Wired-OR-Wireless-802.1x

Description: A Condition To Match An 802.1X Based Authentication Request From Cisco Converged Access Platform.

*Condition Expression

	Condition Name	Expression			OR
◊		Radius:NAS-Port-Typ	Equals	Ethernet	OR
◊		Radius:NAS-Port-Typ	Equals	EEE 802.11	

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:101
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = corp-policy-1
cisco-av-pair = ip:sub-qos-policy-in=Standard-Employee
cisco-av-pair = ip:sub-qos-policy-out=Standard-Employee
```

Converged Access –

Security Features

	Cat 3850	CT5760	CT5508
BYOD Functionality	YES	YES	YES
Rogue detect / classify / contain, RDLP	YES	YES	YES
Port Security	YES	YES	NO
IP Source Guard	YES	YES	NO
Dynamic ARP Inspection	YES	YES	NO
LDAP, TACACS+, RADIUS	YES	YES	YES
LSC and MIC	YES	YES	YES
AP dot1x EAP-FAST	YES	YES	YES
Secure Fast Roaming	YES	YES	YES
802.1X-rev-2010 (MACsec / MKA)	H/W Ready	H/W Ready	NO

Converged Access –

Security Features, continued

	Cat 3850	CT5760	CT5508
IP Theft, DHCP Snooping, Data Gleaning	YES	YES	YES
IOS ACL	YES	YES	YES
Adaptive wIPS, WPS	YES	YES	YES
CIDS	YES	YES	YES
TrustSec SGT / SGACL	H/W Ready	H/W Ready	SXP
Guest Access	YES	YES	YES
IPv6 RA Guard	YES	YES	NO
MFP	YES	YES	YES
IP Device Tracking	YES	YES	NO
CoPP	Static	Static	NO

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- **Converged Access Deployment – IP Addressing**
- Converged Access Deployment – Deployment Options

Summary

Converged Access –
IP Addressing – Options

Multiple options exist for how to assign user subnets in Converged Access.

Several possible IP addressing deployment models exist for wired / wireless use …

Option 1 – Separate wired and wireless VLANs, per wiring closet

Option 2 – Merged wired and wireless VLANs, per wiring closet

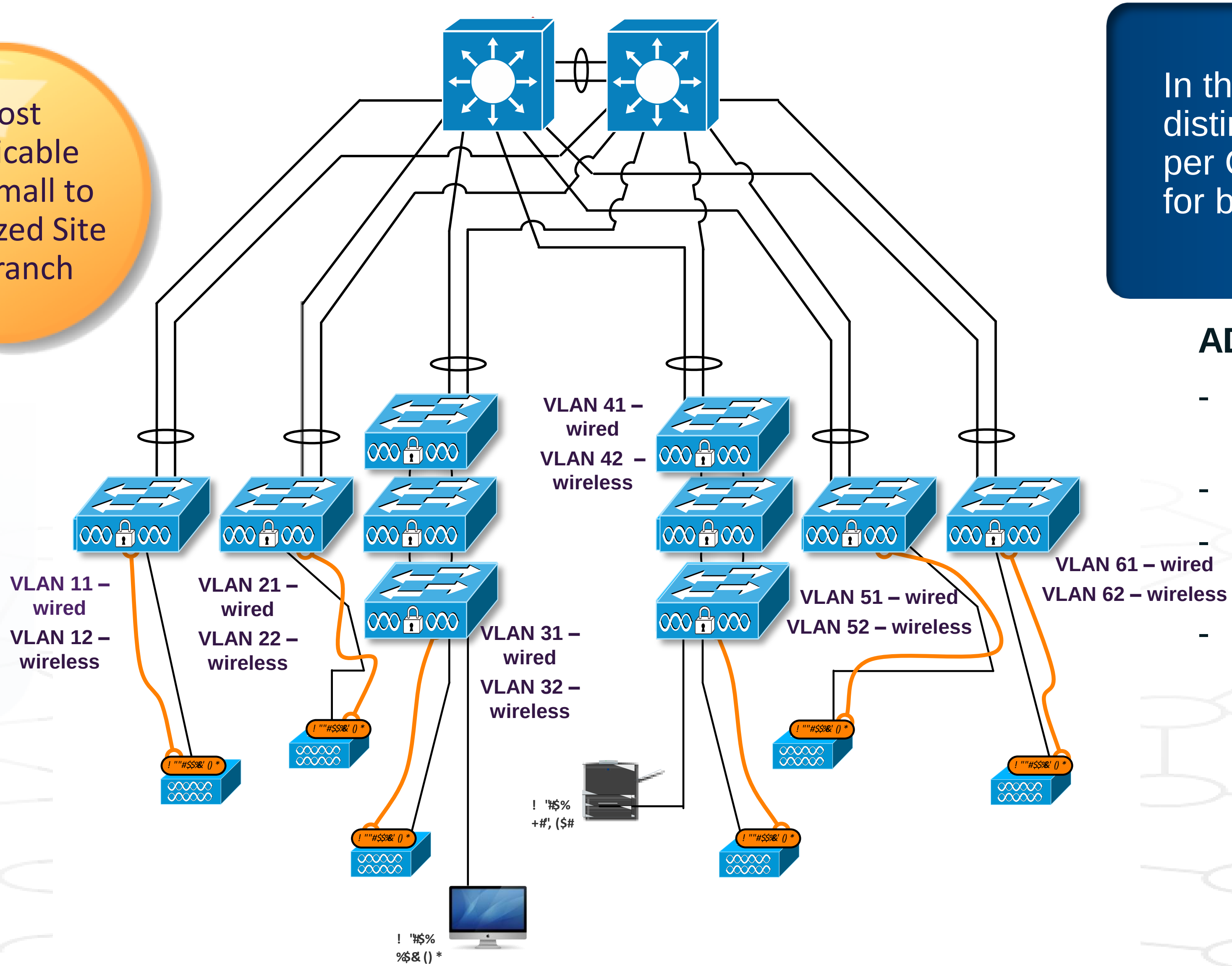
Option 3 – Separate wired VLANs per wiring closet, spanned wireless VLAN across multiple wiring closets (below a single distribution)

There are trade-offs between each of these IP addressing design models ….

On the following slides, we have summarised some of the possible advantages and considerations of each of these IP addressing options. Further and more prescriptive guidance for IP address deployment in Converged Access requires additional solution validation.

Converged Access –
IP Addressing – Option 1

Most Applicable to a Small to Mid-Sized Site or Branch



OPTION 1 – Separate VLANs / subnets per wiring closet, for wired and wireless

In this design option, separate and distinct subnets are configured per Converged Access wiring closet, for both wired and wireless users

ADVANTAGES –

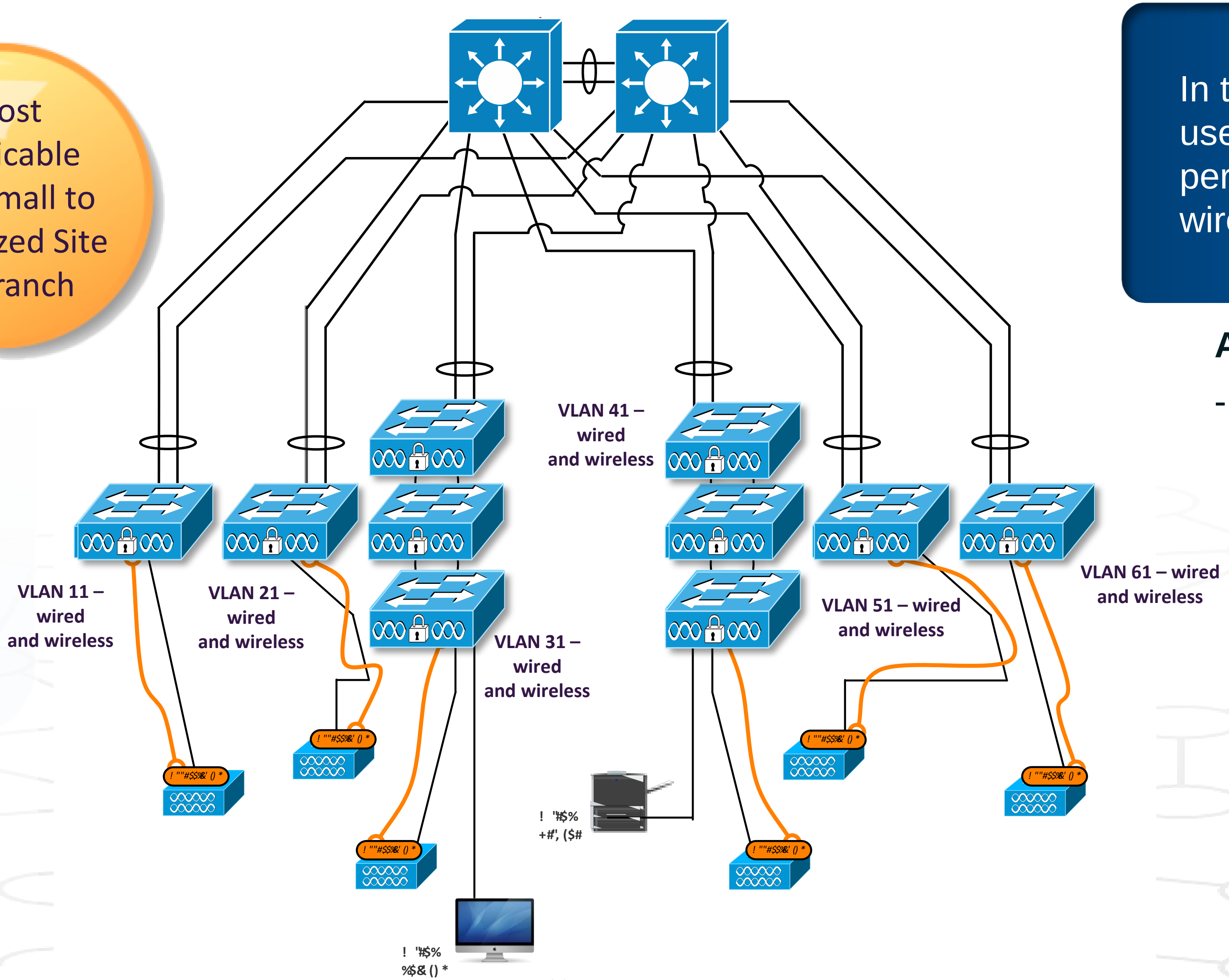
- Easy to understand – maps well to user expectations for wired design
- Can match any wired deployment (L2 / L3)
- Can create separate wired and wireless policies based on VLAN
- Eliminates DHCP contention wired/wireless

CONSIDERATIONS –

- May lead to more subnets required
- May be hard to size wireless subnets for number of anticipated wireless clients, per wiring closet (may lead to wasted IP address space for wireless use, potentially)

Converged Access –
IP Addressing – Option 2

Most
Applicable
to a Small to
Mid-Sized Site
or Branch



OPTION 2 – Merged VLANs / subnets per wiring closet, for wired and wireless

In this design option, wired and wireless users and devices share common subnets per CA wiring closet (i.e. one or more wired / wireless VLANs per wiring closet)

ADVANTAGES –

- Leads to fewer subnets req'd vs. Option 1

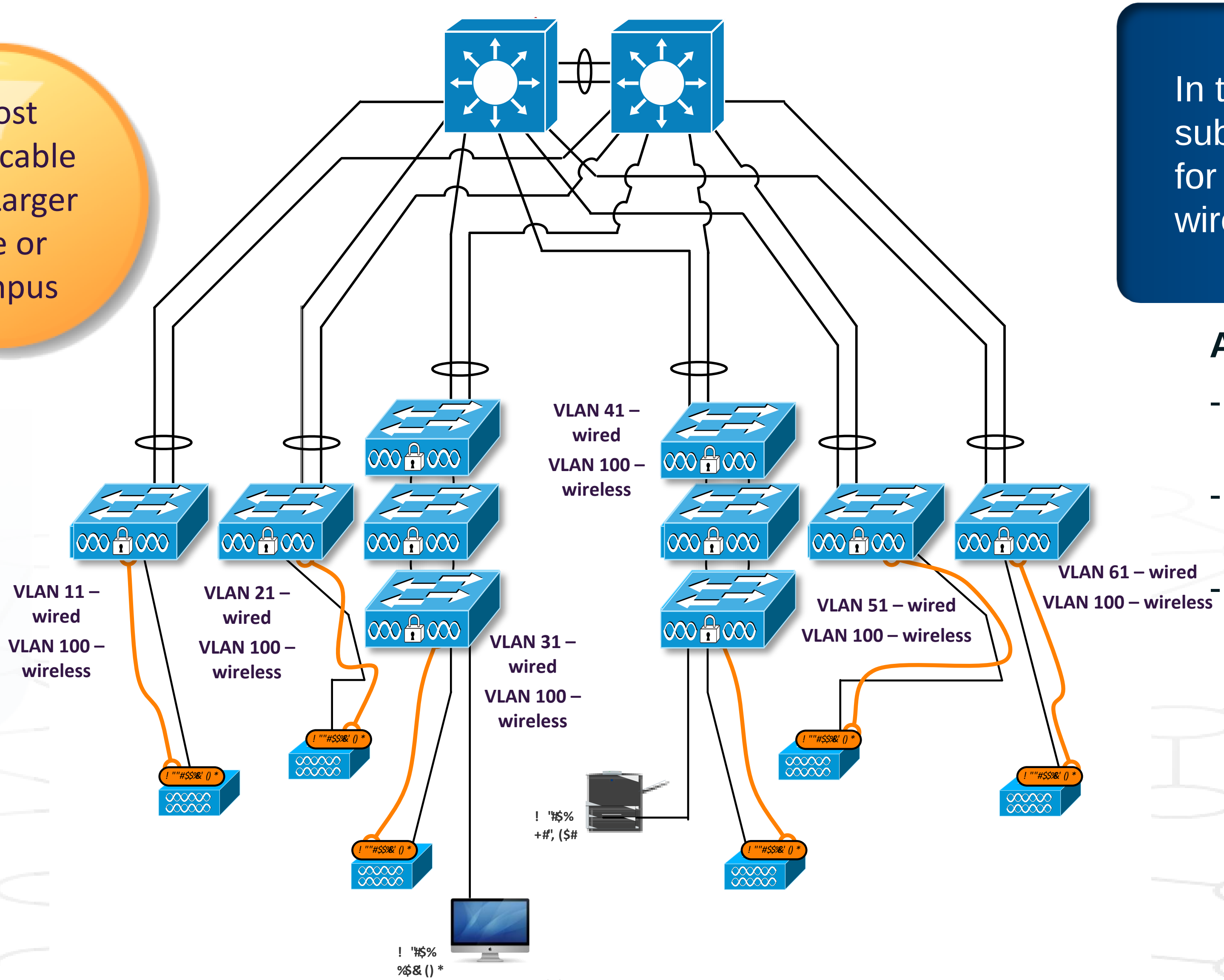
CONSIDERATIONS –

- Potential dual-attached device issues (possible client-side bridging issues)
- No longer possible to apply separate per-VLAN policies for wired / wireless
- May be hard to size combined subnets appropriately for number of wired / wireless clients, per wiring closet (may be slightly more efficient vs. Option 1)
- Possible DHCP contention, wired / wireless

Converged Access –

IP Addressing – Option 3

Most Applicable to a Larger Site or Campus



OPTION 3 – Separate wired VLANs / subnets per wiring closet, with wireless VLAN spanned

In this design option, separate and distinct subnets are configured per CA wiring closet, for both wired and wireless users, with wireless spanned below dist.

ADVANTAGES –

- Can create separate wired and wireless policies based on VLAN
- Leads to fewer subnets req'd vs. Option 1 (only one wireless subnet below dist.)
- Easier to size wireless subnet(s) below distribution layer (closer correspondence to IP addressing in the CUWN model)

CONSIDERATIONS –

- Optimised with VSS, or other similar single-switch-equivalent model, at distribution (to avoid L2 loops)
- Topology differs, wired vs. wireless

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

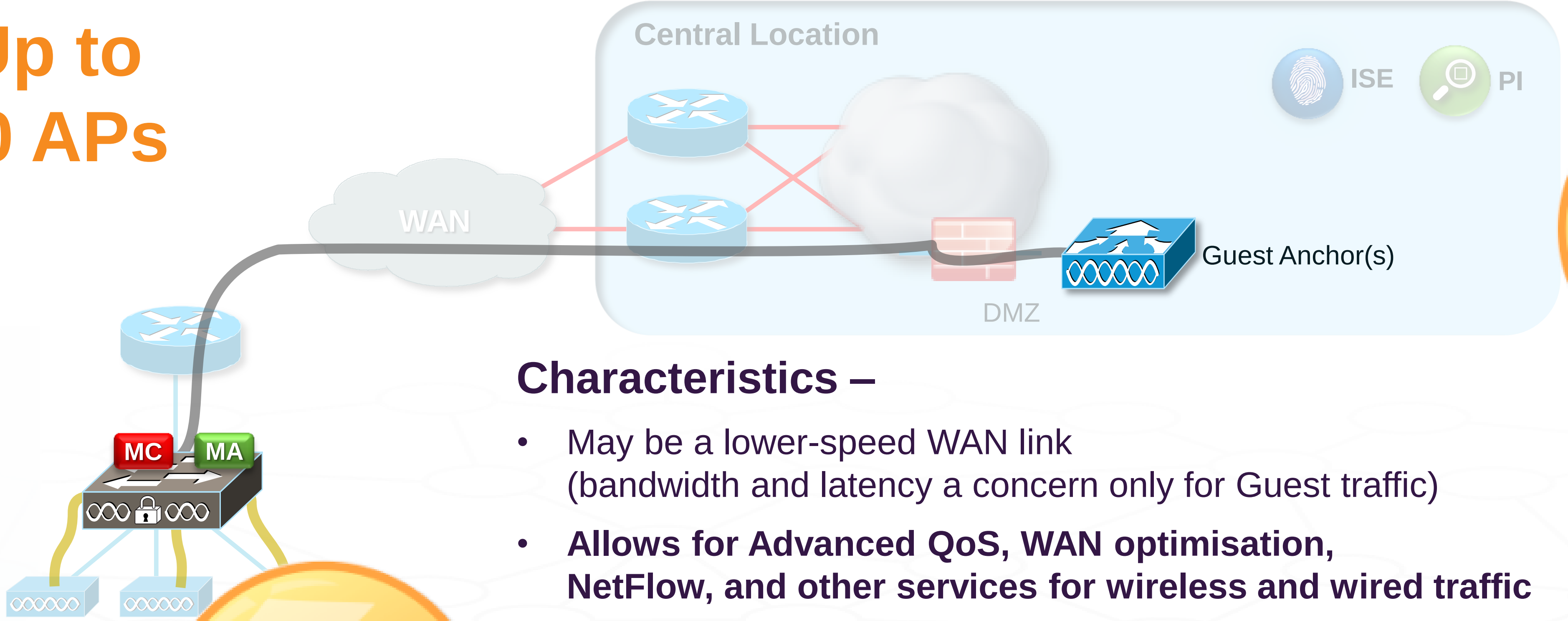
- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- **Converged Access Deployment – Deployment Options**

Summary

Converged Access –

Small Branch – No Discrete Controllers, Catalyst 3850s as MC / MAs

Up to 50 APs



Applicable to a Small Branch Deployment

Deployment could consist of multiple stacks – one stack as MC/MA, rest of stacks as MAs only

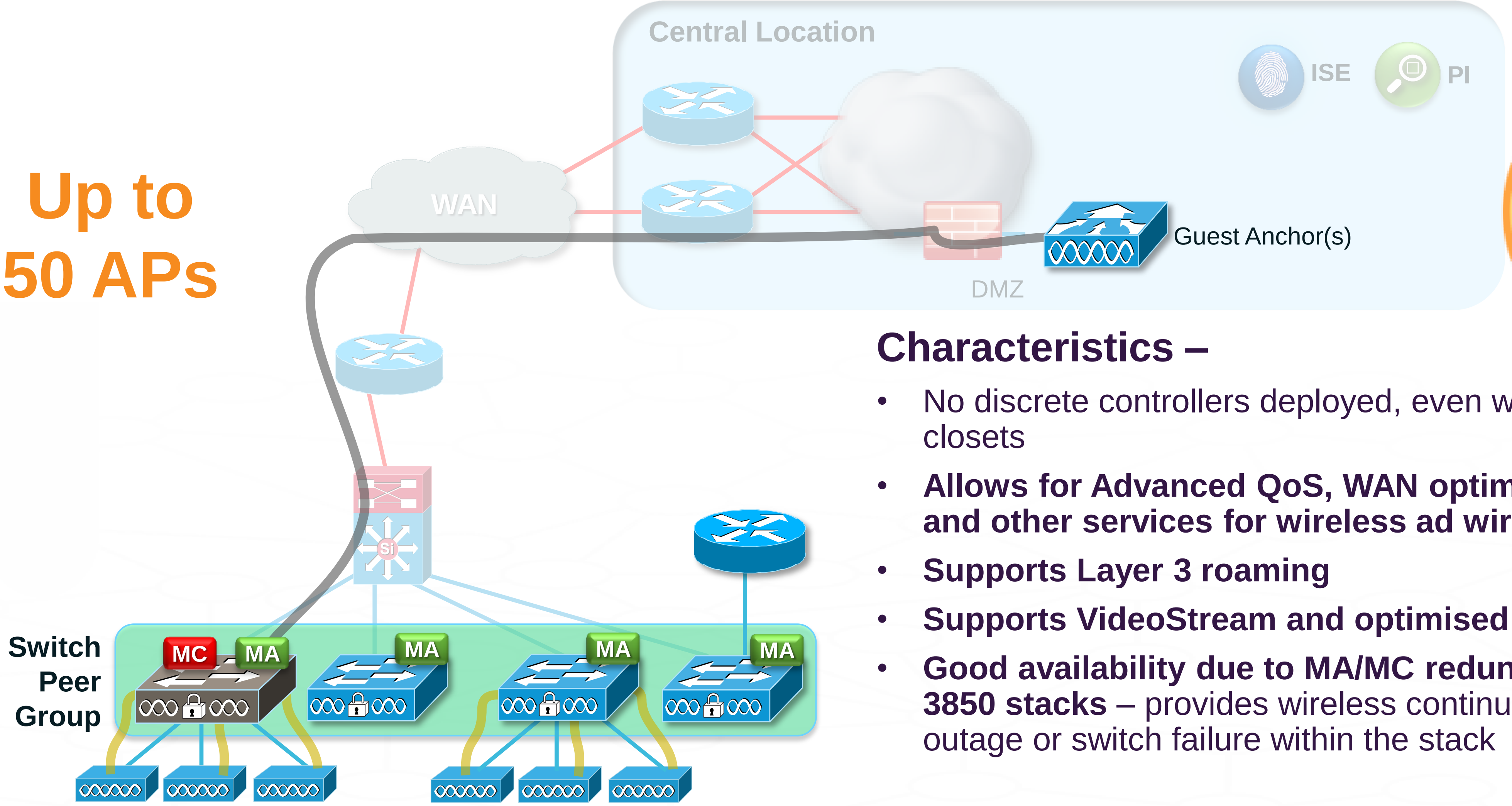
Characteristics –

- May be a lower-speed WAN link (bandwidth and latency a concern only for Guest traffic)
- **Allows for Advanced QoS, WAN optimisation, NetFlow, and other services for wireless and wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimised multicast**
- **Good availability due to MA/MC redundancy within the 3850 stack** – provides wireless continuity with either WAN outage or switch failure within the stack

Converged Access – Small / Medium Branch

No Discrete Controllers, Catalyst 3850s as MC / MAs, Single SPG

Up to 50 APs



Applicable to a Small to Medium Branch Deployment

Characteristics –

- No discrete controllers deployed, even with multiple wiring closets
- **Allows for Advanced QoS, WAN optimisation, NetFlow, and other services for wireless ad wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimised multicast**
- **Good availability due to MA/MC redundancy within the 3850 stacks** – provides wireless continuity with either WAN outage or switch failure within the stack

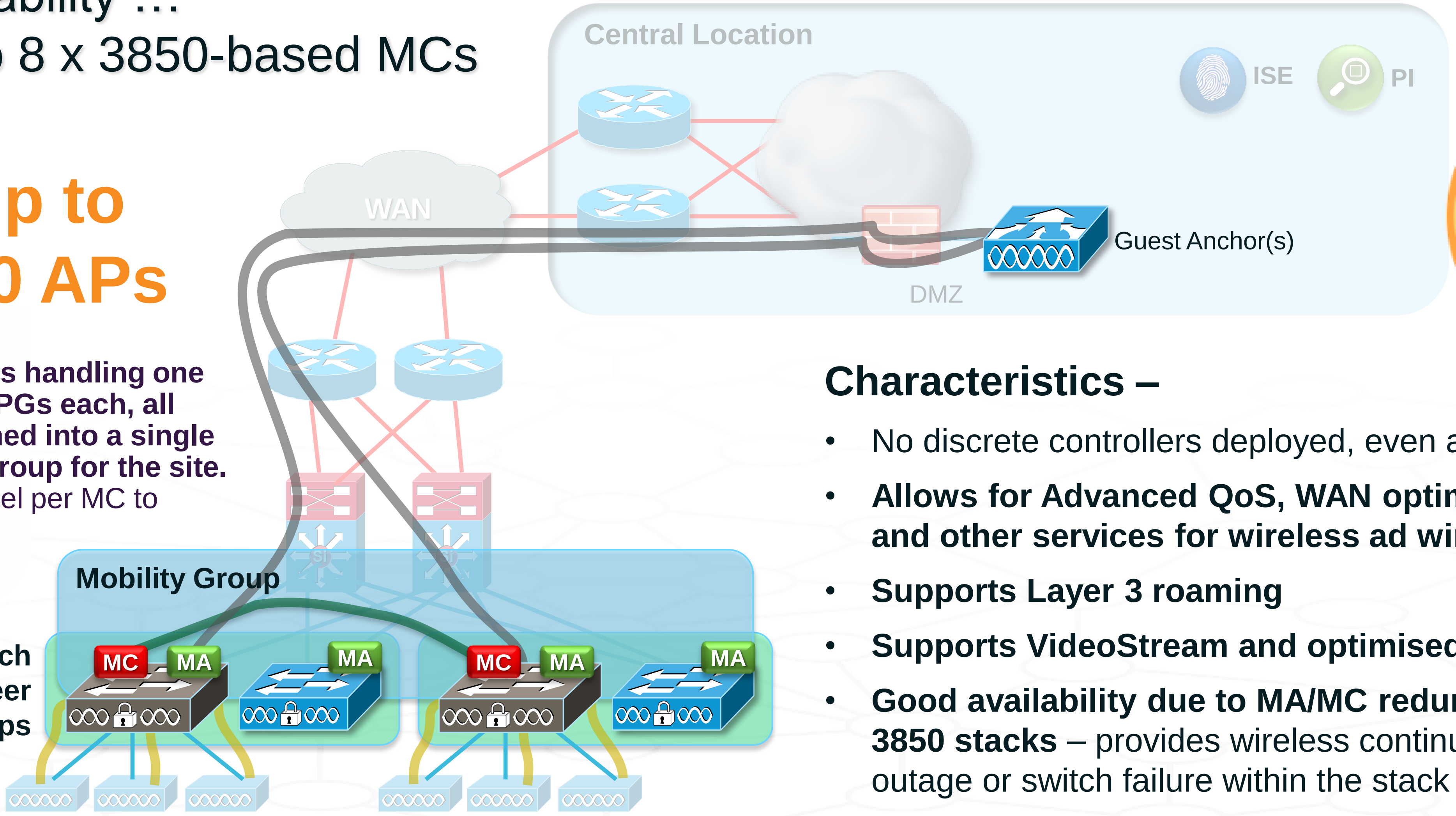
Converged Access – Large Branch

No Discrete Controllers, Catalyst 3850s as MCs / MAs, Multiple SPGs

Scalability …
up to 8 x 3850-based MCs

Up to 250 APs

Note – MCs handling one or more SPGs each, all MCs meshed into a single Mobility Group for the site. Guest tunnel per MC to Anchor.



Applicable to a Larger Branch Deployment

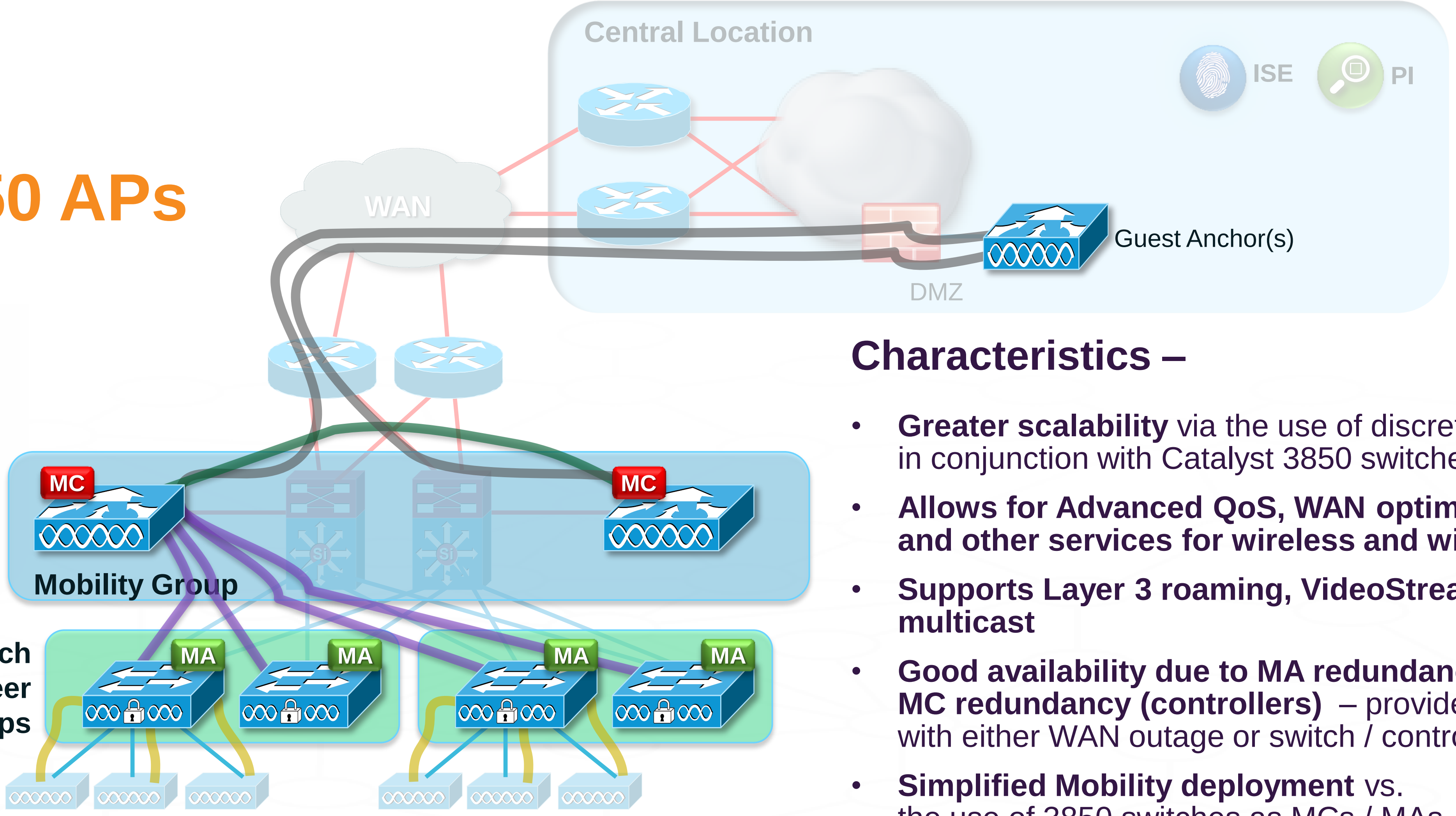
Characteristics –

- No discrete controllers deployed, even at a larger branch
- **Allows for Advanced QoS, WAN optimisation, NetFlow, and other services for wireless ad wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimised multicast**
- **Good availability due to MA/MC redundancy within the 3850 stacks** – provides wireless continuity with either WAN outage or switch failure within the stack

Converged Access – Large Branch

Controllers as MCs, Catalyst 3850s as MAs only, Multiple SPGs

>250 APs



Applicable to a Larger Branch or Small Campus

Characteristics –

- **Greater scalability** via the use of discrete controllers as MCs, in conjunction with Catalyst 3850 switches as Mas
- **Allows for Advanced QoS, WAN optimisation, NetFlow, and other services for wireless and wired traffic**
- **Supports Layer 3 roaming, VideoStream, and optimised multicast**
- **Good availability due to MA redundancy (3850 stacks) and MC redundancy (controllers)** – provides wireless continuity with either WAN outage or switch / controller failure
- **Simplified Mobility deployment** vs. the use of 3850 switches as MCs / MAs

Converged Access –

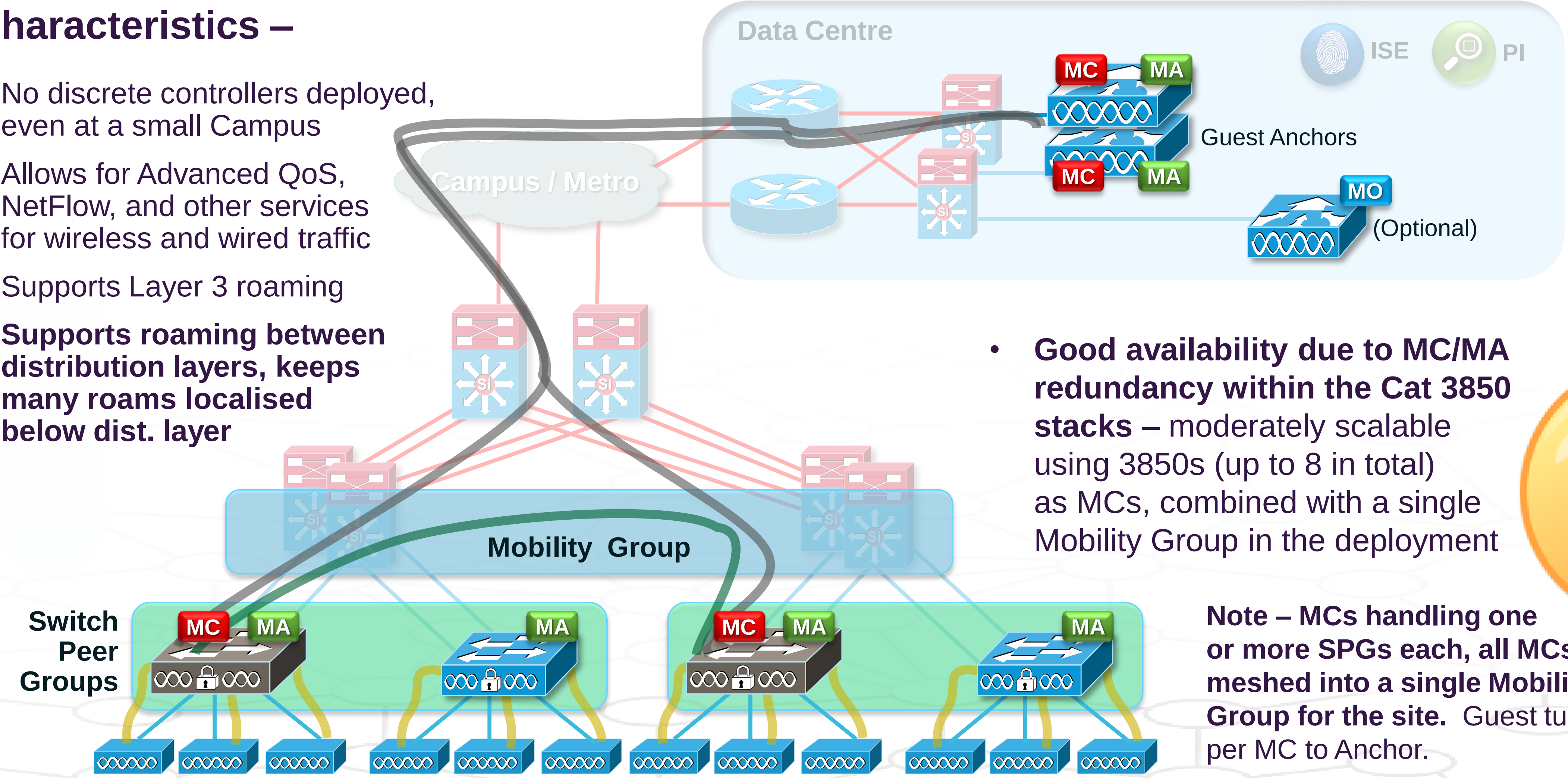
Small Campus – 3850s as MCs / MAs, Single Mobility Group

Up to 250 APs

Scalability … up to 8 x 3850-based MCs

Characteristics –

- No discrete controllers deployed, even at a small Campus
- Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
- Supports Layer 3 roaming
- **Supports roaming between distribution layers, keeps many roams localised below dist. layer**



- **Good availability due to MC/MA redundancy within the Cat 3850 stacks** – moderately scalable using 3850s (up to 8 in total) as MCs, combined with a single Mobility Group in the deployment

Applicable to a Small Campus Deployment

Note – MCs handling one or more SPGs each, all MCs meshed into a single Mobility Group for the site. Guest tunnel per MC to Anchor.

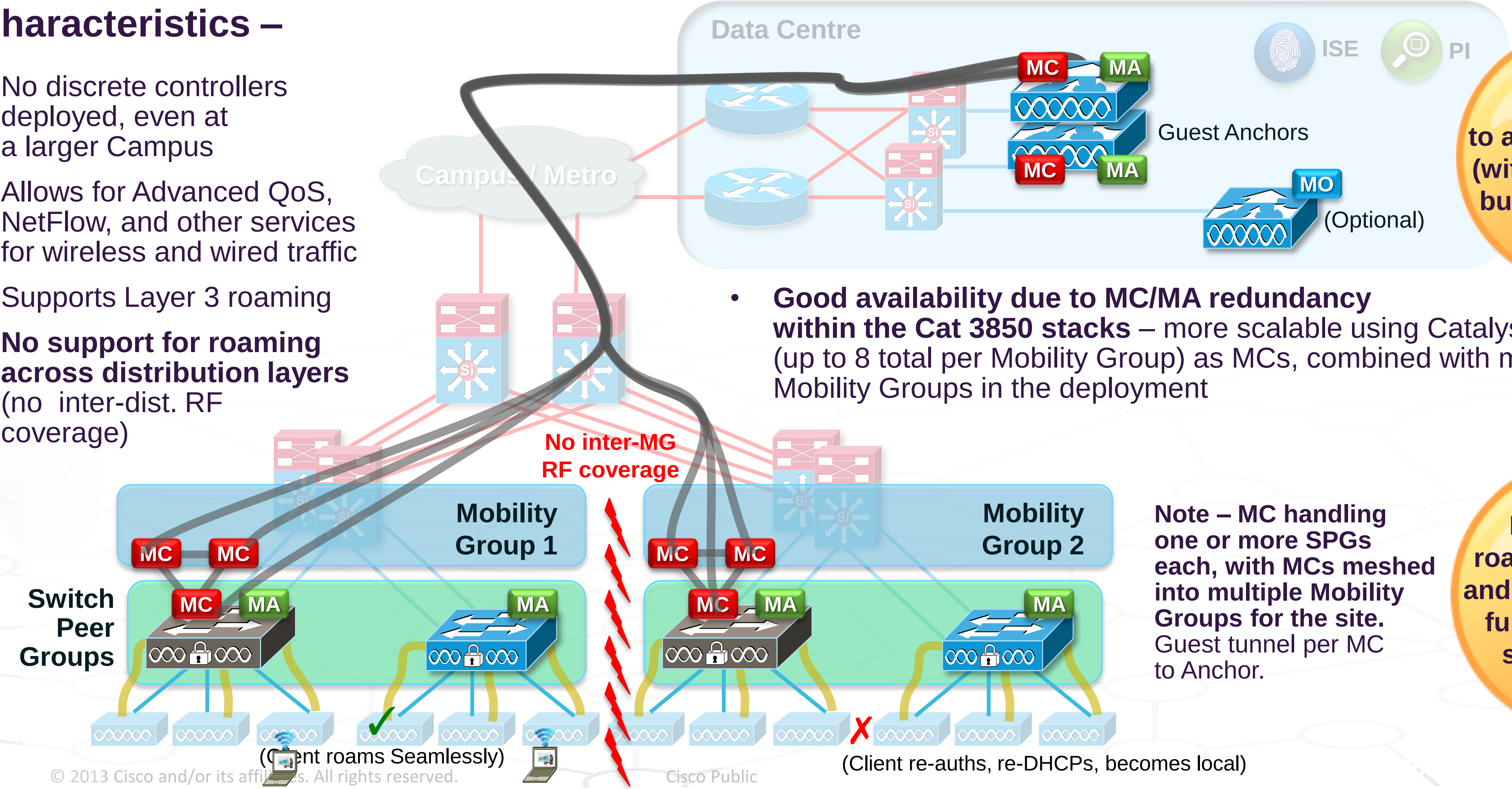
Converged Access –

Small Campus – 3850s as MCs / MAs, Multiple Mobility Groups

Scalability…. > 8 x 3850 MCs, > 250 APs total (w/o inter-dist. roaming)

Characteristics –

- No discrete controllers deployed, even at a larger Campus
- Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
- Supports Layer 3 roaming
- **No support for roaming across distribution layers** (no inter-dist. RF coverage)



- **Good availability due to MC/MA redundancy within the Cat 3850 stacks** – more scalable using Catalyst 3850s (up to 8 total per Mobility Group) as MCs, combined with multiple Mobility Groups in the deployment

Note – MC handling one or more SPGs each, with MCs meshed into multiple Mobility Groups for the site. Guest tunnel per MC to Anchor.

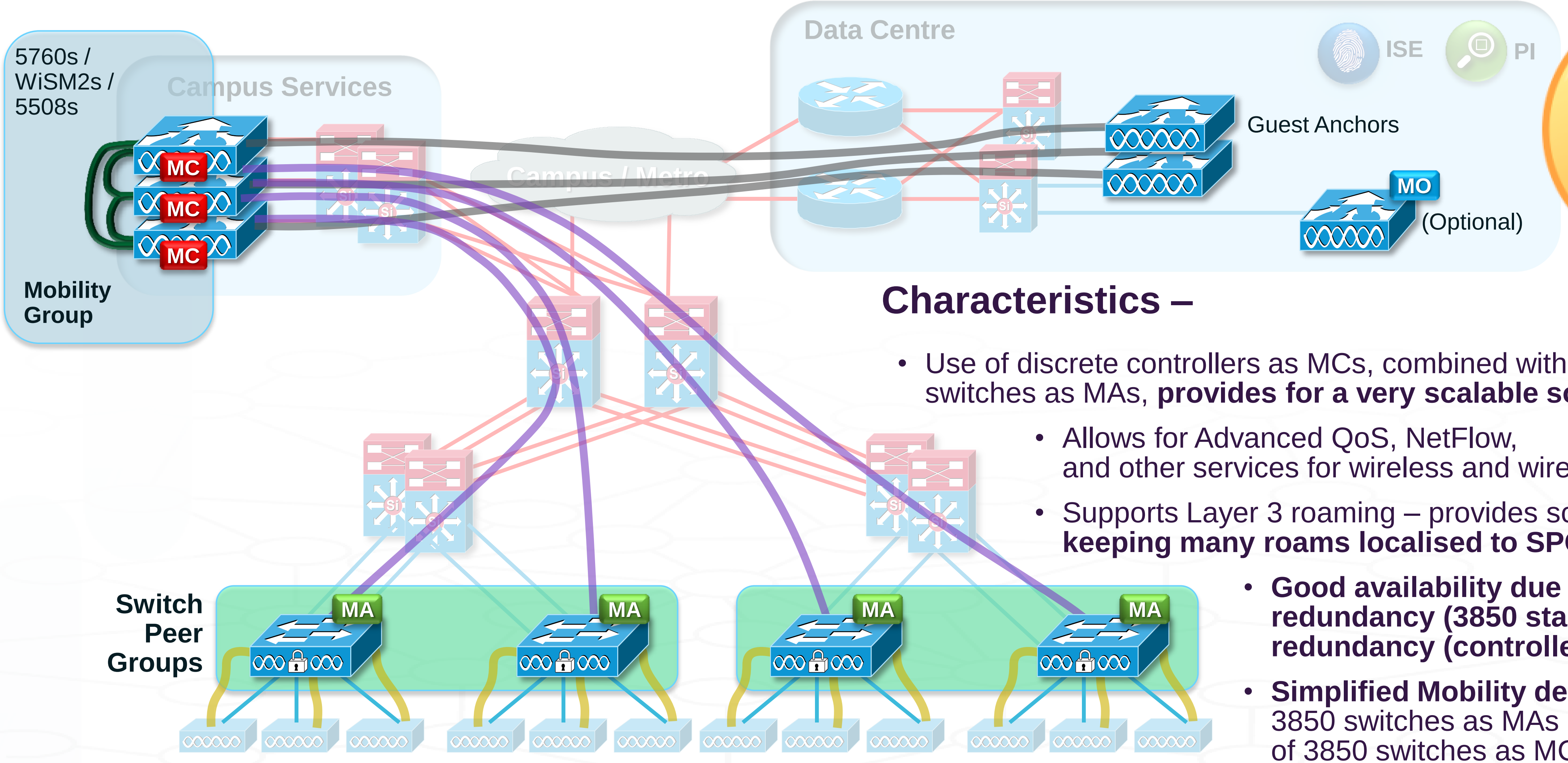
May by Applicable to a Small Campus (without any inter-building wireless coverage)

No inter-dist. roaming – no RRM and other MC-based functions across separate Mob. Groups

Converged Access –

Campus – Centralised MCs, 3850s as MAs only

>250 APs



Applicable to a Larger Campus

Characteristics –

- Use of discrete controllers as MCs, combined with Catalyst 3850 switches as MAs, **provides for a very scalable solution**
  - Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
  - Supports Layer 3 roaming – provides scalability by **keeping many roams localised to SPGs** (below dist.)
- **Good availability due to MA redundancy (3850 stacks) and MC redundancy (controllers)**
- **Simplified Mobility deployment** using 3850 switches as MAs only, vs. the use of 3850 switches as MCs / MAs

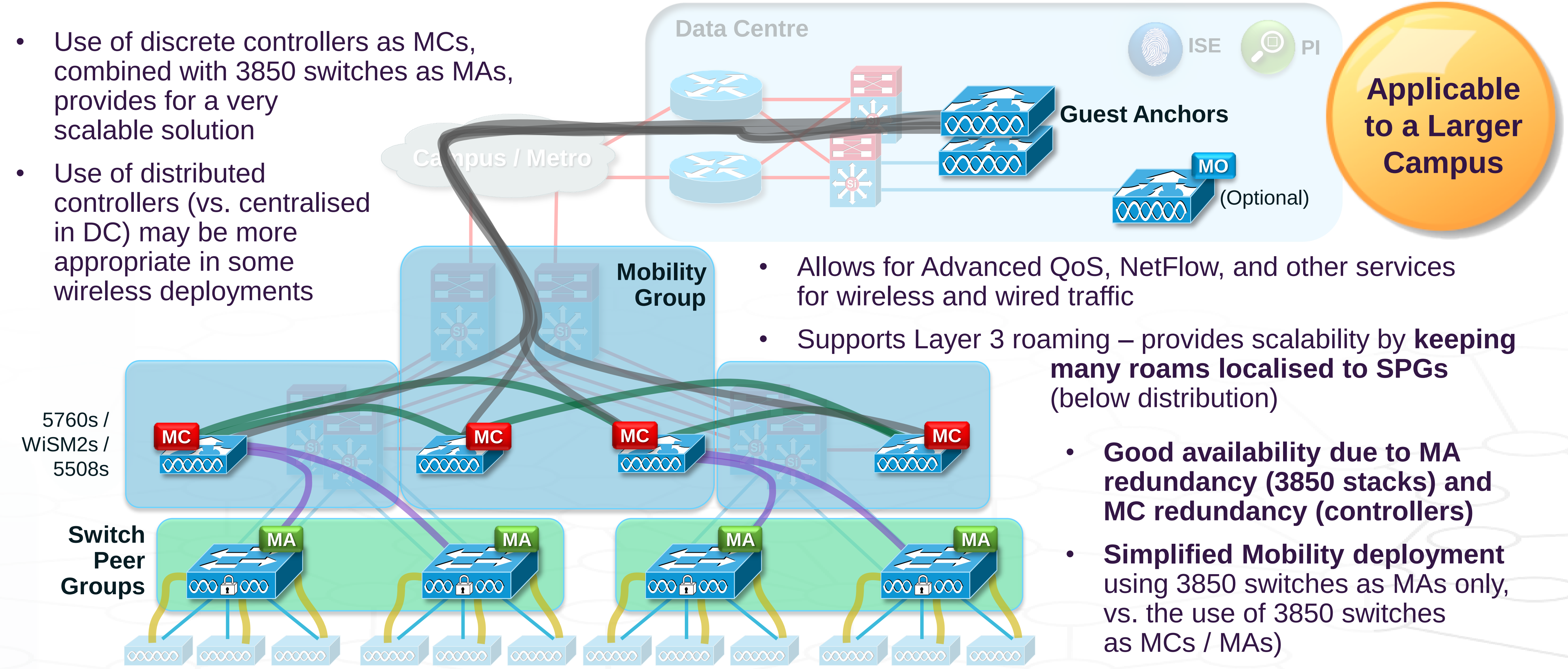
Converged Access –

Campus – Distributed MCs, 3850s as MAs only

>250 APs

Characteristics –

- Use of discrete controllers as MCs, combined with 3850 switches as MAs, provides for a very scalable solution
- Use of distributed controllers (vs. centralised in DC) may be more appropriate in some wireless deployments



Applicable to a Larger Campus

- Allows for Advanced QoS, NetFlow, and other services for wireless and wired traffic
- Supports Layer 3 roaming – provides scalability by **keeping many roams localised to SPGs** (below distribution)
  - **Good availability due to MA redundancy (3850 stacks) and MC redundancy (controllers)**
  - **Simplified Mobility deployment** using 3850 switches as MAs only, vs. the use of 3850 switches as MCs / MAs)

Agenda BRKARC-2666 … Converged Access – Campus and Branch, Design Guidance

Evolution – Towards One Policy, One Management, One Network

Converged Access – Platform Overviews

Converged Access – Catalyst 3850 Platform in Detail

Existing Wireless Deployment – Architecture Refresher

The Converged Access Deployment in Detail –

- Components of the Deployment – Terminology Review
- Converged Access Deployment – Roaming Overview
- Converged Access Deployment – Quality of Service
- Converged Access Deployment – Security
- Converged Access Deployment – IP Addressing
- Converged Access Deployment – Deployment Options

Summary

Bringing Together Wired and Wireless –

How Are We Addressing This Shift?

Controller

Control plane functionality on NG Controller

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

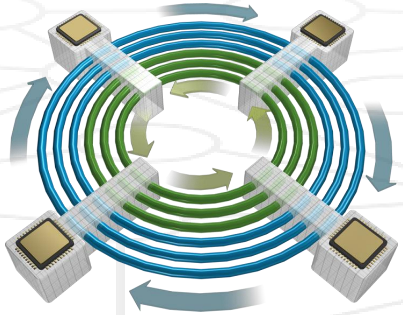
Next-Generation WLAN Controller (5760)

Data plane functionality on NG Switches

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

Next-Generation Switches (Catalyst 3850s)

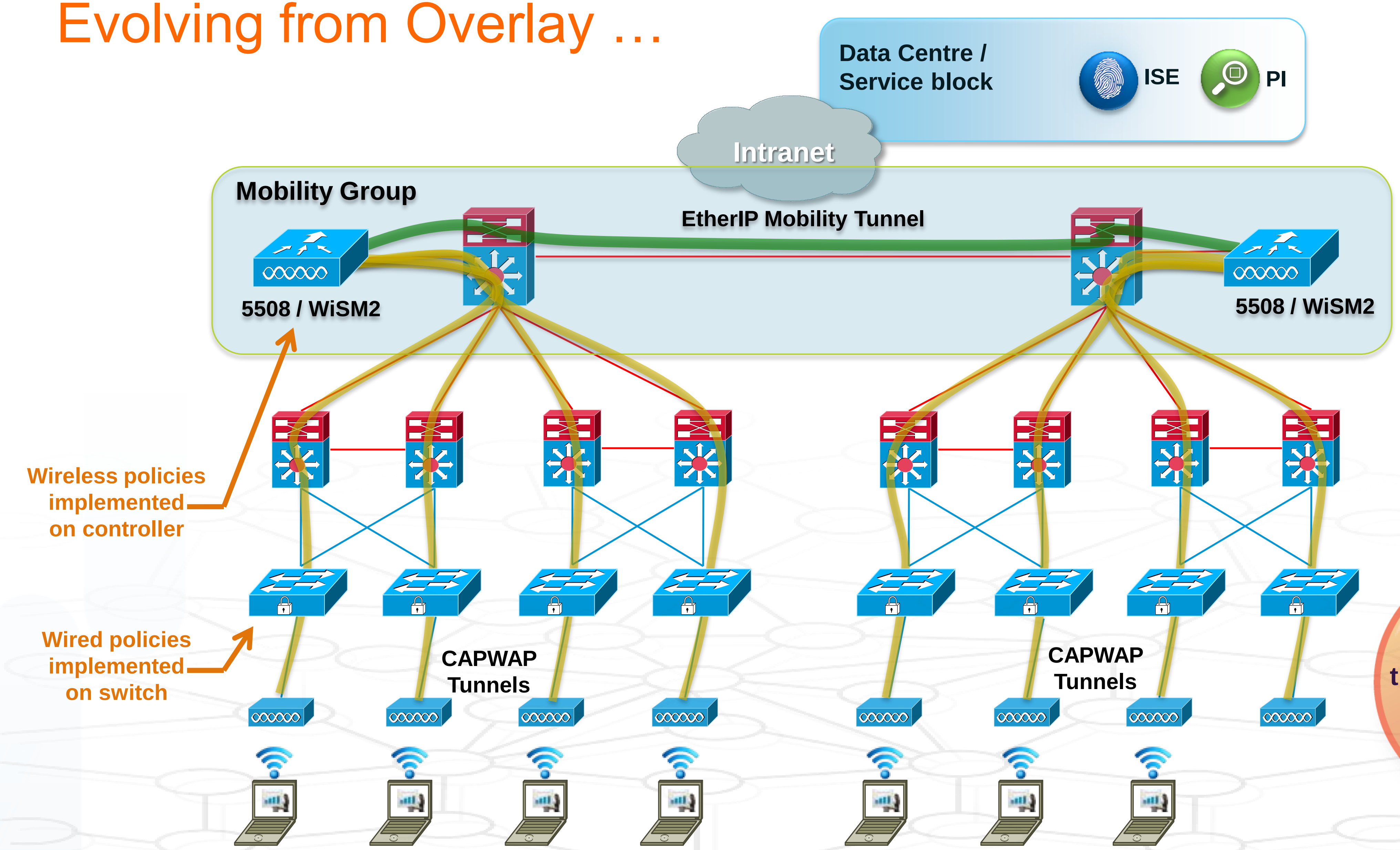
Enabled by Cisco's strength
in Silicon and Systems …
UADP ASIC



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

Converged Wired / Wireless Access –

Evolving from Overlay …



Wireless policies implemented on controller

Wired policies implemented on switch

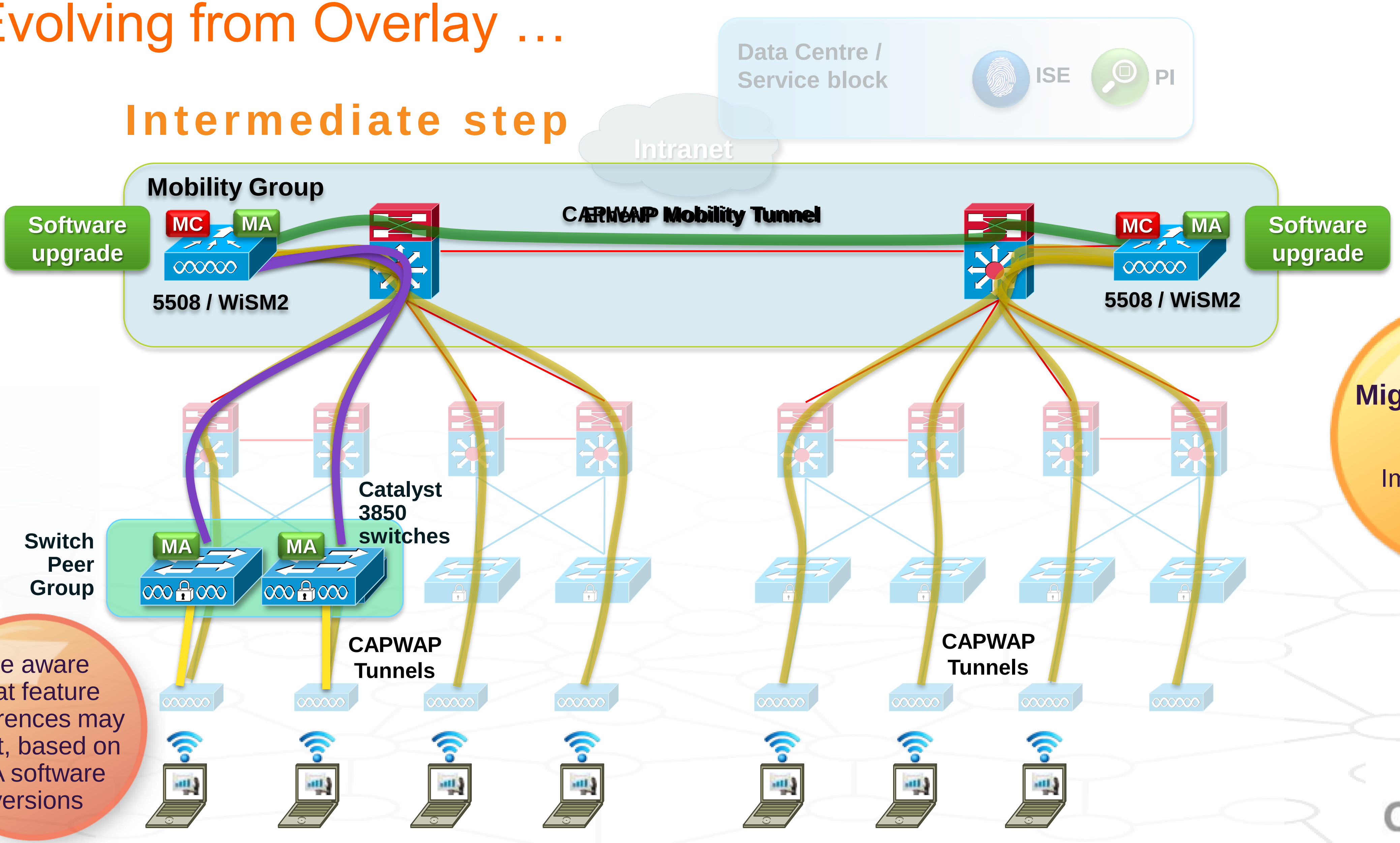
Well-known and well-proven … Prior to Migration to Converged Access

Separate policies and services for wired and wireless users

All wireless traffic centralised via controllers as shown

Converged Wired / Wireless Access –

Evolving from Overlay …

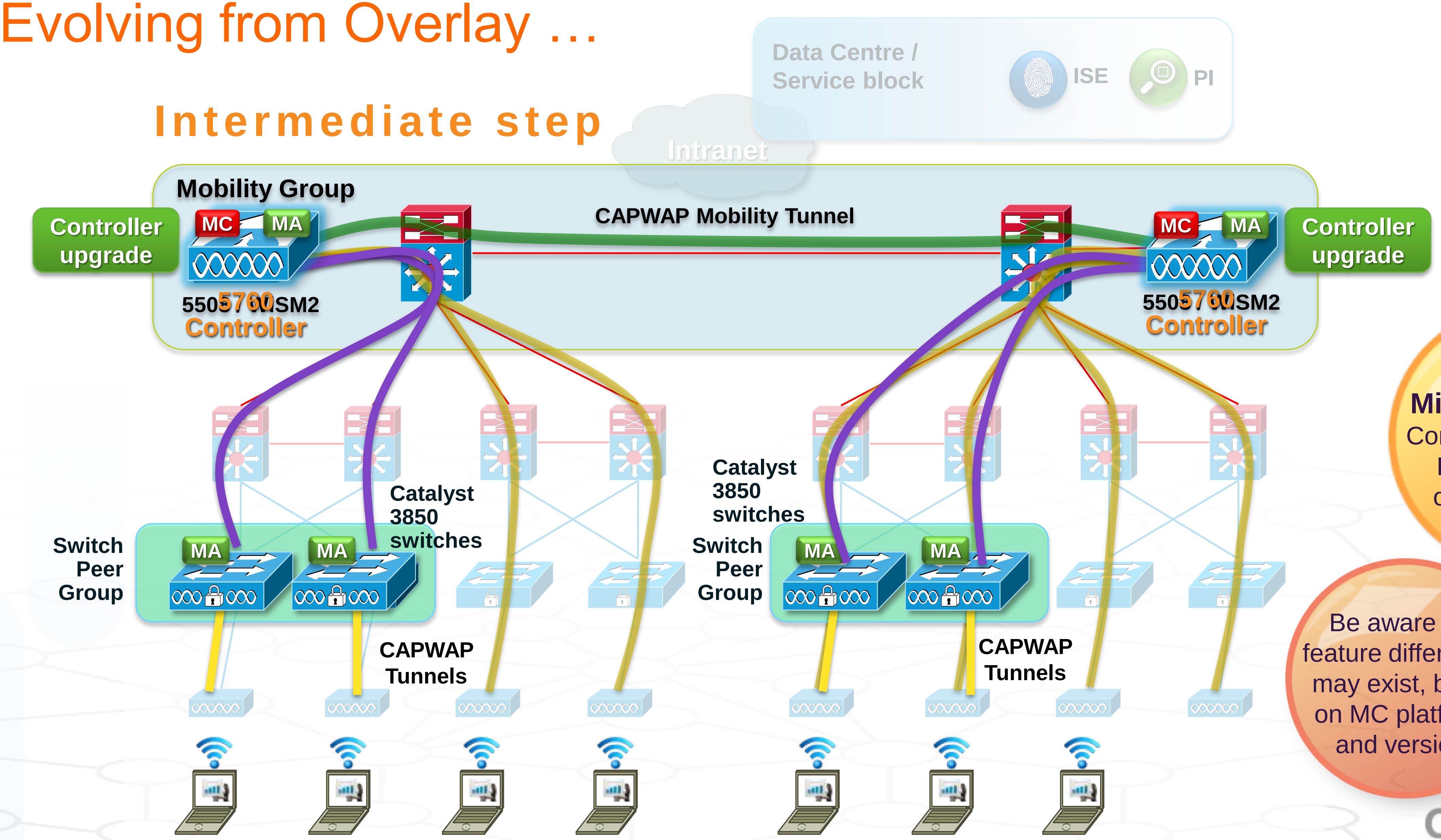


Initial Migration Step – Controller Upgrades, Implementation of First CA Switches

Be aware that feature differences may exist, based on MA software versions

Converged Wired / Wireless Access –

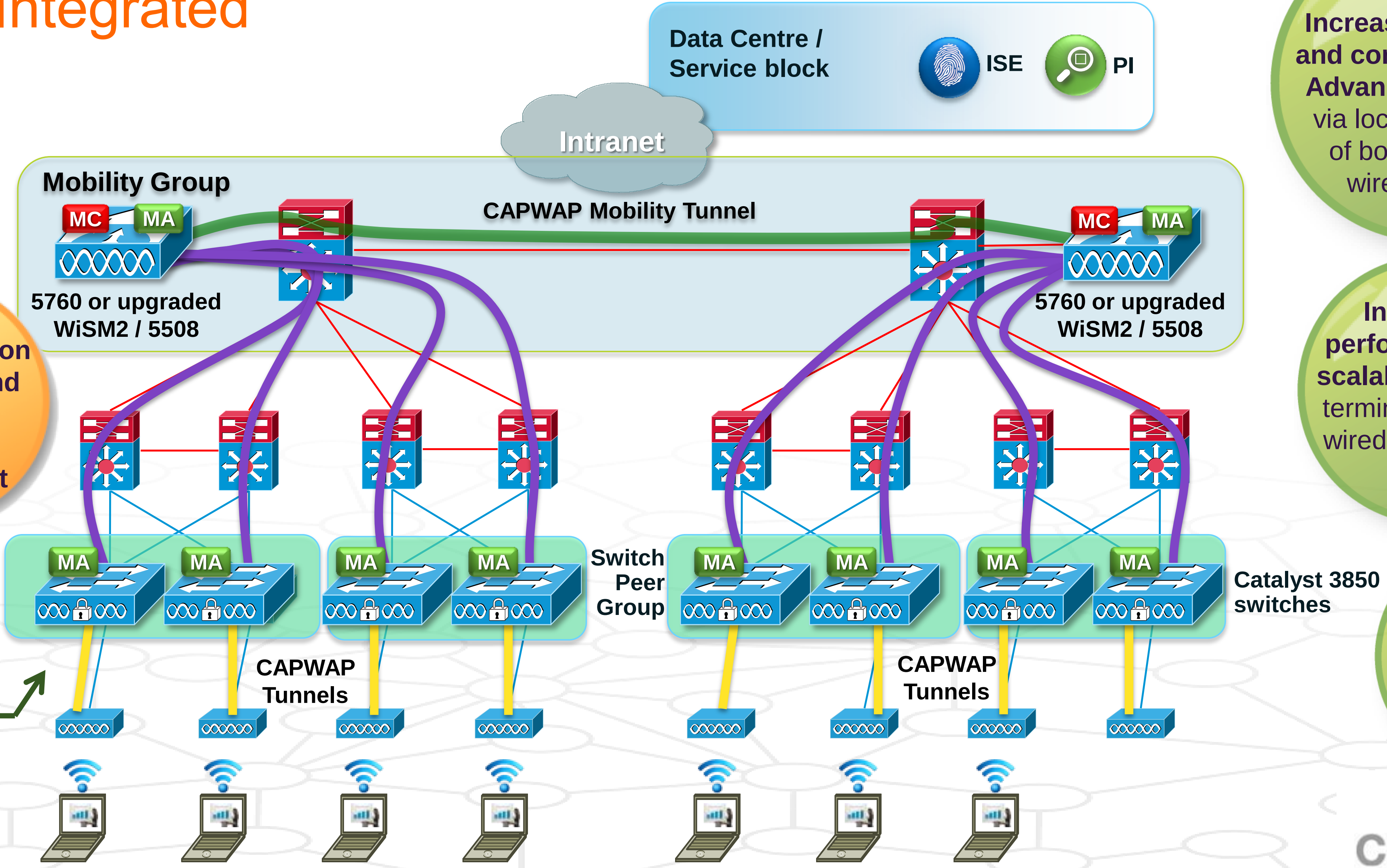
Evolving from Overlay …



Further Migration Step – Controller Upgrades, Implementation of Additional CA Switches

Be aware that feature differences may exist, based on MC platforms and versions

Converged Wired / Wireless Access – … to Integrated



Implementation of End-to-End Converged Access Deployment

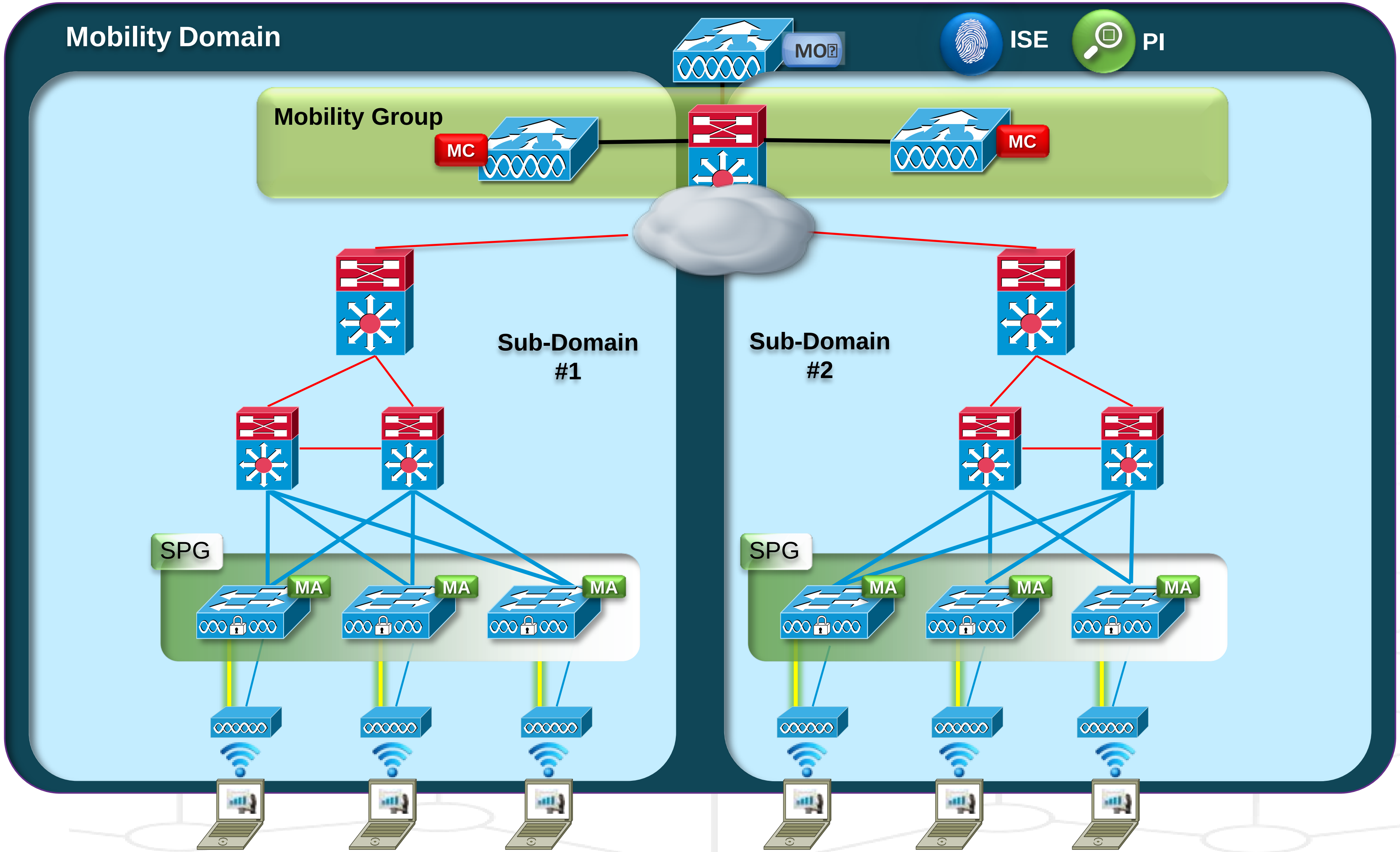
Wired and wireless policies implemented on 3850 switch

Increase in visibility and control (NetFlow, Advanced QoS, etc) via local termination of both wired and wireless traffic

Increase in performance and scalability via local termination of both wired and wireless traffic

Converged policies and services for wired and wireless users

Bringing Together Wired and Wireless – With a Next-Generation Deployment and Solution



Cisco **Converged Access** Deployment

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

Converged Access –
Tell Me How I Did!

Did I Achieve My Objective?

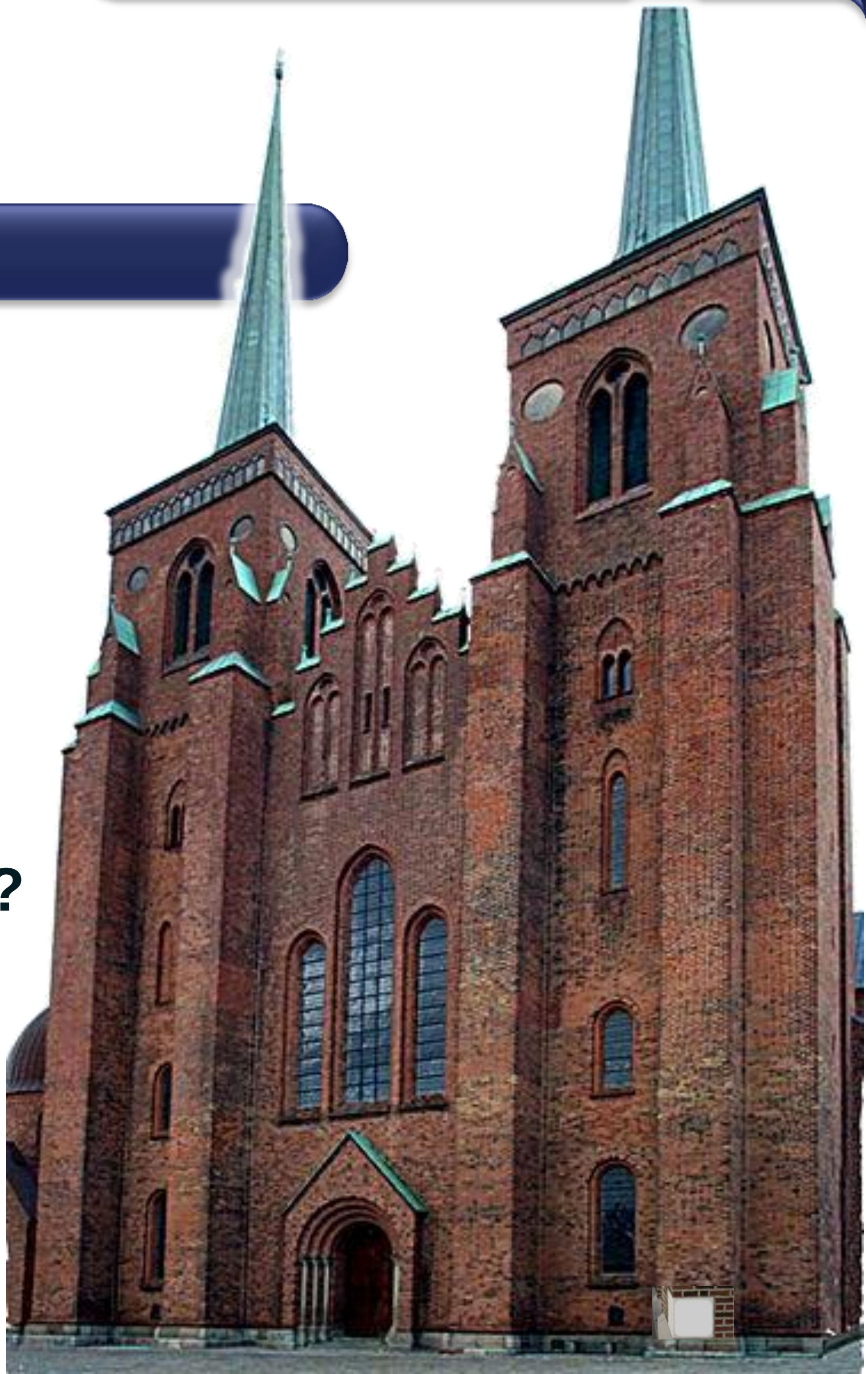
Do You Have a Better Understanding …

of **what Converged Access is** …

of **how Converged Access works** …

**and do you now have what you need
to start designing for Converged Access?**

Don’t Forget
to fill out your evaluations!



Complete Your Online Session Evaluation

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

Complete your Overall Event Survey and 5 Session Evaluations.

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

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

Cisco live! 365

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

Cisco live!

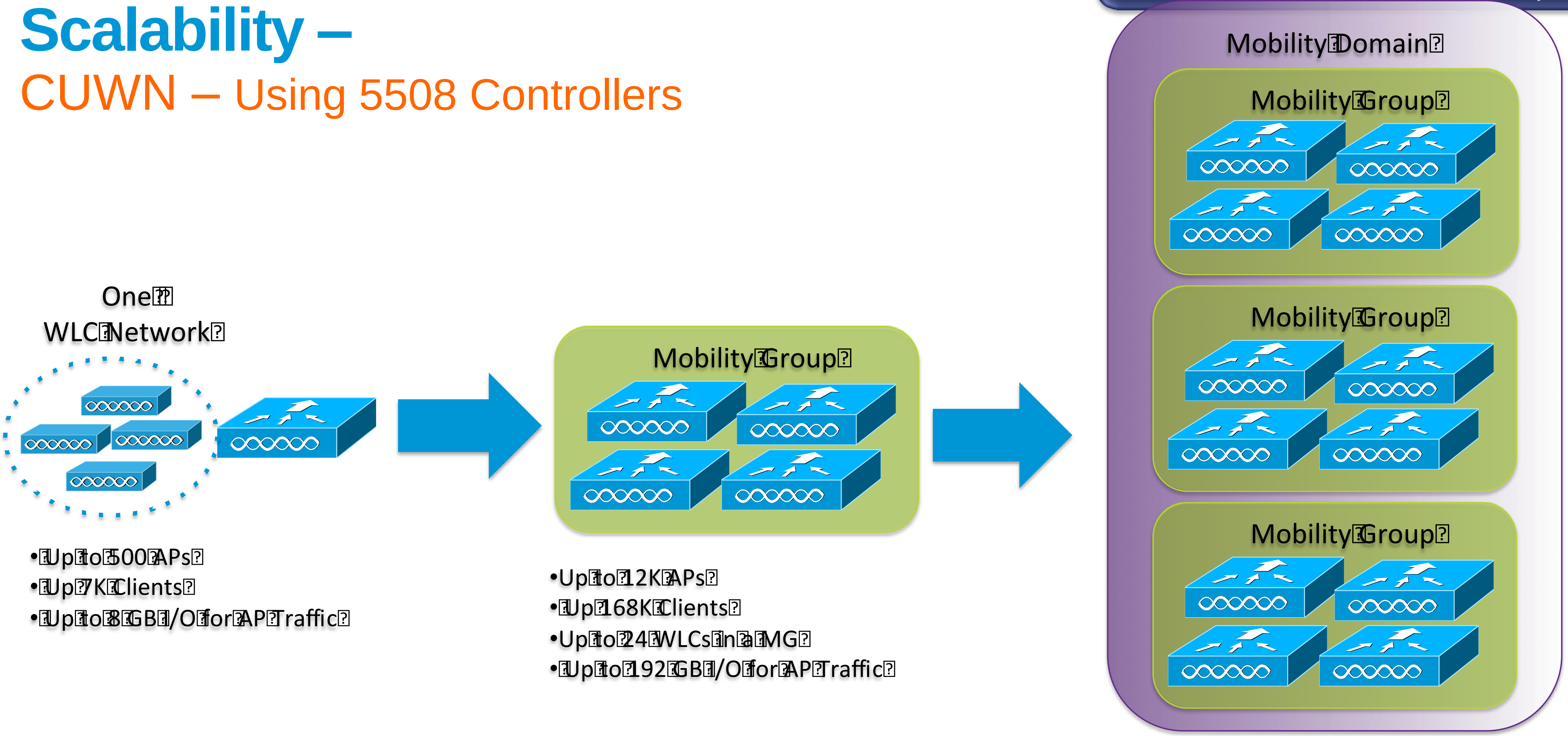
REFERENCE MATERIAL

SCALABILITY

Scalability –

CUWN – Using 5508 Controllers

Existing Unified Wireless Deployment today …



- Up to 500 APs
- Up 7K Clients
- Up to 8 GB I/O for AP Traffic

- Up to 12K APs
- Up 168K Clients
- Up to 24 WLCs in a MG
- Up to 192 GB I/O for AP Traffic

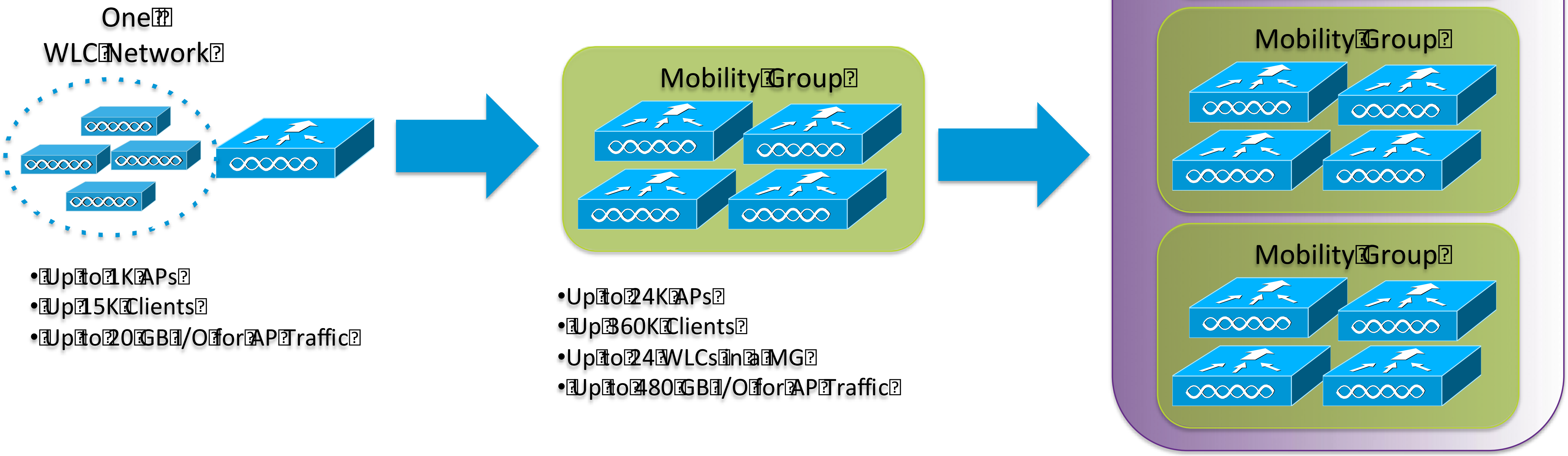
- Up to 36K APs
- Up to 504K Clients
- Up to 72 WLCs in a MD
- Up to 576GB I/O for AP Traffic

- CT5508 rel 7.3
- Max theoretical scalability numbers
- Without Considering FlexConnect

Scalability –

CUWN – Using WiSM2 Controllers

Existing Unified Wireless Deployment today …



- Up to 1K APs
- Up 15K Clients
- Up to 20 GB I/O for AP Traffic

- Up to 24K APs
- Up 360K Clients
- Up to 24 WLCs in a MG
- Up to 480 GB I/O for AP Traffic

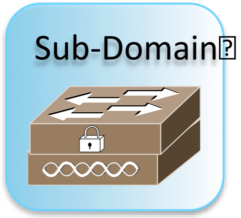
- Up to 72K APs
- Up to 1.08M Clients
- Up to 72 WLCs in a MD
- Up to 1.44TB I/O for AP Traffic

- WiSM-2 rel 7.3
- Max theoretical scalability numbers
- Without Considering FlexConnect

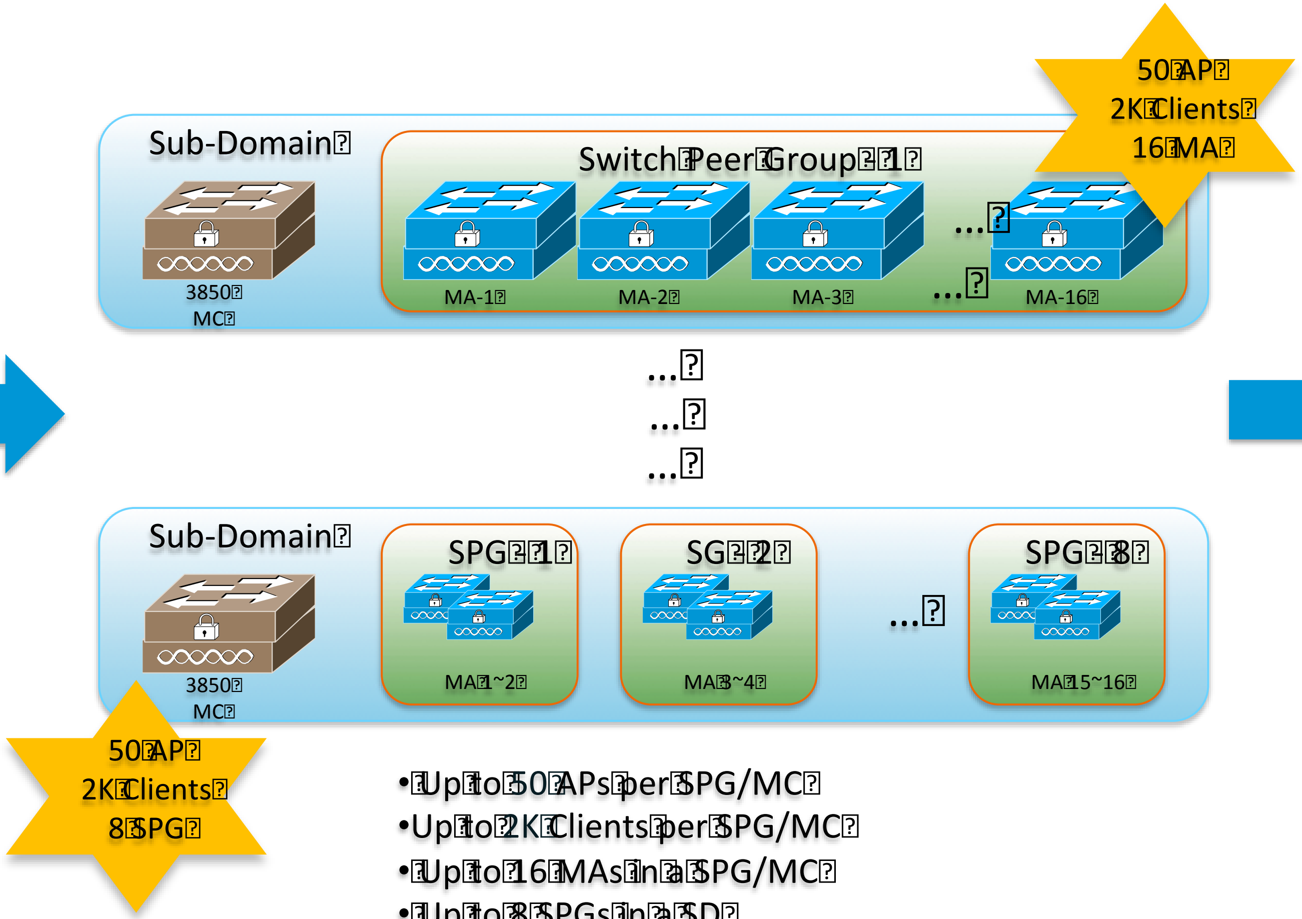
Scalability –
Converged Access – Using Catalyst 3850 as MC

Cat3850
MA
Cat3850
MC

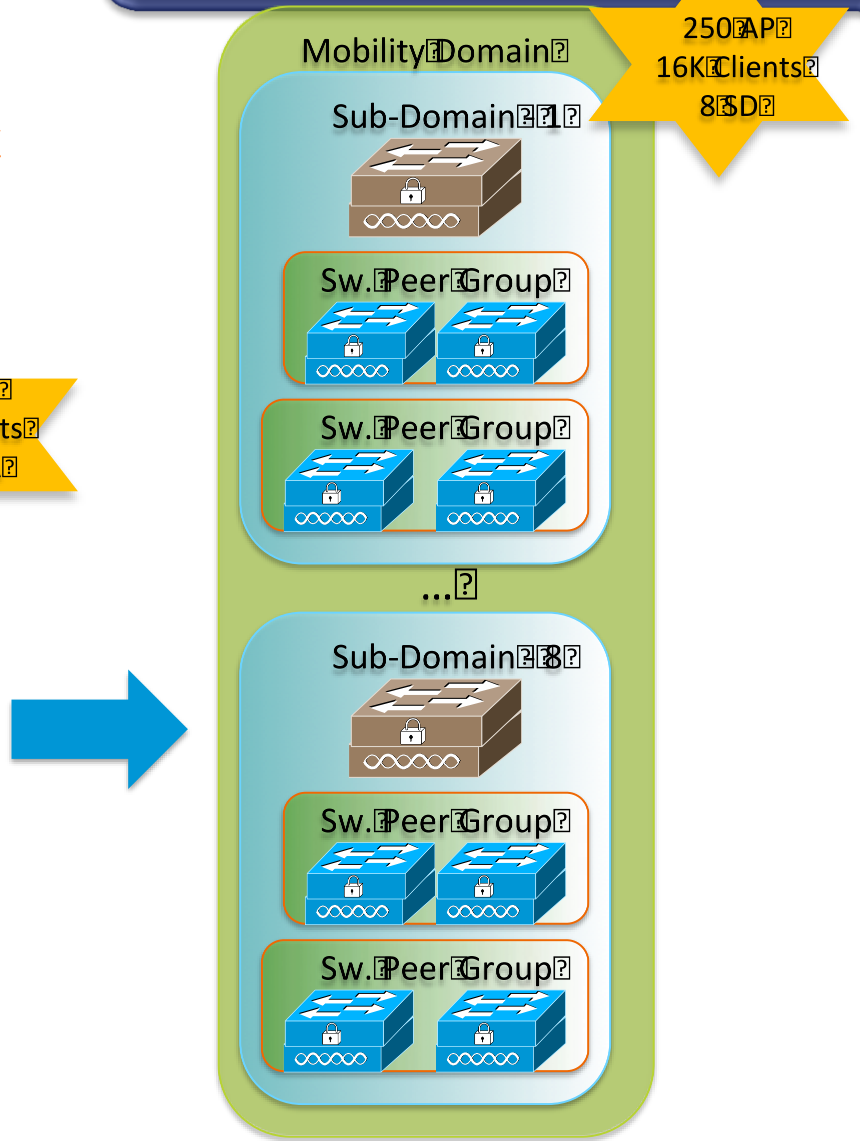
MA=Mobility Agent MC=Mobility Controller
SPG=Switch Peer Group SD=Sub-Domain



- 1 MC=1 SD
- Up to 50 APs
- Up to 2K Clients
- Up to 40G I/O for AP Traffic



- Up to 50 APs per SPG/MC
- Up to 2K Clients per SPG/MC
- Up to 16 MAs in a SPG/MC
- Up to 8 SPGs in a SD
- Up to 50G I/O for AP Traffic

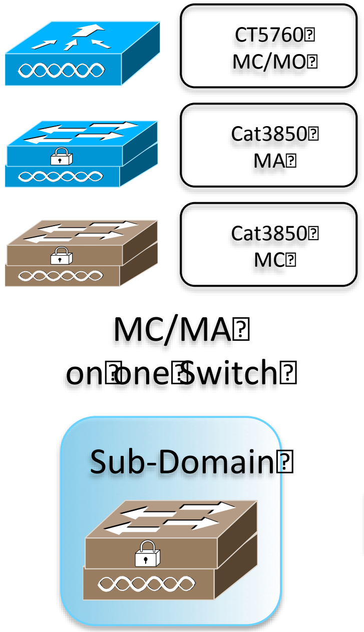


- Up to 250 APs per MD
- Up to 8 SDs per MD
- Up to 128 MAs per MD
- Up to 16K Clients per MD
- Up to 250G I/O for AP Traffic

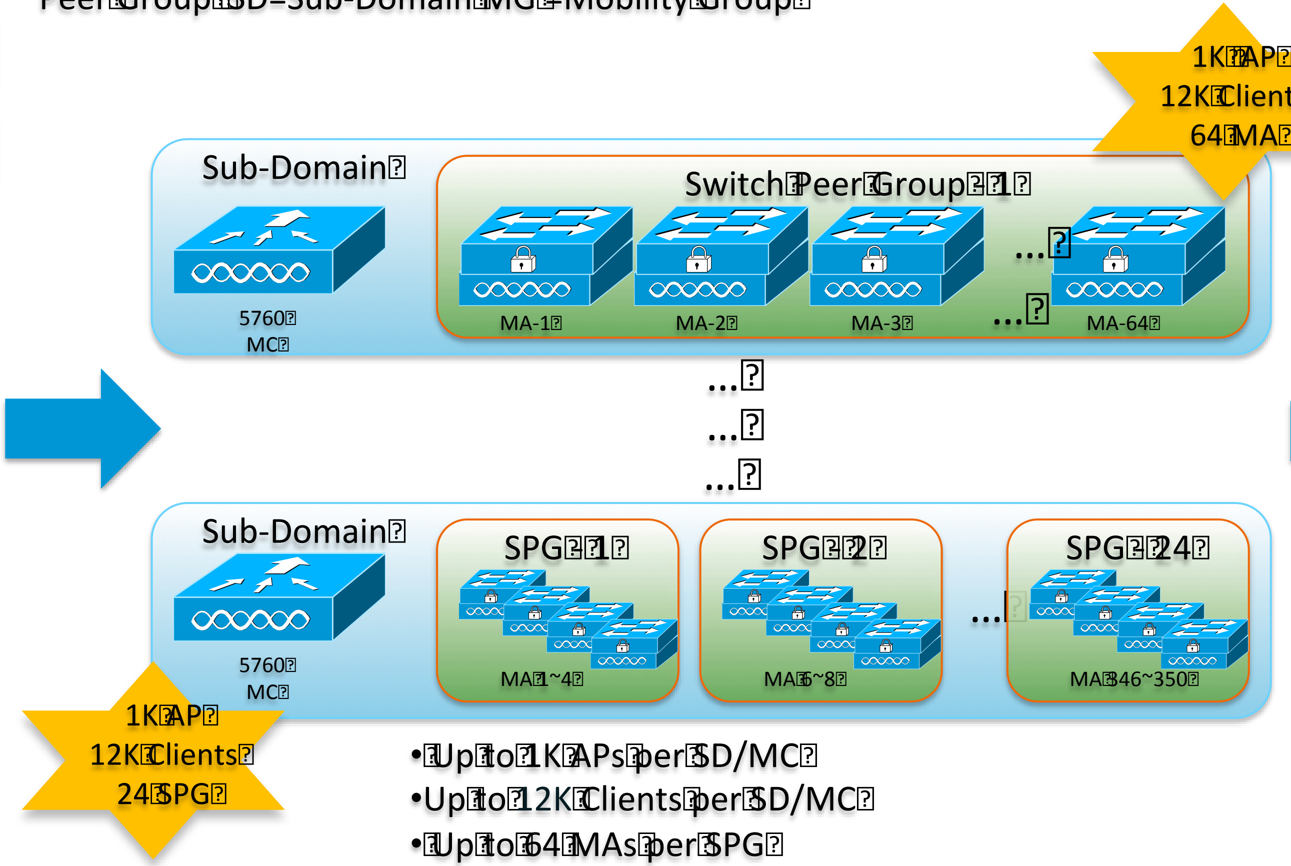
Scalability –

Converged Access – 5760 as MC, 3850s as MAs

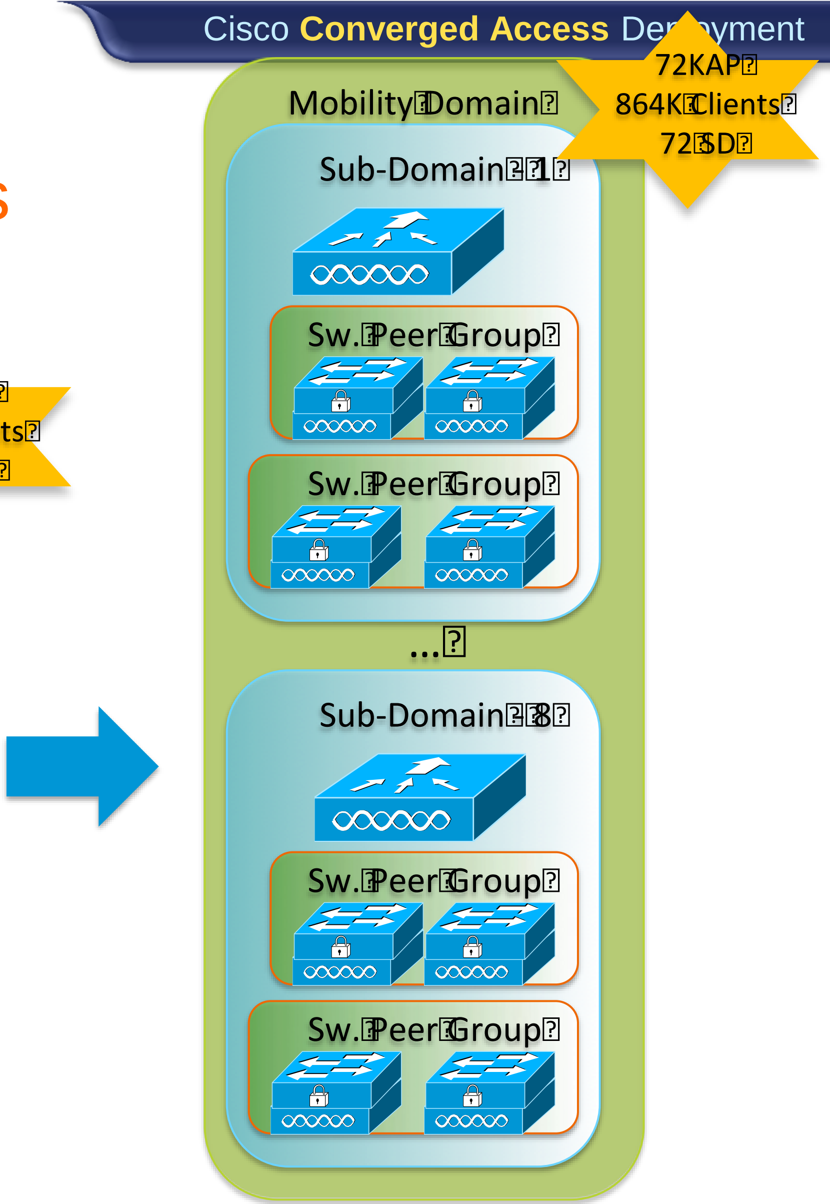
MA=Mobility Agent MC=Mobility Controller SPG=Switch Peer Group SD=Sub-Domain MG=Mobility Group



- 1 MC=1 SD
- Up to 50 APs
- Up to 2K Clients
- Up to 40GB I/O for AP Traffic



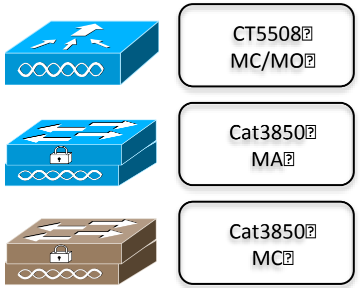
- Up to 1K APs per SD/MC
- Up to 12K Clients per SD/MC
- Up to 64 MAs per SPG
- Up to 24 SPGs per SD/MC
- Up to 24 SD/MC per MG
- Up to 350 MAs per SD/MC
- Up to 1TB I/O for AP Traffic



- Up to 72K APs per MD
- Up to 864K Clients per MD
- Up to 72 SD per MD
- Up to 25,200 MAs per MD
- Up to 72TB I/O for AP Traffic

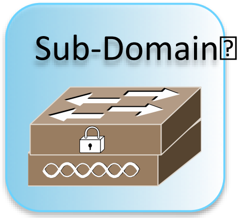
Scalability –

Converged Access – 5508 as MC, 3850s as MAs

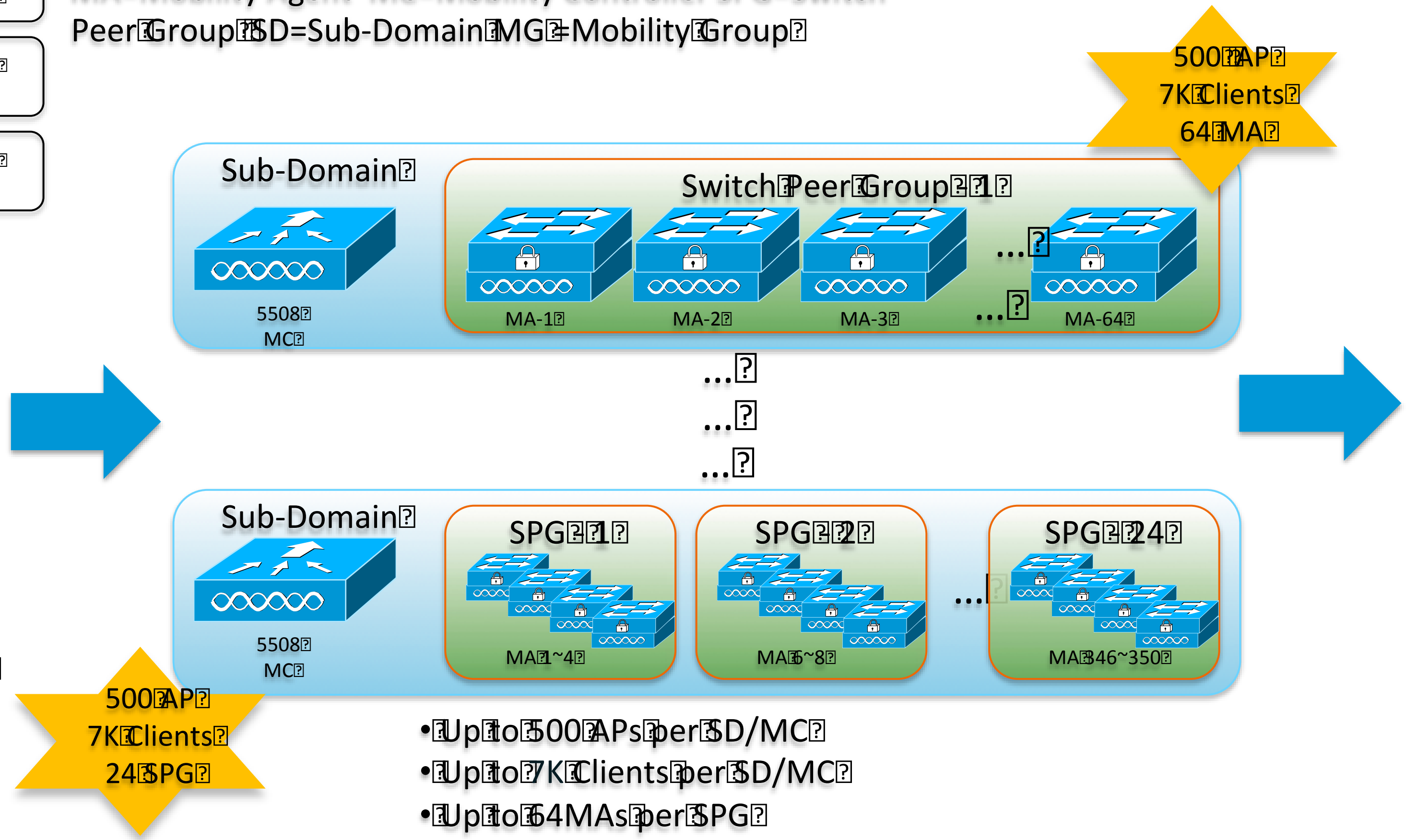


MA=Mobility Agent MC=Mobility Controller SPG=Switch Peer Group SD=Sub-Domain MG=Mobility Group

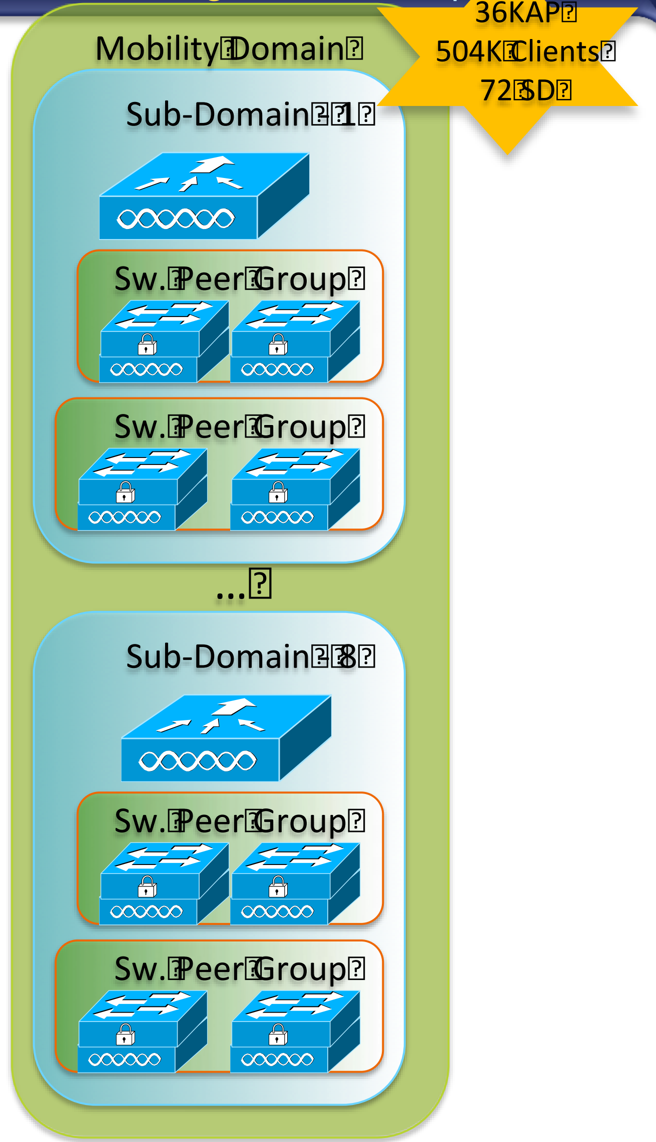
MC/MA on one Switch



- 1 MC=1 SD
- Up to 50 APs
- Up to 2K Clients
- Up to 40GB I/O for AP Traffic



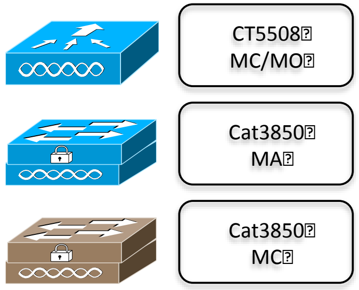
- Up to 500 APs per SD/MC
- Up to 7K Clients per SD/MC
- Up to 64 MAs per SPG
- Up to 24 SPGs per SD/MC
- Up to 24 SD/MC per MG
- Up to 350 MAs per SD/MC
- Up to 500GB I/O for AP Traffic



- Up to 36K APs per MD
- Up to 504K Clients per MD
- Up to 72 SD per MD
- Up to 25,200 MAs per MD
- Up to 36TB I/O for AP Traffic

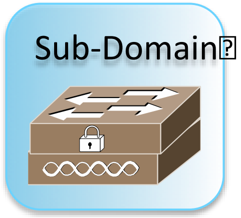
Scalability –

Converged Access – WiSM2 as MC, 3850s as MAs

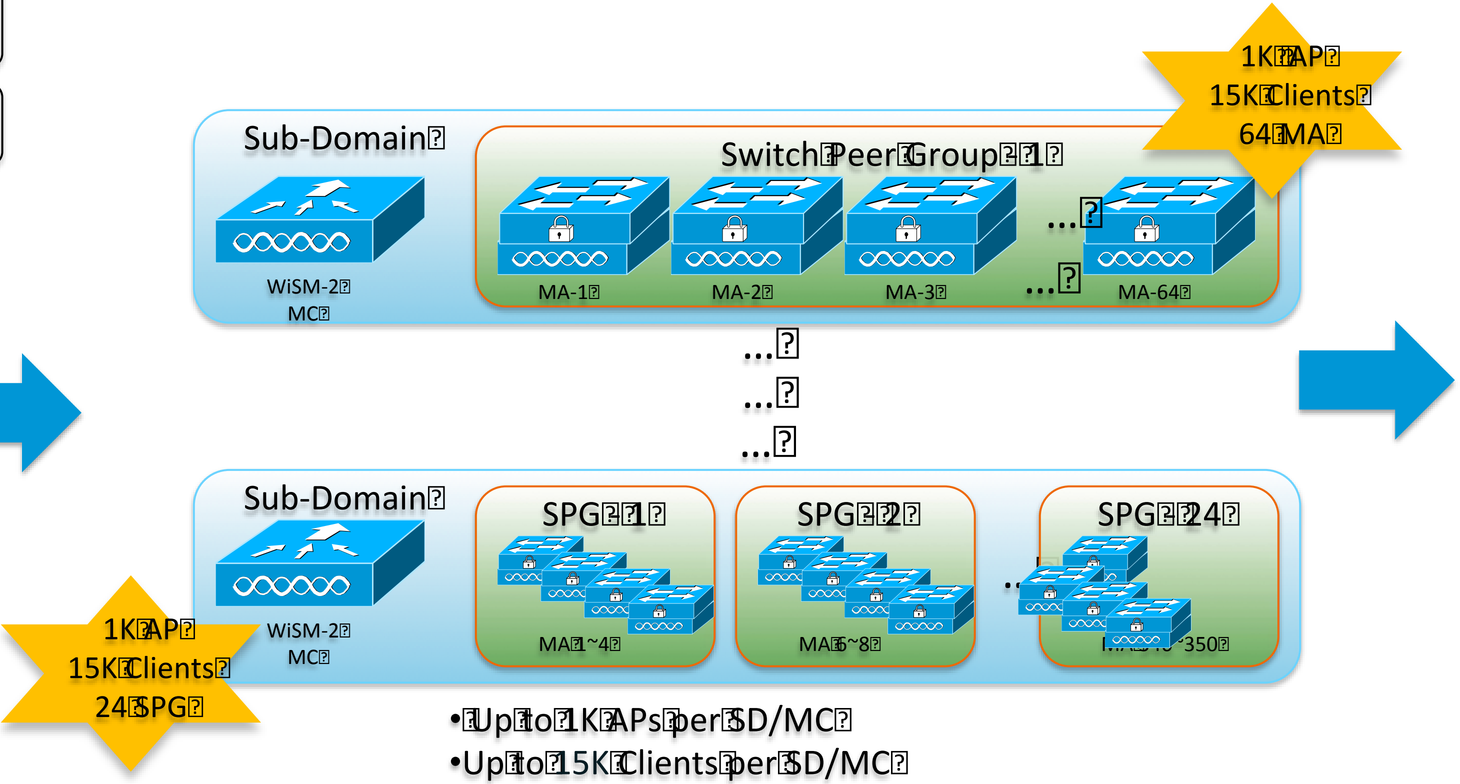


MA=Mobility Agent MC=Mobility Controller SPG=Switch Peer Group SD=Sub-Domain MG=Mobility Group

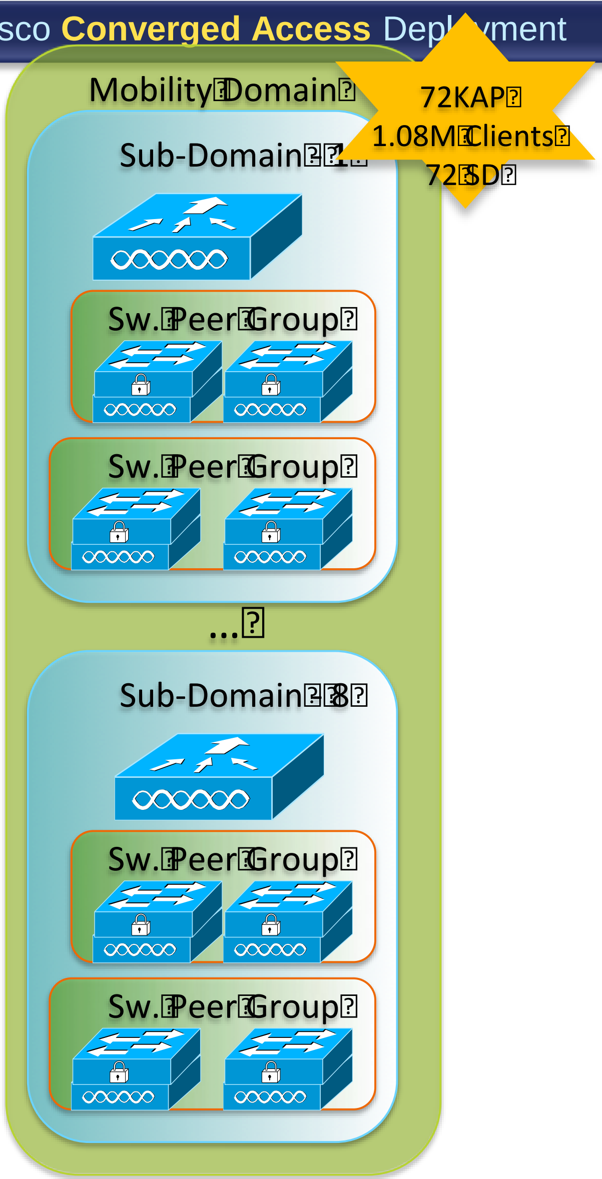
MC/MA on one Switch



- 1 MC=1 SD
- Up to 50 APs
- Up to 2K Clients
- Up to 40GB I/O for AP Traffic



- Up to 1K APs per SD/MC
- Up to 15K Clients per SD/MC
- Up to 16 MAs per SPG
- Up to 24 SPGs per SD/MC
- Up to 24 SD/MC per MG
- Up to 350 MAs per SD/MC
- Up to 1TB I/O for AP Traffic



- Up to 72K APs per MD
- Up to 1.08M Clients per MD
- Up to 72 SD per MD
- Up to 25,200 MAs per MD
- Up to 72TB I/O for AP Traffic

REFERENCE MATERIAL

CATALYST 3850-BASED MCS – ROAMING DETAILS

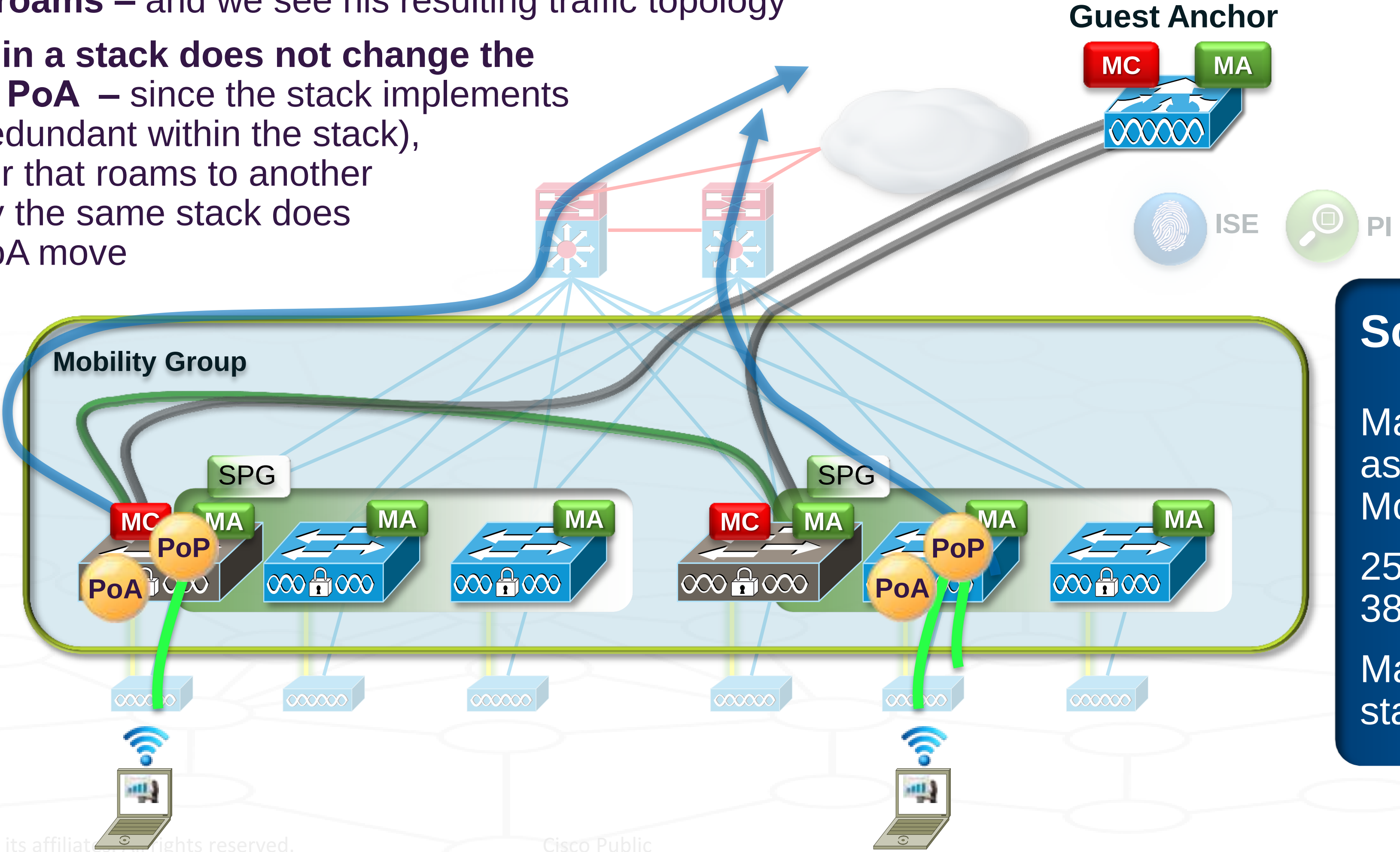
Converged Access –

Catalyst 3850-based MCs – Roaming, within a Stack

Roaming, within a Stack (3850 Switches as MCs) –

- **Initially, all clients in this example are on their initial, local Converged Access switches**
- **Now, a client roams –** and we see his resulting traffic topology
- **Roaming within a stack does not change the user's PoP or PoA –** since the stack implements a single MA (redundant within the stack), and thus a user that roams to another AP serviced by the same stack does not cause a PoA move

No change to user's PoP or PoA



Scalability –

Max of 8 x 3850 switches as MCs, grouped into a Mobility Group

250 APs total across all 3850 MCs

Max. 50 APs per 3850 stack / SPG

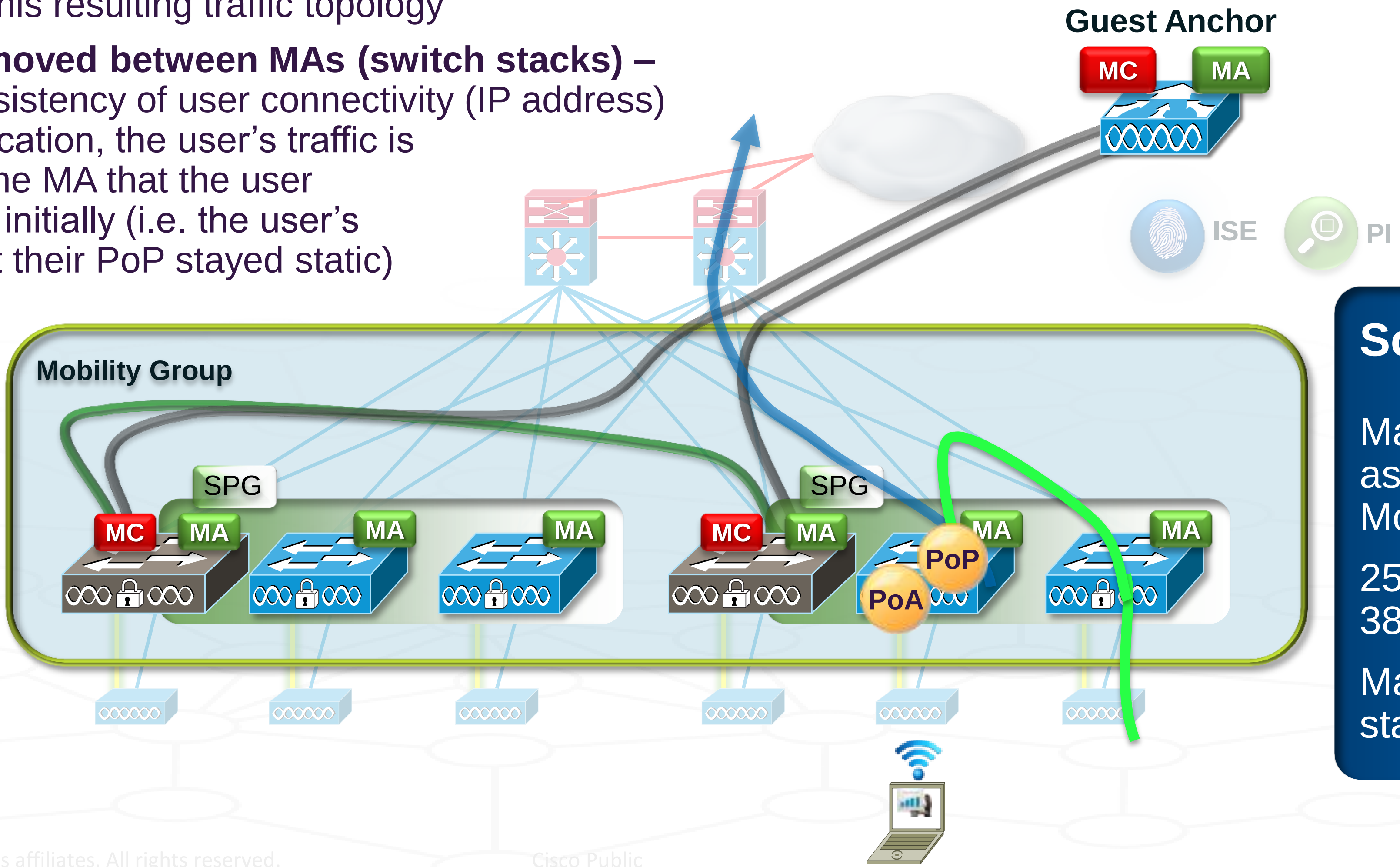
Converged Access –

Catalyst 3850-based MCs – Roaming, within an SPG

Roaming, within a Switch Peer Group (3850 Switches as MCs) –

- **Now, the client roams to an AP serviced by another switch stack (within the same SPG)**
- **Let's examine** his resulting traffic topology
- **The user has moved between MAs (switch stacks) –** to maintain consistency of user connectivity (IP address) and policy application, the user's traffic is transported to the MA that the user associated with initially (i.e. the user's PoA moved, but their PoP stayed static)

Most Common Roaming Case



Scalability –

Max of 8 x 3850 switches as MCs, grouped into a Mobility Group

250 APs total across all 3850 MCs

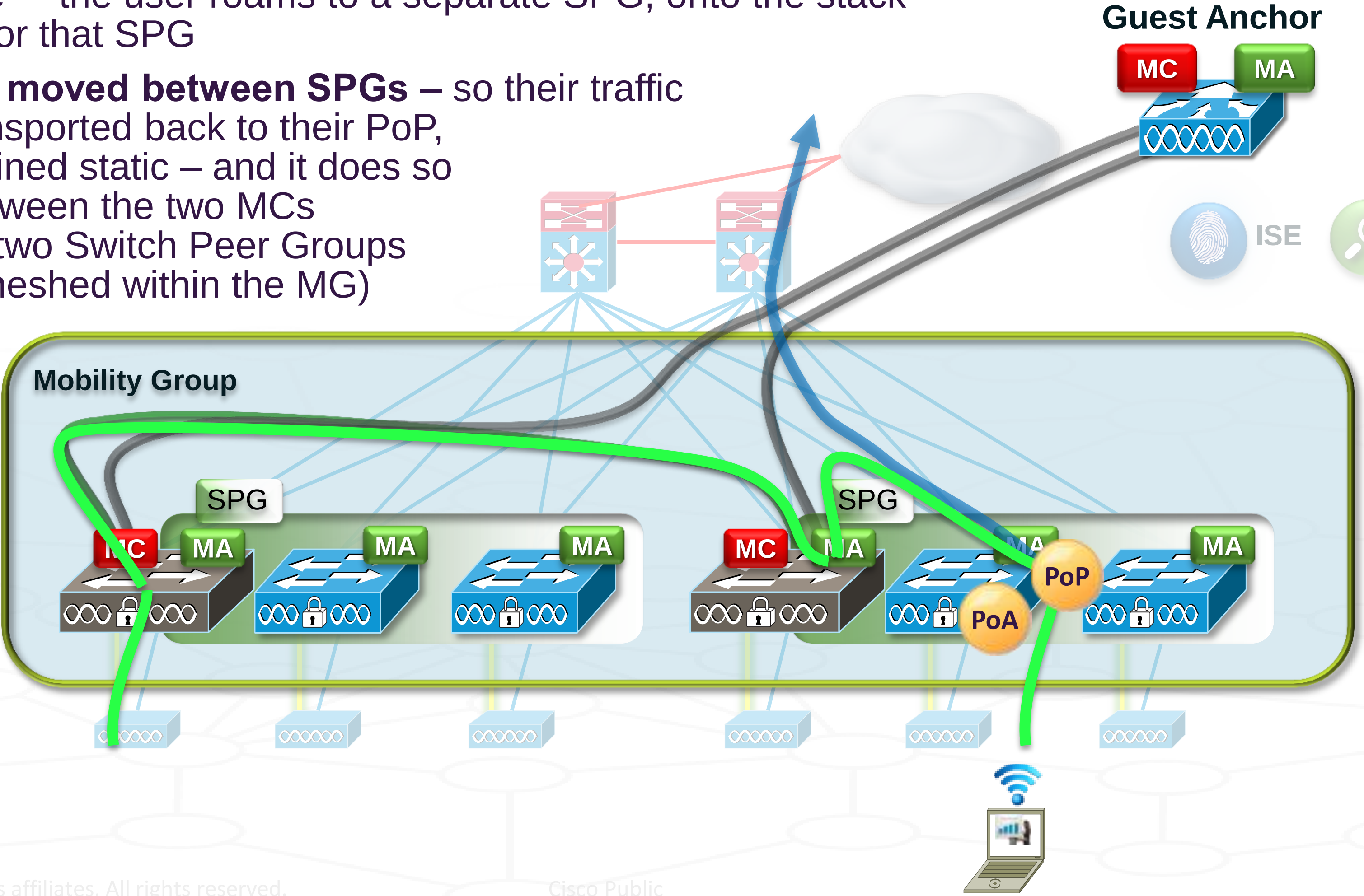
Max. 50 APs per 3850 stack / SPG

Converged Access –
Catalyst 3850-based MCs – Roaming, across SPGs

Roaming, across Switch Peer Groups (3850 Switches as MCs) –

- **Now, let's examine a more complex roam where the user roams across SPGs**
- **In this example – **the user roams to a separate SPG, onto the stack serving as MC for that SPG
- **The user's has moved between SPGs –** so their traffic needs to be transported back to their PoP, which has remained static – and it does so by transiting between the two MCs servicing these two Switch Peer Groups (MCs are fully meshed within the MG)

Roaming between SPGs (geographically-separated)



Scalability –

Max of 8 x 3850 switches as MCs, grouped into a Mobility Group

250 APs total across all 3850 MCs

Max. 50 APs per 3850 stack / SPG

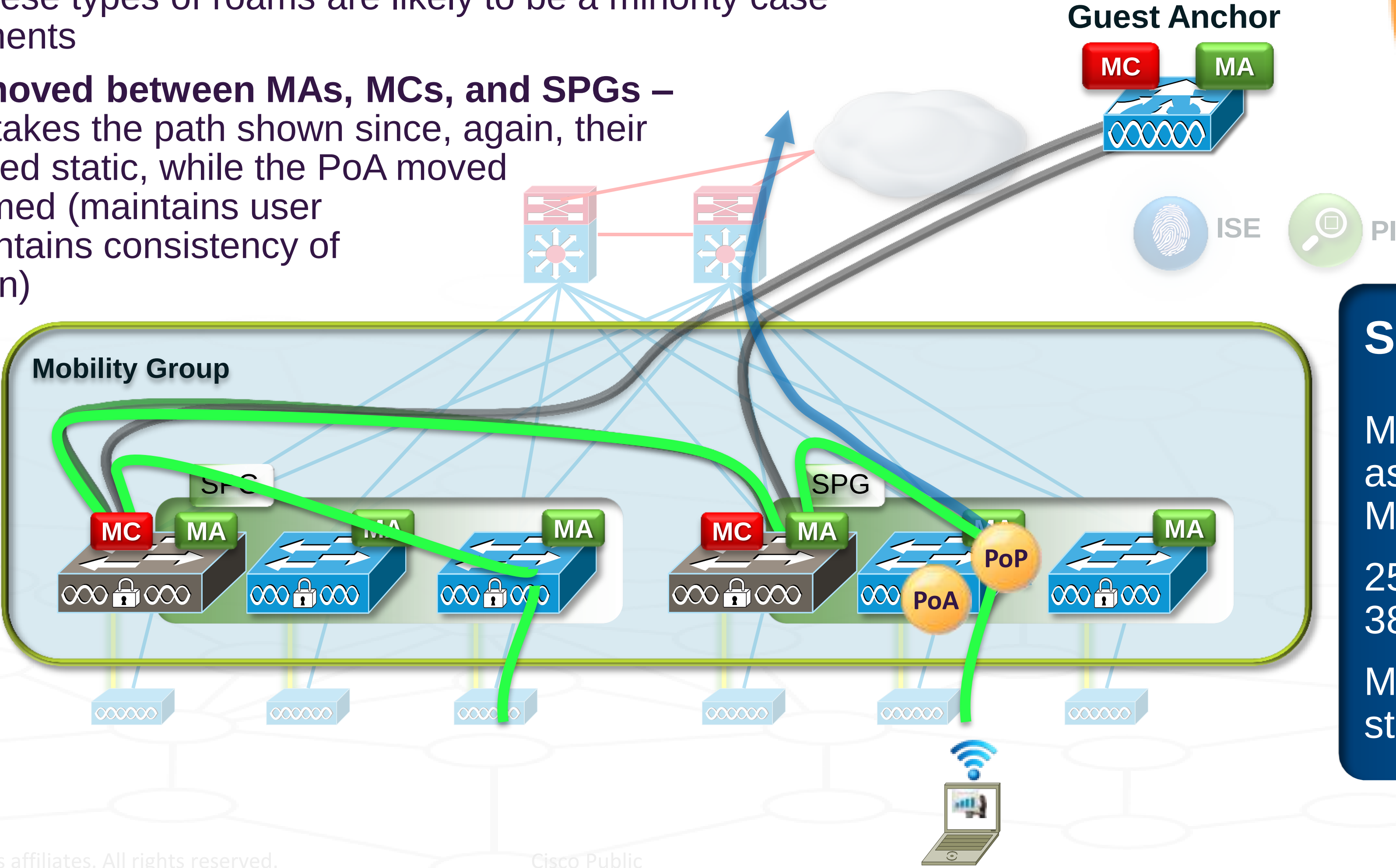
Converged Access –

Catalyst 3850-based MCs – Roaming, across SPGs & MCs

Roaming, across Switch Peer Groups and MCs (3850 Switches as MCs) –

- **Now, lets' examine the most complex type of roam – across SPGs and MCs / MAs**
- **Remember –** these types of roams are likely to be a minority case in most deployments
- **The user has moved between MAs, MCs, and SPGs –** and their traffic takes the path shown since, again, their PoP has remained static, while the PoA moved as the user roamed (maintains user IP address, maintains consistency of policy application)

Roaming between SPGs and MCs (geographically-separated)



Scalability –

Max of 8 x 3850 switches as MCs, grouped into a Mobility Group

250 APs total across all 3850 MCs

Max. 50 APs per 3850 stack / SPG

REFERENCE MATERIAL

LOBBY ISSUE / SOLUTION

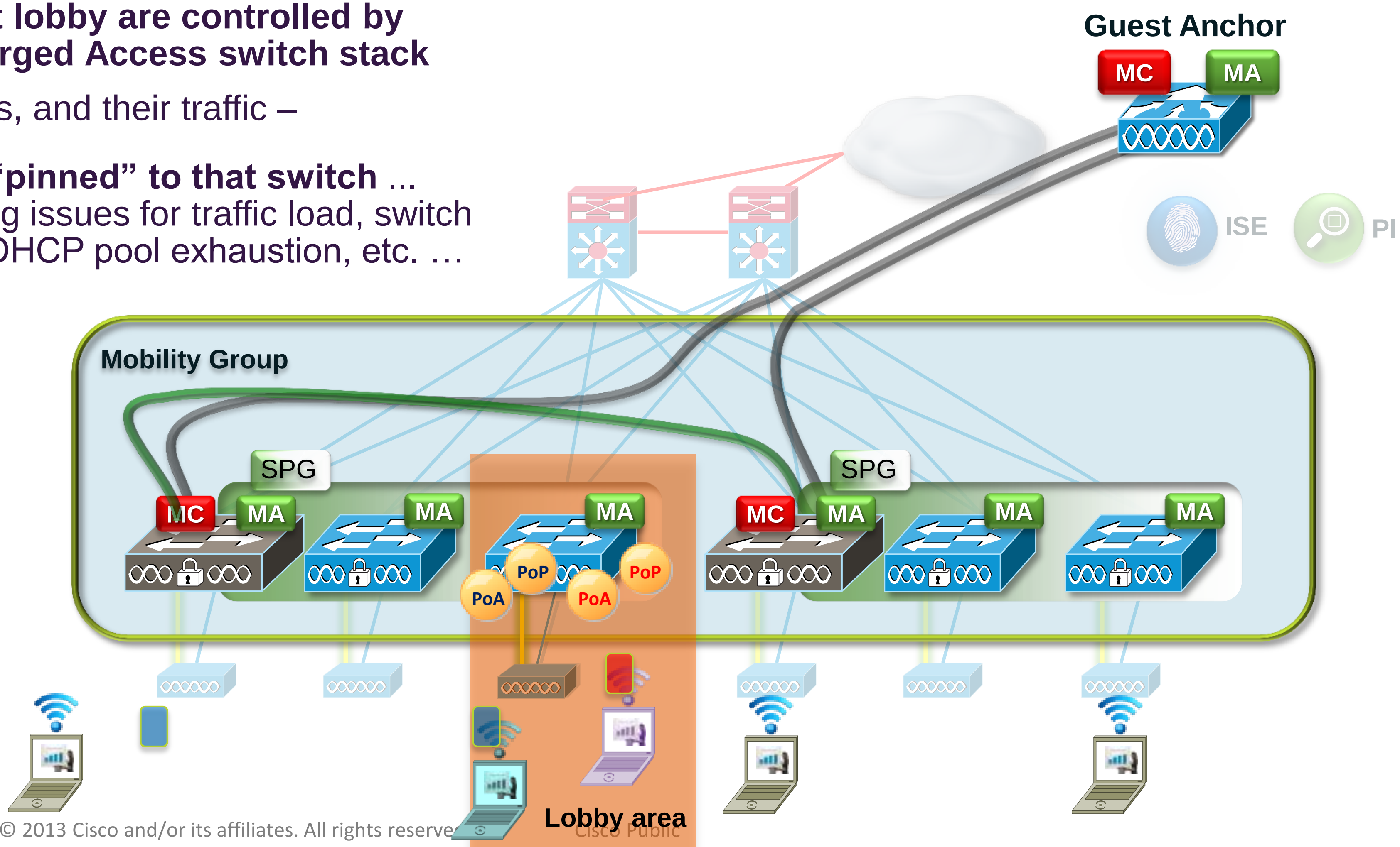
Converged Access –

Common Building Access – The “Lobby Issue”

What happens when –

- **Everyone enters the building** via a common lobby
- **APs in that lobby are controlled by one Converged Access switch stack**
- All the users, and their traffic –
  - **Gets “pinned” to that switch …** causing issues for traffic load, switch load, DHCP pool exhaustion, etc. …

Many users could end up “staying in the lobby” logically

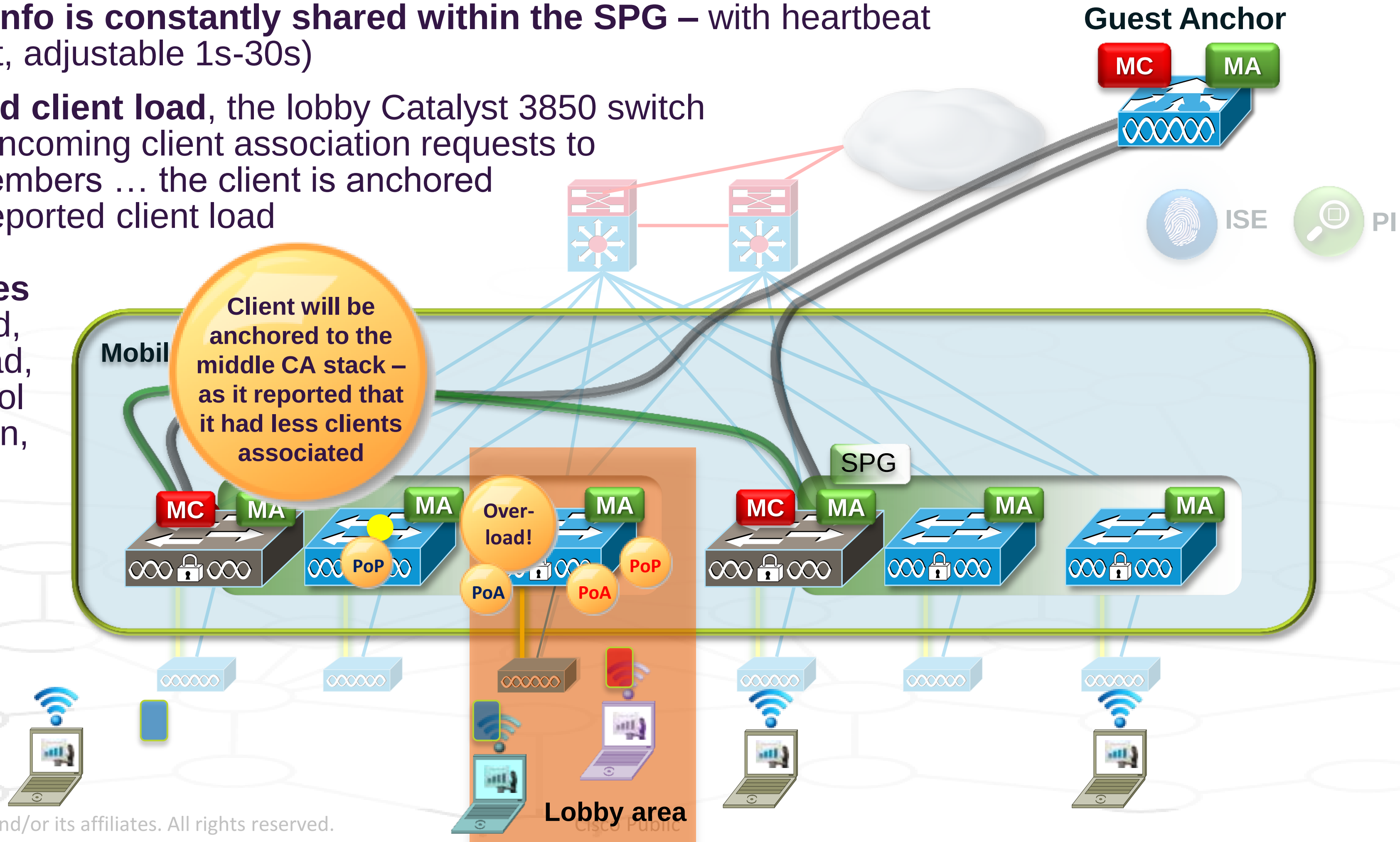


Converged Access –

Common Building Access – The “Lobby Solution”

What can we do to address this issue?

- **User client association can be distributed** across Converged Access switches in the Switch Peer Group
- **User load info is constantly shared within the SPG –** with heartbeat (10s default, adjustable 1s-30s)
- **At a defined client load**, the lobby Catalyst 3850 switch distributes incoming client association requests to it’s SPG members … the client is anchored based on reported client load
  - **Addresses** traffic load, switch load, DHCP pool exhaustion, etc.


Guest Anchor
MC
MA
ISE
PI
Mobil
Client will be anchored to the middle CA stack – as it reported that it had less clients associated
MC
MA
MA
Over-load!
MA
PoP
PoA
PoA
PoP
SPG
MC
MA
MA
MA
Lobby area

Converged Access –

Common Building Access – The “Lobby Solution”, Detail

- **What**: when configured, the client first PoA is load balanced across the switches in the SPG. When the client joins, the switch checks if its load is over a configurable threshold and send a message to anchor the client to least loaded switch in the SPG.
- **Why**: large number of clients could potentially attach to a single MA whose APs are situated close to the front door / lobby. This would result into congestion at that home switch, whereas other MAs would be under-utilised. This is even worse if the client’s data path is anchored at the home switch.
- **How to configure it**: the feature is ON by DEFAULT and it’s possible to change the threshold value. By default is 50% (of the max client allowed)

  To configure a different threshold use the following command on a per MA basis –

```
3850(config)# wireless mobility load-balance threshold ?

 <100-2000>  Threshold value for number of clients that can be anchored locally
```