# Technical Deep Dive (Wireless)

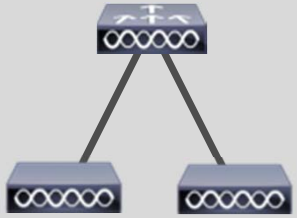
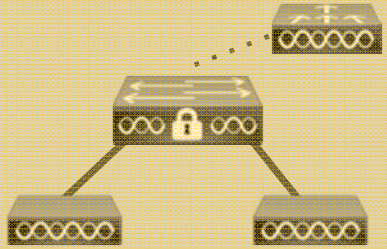
## Unified Access Roadshow Austria

**Seppi Dittli**
Consulting Systems Engineer
Borderless Mobility / Unified Access
EMEAR Central

13th March 2013 – Vienna
14th March 2013 – Linz

# One Network –
## Wireless Deployment Mode Options, Detail

| | Autonomous | FlexConnect | Centralized | Converged Access |
|---|---|---|---|---|
| |  Standalone APs |   Traffic Distributed at AP |  Traffic Centralized at Controller |  Traffic Distributed at Switch |
| **Target Positioning** | **Small Wireless Network** | **Branch** | **Campus** | **Branch and Campus** |
| **Purchase Decision** | Wireless only | Wireless only | Wireless only | Wired and Wireless |
| **Benefits** | • Simple and cost-effective for small networks | • Highly scalable for large number of remote branches<br>• Simple wireless operations with DC hosted controller | • Simplified operations with centralized control for Wireless<br>• Wireless Traffic visibility at the controller | • Wired and Wireless common operations<br>• One Enforcement Point<br>• One OS (IOS)<br>• Traffic visibility at every network layer<br>• Performance optimized for 11ac |
| **Key Considerations** | • Limited RRM, no Rogue detection | • L2 roaming only<br>• WAN BW and latency requirements | • System throughput | • Catalyst 3850 in the access layer |

# Catalyst 3850 – Wireless Capabilities

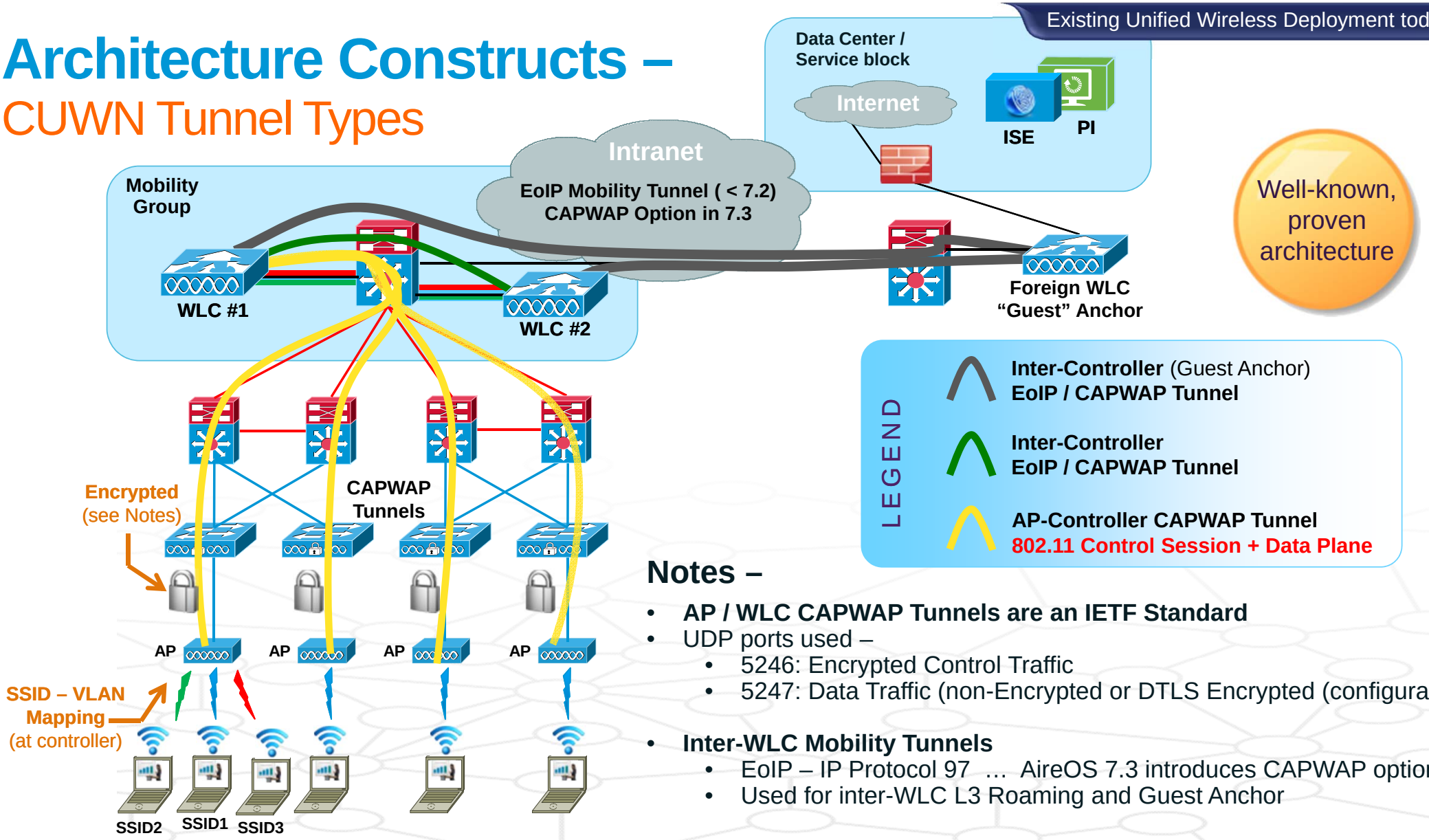
- CAPWAP termination and DTLS in Hardware
- 40G wireless capacity/switch
  - Capacity increases with members
- 50 APs and 2000 clients/switch stack
- Wireless switch peer group support for faster roaming: latency sensitive applications
- Supports IPv4 and IPv6 client mobility
- AP's must be directly connected to Catalyst 3850
- Requires IP Base license level for Wireless functionality



5

# Existing Wireless Deployments – Architecture Refresher

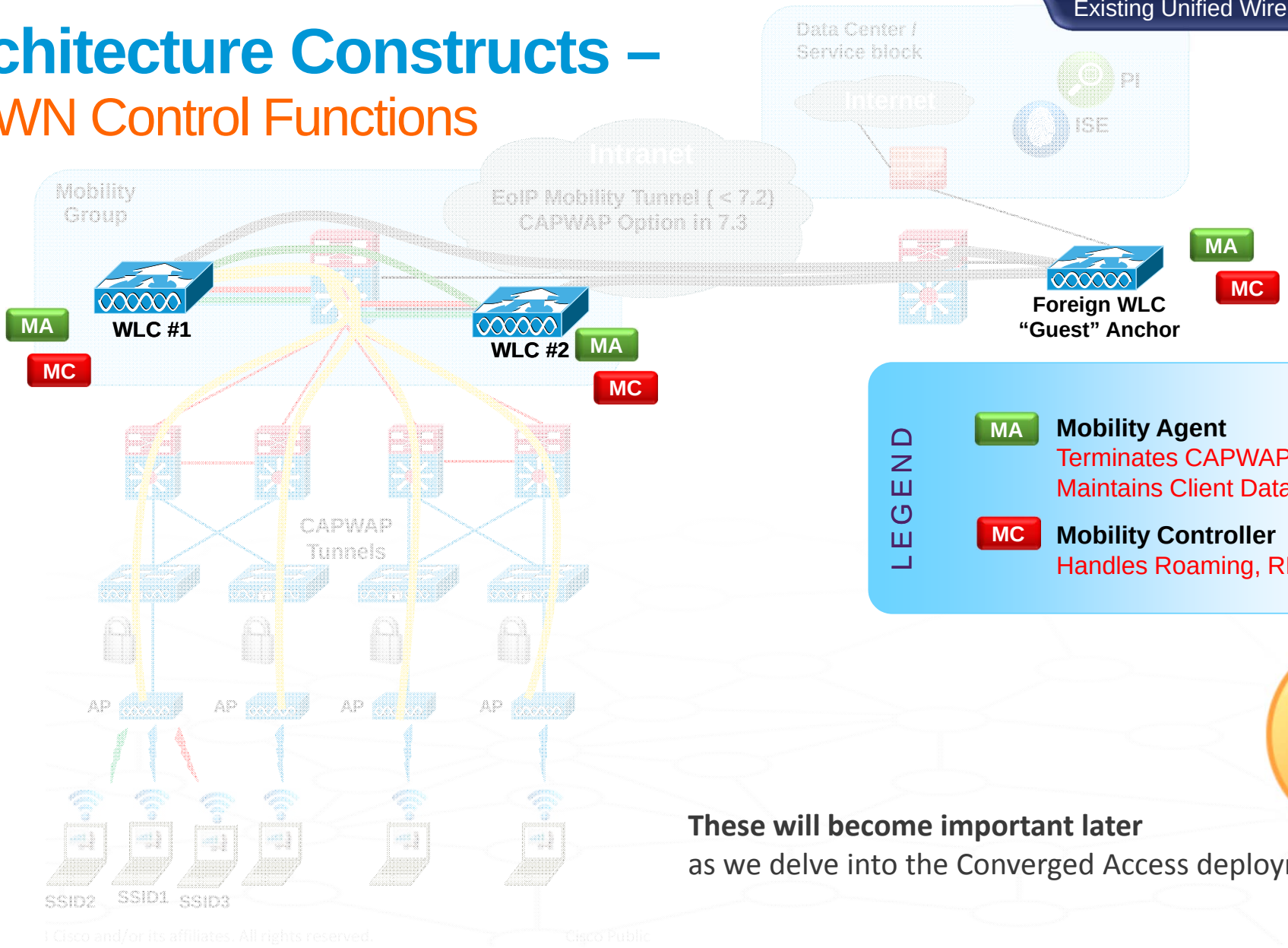
# Architecture Constructs –
## CUWN Tunnel Types




## Notes –

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

# Architecture Constructs –
## CUWN Control Functions




LEGEND

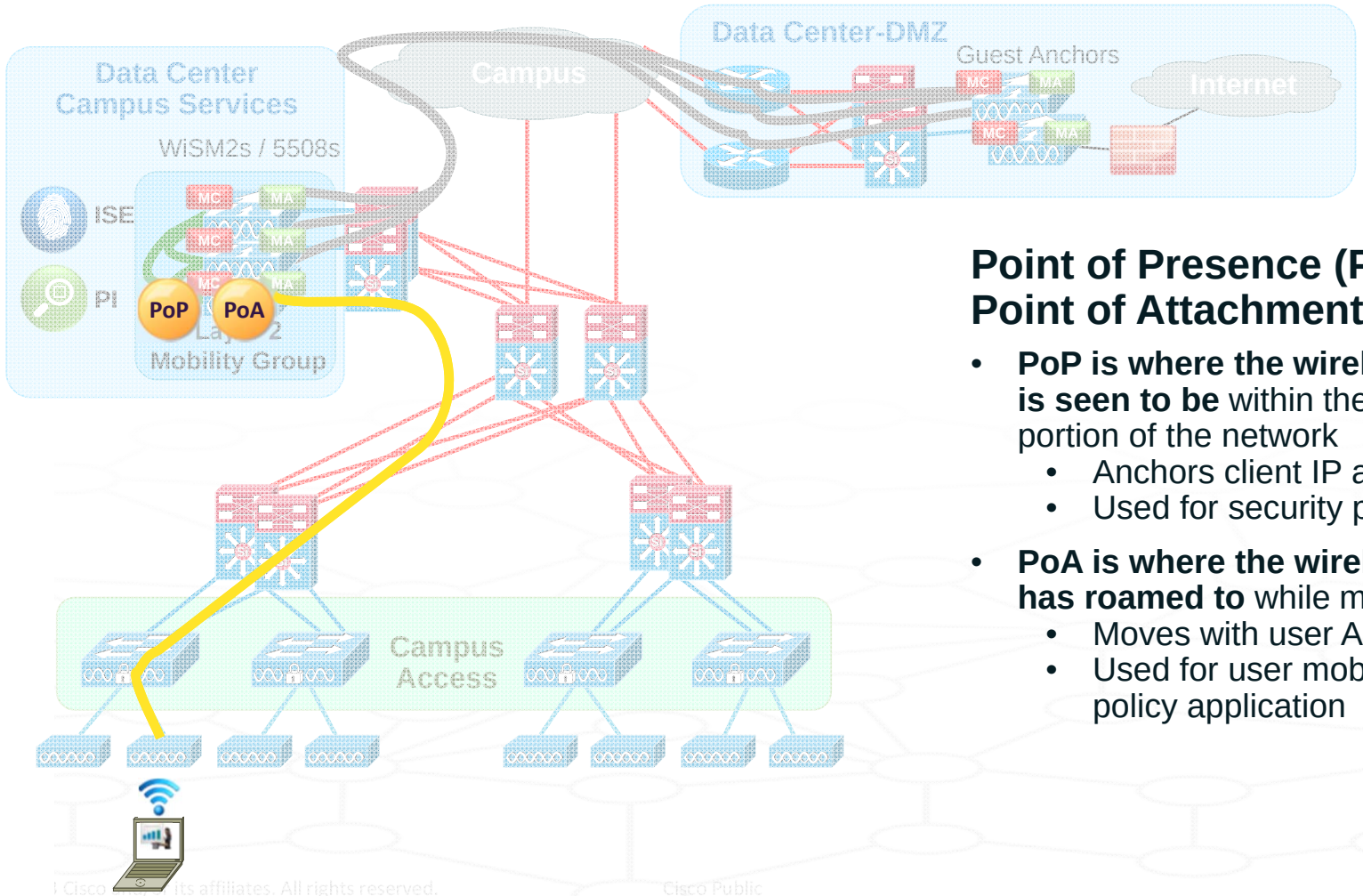
**MA** **Mobility Agent**
Terminates CAPWAP Tunnels, Maintains Client Database

**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)

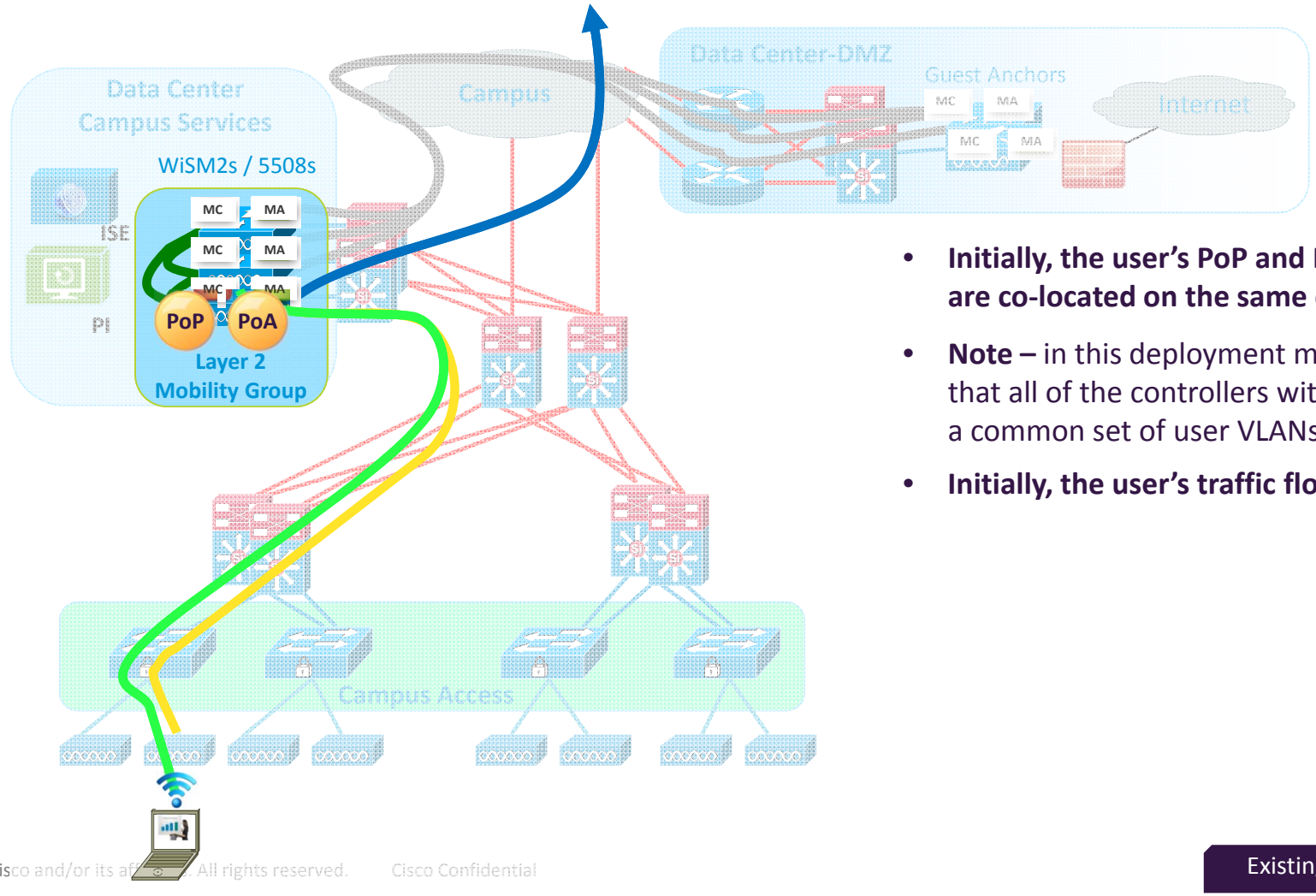



### Point of Presence (PoP) vs. Point of Attachment (PoA) –

- **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

# Existing Wireless Deployments – How does roaming work

# Architecture Constructs –
## Layer 2 Roaming (Campus Deployment)

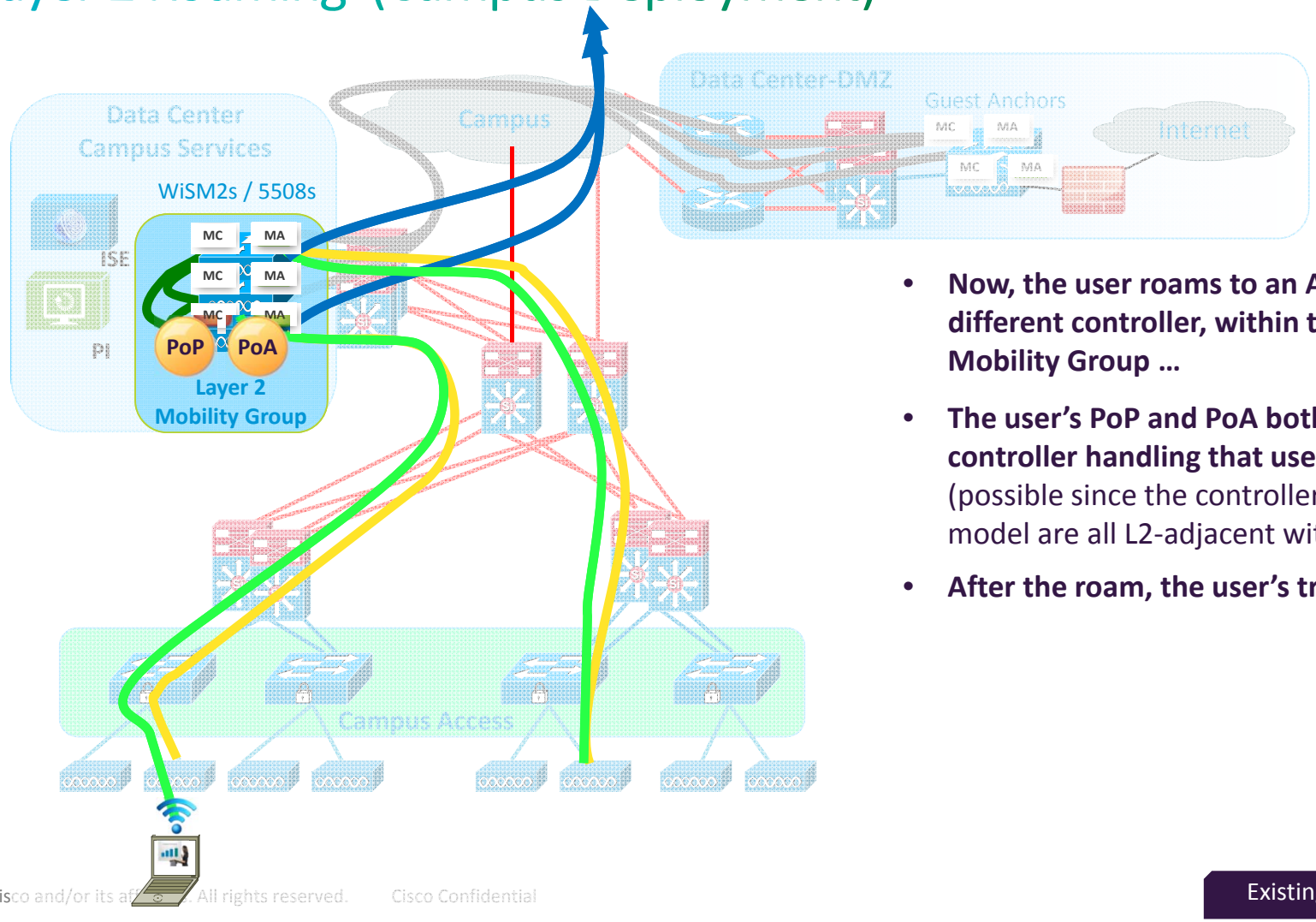



- **Initially, the user's PoP and PoA are co-located on the same controller**
- **Note –** in this deployment model, it is assumed that all of the controllers within the DC share a common set of user VLANs at Layer 2
- **Initially, the user's traffic flow is as shown …**




Existing Unified Wireless Deployment today …

# Architecture Constructs –
## Layer 2 Roaming (Campus Deployment)



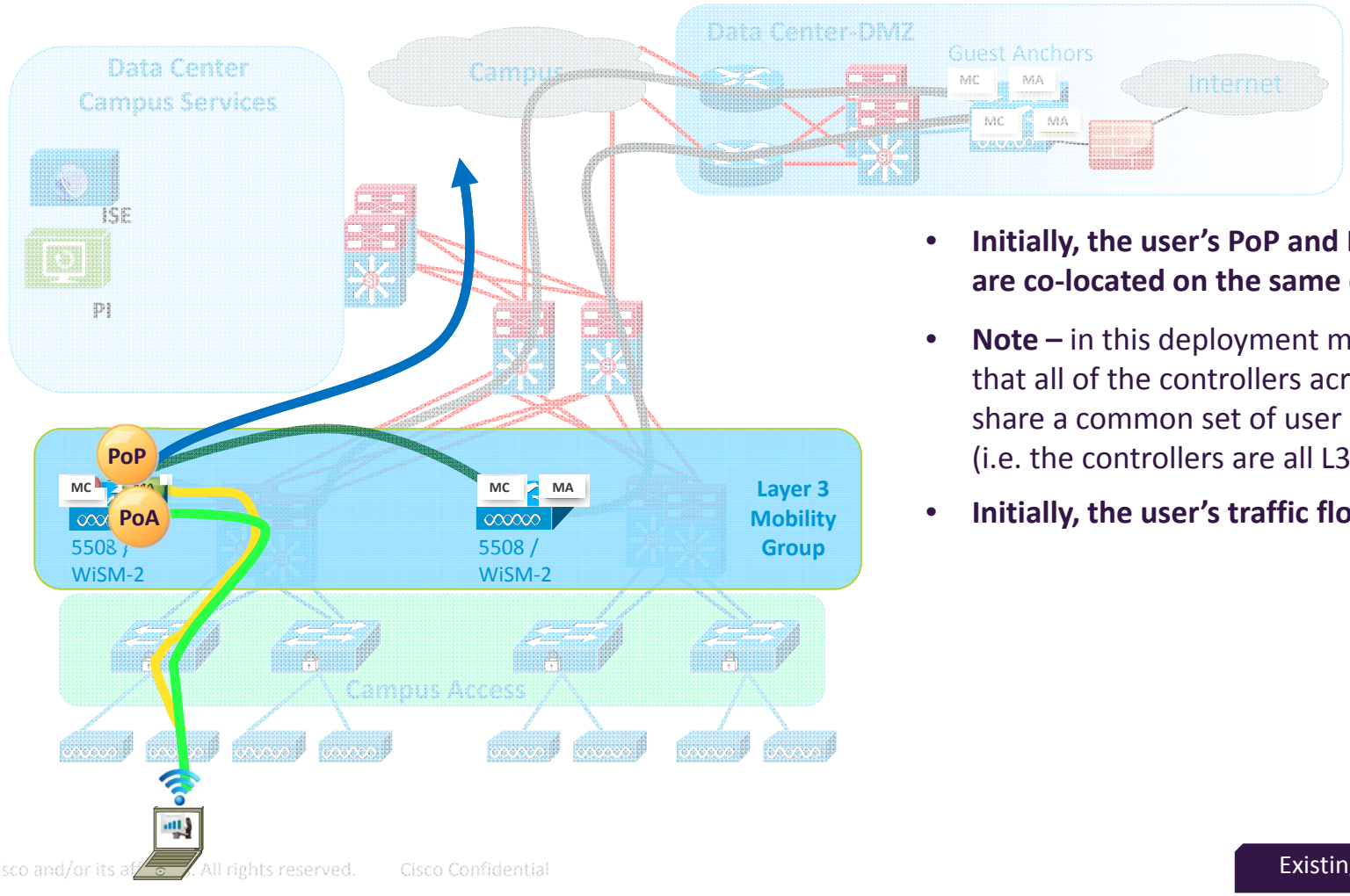

Move of the user's entire Mobility Context

- **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 …**




Existing Unified Wireless Deployment today …

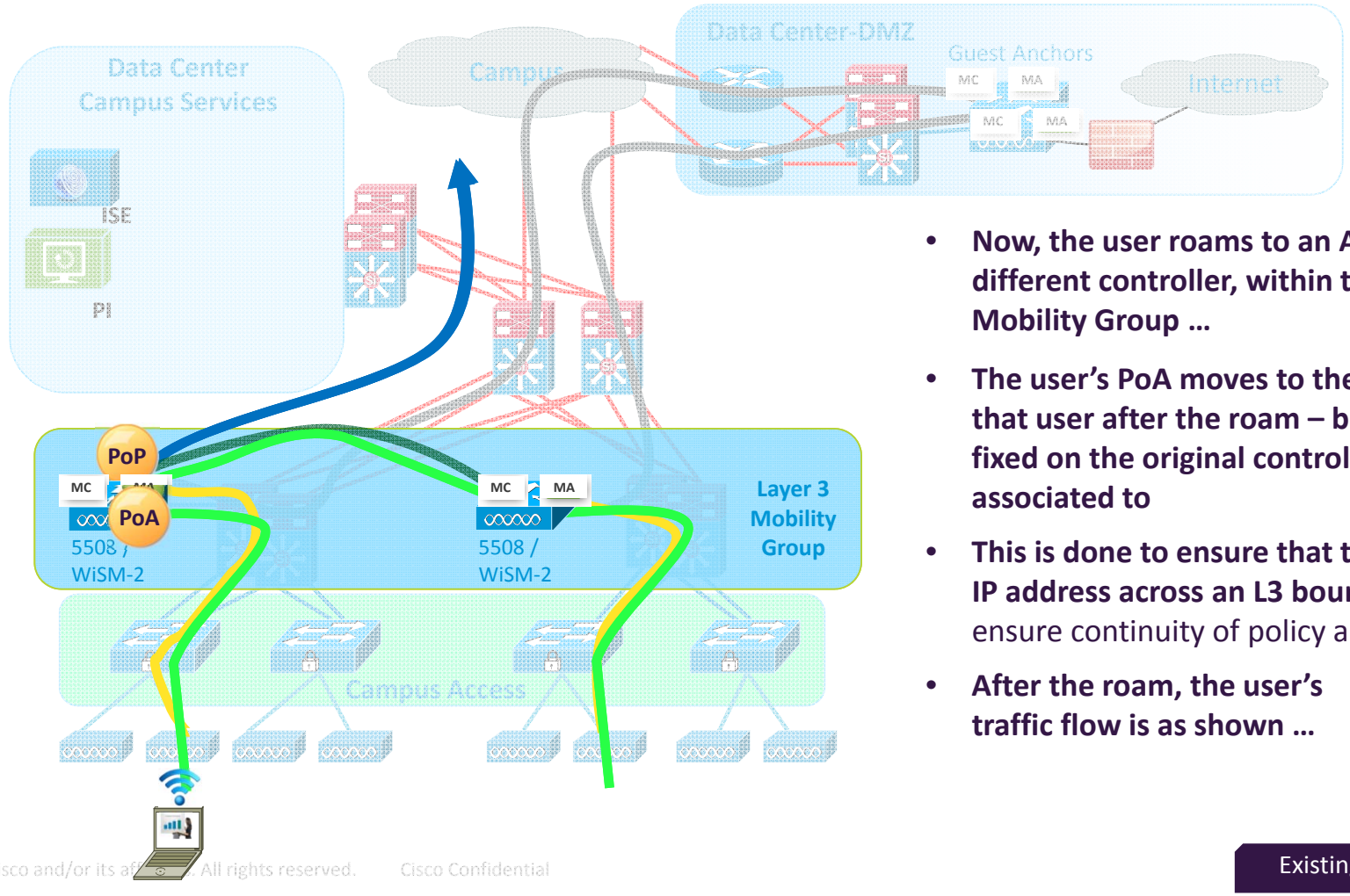
# Architecture Constructs –
## Layer 3 Roaming (Campus Deployment)




- **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 …**

Existing Unified Wireless Deployment today …

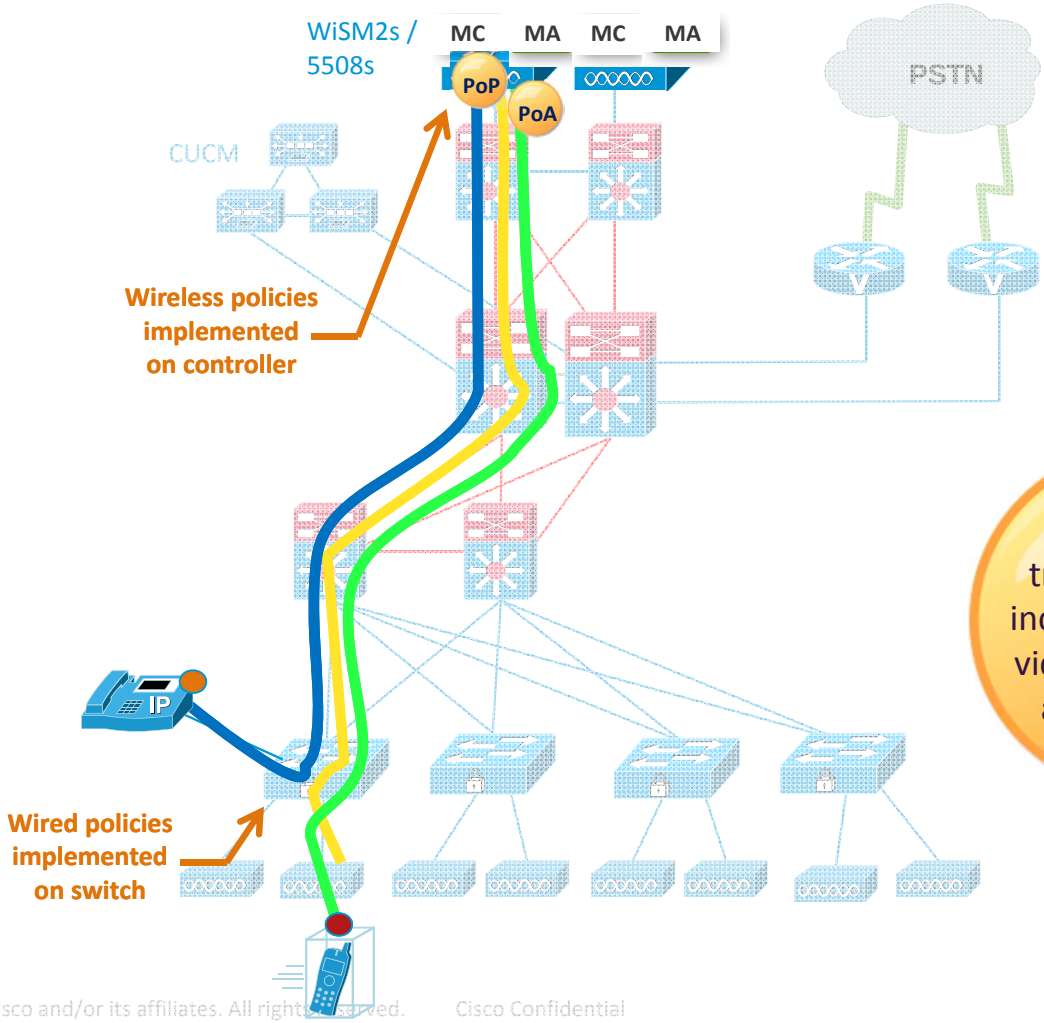
# Architecture Constructs –
## Layer 3 Roaming (Campus Deployment)




- **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 …**

Existing Unified Wireless Deployment today …

# Unified Wireless –
## Traffic Flow




**Separate policies and services** for wired and wireless users

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

### Traffic Flows, Unified Wireless –

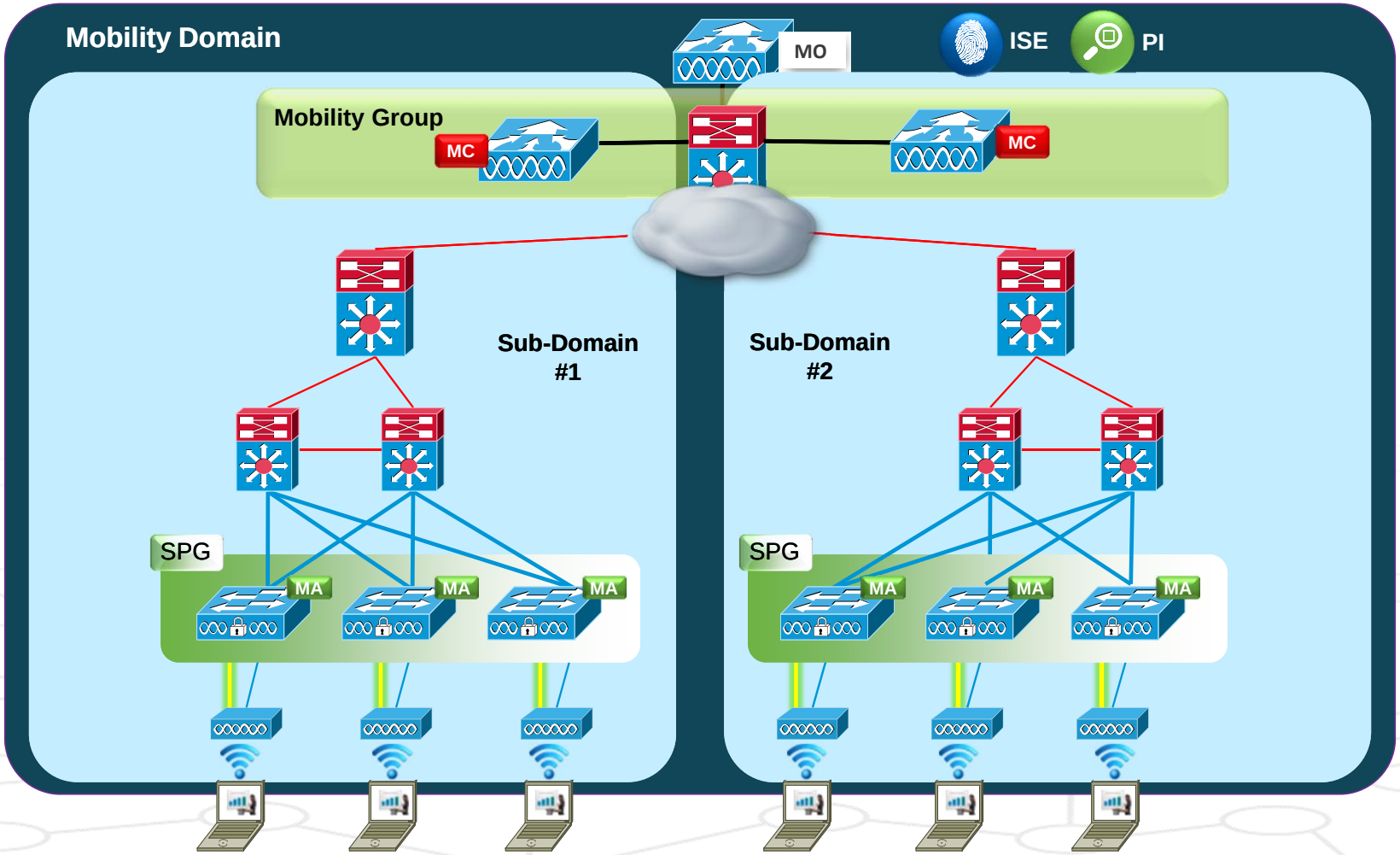
- In this example, a VoIP user is on today's CUWN network, and is making a call from a wireless handset to a wired handset …
- **We can see that all of the user's traffic needs to be hairpinned back through the centralized controller,** in both directions …

  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) …

Existing Unified Wireless Deployment today …

# Converged Access – Terminology and Building Blocks

# Converged Access –
## Deployment Overview



# Converged Access –
## Components – Physical vs. Logical Entities

**Physical Entities –**

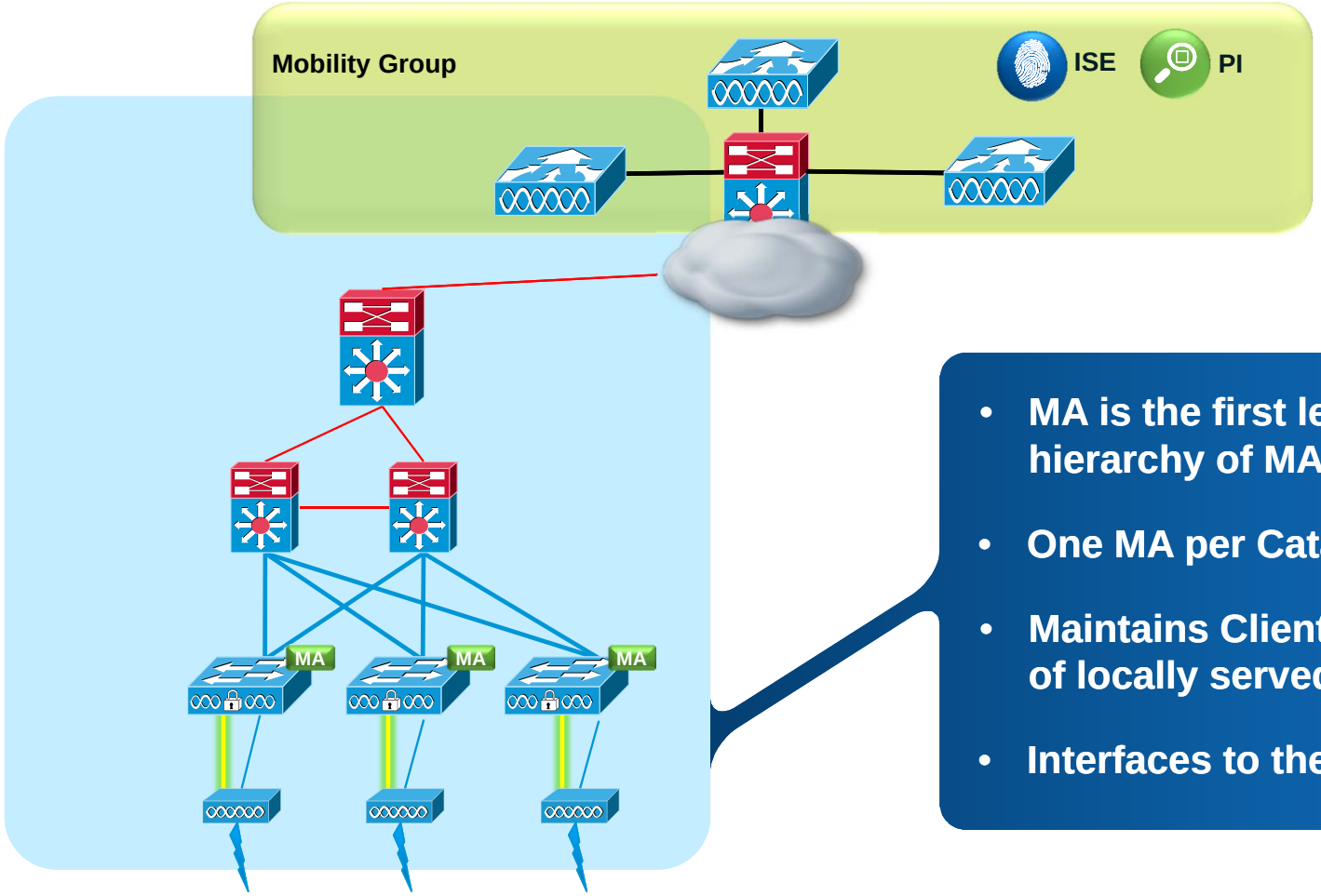
- **Mobility Agent (MA)** – Terminates CAPWAP tunnel from AP
- **Mobility Controller (MC)** – Manages mobility within and across Sub-Domains
- **Mobility Oracle (MO)** – Superset of MC,
  allows for Scalable Mobility Management within a Domain

**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) –** Localizes traffic for roams within Distribution Block

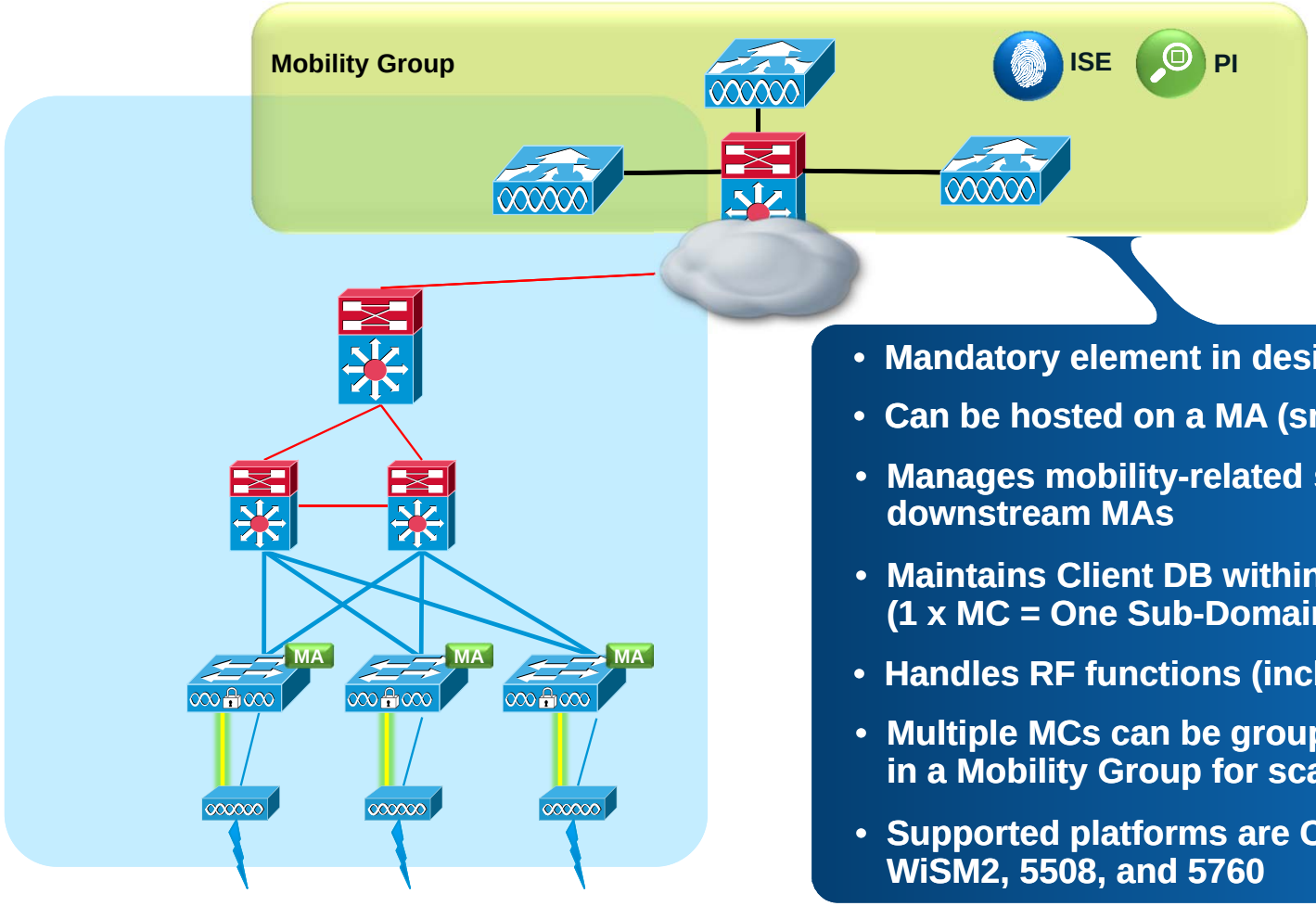
**MA, MC, Mobility Group functionality** all exist in today's controllers (4400, 5500, WiSM2)

# Converged Access –
## Physical Entities – Mobility Agents (MAs)




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

# Converged Access –
## Physical Entities – Mobility Controllers (MCs)




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

# Converged Access –
## Physical Entities – Catalyst 3850 Switch Stack

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

**MA**

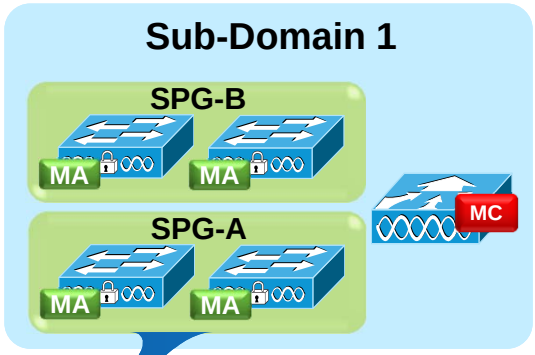
- Can act as a **Mobility Agent** (MA)
  for terminating CAPWAP tunnels for locally connected APs …

**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 synchronizes 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 optimize roaming capabilities and performance

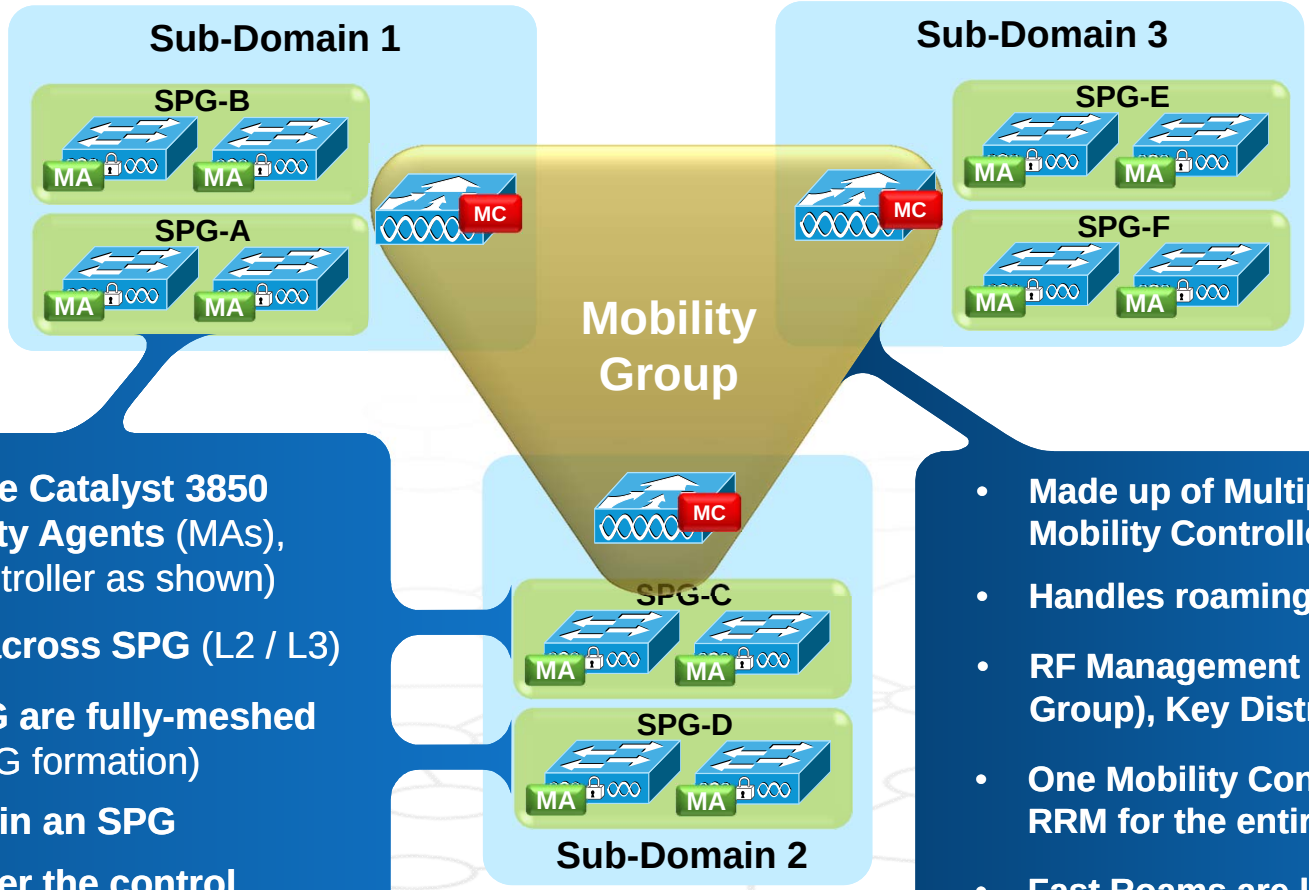
Current thinking on best practices dictates that **SPGs will likely be built around buildings, around floors within a building, or other areas that users are likely to roam most within**

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 optimized for scalability and roaming

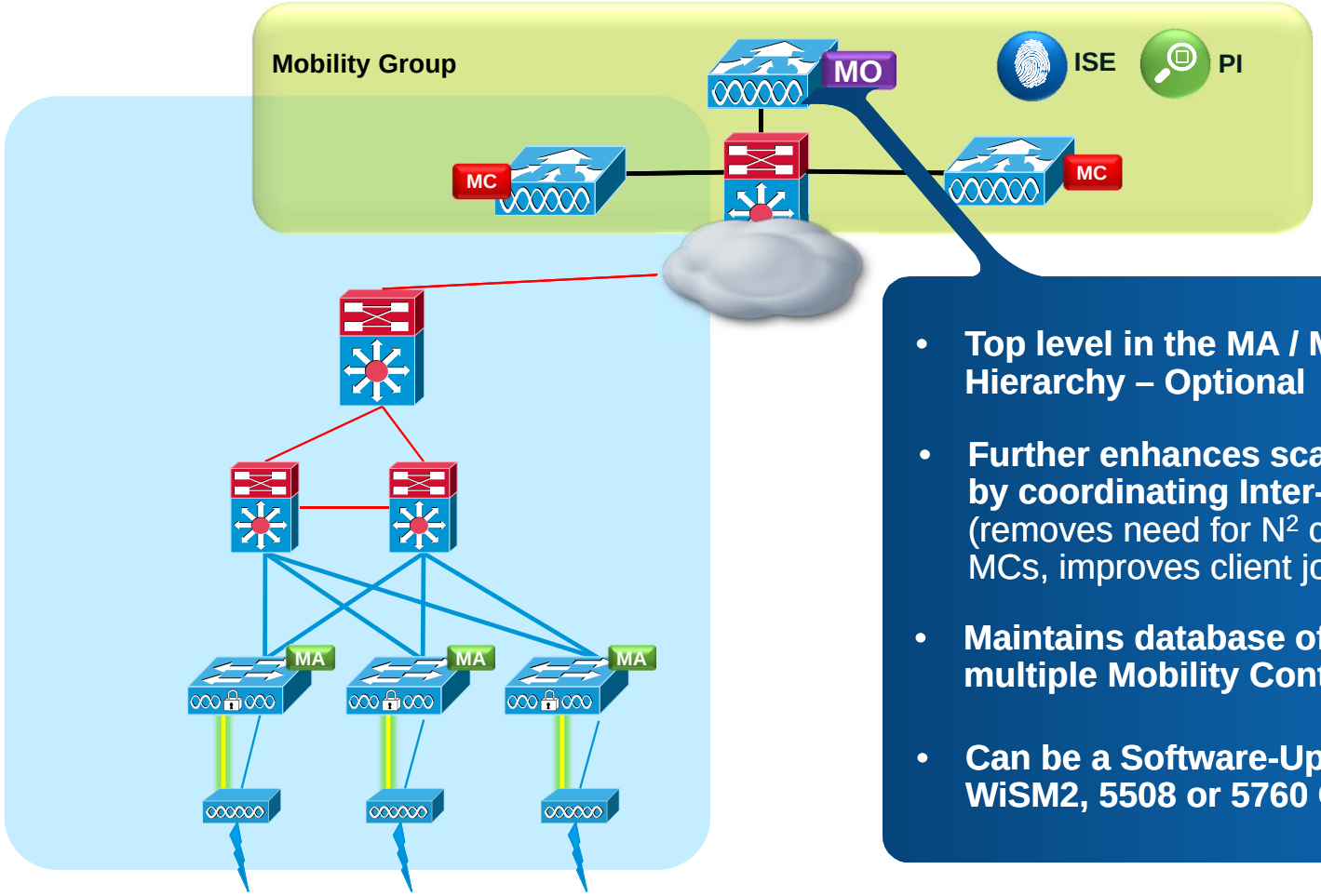
# Converged Access –
## Logical Entities – Switch Peer Groups and Mobility Group




- **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 –
## Physical Entities – Mobility Oracle (MO)



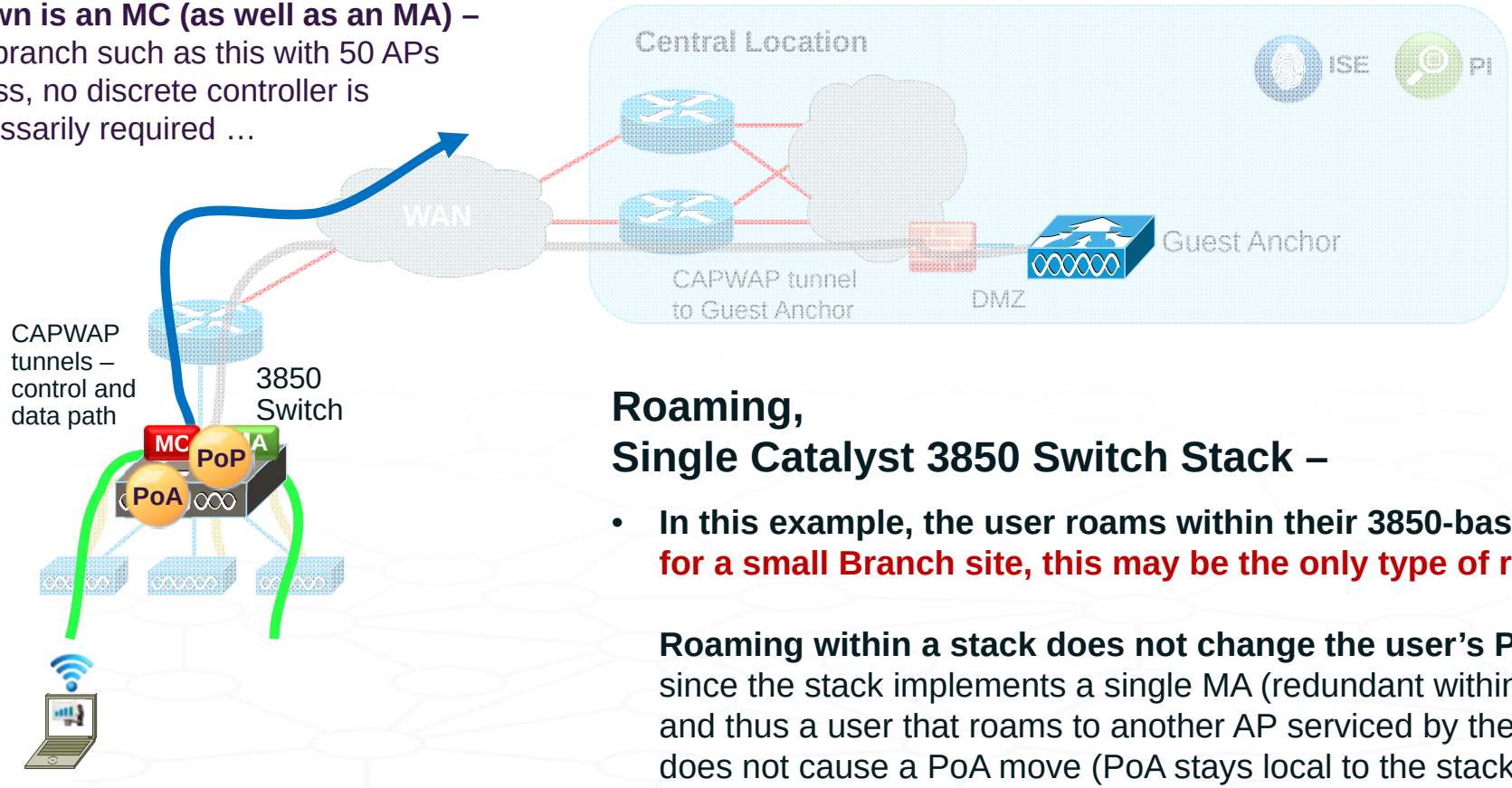

- **Top level in the MA / MC / MO Hierarchy – Optional**
- **Further enhances scalability and performance by coordinating Inter-MC roams** (removes need for $N^2$ communications between MCs, improves client join performance)
- **Maintains database of clients across multiple Mobility Controllers (MCs)**
- **Can be a Software-Upgraded WiSM2, 5508 or 5760 Controller**

# Converged Access – Traffic Flows and Roaming

# 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 …




Roaming within Stack (small branch)

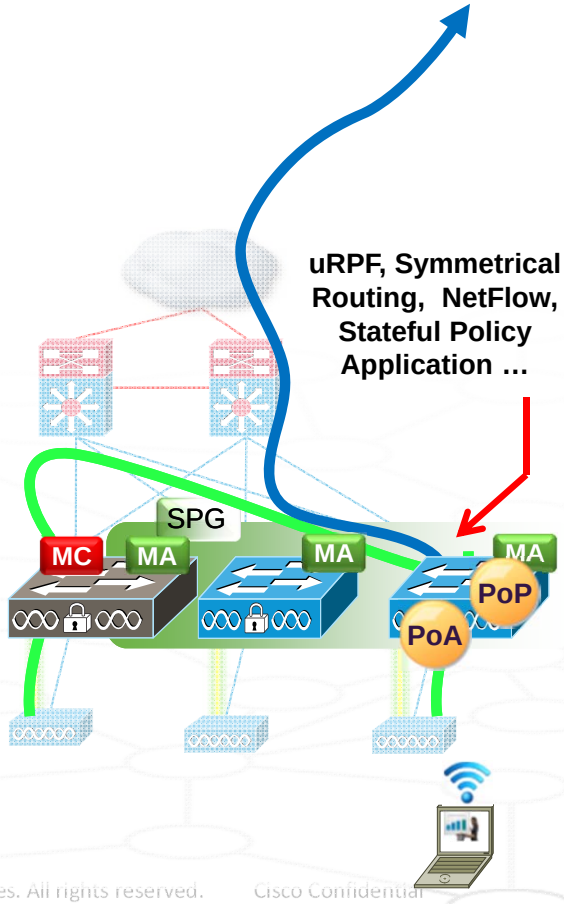
### Roaming, Single Catalyst 3850 Switch Stack –

- **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)

### 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**

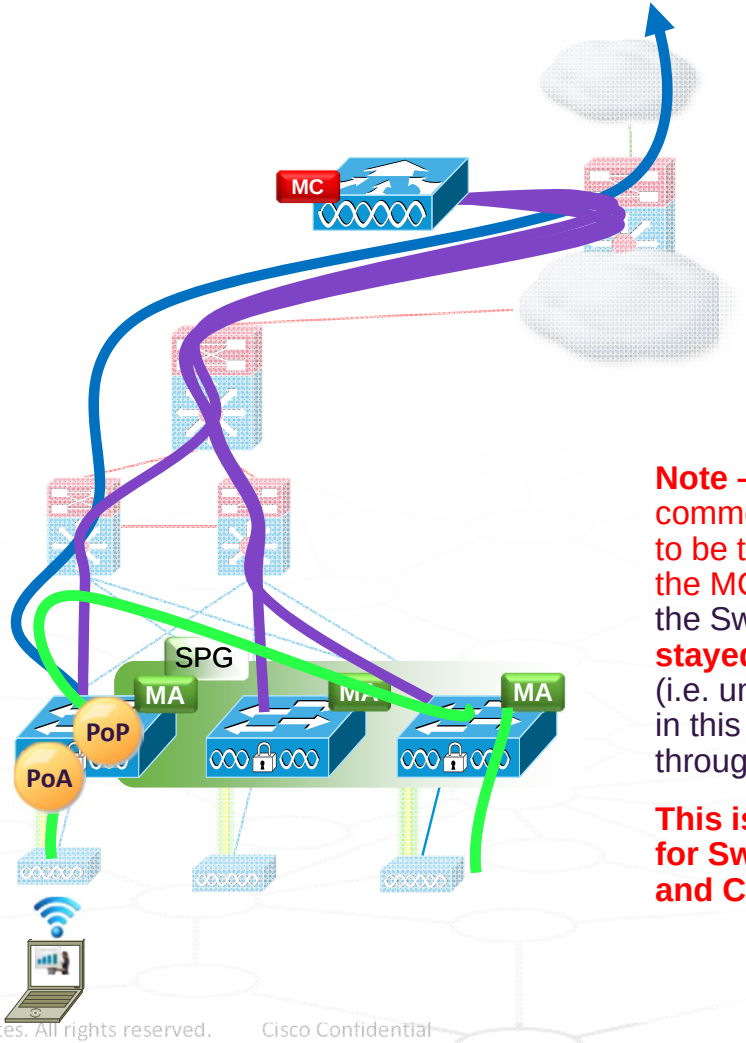
**The user may or may not have roamed across an L3 boundary** (depends on wired setup) – **however, users are always* taken back to their PoP** for policy application

** Adjustable via setting, may be useful for L2 roams*

**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 …

# 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.**

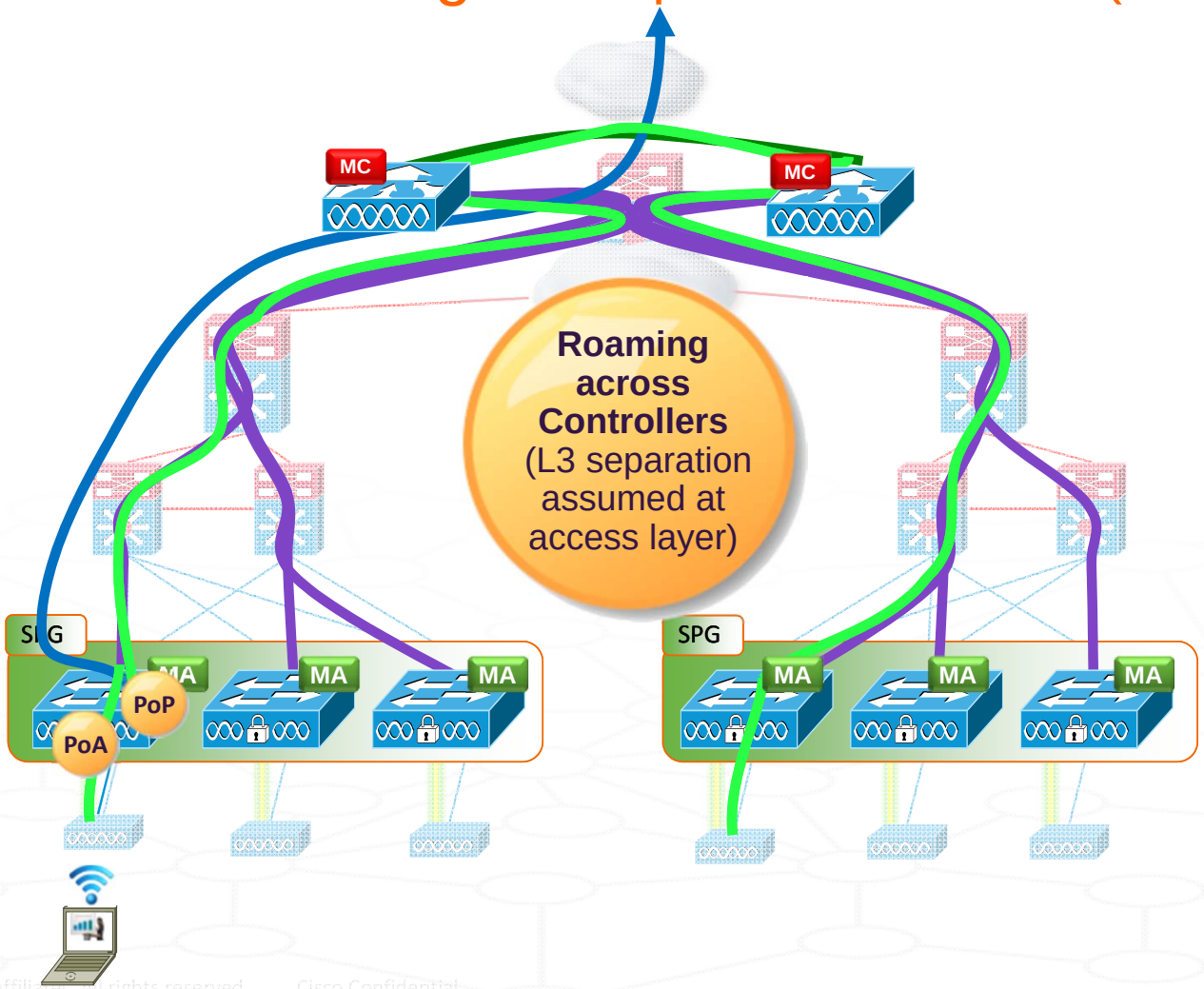
### Roaming, Within an SPG (Campus) –

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

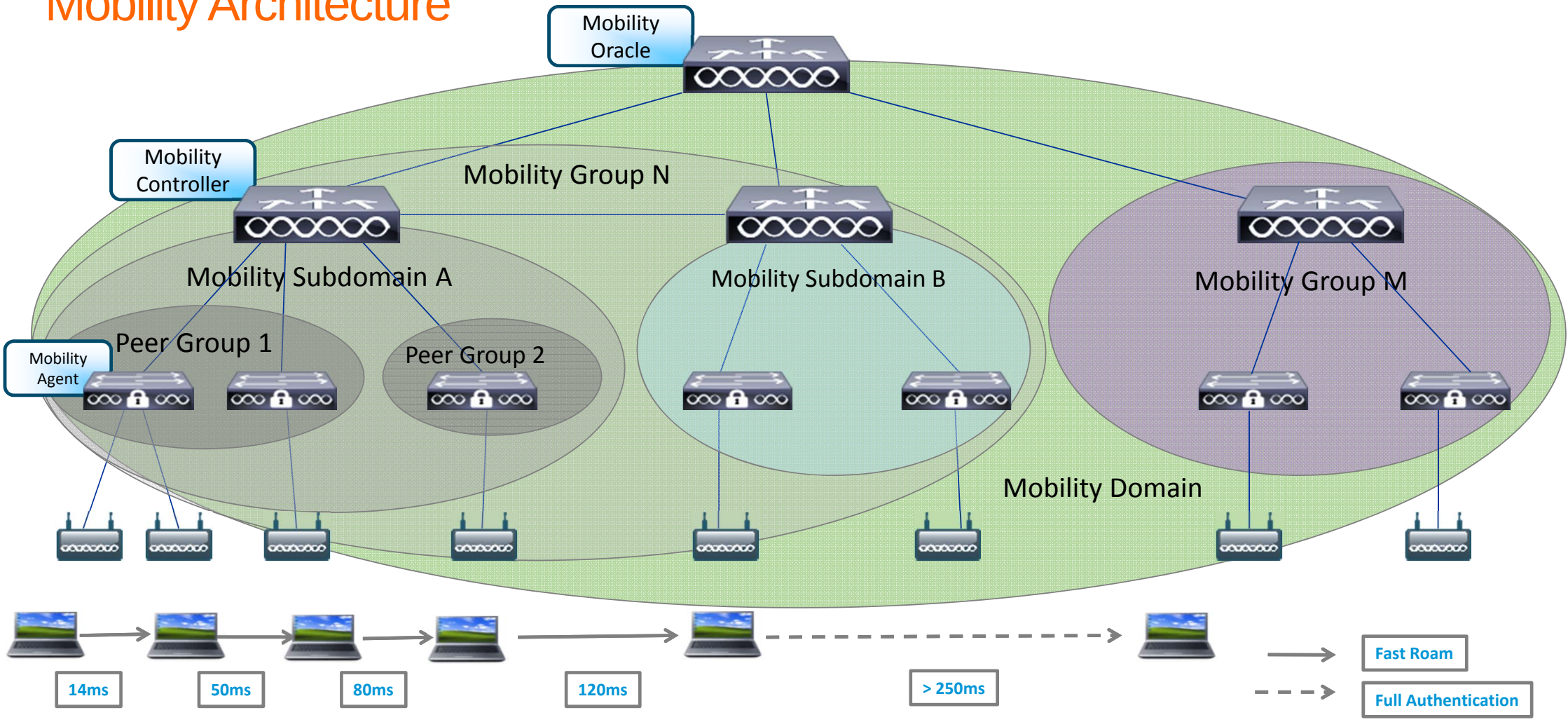



### Roaming, Across SPGs and MCs (Campus) –

- 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 –
## Mobility Architecture

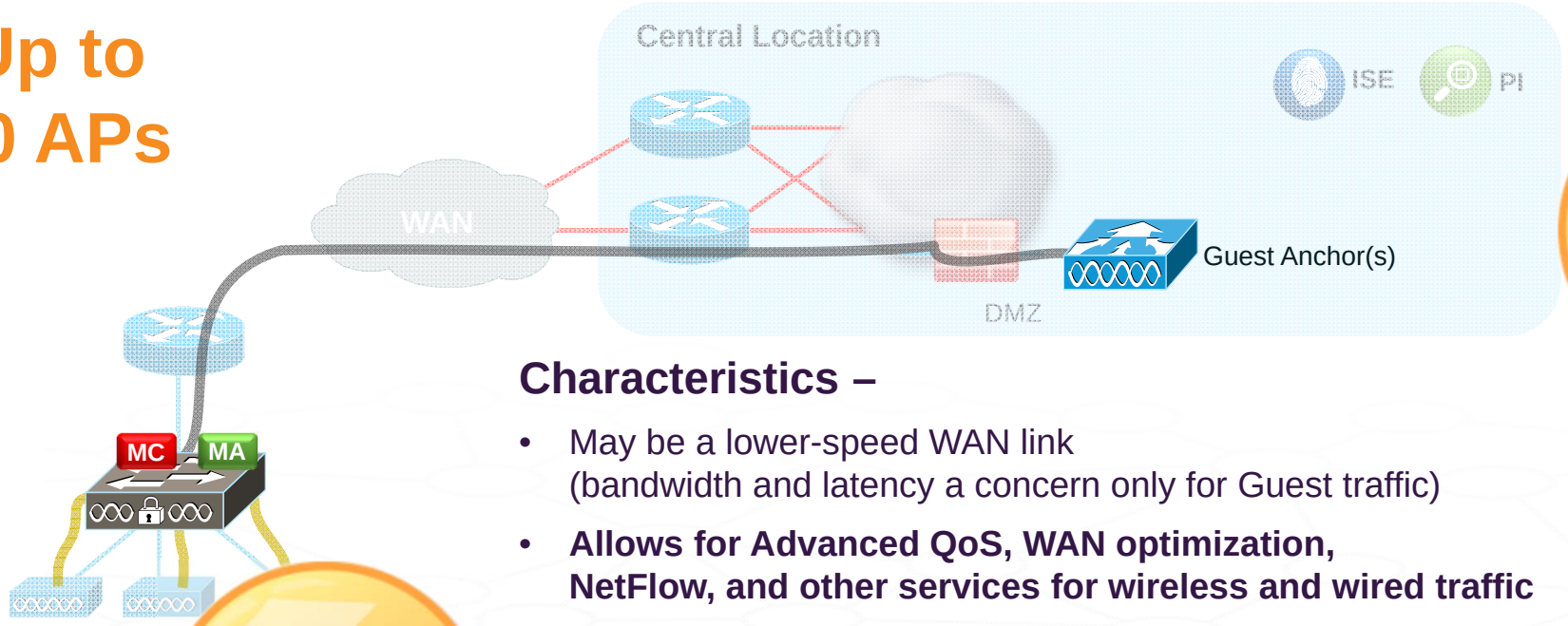


# Converged Access – Design Options

# 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

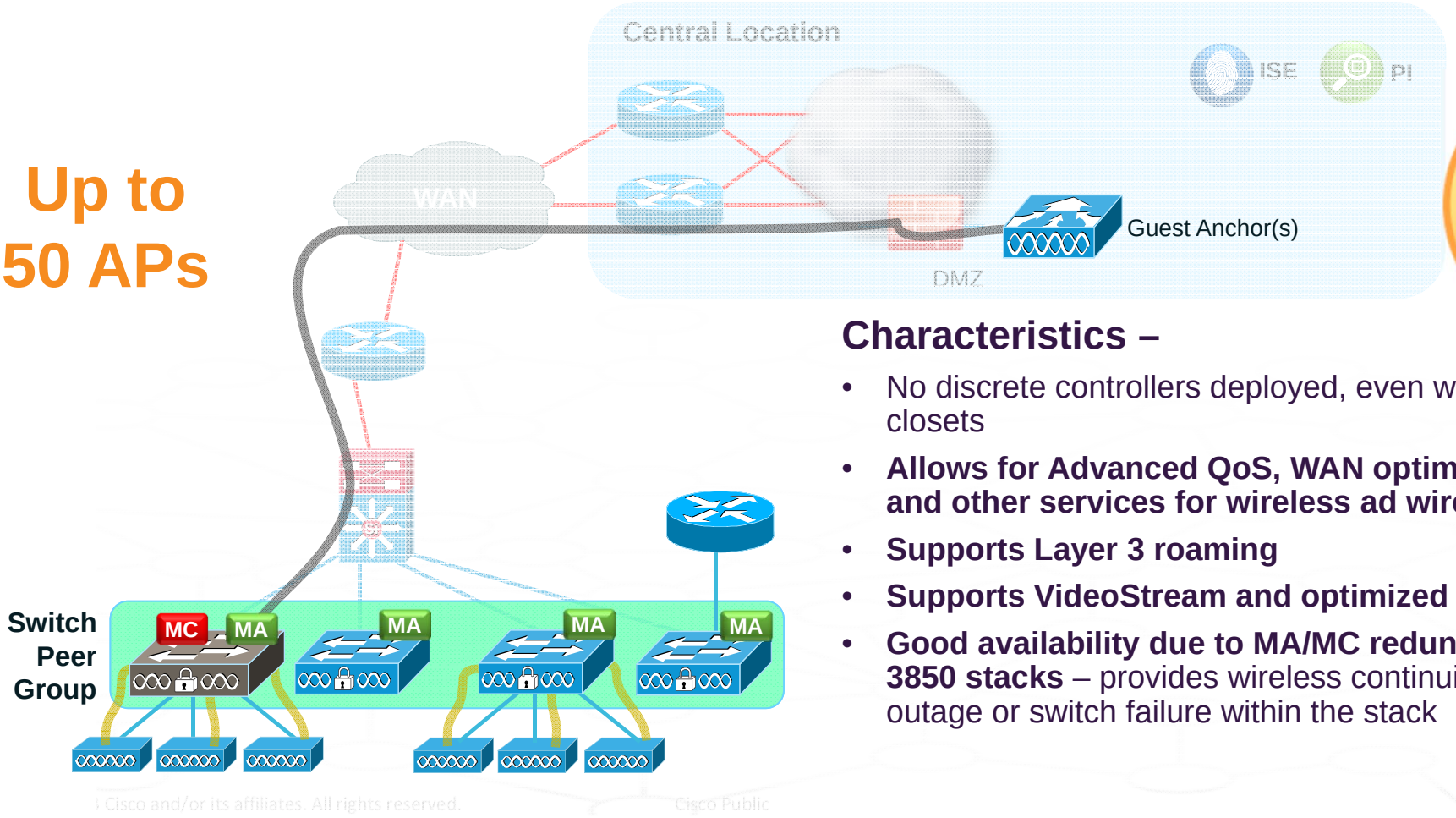
### Characteristics –

- May be a lower-speed WAN link (bandwidth and latency a concern only for Guest traffic)
- **Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless and wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimized 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 –

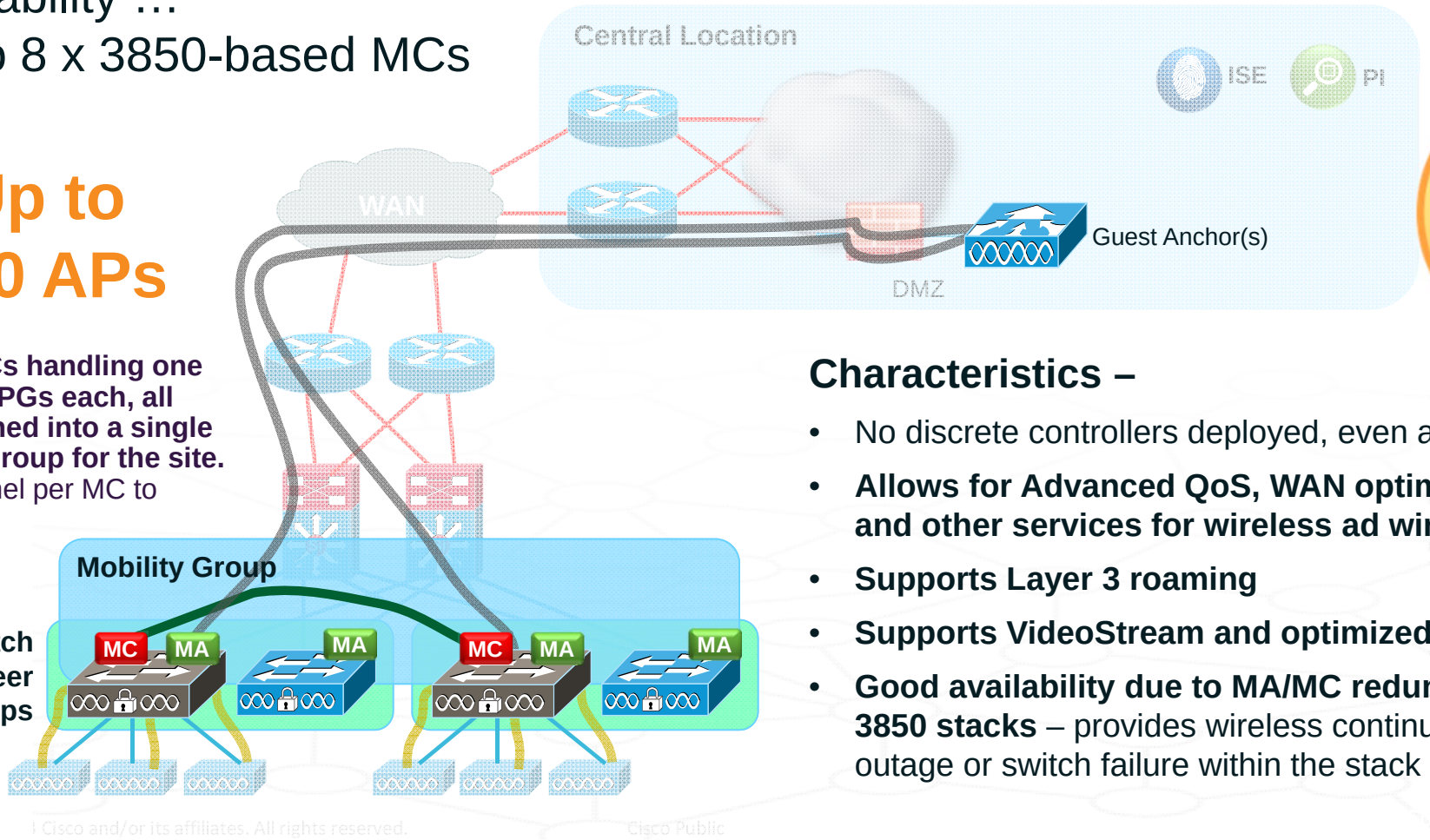
- No discrete controllers deployed, even with multiple wiring closets
- **Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless ad wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimized multicast**
- **Good availability due to MA/MC redundancy 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**




**Applicable to a Larger Branch 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.

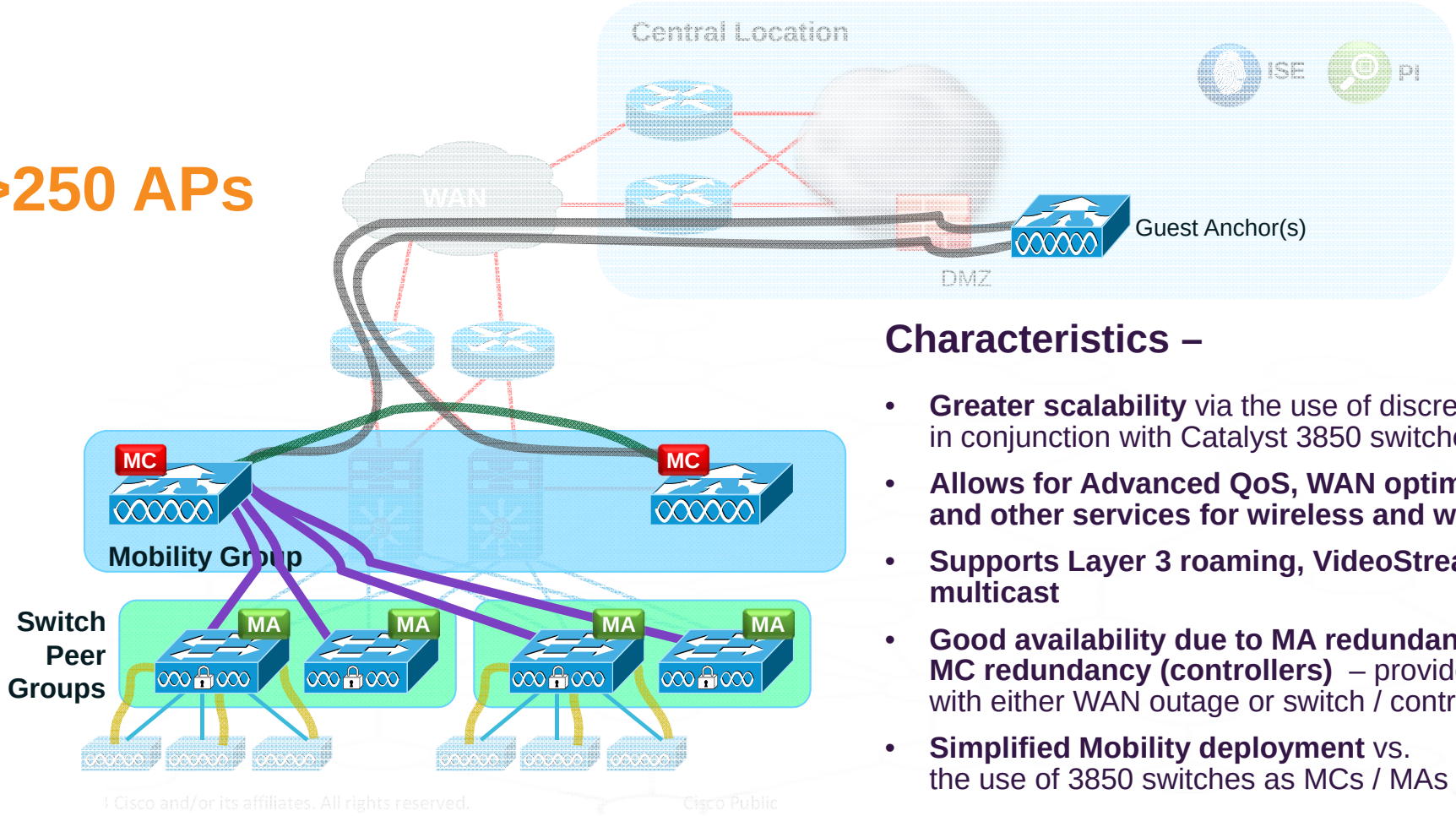
### Characteristics –

- No discrete controllers deployed, even at a larger branch
- **Allows for Advanced QoS, WAN optimization, NetFlow, and other services for wireless ad wired traffic**
- **Supports Layer 3 roaming**
- **Supports VideoStream and optimized 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 optimization, NetFlow, and other services for wireless and wired traffic**
- **Supports Layer 3 roaming, VideoStream, and optimized 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

# Wired and Wireless – Deployment options summary

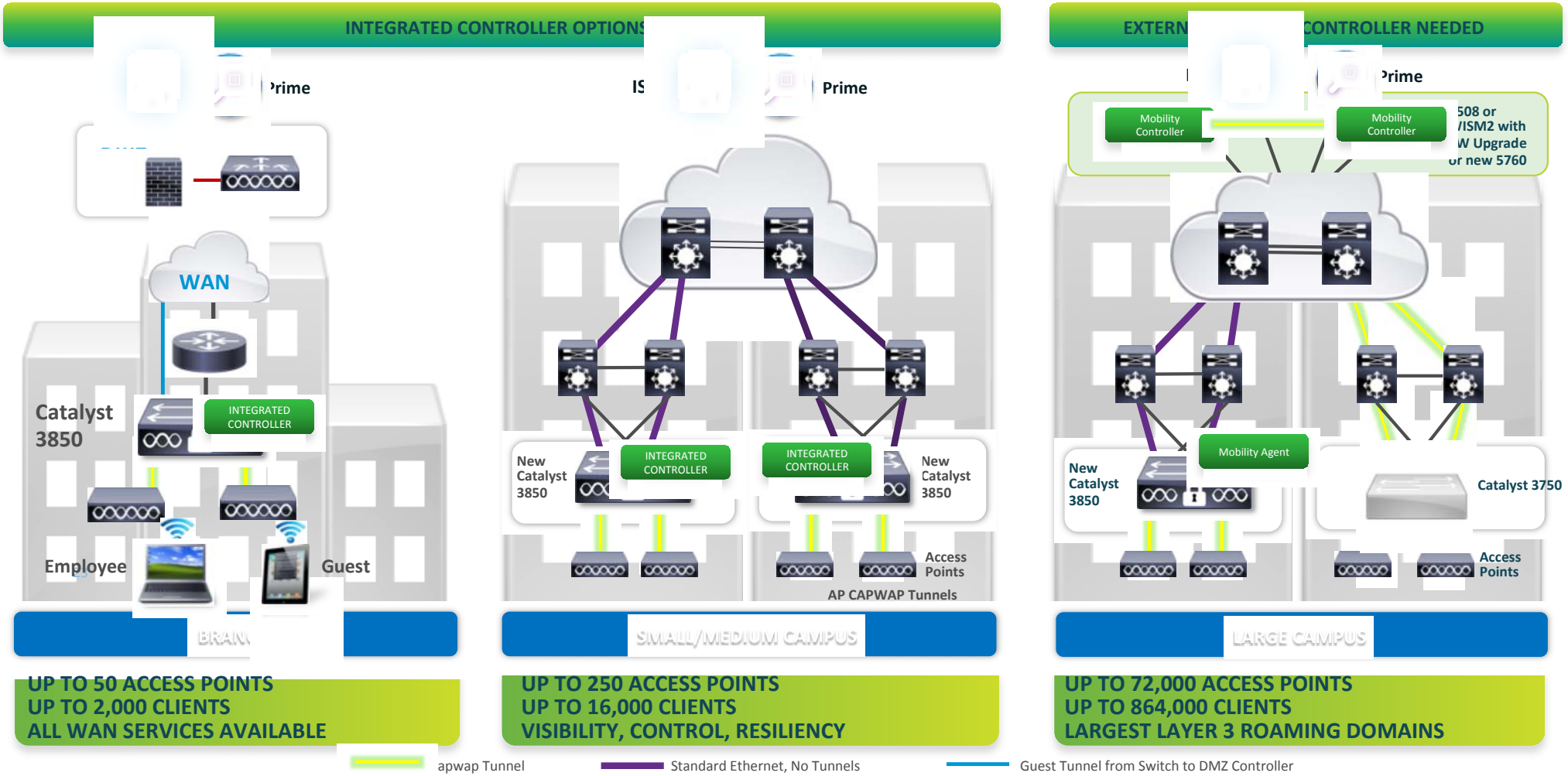
# Converged Access –
## Scalability Considerations

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

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

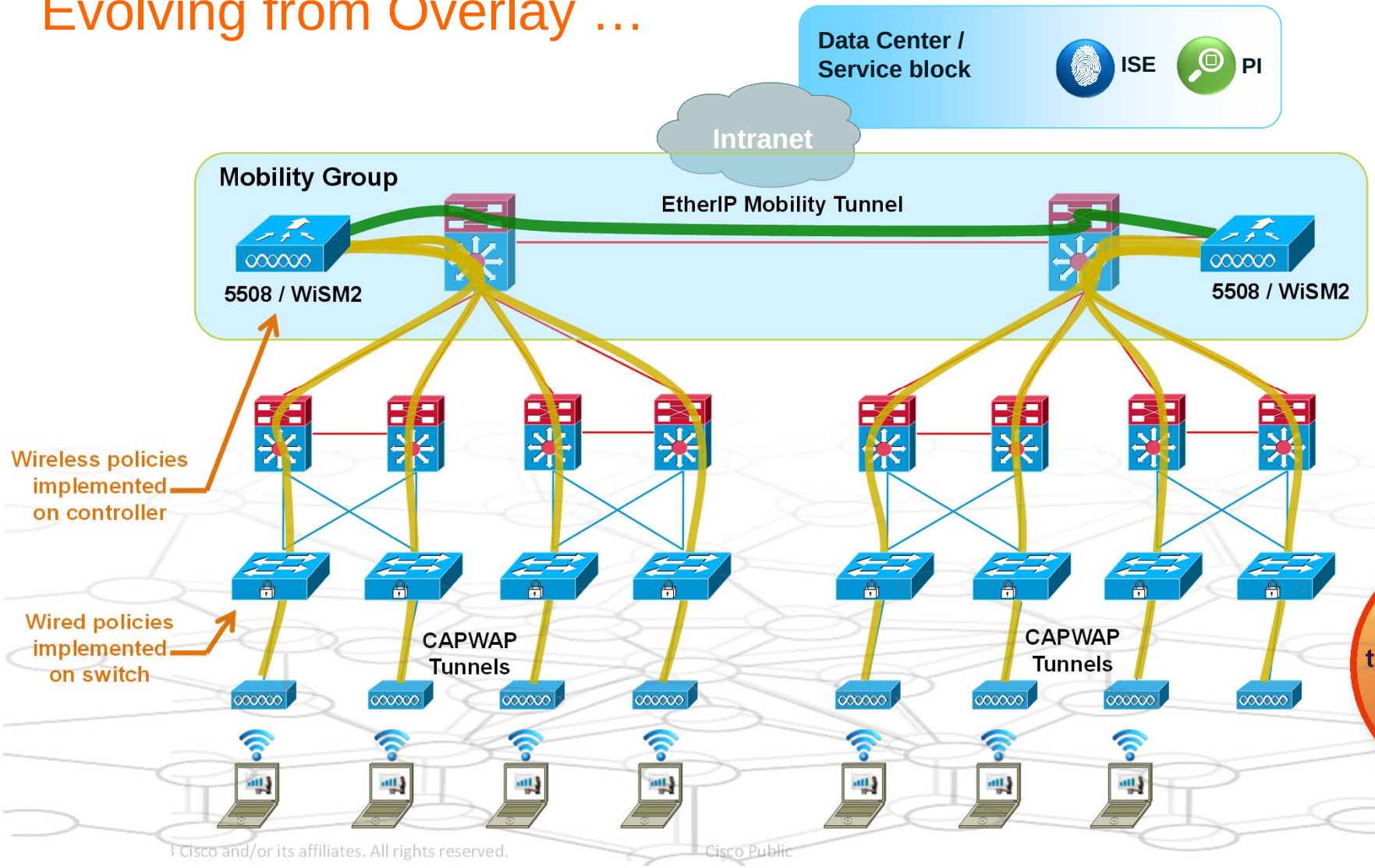
| Scalability | 3850 as MC | 5760 | 5508 | WiSM2 |
|---|---|---|---|---|
| Max number of MCs in a Mobility Domain | 8 | 72 | 72 | 72 |
| Max number of MCs in a Mobility Group | 8 | 24 | 24 | 24 |
| Max number of MAs in a Sub-domain (per MC) | 16 | 350 | 350 | 350 |
| Max number of SPGs in a Mobility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

# Converged Access Deployment –
## Use Cases



# Evolving from overlay … to integrated

# Converged Wired / Wireless Access –
## Evolving from Overlay …



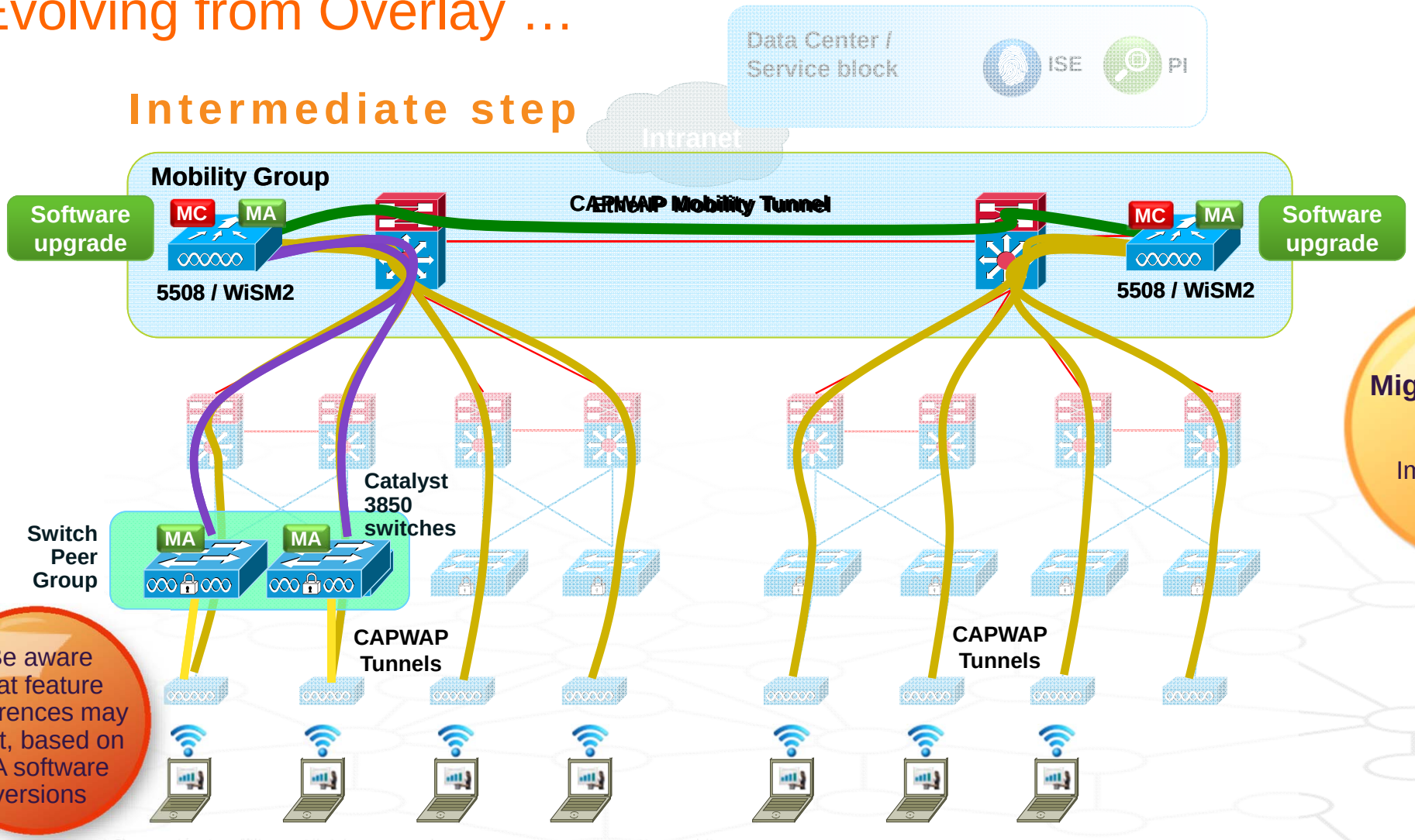

**Well-known and well-proven …** Prior to Migration to Converged Access

**Separate policies and services** for wired and wireless users

**All wireless traffic centralized** via controllers as shown

# Converged Wired / Wireless Access –
## Evolving from Overlay …

**Intermediate step**

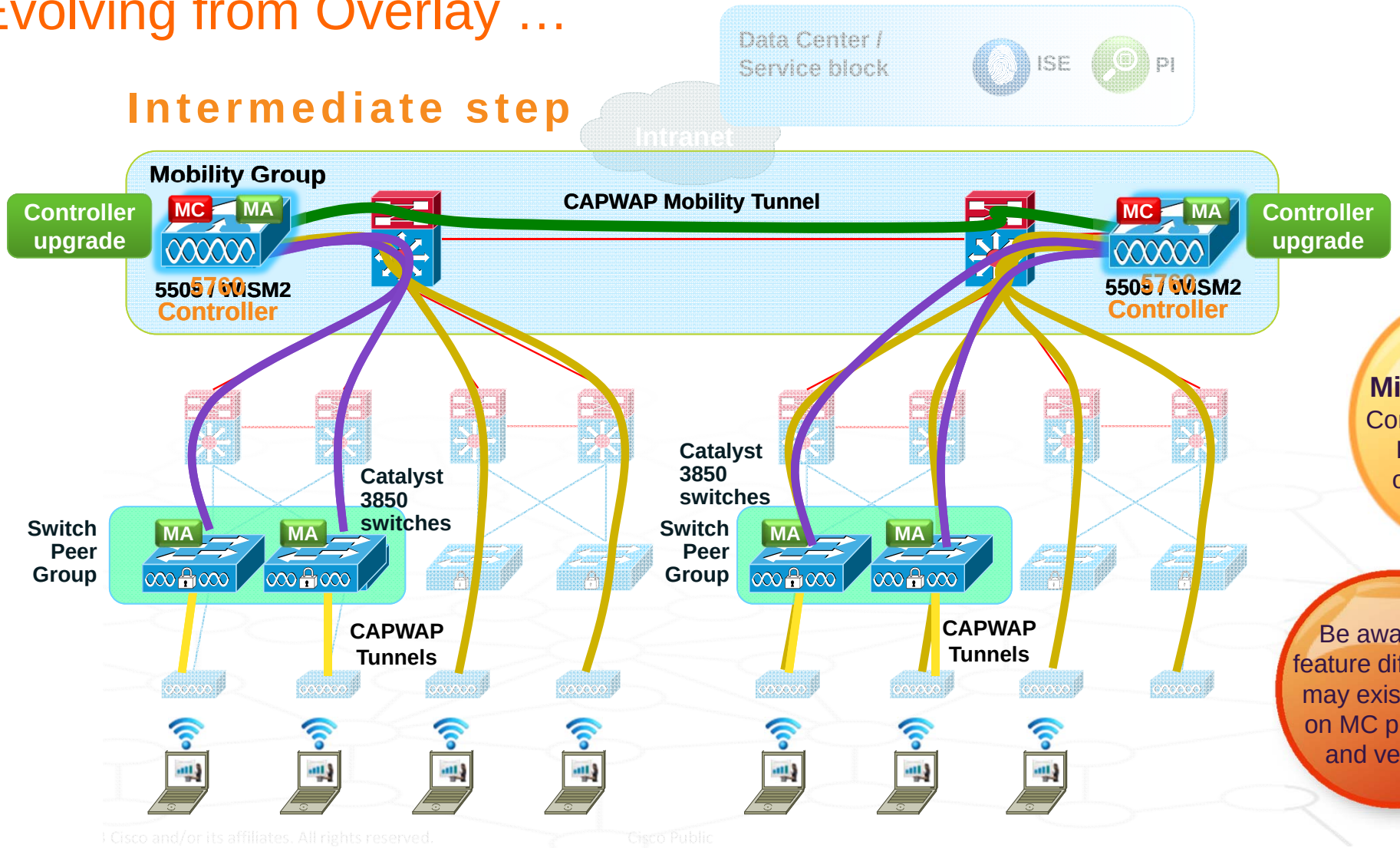



**Initial Migration Step –** Controller Upgrades, Implementation of First CA Switches

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

# Converged Wired / Wireless Access –
## Evolving from Overlay …

**Intermediate step**

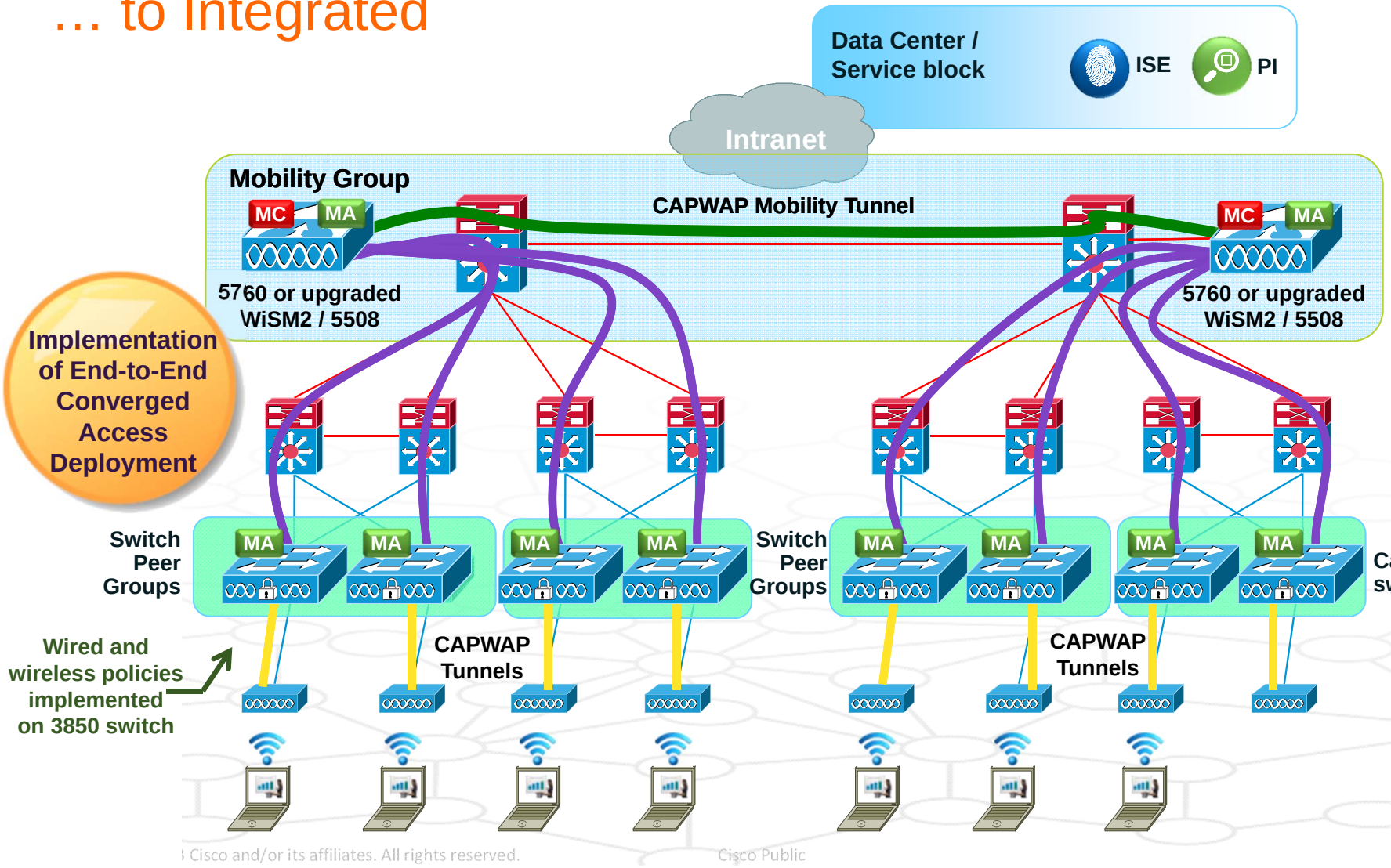



**Further Migration Step –** Controller Upgrades, Implementation of Additional CA Switches

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**

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

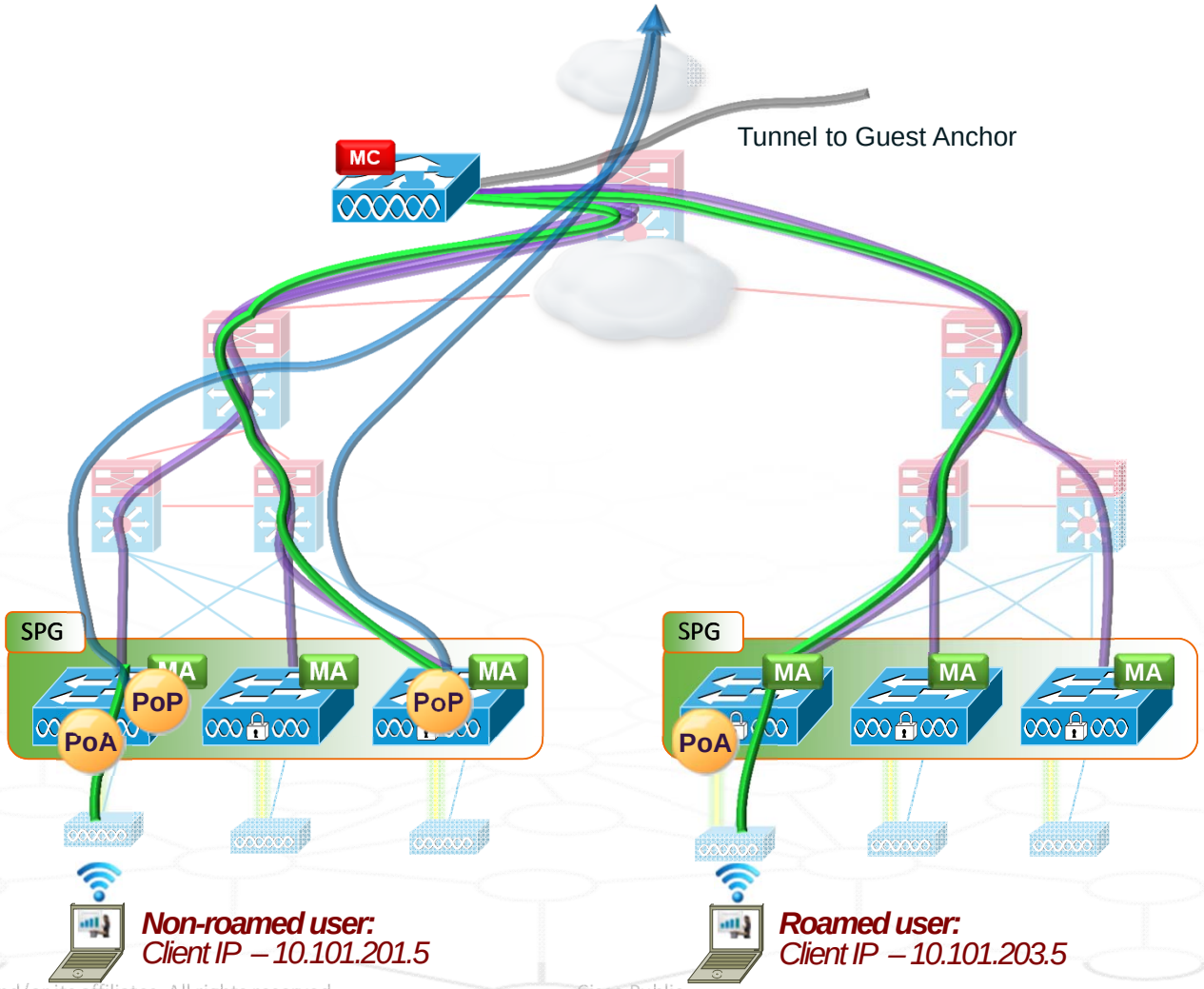
**Increase in performance and scalability** via local termination of both wired and wireless traffic

**Converged policies and services** for wired and wireless users

# Converged Access – High Availability

# High Availability –

## State Held within the Network – for Local Users and Roamed Users

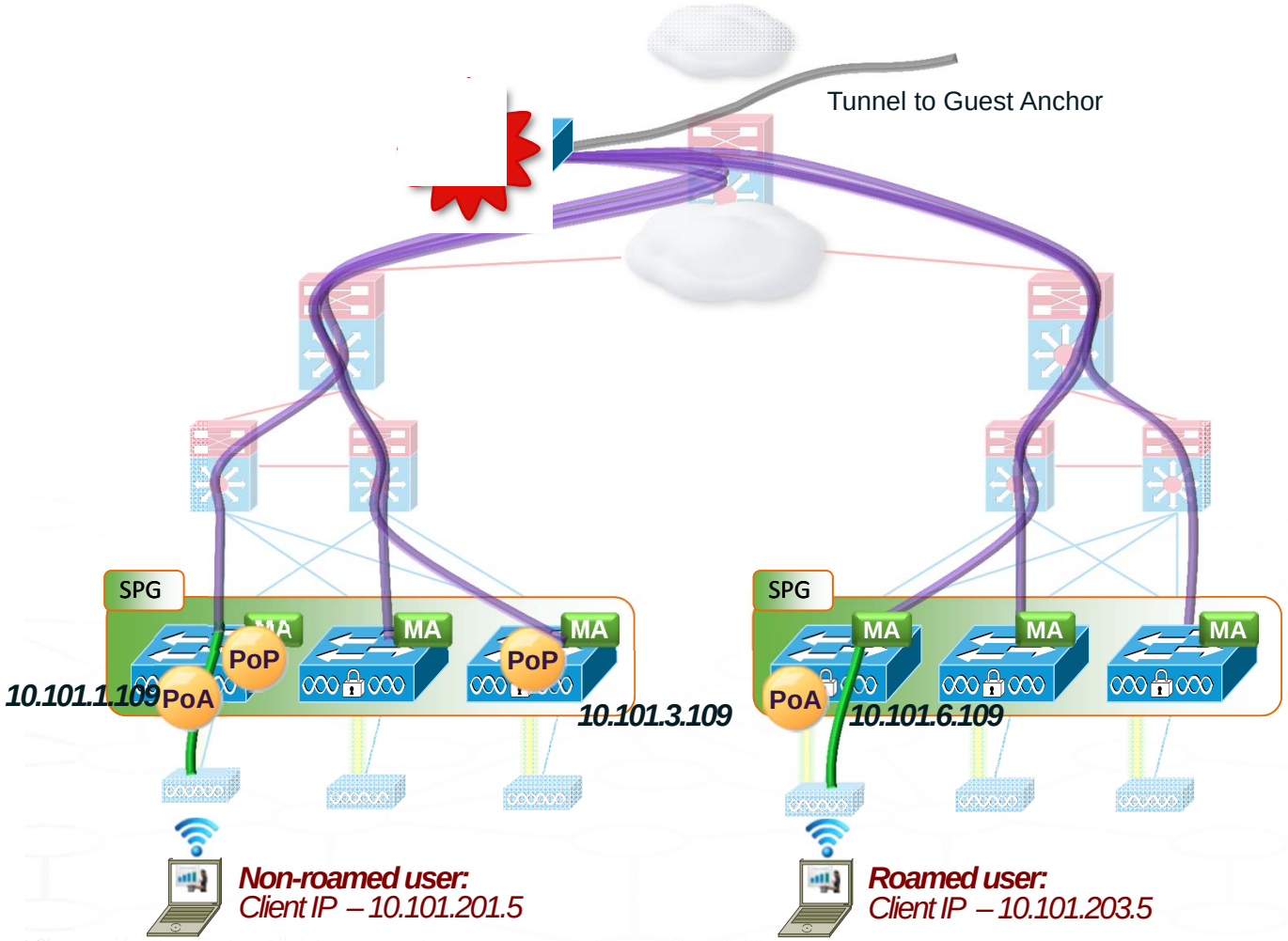



### Roamed and Local users, High Availability Considerations –

- State for users is held within the network (on MAs and MCs) – in this case, we are using a discrete controller (5760, 5508, or WiSM2) as an MC
- **In this example as shown,** we have two users – one local (non-roaming), and the other roamed across SPGs (same MC) …
- **Note that in this case, the roamed user's client IP address is associated with the IP address pool on the right-hand switch in the left-side SPG** (where the user originally associated) …

# High Availability –

## MC Failure – and the Effect on the MC's Sub-Domain and Anchor Connections



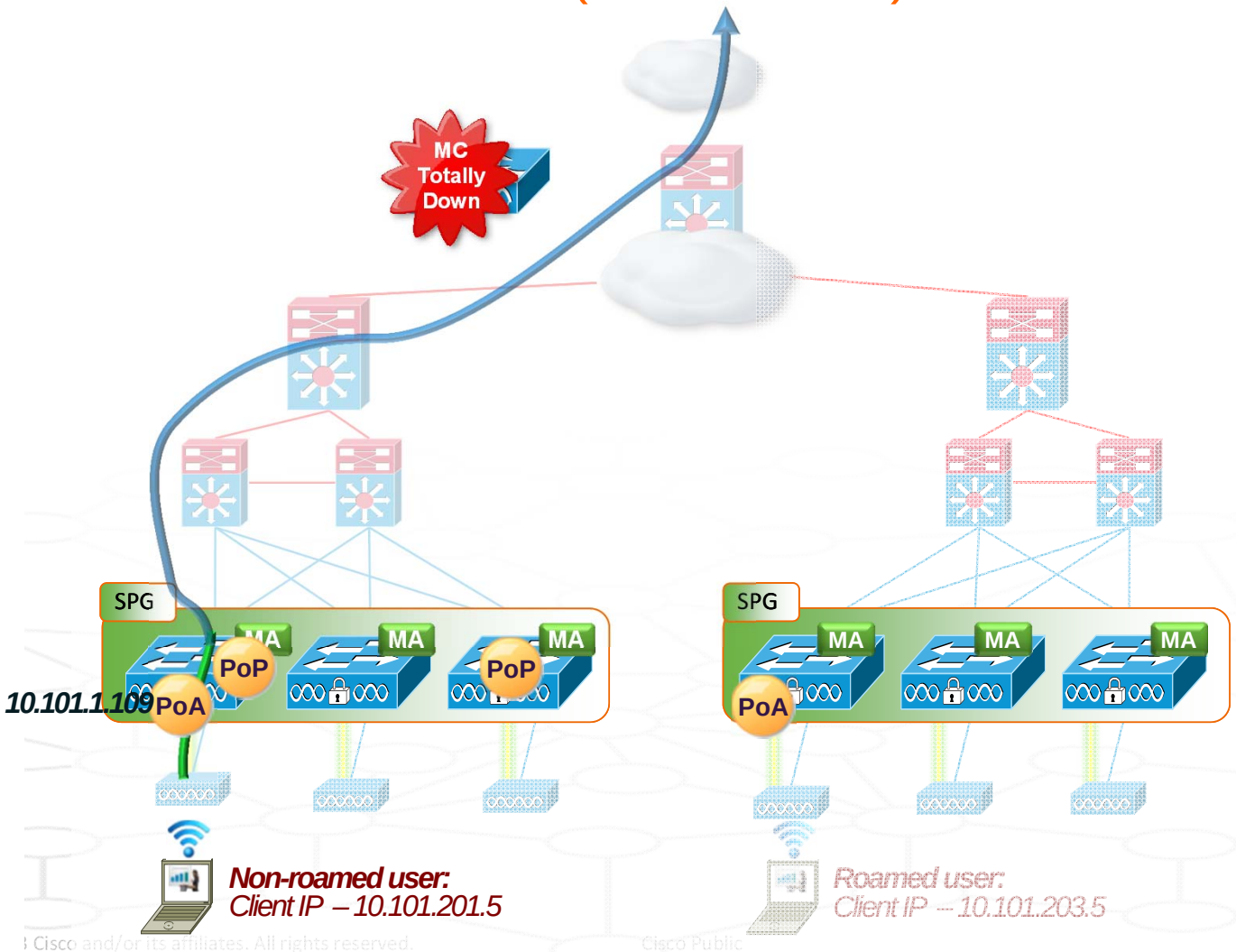

### Roamed and Local users, High Availability Considerations –

- **Now, the MC fails (power down in this case)** … let's examine the effects …
- **When the MC for a given Sub-Domain goes down, all of the tunnels serviced by that MC go down** – this includes all MA-MC tunnels (purple tunnels as shown on this diagram), as well as any MC-Guest Anchor tunnel (if present – grey tunnel as shown on this diagram)

  **Note that all of the tunnel connections between switches within the SPGs themselves stay up** – as these are pre-formed at SPG creation, and once up, do not depend on the MC to stay up …

# High Availability –

## MC Failure – Effect on Local (Non-Roamed) Clients





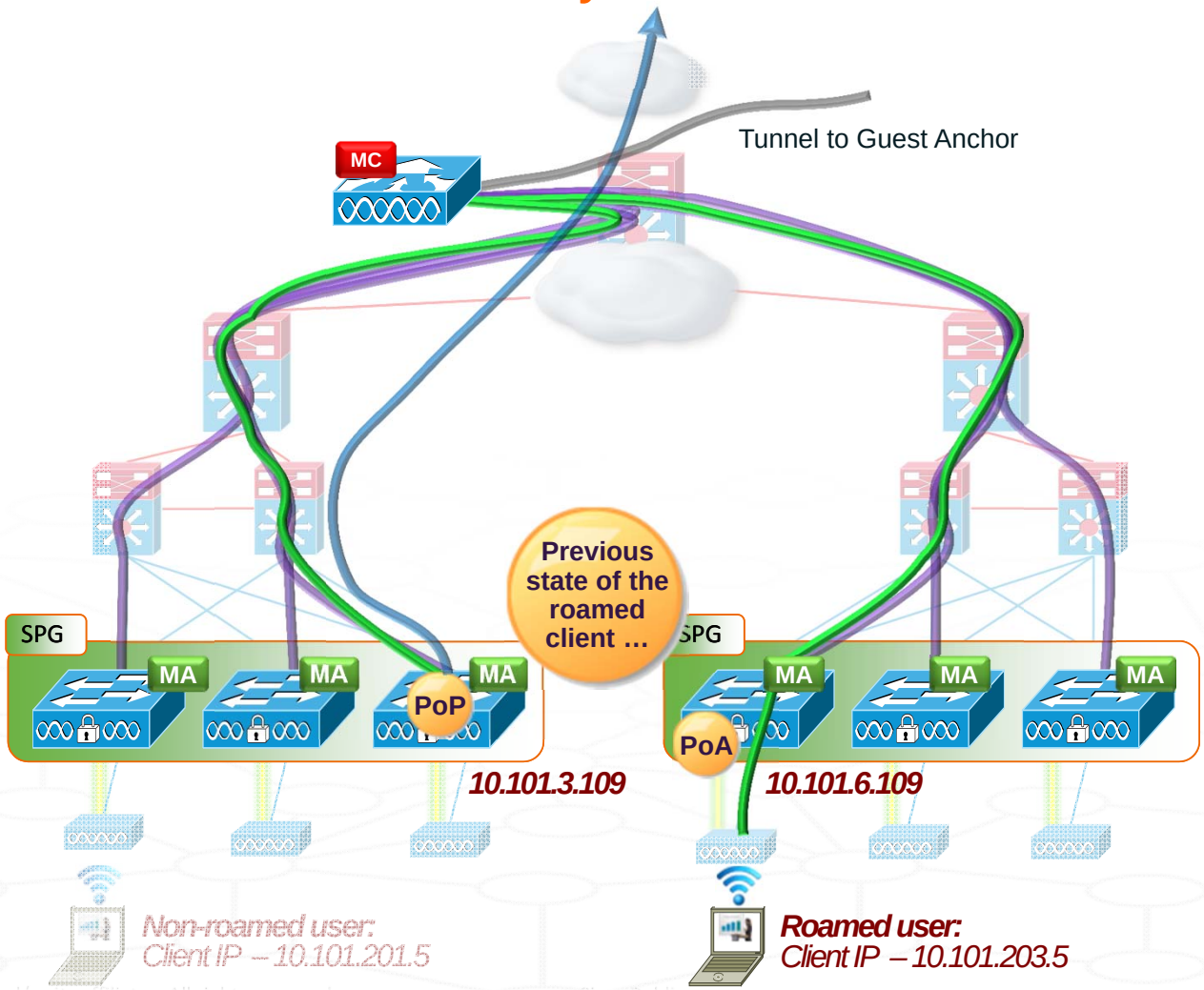



**Roamed and Local users, High Availability Considerations –**

- **For a local (non-roamed) user, the effect of an MC failure is not that severe …**
- **The local user still continues to operate,** as their traffic flow is terminated locally at their MA switch …
- **However, the user may be missing some services (Guest Access, RRM, Fast Roaming, etc) for the duration of the MC failure …** as these functions depend on the MC servicing the SPG(s) …

  and as well, **inter-SPG roaming will be affected**, as shown on the following slides …

# High Availability –
## MC Failure – Effect on Previously-Roamed Clients

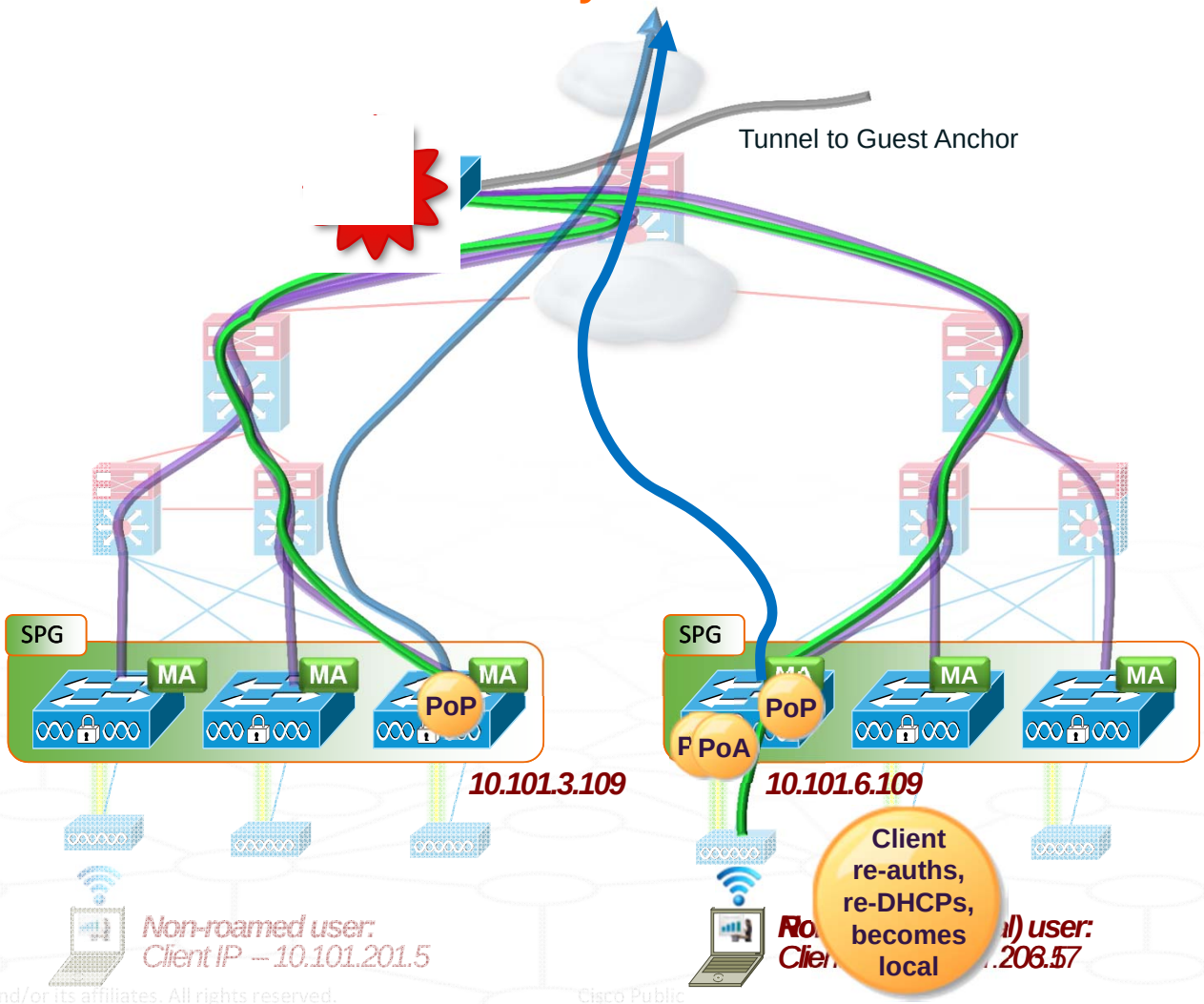



**Roamed and Local users, High Availability Considerations –**

- **Here is a client who has roamed** from the 10.101.3.109 switch, to the 10.101.6.109 switch, as shown …

# High Availability –

## MC Failure – Effect on Previously-Roamed Clients

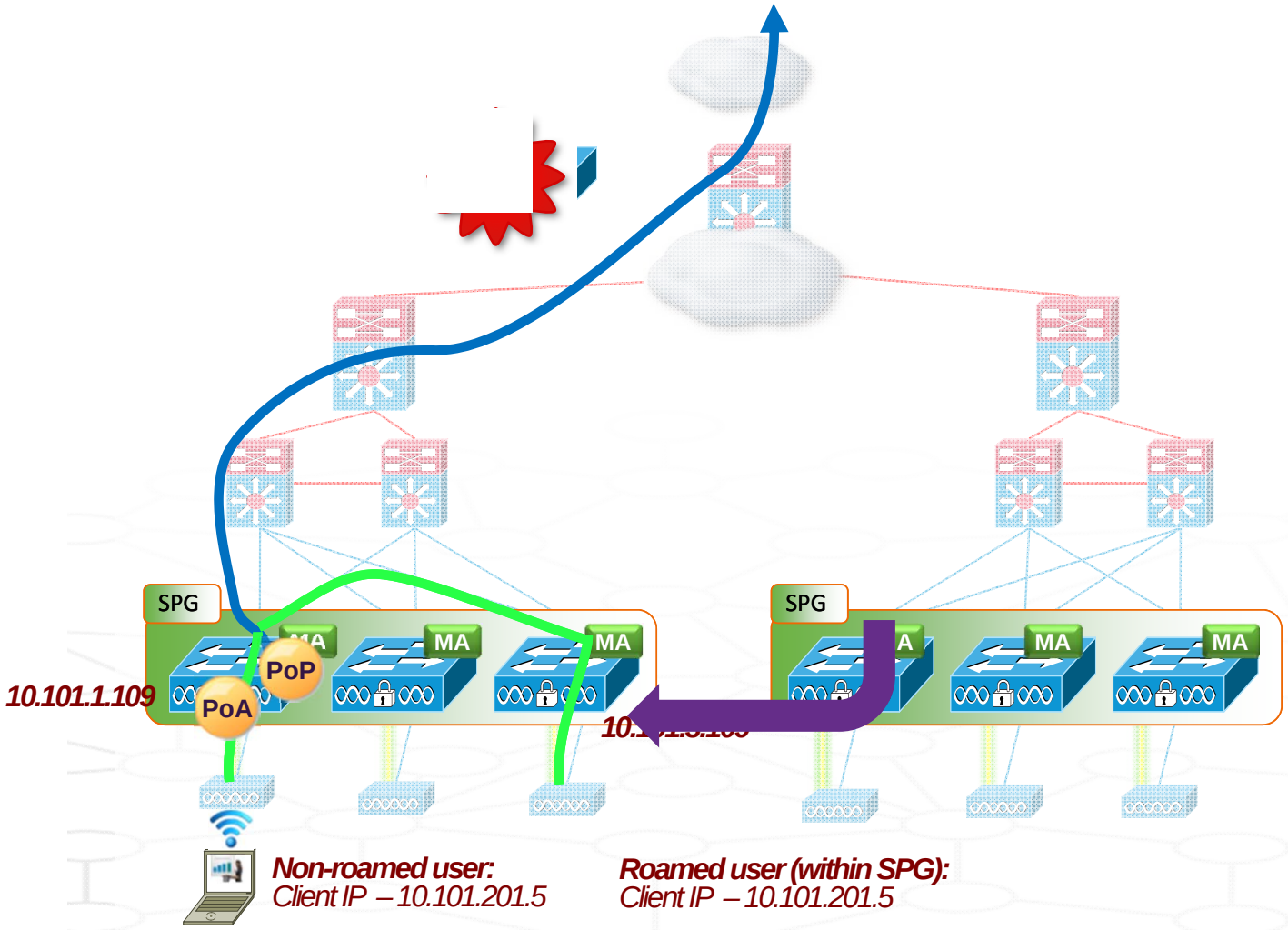



**Roamed and Local users, High Availability Considerations –**

- **For a previously-roamed client, the loss of the MC also results in the roamed client "becoming local" on their roamed-to switch**, as shown …

# High Availability –

## MC Failure – Effect on Intra-SPG Client Roams after MC Down

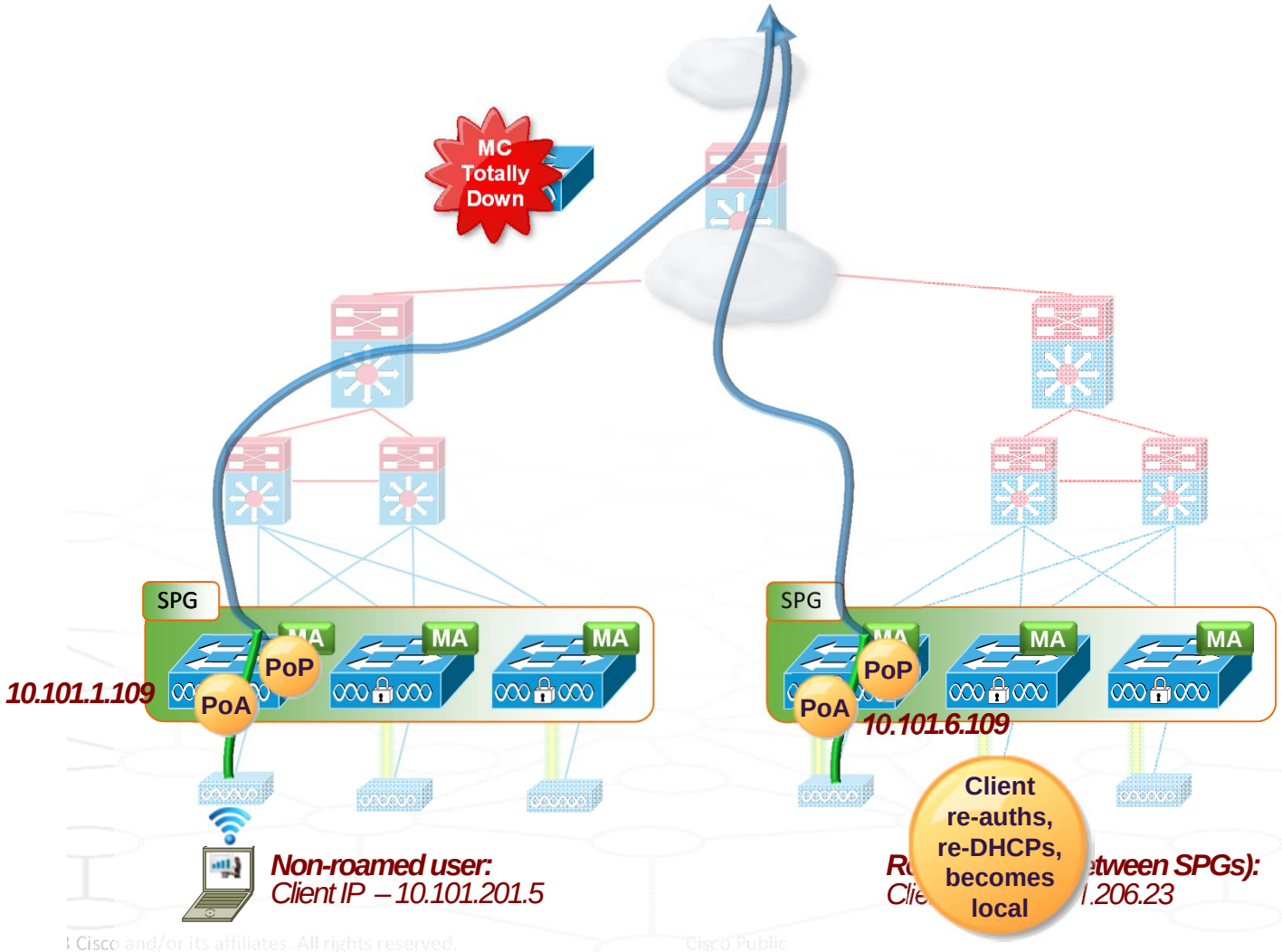



**Roamed and Local users, High Availability Considerations –**

- **Roaming within the SPG still works, even with the MC down …** since all of the connection between the MA switches within the same SPG are pre-built at SPG formation, and traffic flows between switches in the same SPG do not depend on the MC …
- **However, this will not be a Fast Roam for any new clients coming into the network after the MC failure …** since only the MC distributes PMKs for new clients throughout the SPG …

# High Availability –

## MC Failure – Effect on Inter-SPG Client Roams after MC Down

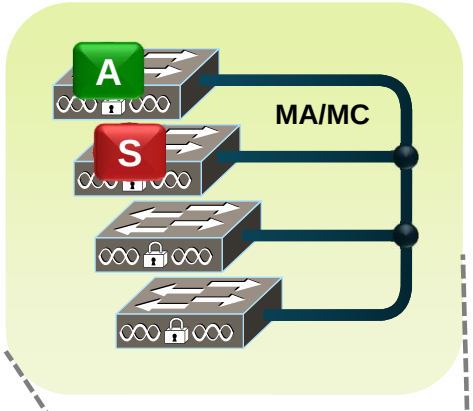



**Roamed and Local users, High Availability Considerations –**

- **Roaming between SPGs will result in a "hard roam" (re-auth, re-DHCP, change of client IP address, known as "becoming local") with the MC down …** since connection between the SPGs depends on the MC, which has failed

# High Availability –

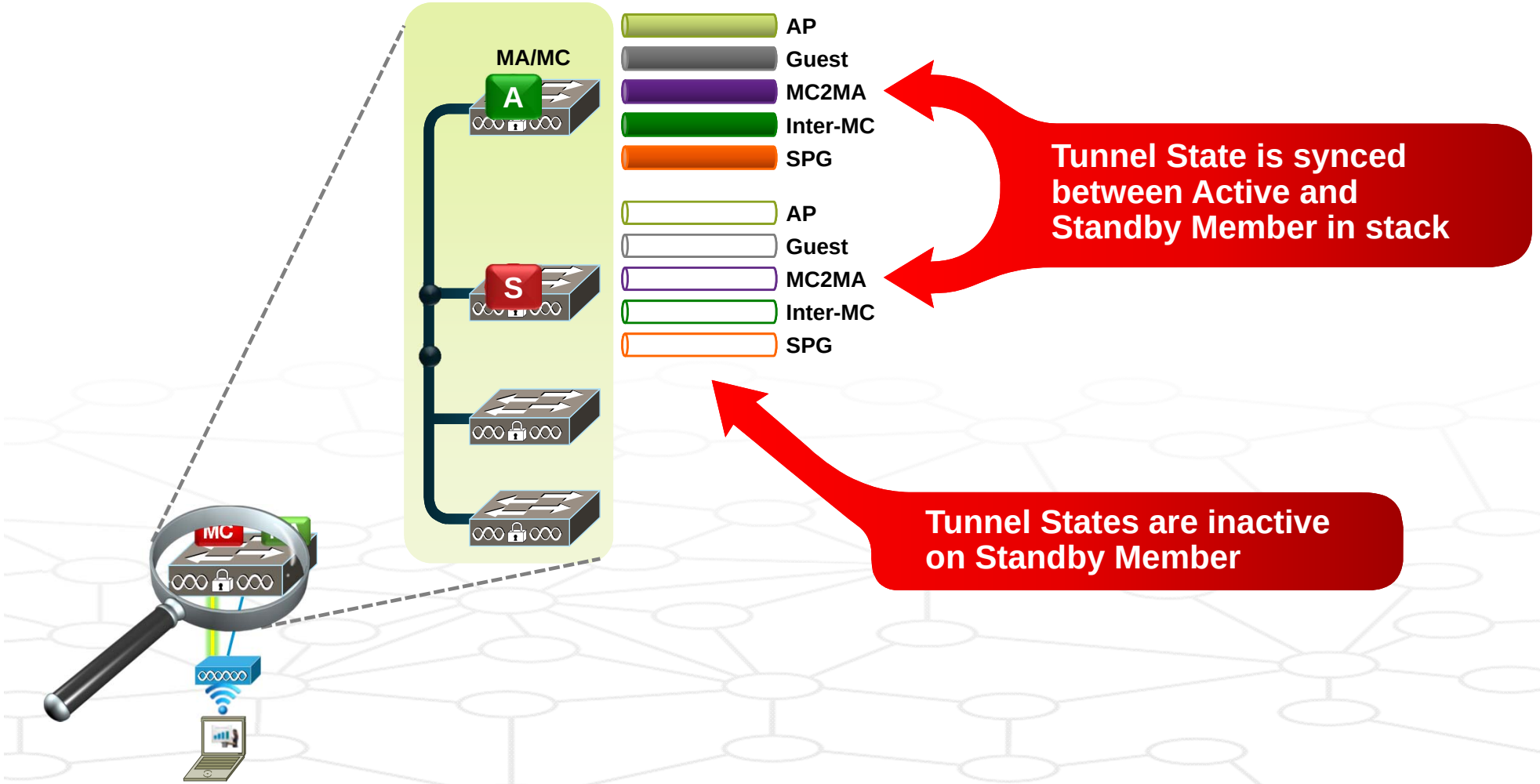
## Catalyst 3850-based MCs – Fault Tolerance in Stack




### Examining state within the stack (for MC) –

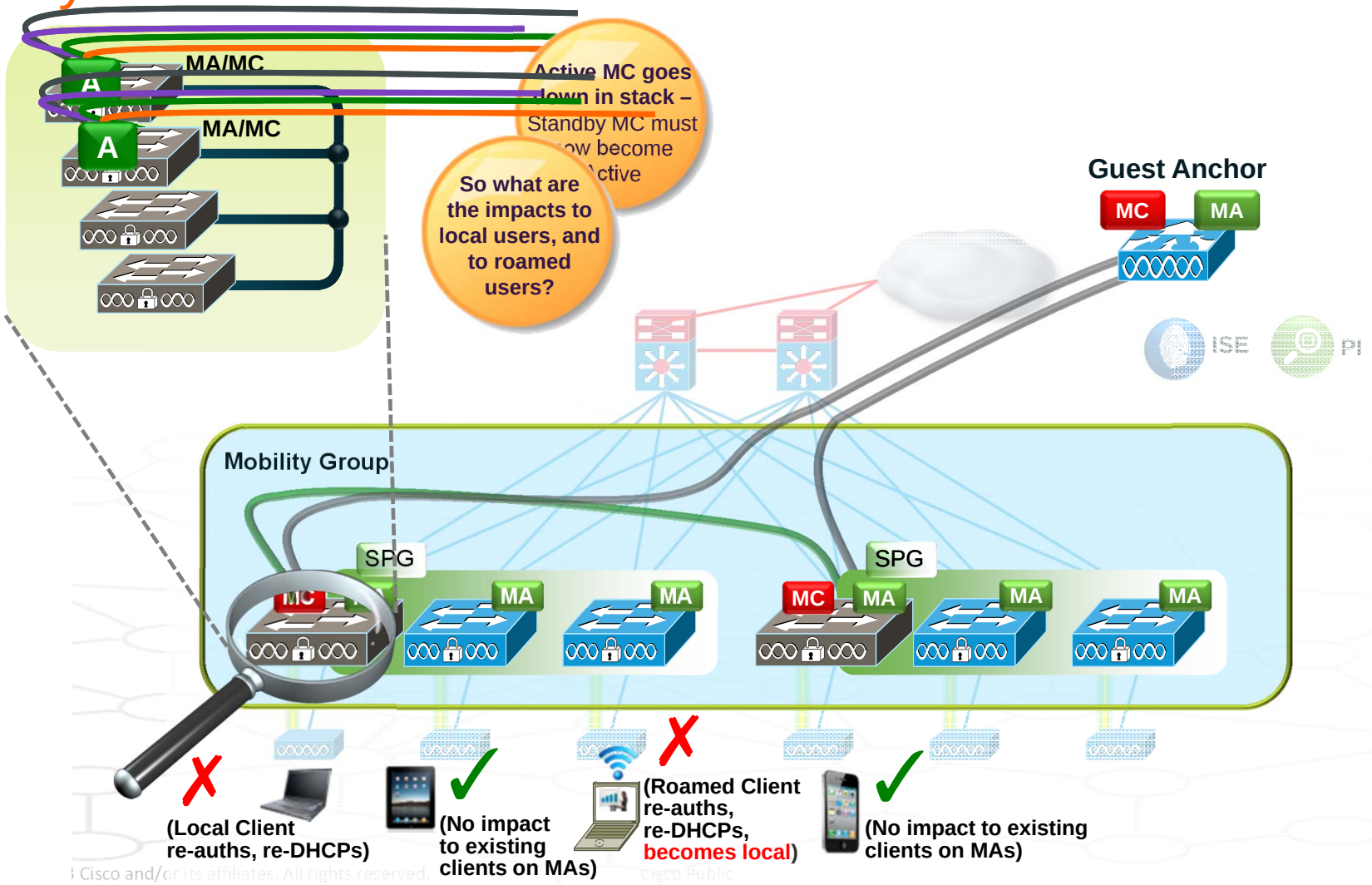
- **Let's now examine the state maintained by the MC within a stack,** and see what redundancy we provide for this …

# High Availability –
## Catalyst 3850-based MCs – Tunnel SSO



# High Availability –

## Catalyst 3850-based MCs – Fault Tolerance in Stack



# Summary

# Bringing Together Wired and Wireless –
## How Are We Addressing This Shift?

**Control plane functionality on NG Controller**

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

**Next-Generation WLAN Controller** (5760)

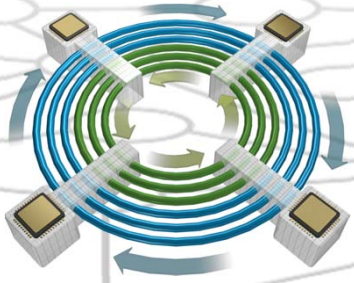
**Controller**

**Data plane functionality on NG Switches**

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

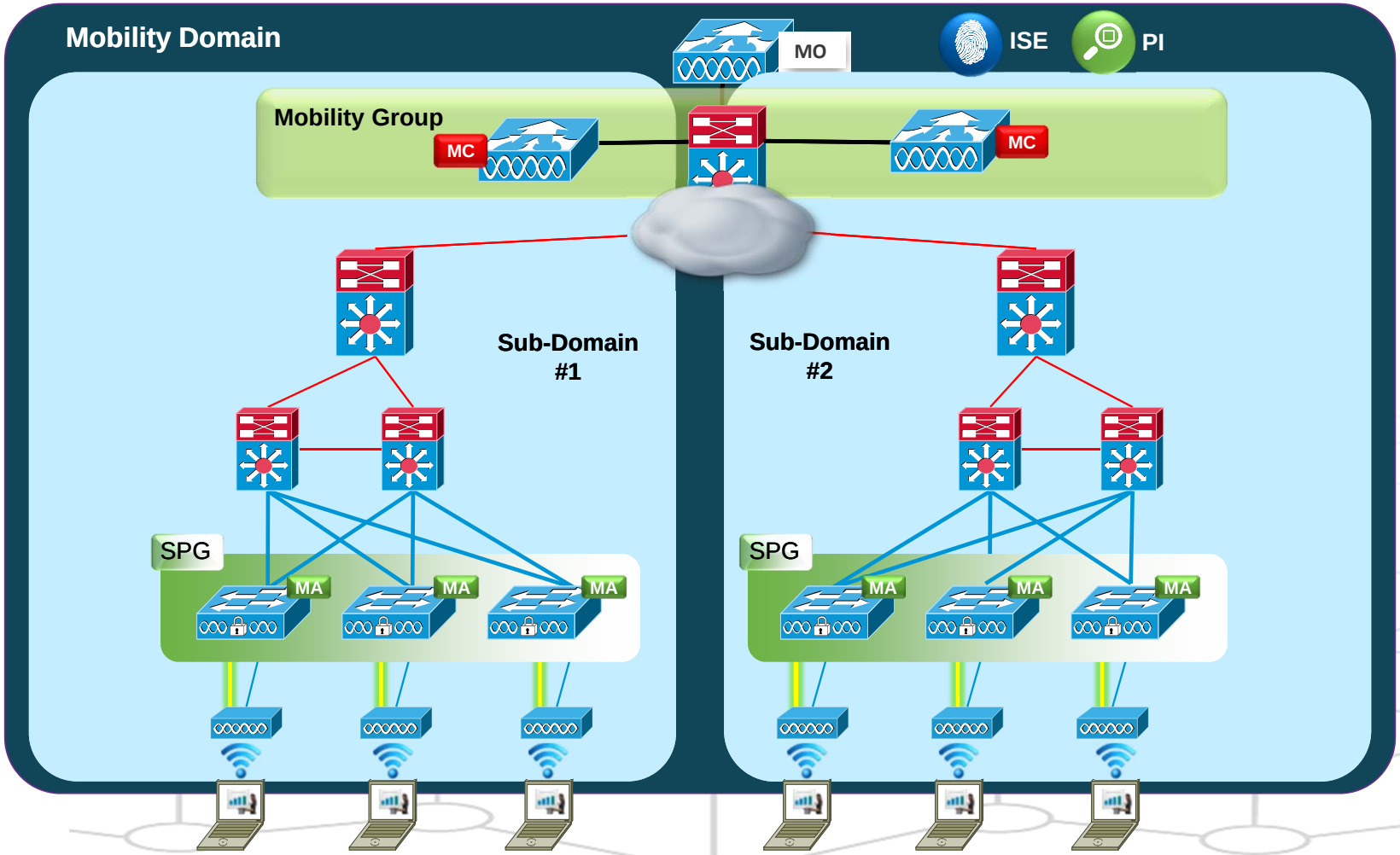
**Next-Generation Switches** (Catalyst 3850s)

**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 ….

# 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 ….

Thank you.