

What You Make Possible



Converged Access Mobility Design & Architecture

BRKEWN-2662

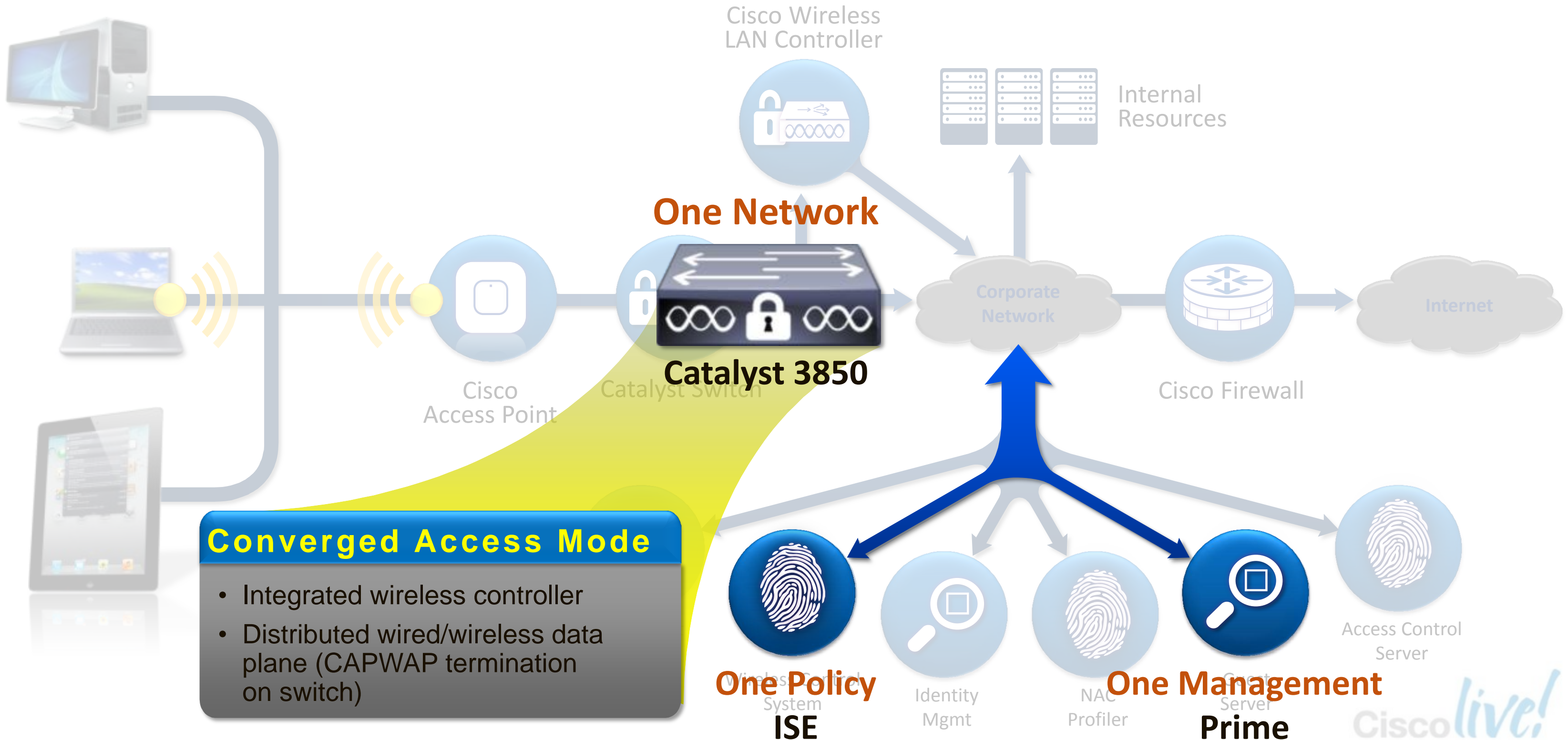
Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

Agenda

- **What is Converged Access ?**
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

One Network with Converged Access



Converged Access Mode

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



Converged Wired/Wireless Access – Benefits



Single platform for wired and wireless

Common IOS, same administration point, one release



Network wide **visibility** for faster troubleshooting

Wired and wireless traffic visible at every hop



Consistent security and quality of service **control**

Hierarchical bandwidth management and distributed policy enforcement



Maximum **resiliency** with fast stateful recovery

Layered network high availability design with stateful switchover



Scale with distributed wired and wireless data plane

480G stack bandwidth; 40G wireless/switch; efficient multicast

Unified Access - One Policy | One Management | One Network

Agenda

- What is Converged Access ?
- **Deploying One Network: Converged Access**
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

UA One Network: Converged Wired/Wireless Access Components

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

Sup 8E on Catalyst 4500E

- 888 Gbps. Sup 7-E equiv TCAM
- Wireless: 40G Capacity, 50 APs, 2K clients
- 8 x 10G SFP+
- FNF, VSS*

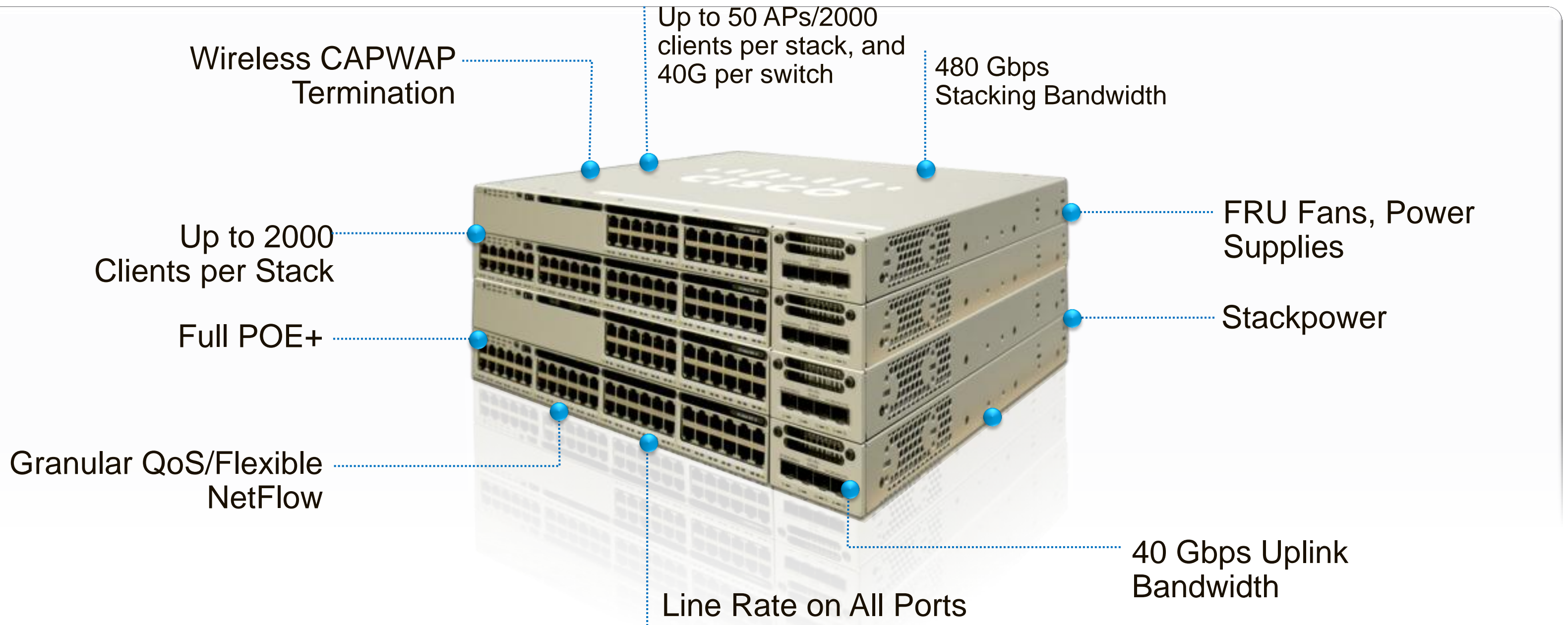
5760 Wireless Controller

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

Best-in-Class Performance, Security, and Resiliency

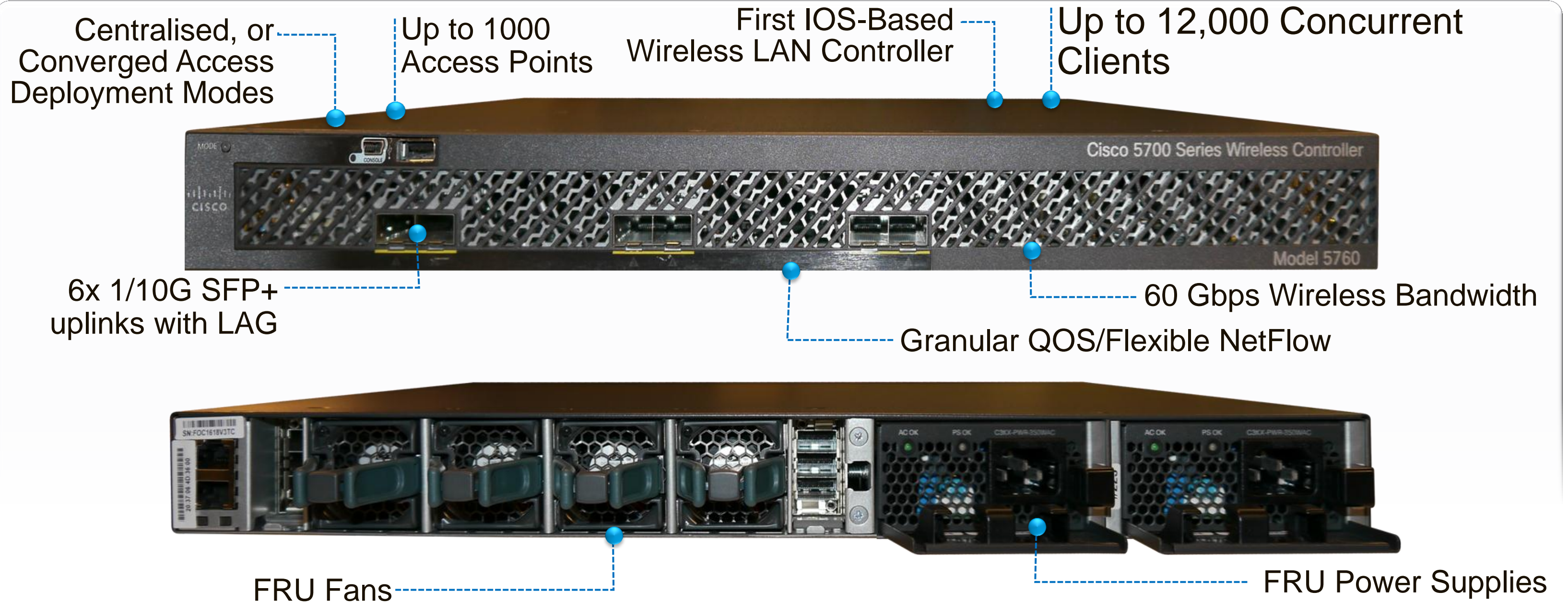


NEW Catalyst 3850 Switch



Built on Cisco's Innovative "Doppler" ASIC

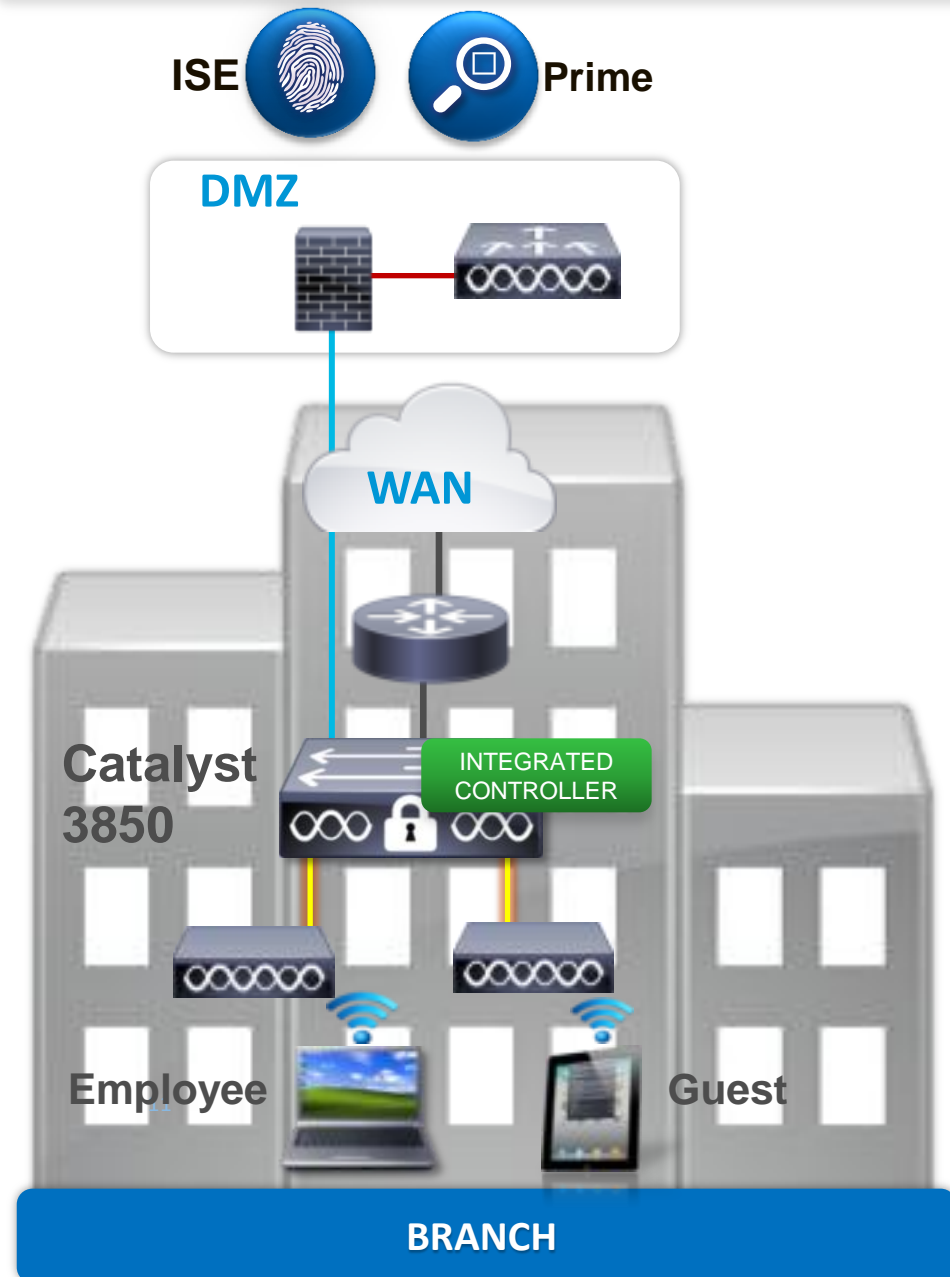
Cisco WLC 5760



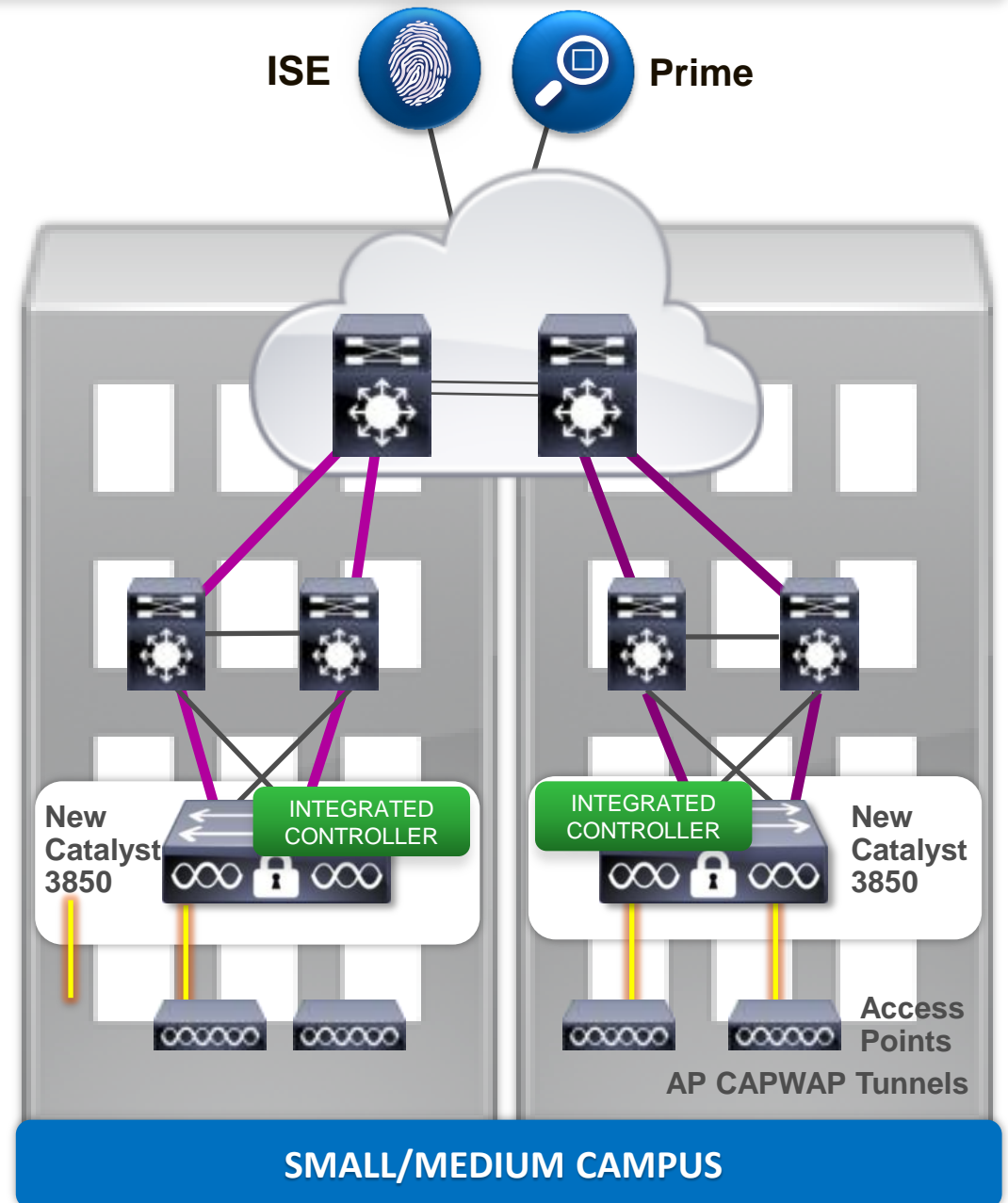
Built on Cisco's Innovative "Doppler" ASIC

Converged Access Deployment Mode - Three Use Cases

INTEGRATED CONTROLLER OPTIONS

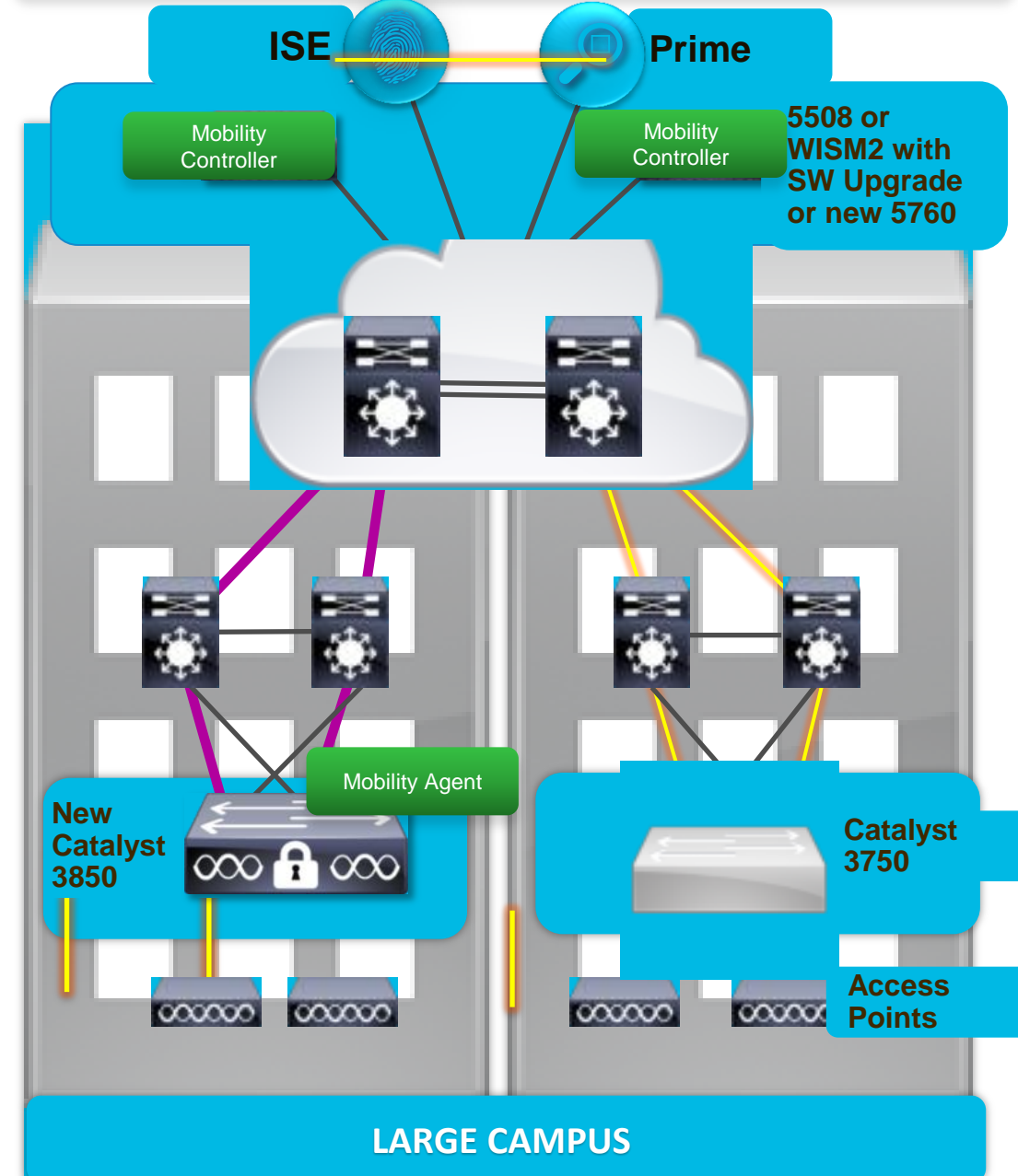


UP TO 50 ACCESS POINTS
UP TO 2,000 CLIENTS
ALL WAN SERVICES AVAILABLE



UP TO 250 ACCESS POINTS
UP TO 16,000 CLIENTS
VISIBILITY, CONTROL, RESILIENCY

EXTERNAL MOBILITY CONTROLLER NEEDED



UP TO 72,000 ACCESS POINTS
UP TO 864,000 CLIENTS
LARGEST LAYER 3 ROAMING DOMAINS

Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- **Wireless Deployment Options**
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

Cisco One Network: Wireless Deployment Modes

One Policy, One Management, One Network

Unified Access Wireless

Autonomous

FlexConnect

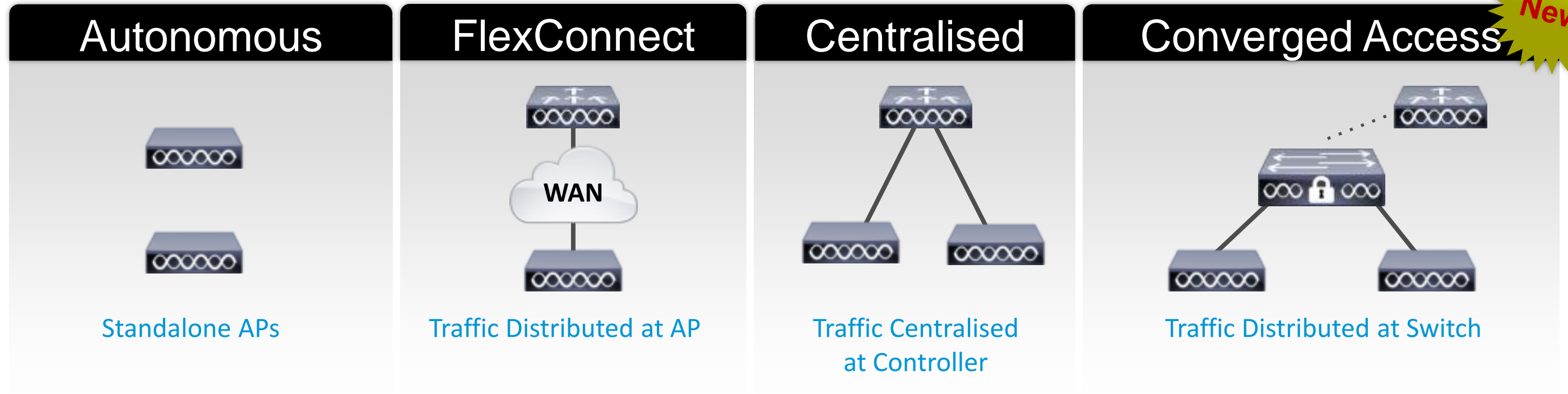
Centralised

Converged Access

New

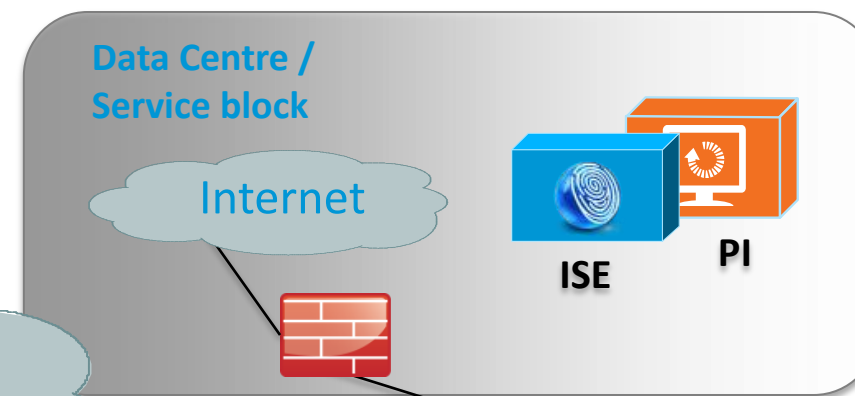
Unparalleled Deployment Flexibility

Unified Access—Wireless Deployment Modes

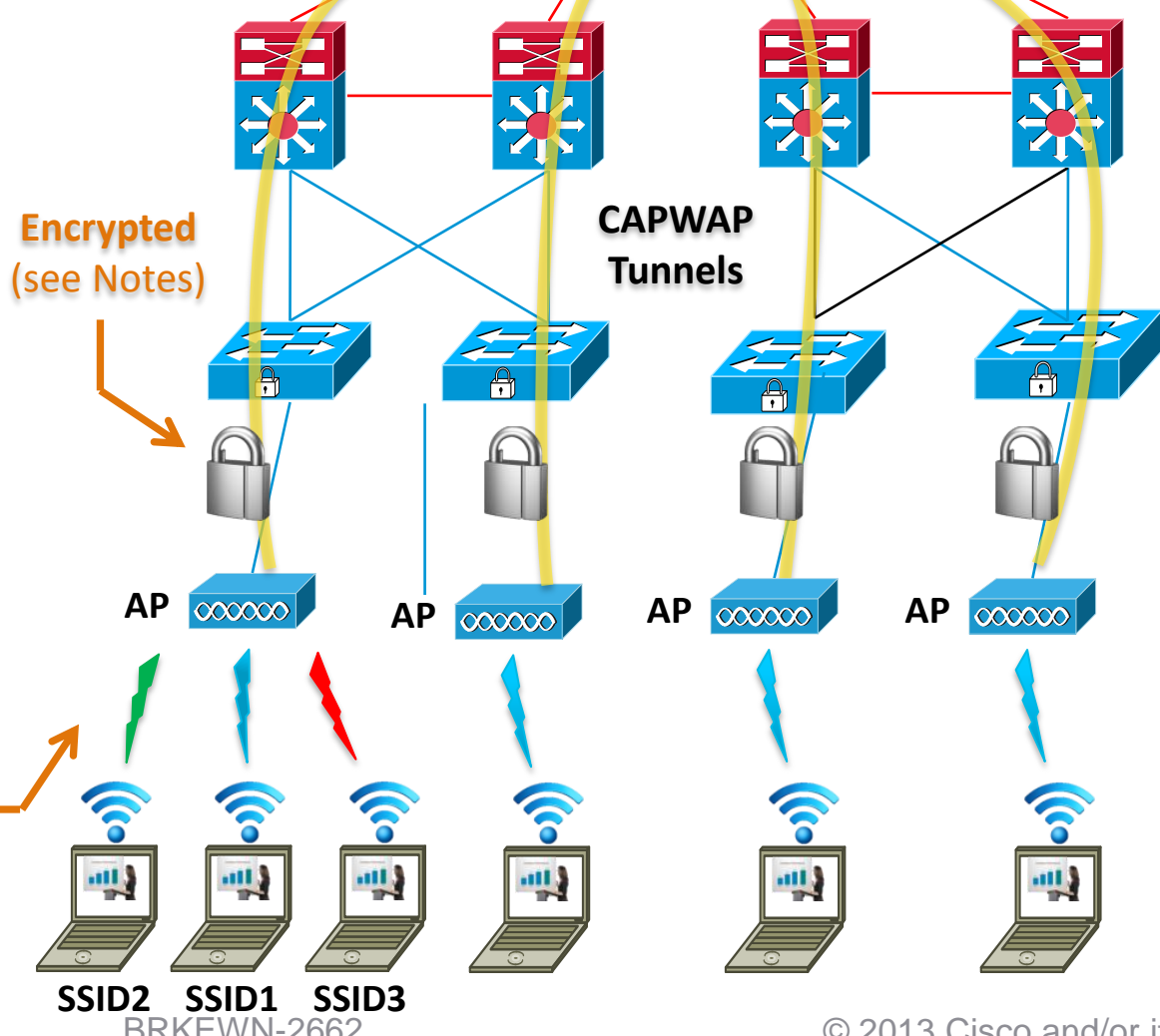
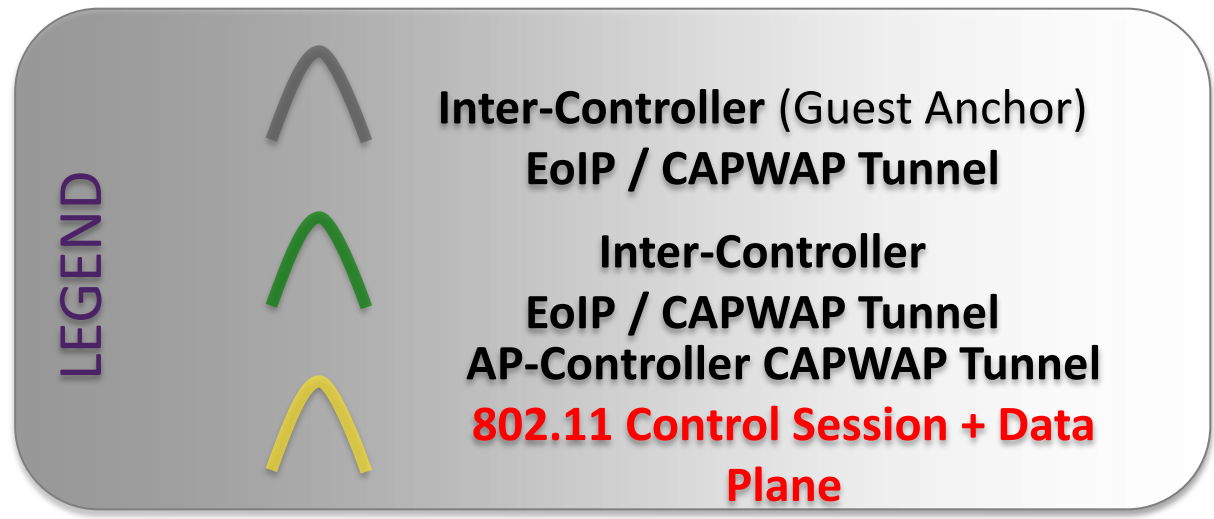
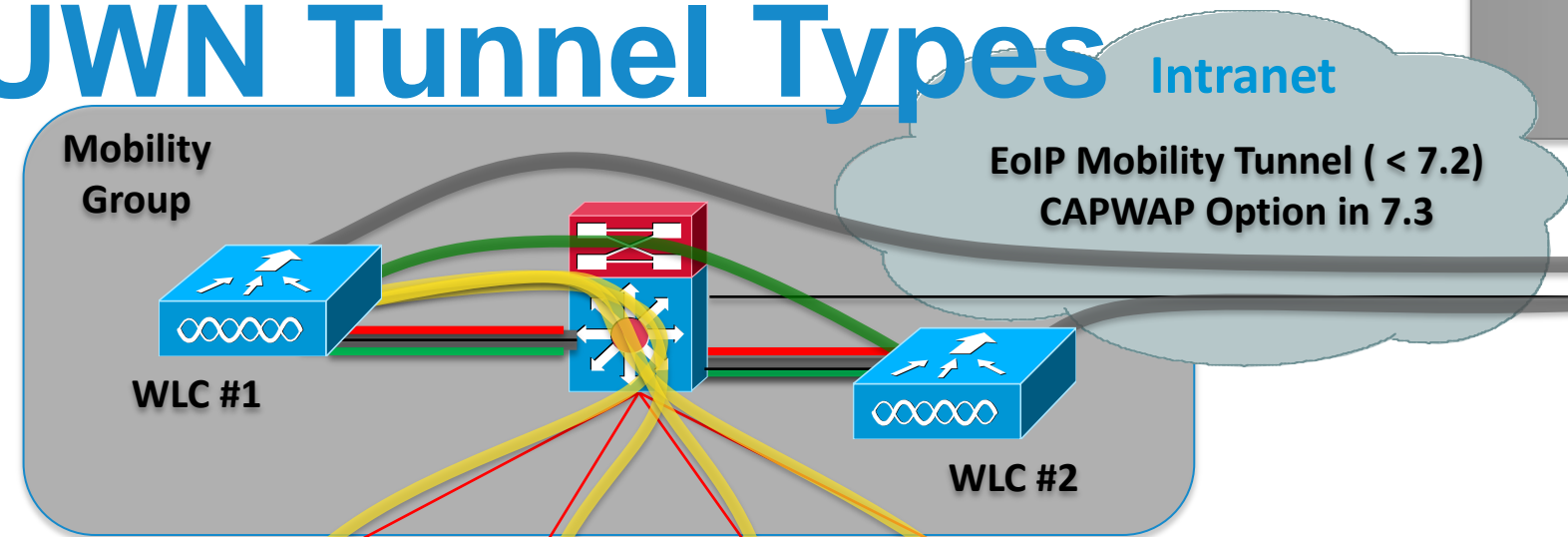


Target Positioning	Small Wireless Network	Branch	Campus	Branch and Campus
Purchase Decision	Wireless only	Wireless only	Wireless only	Wired and Wireless
Benefits	<ul style="list-style-type: none"> Simple and cost-effective for small networks 	<ul style="list-style-type: none"> Highly scalable for large number of remote branches Simple wireless operations with DC hosted controller 	<ul style="list-style-type: none"> Simplified operations with centralised control for Wireless Wireless Traffic visibility at the controller 	<ul style="list-style-type: none"> Wired and Wireless common operations One Enforcement Point One OS (IOS) Traffic visibility at every network layer Performance optimised for 11ac
Key Considerations	<ul style="list-style-type: none"> Limited RRM, no Rogue detection 	<ul style="list-style-type: none"> L2 roaming only WAN BW and latency requirements 	<ul style="list-style-type: none"> System throughput 	<ul style="list-style-type: none"> Catalyst 3850 in the access layer

Architecture Constructs – CUWN Tunnel Types



Well-known, proven architecture

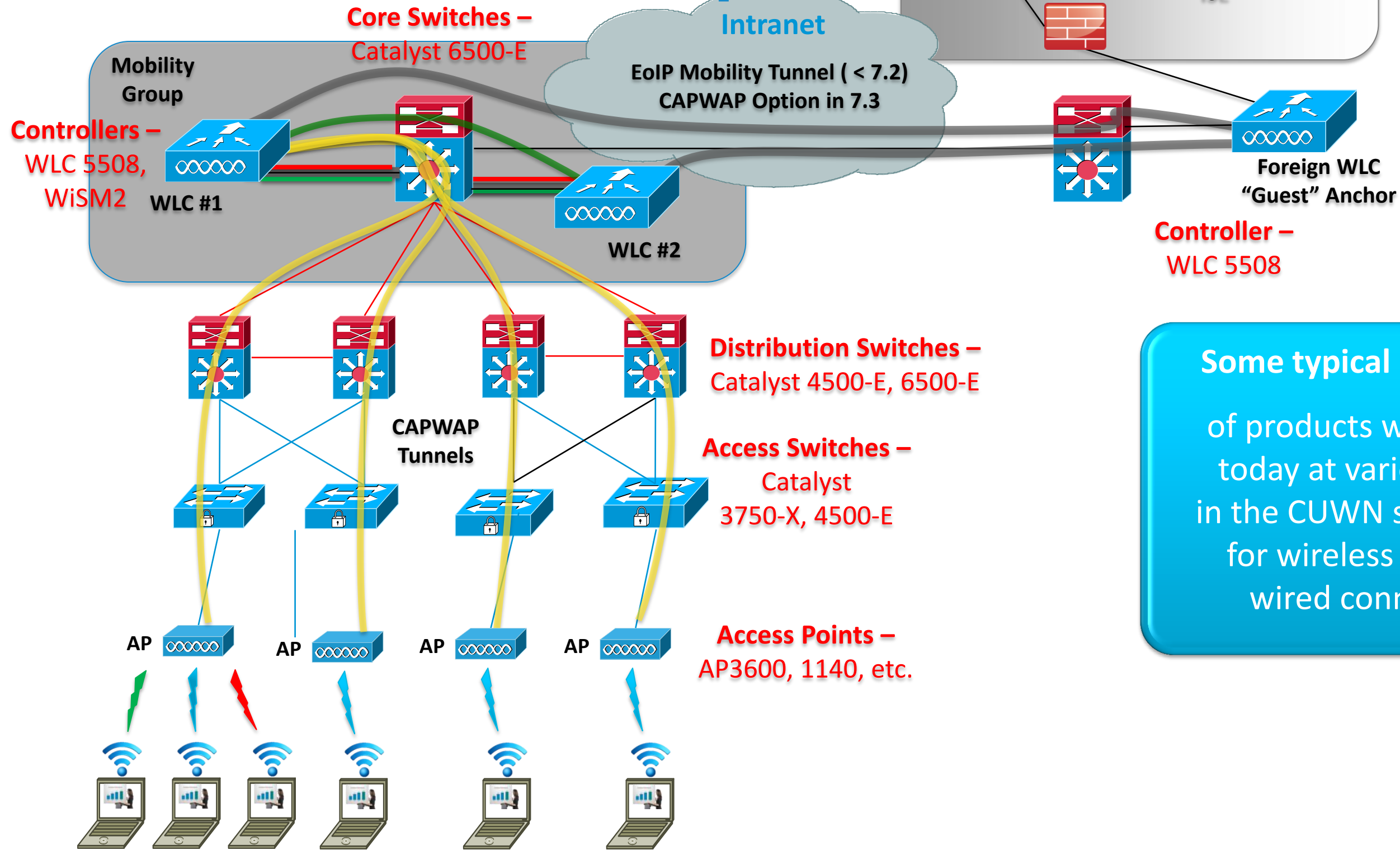
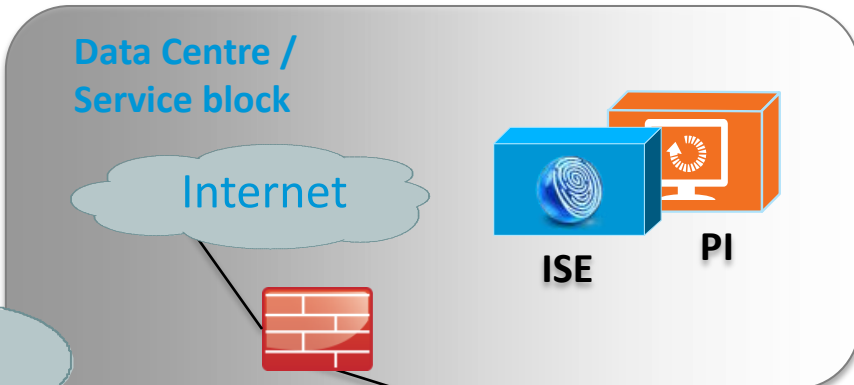


Notes –

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



Architecture Constructs – CUWN Product Examples

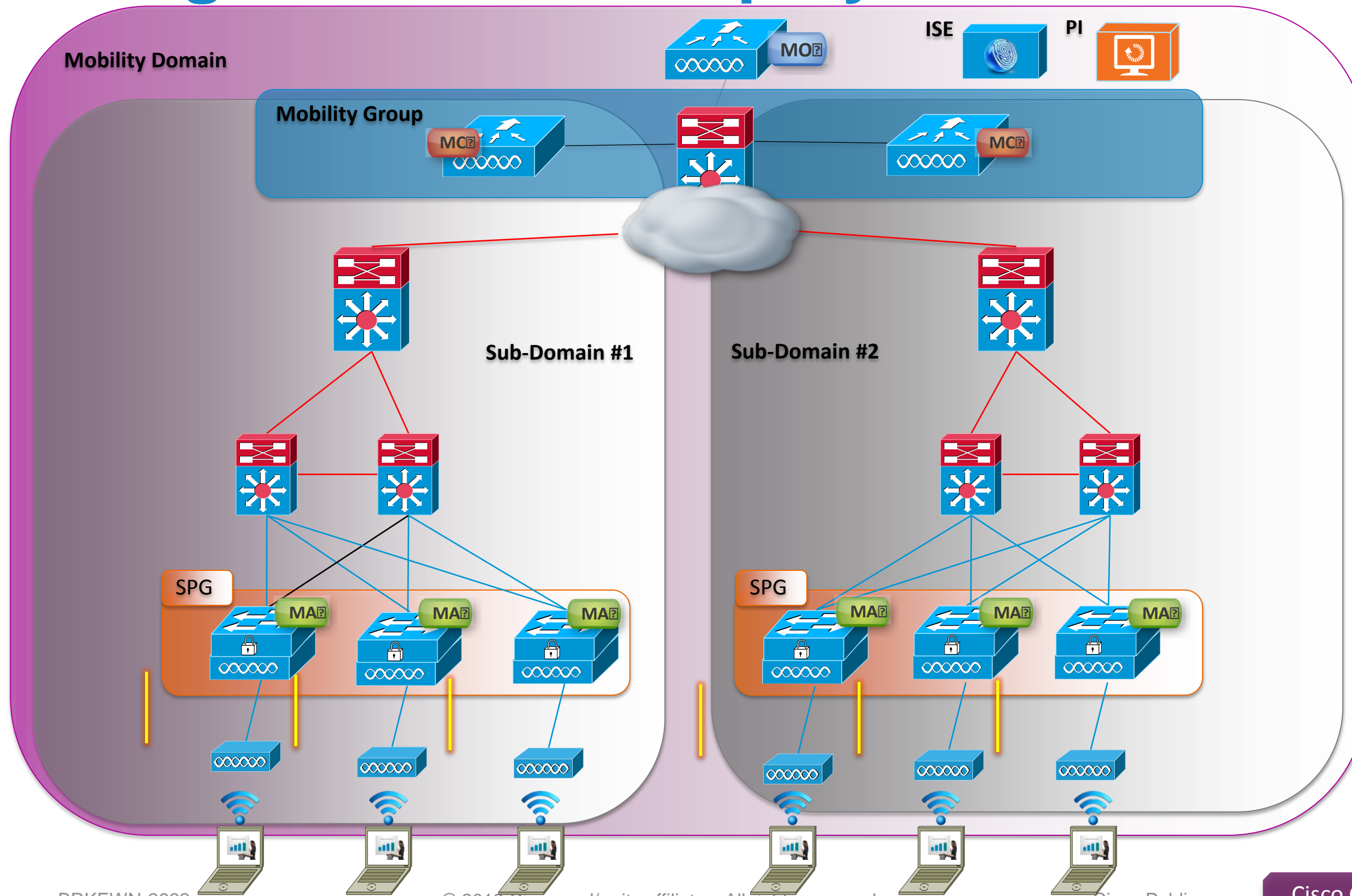


Well-known, proven architecture

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



Converged Access – Deployment Overview



Converged Access – Components – Physical vs. Logical Entities

Physical Entities –

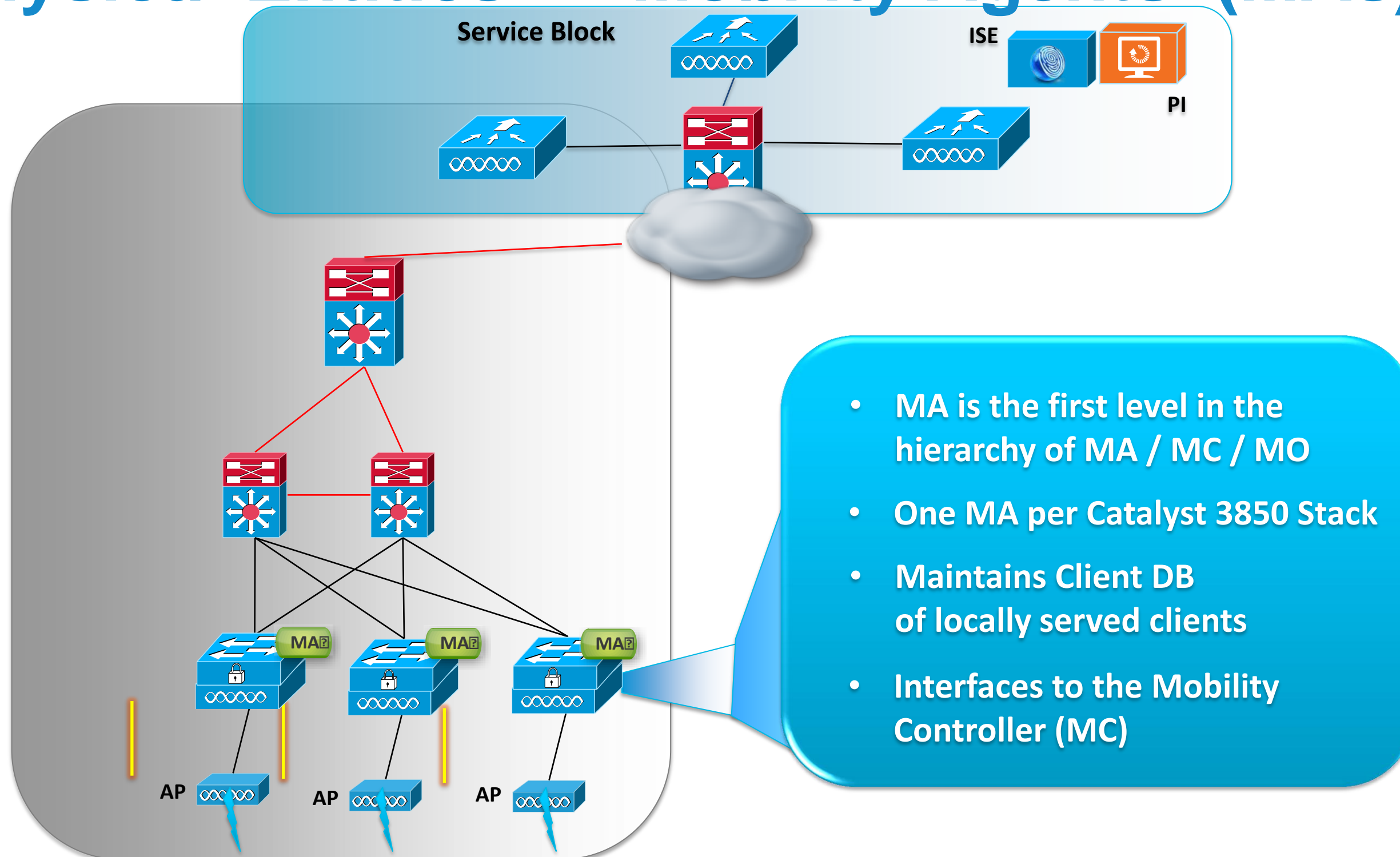
- **Mobility Agent (MA)** – Terminates CAPWAP tunnel from AP
- **Mobility Controller (MC)** – Manages mobility within and across Sub-Domains
- **Mobility Oracle (MO)** – Superset of MC, allows for Scalable Mobility Management within a Domain

Logical Entities –

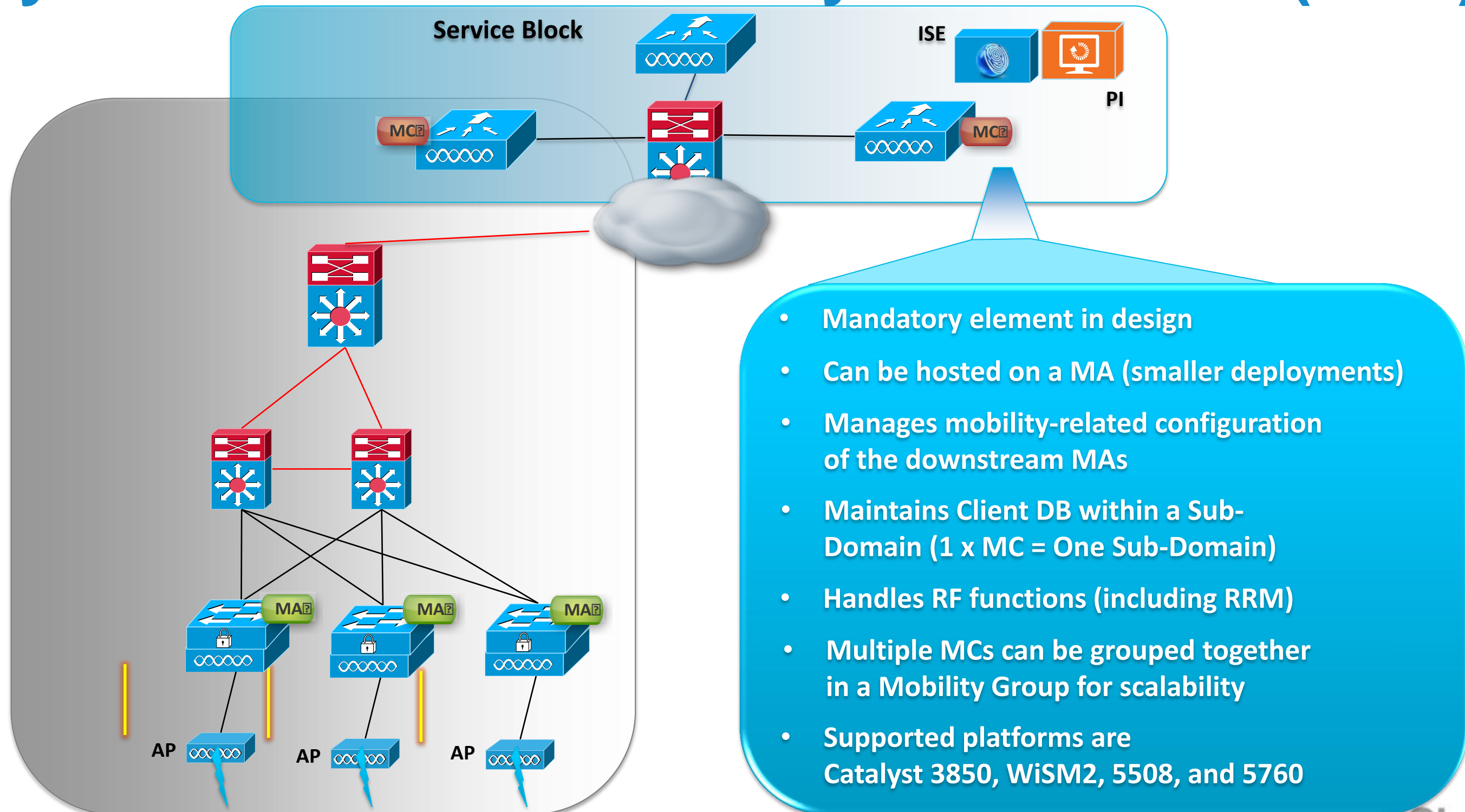
- **Mobility Groups** – Grouping of Mobility Controllers (MCs) to enable Fast Roaming, Radio Frequency Management, etc.
- **Switch Peer Group (SPG)** – Localises traffic for roams within its Distribution Block

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

Converged Access – Physical Entities – Mobility Agents (MAs)



Converged Access – Physical Entities – Mobility Controllers (MCs)

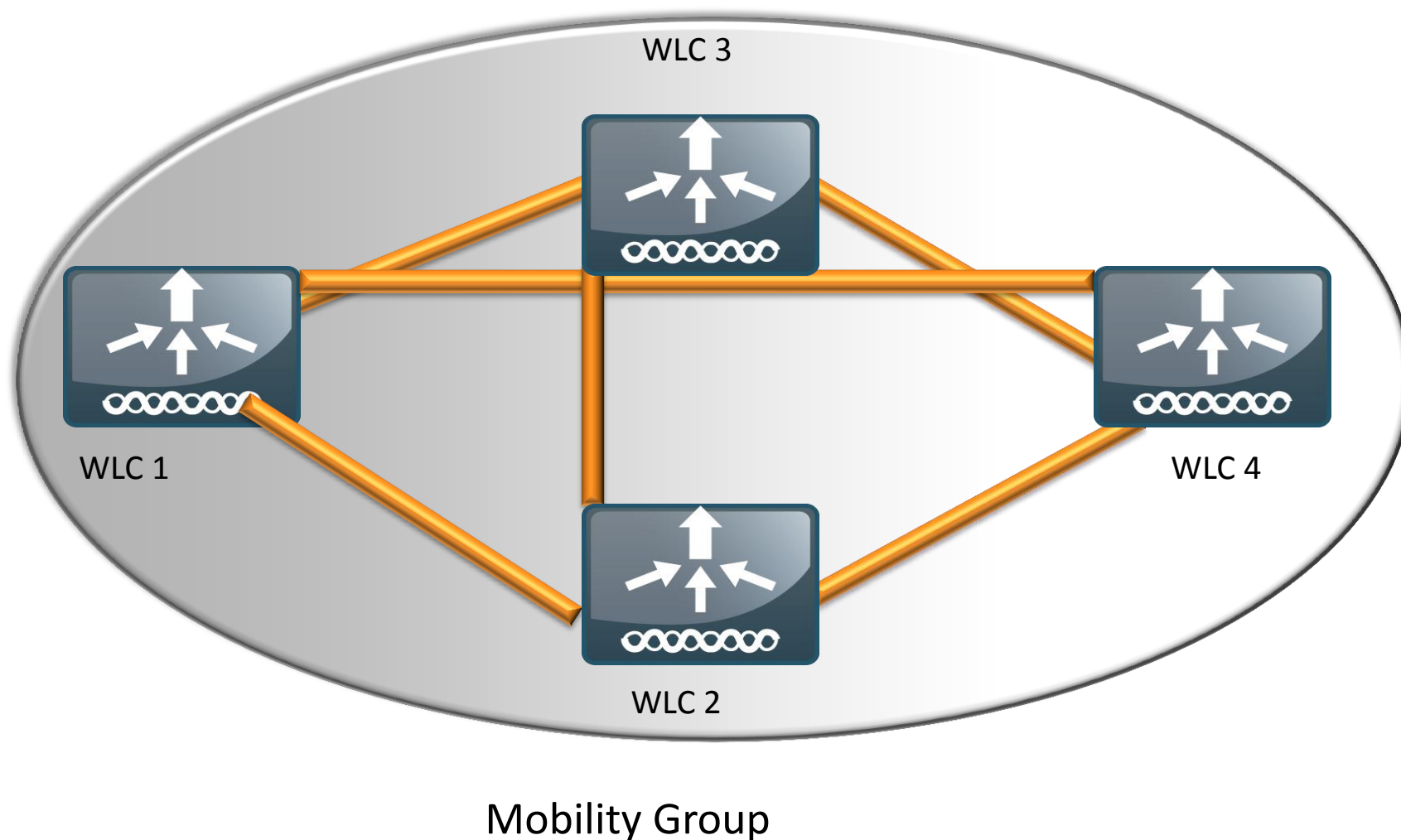


Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- **The new Converged Access Mobility Architecture**
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

Mobility Architecture AirOS

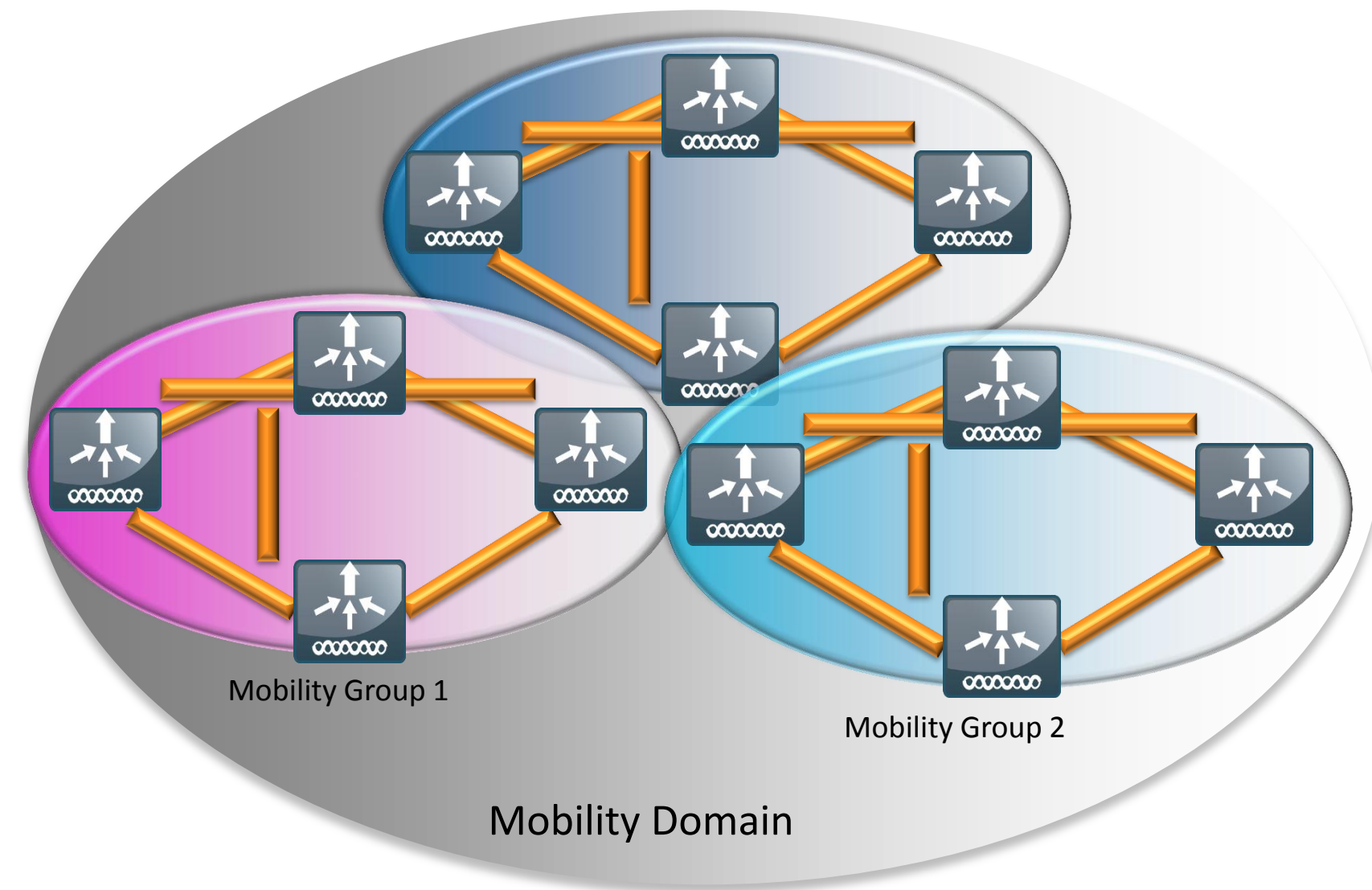
Mobility Group defined:



- Group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name
- Provides Seamless Mobility and Fast roaming for clients
- Up to 24 WLCs members in one Mobility Group, statically configured
- Full mesh of tunnels between members
 - Messages can be sent using Multicast
- Mobility Control Messages
 - UDP port 1666 for un-encrypted traffic
- User Data traffic
 - EoIP (IP protocol 97)
- NAT between members is supported

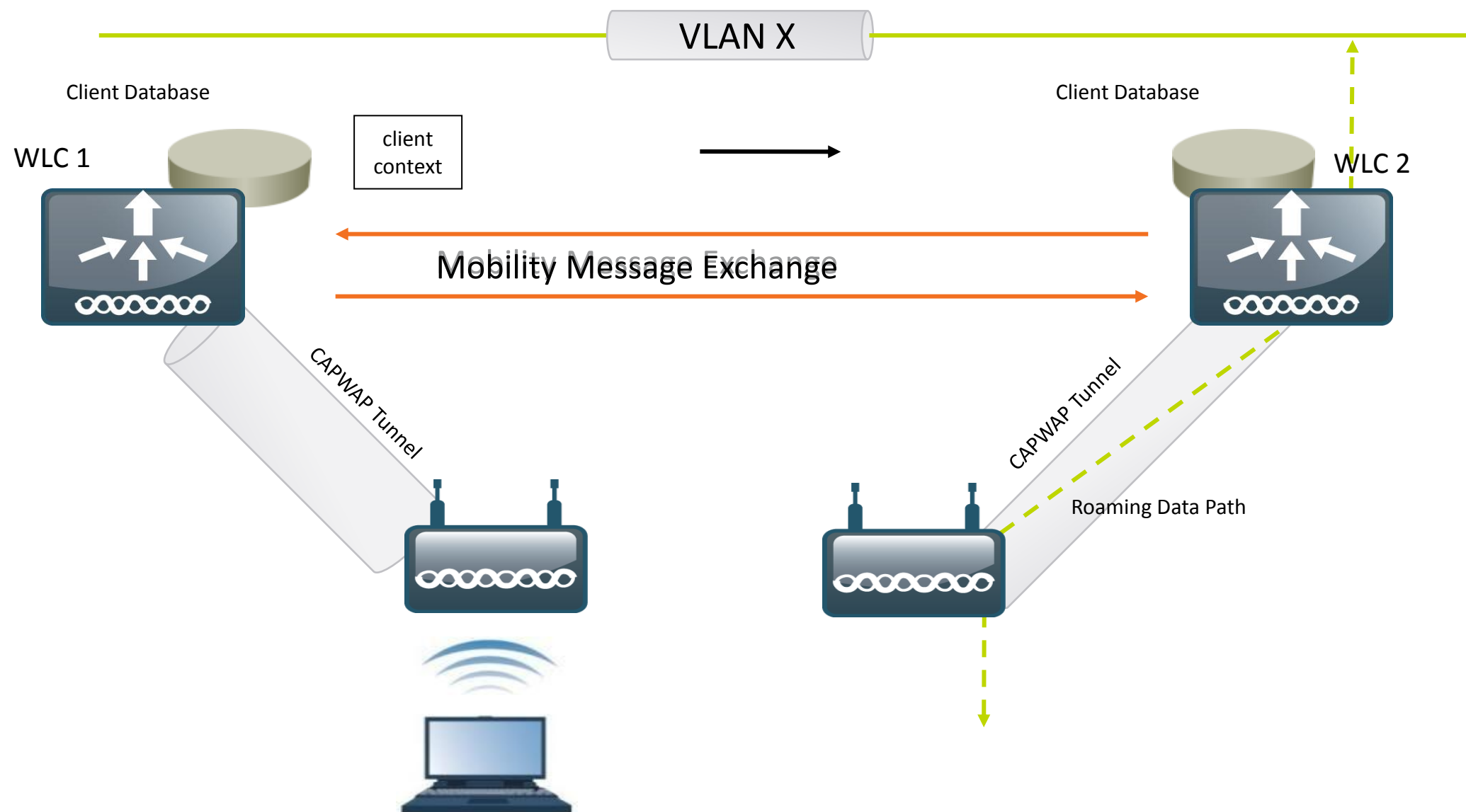
Mobility Architecture AirOS

Mobility Domain (List) defined:



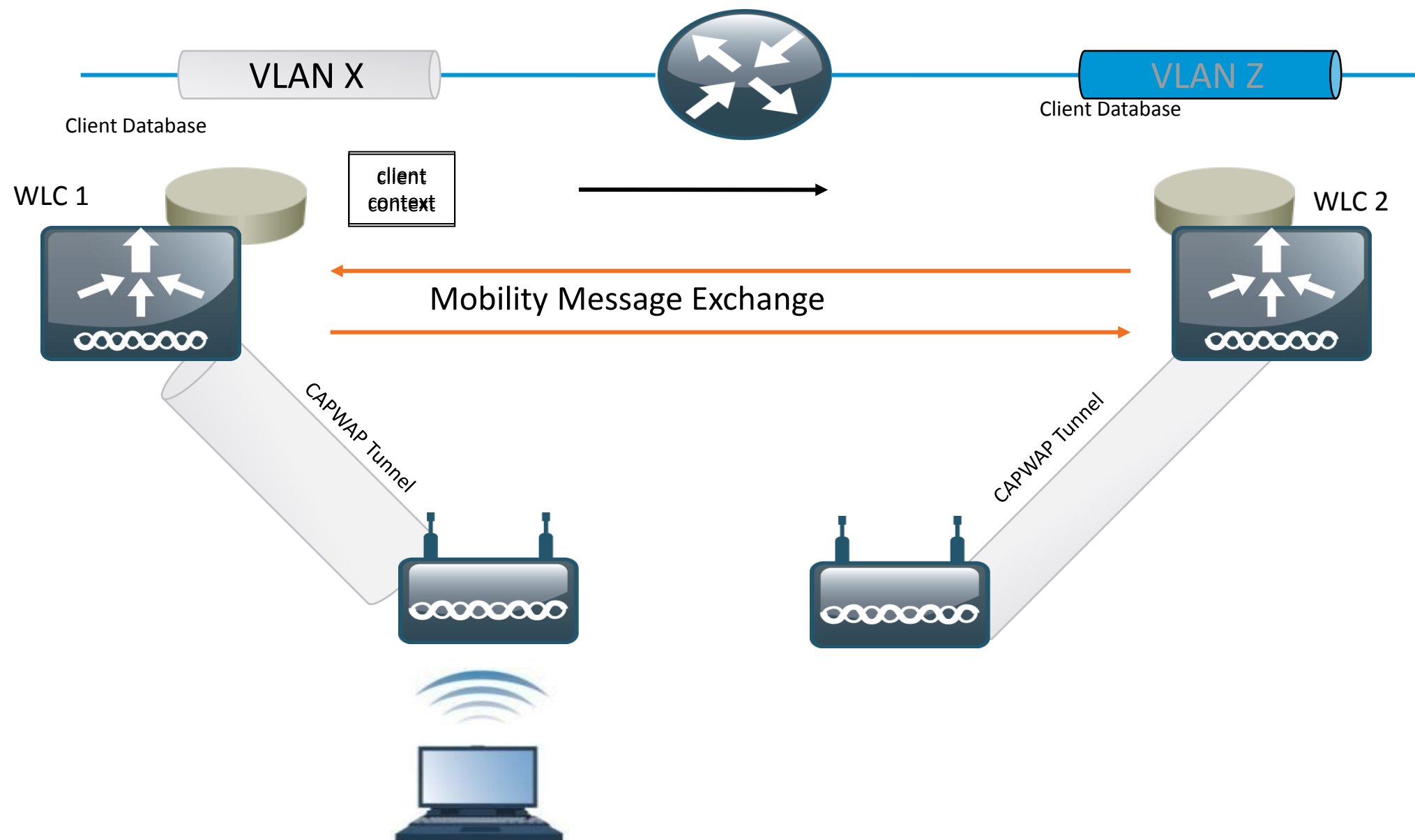
- Group of controllers configured on a single WLC that specifies members in different mobility groups
- Provides seamless Mobility for clients (client keep original IP address)
- Up to 72 WLCs in one WLC's Mobility List
- Full mesh of tunnels between members
Messages can be sent using Multicast
- Mobility Control Messages
UDP port 1666 for un-encrypted traffic
- User Data traffic
EoIP (IP protocol 97)
- NAT between members is supported

Inter-Controller Roaming: Layer 2



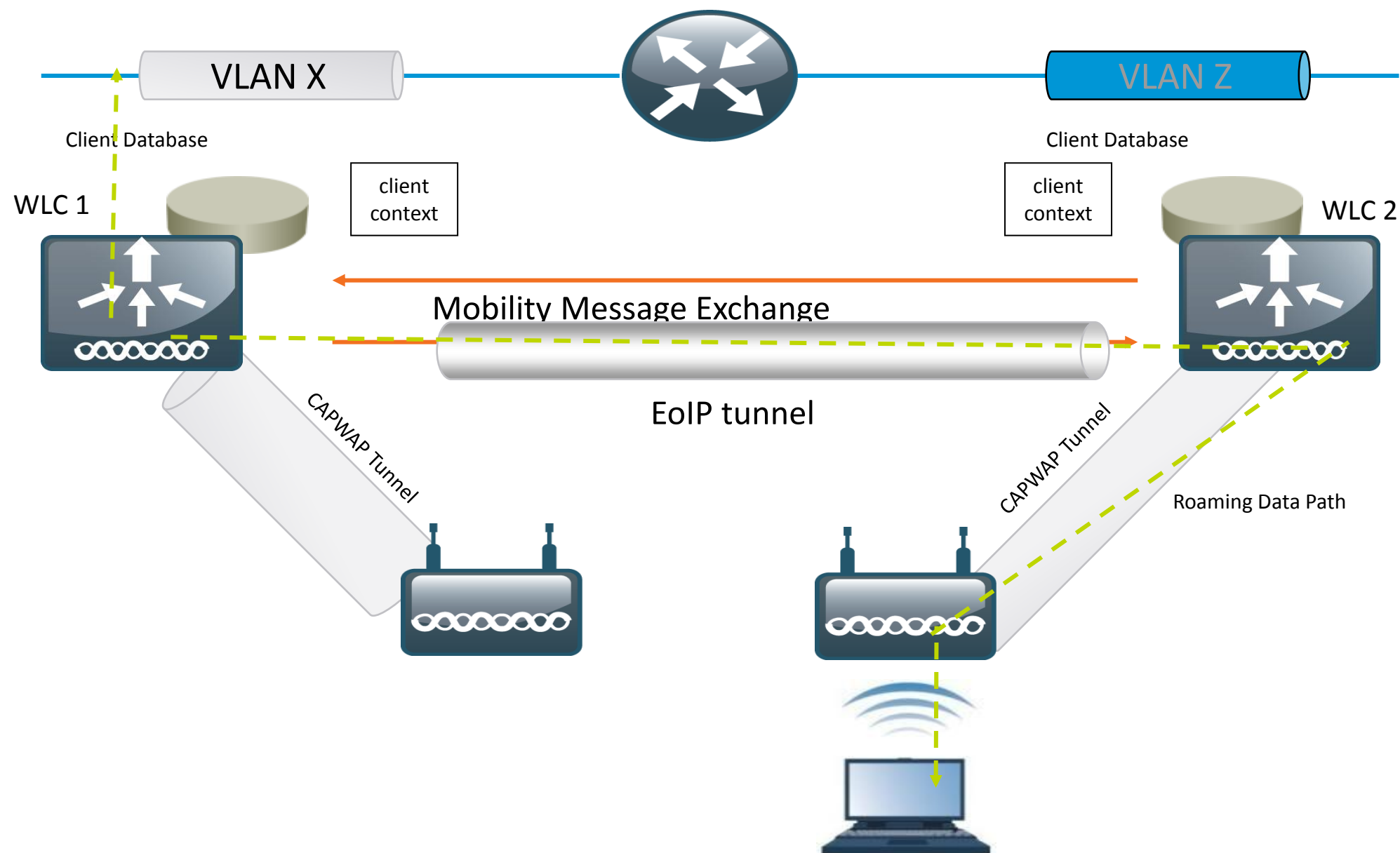
- Layer 2: same VLAN present on both controllers
- Client database context is **moved** from WLC1 to WLC2
- Client database is updated with new AP and security info
- Client becomes LOCAL to WLC-2
- No IP address refresh needed. Data flows as shown

Inter-Controller Roaming: Layer 3



- Layer 3: different client VLAN on controllers
- WLC-2 knows it doesn't have VLAN X
- Client database entry is **copied** from WLC1 to WLC2
- Client database is updated with new AP and security info

Inter-Controller Roaming: Layer 3 (continue..)



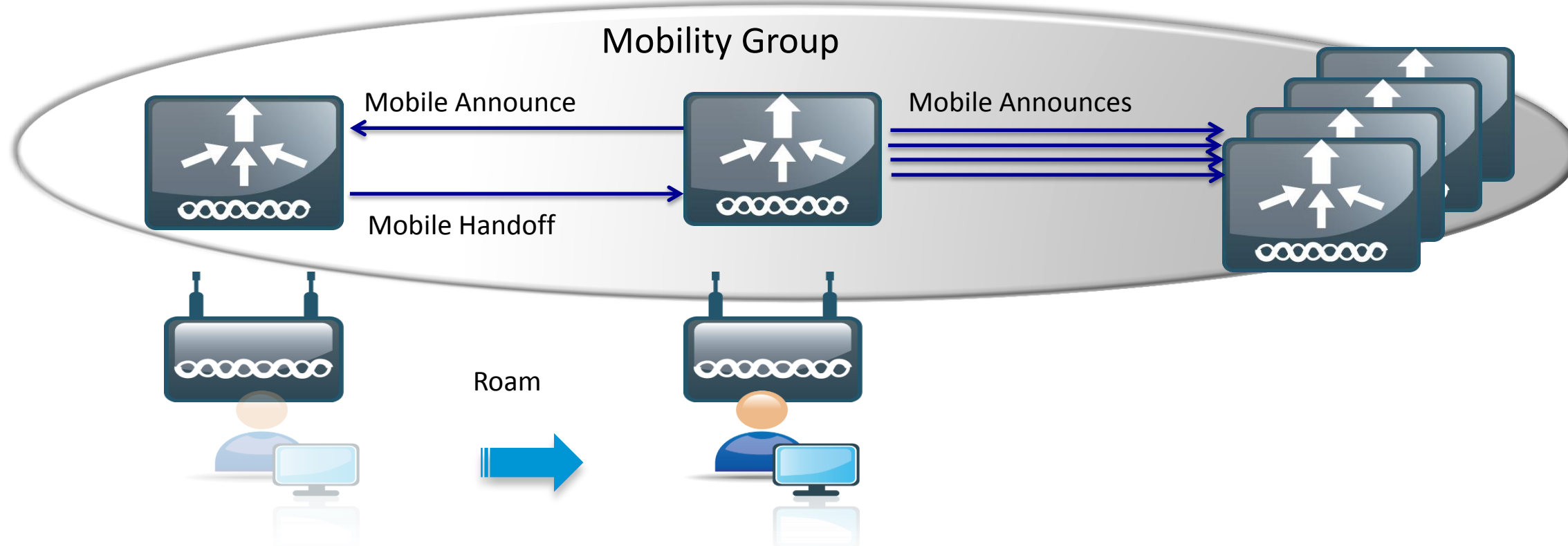
- WLC-1 is still the “anchor” for the client session
- Traffic goes through the EoIP tunnel and exit again in VLAN X
- No IP address change needed

Key considerations: Control Plane

- Full mesh of mobility tunnels among all controllers in a mobility group:

Every mobility event (first association or roaming) interrupts all controllers in the Mobility Group, since messages are sent to all the controllers in the Mobility Group.

Station initial attachment: Mobile Announce messages need to timeout 3 times before WLC realizes it's a new client and station's association is processed

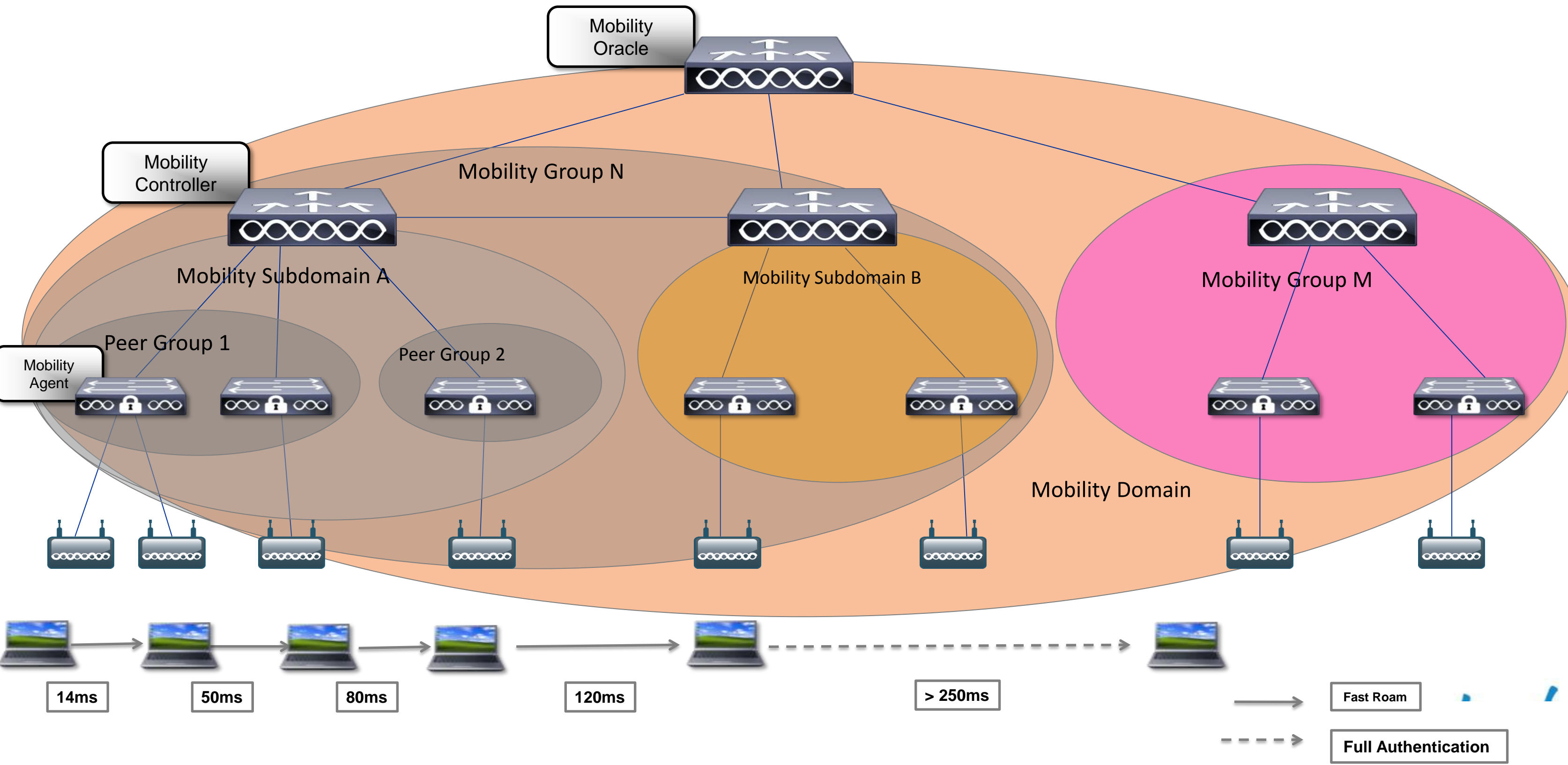


- A distributed and hierarchical approach to mobility, instead of a full mesh, limits the scope of the mobile announcements

Key considerations: Data Plane

- Today wireless Data Plane is centralised, wireless traffic is overlaid on top of the wired network:
 - All traffic hair-pinned back through the central Controller (local mode)
 - Traffic is not visible as it's inside a CAPWAP tunnel
 - Policies are usually applied in different places of the network for wired (switch) and wireless (Controller)
- A distributed wireless and wired data plane brings:
 1. Scalability: as wireless is terminated at access switch, same level of performance is delivered for wireless and wired
 2. Enable end to end traffic visibility for all traffic types from network access. Same tool for troubleshooting that are available for wired
 3. Common policy enforcement point for wired and wireless
 4. High Availability: wireless controller fault is isolated (for example to a single switch/floor)
 5. Rich media optimisation: support mission critical application with Qos applied closest to the source

Converged Access: Mobility Architecture

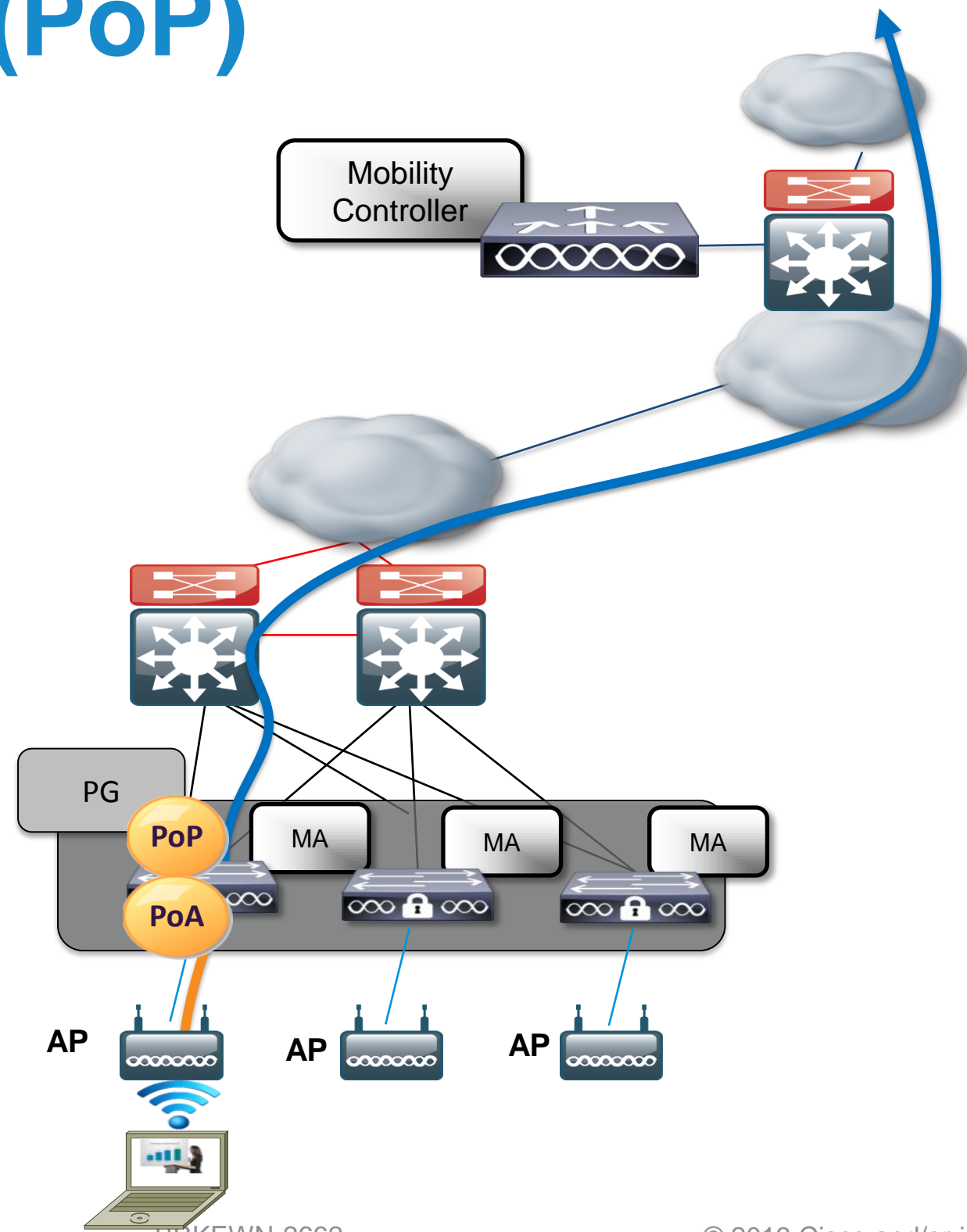


Converged Access Components

Scalability

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

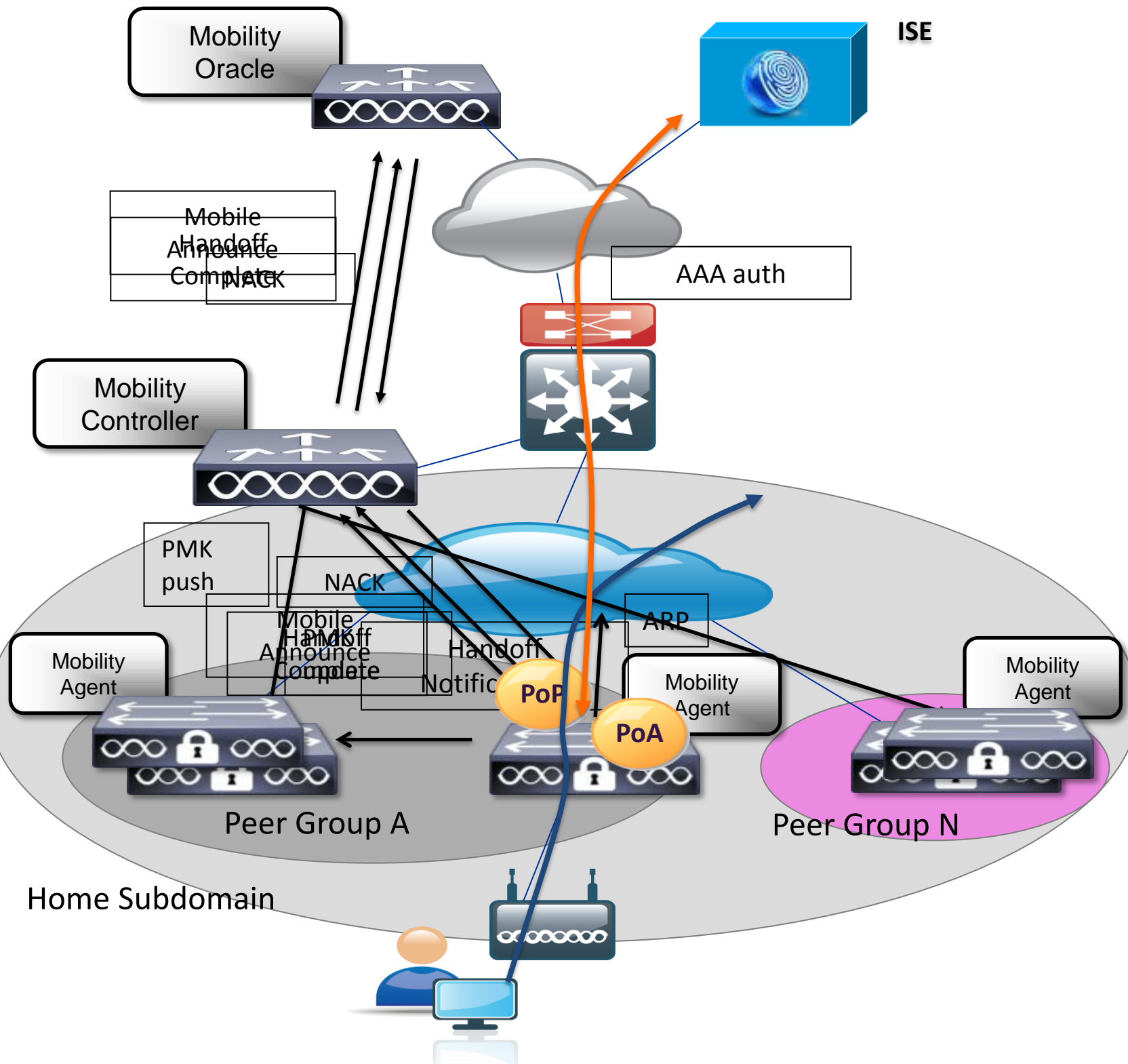
Point of Attachment (PoA) vs Point of Presence (PoP)



1. The station's **PoA** is where its data path is initially processed upon entry in the network
2. The station's **PoP** is the place in the wired network where the station is being advertised
3. Before a user roams, PoP and PoA are in the same place
4. If users associate and remain stationary, this is their traffic flow
5. Note: traffic doesn't flow through MC

— 802.11 in CAPWAP traffic
— 802.3 traffic

Mobility Protocol: Client first association



1. AAA client Authentication
2. **PMK update**
3. PMK Push (to all MAs in subdomain and other MCs in Mobility Group)
4. **Mobile Announce** MA to MC
5. Mobile Announce MC to MO
6. Mobile Announce NACK MO to MC
7. Mobile Announce NACK MC to MA
8. **Handoff Complete** MA to MC
9. Handoff Complete MC to MO
10. **Handoff Notification** to MAs (in the Peer Group)
11. PoP sends ARP and traffic flows as shown

Client First Association:

Front Lobby Feature

- **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 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 base:

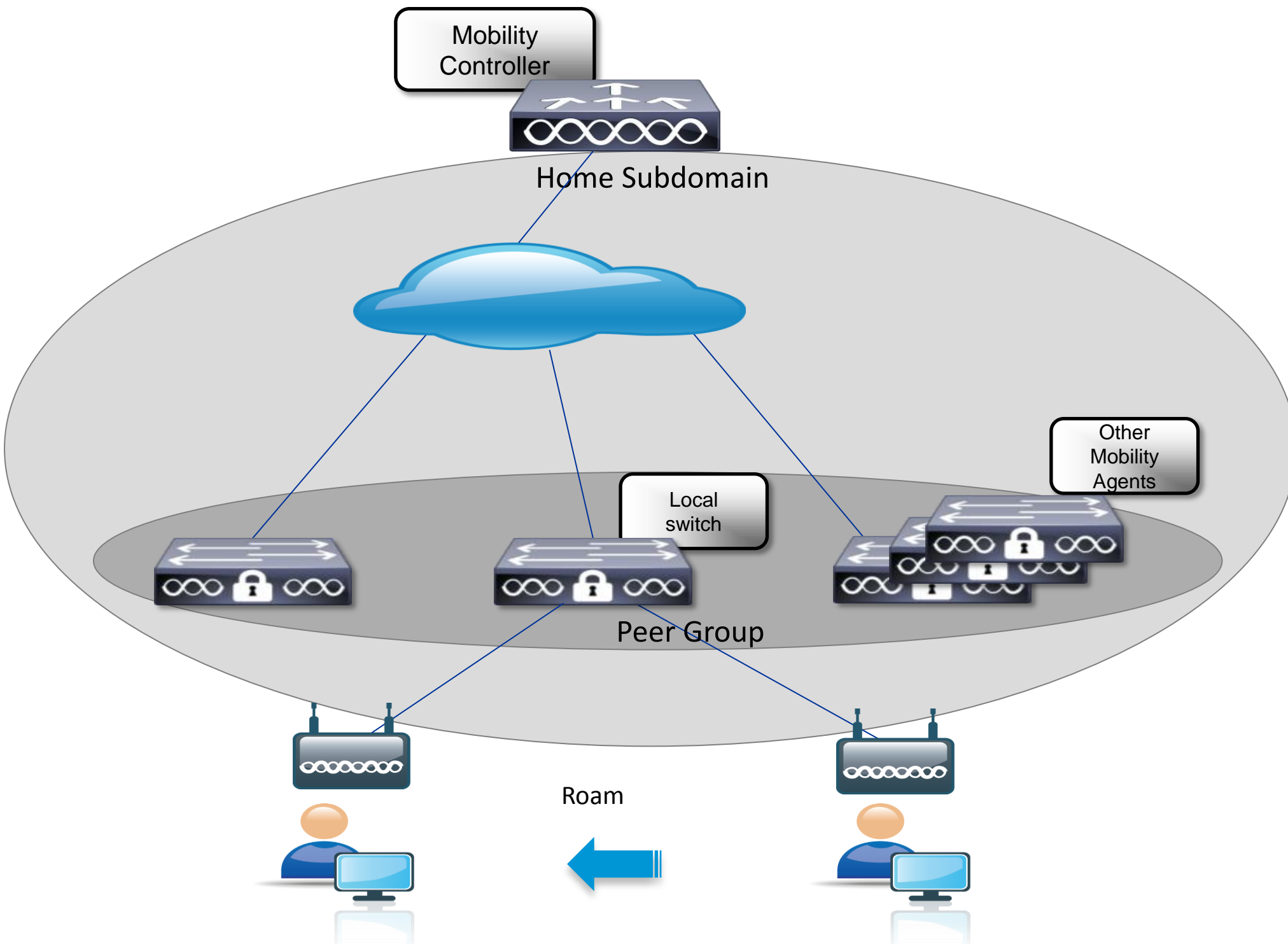
```
3850(config)#wireless mobility load-balance threshold ?
```

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

Basic Roam types: L2/L3

- When wireless client roams to a switch where client VLAN is present, it is considered as L2 Roam
 - In CUWN this would imply that the PoP moves to the new switch
 - In Converged Access this is configurable and by default the data path is anchored at the home switch (feature called “Sticky/L2 anchoring”, see next slides).
- When wireless client roams across L3 subnets (i.e. to switches where its own VLAN is not present), it is considered as L3 Roam.
 - same as CUWN, tunnelling is used to keep the client’s IP address
- In both cases, client will continue to maintain its original IP address: this is called seamless mobility.

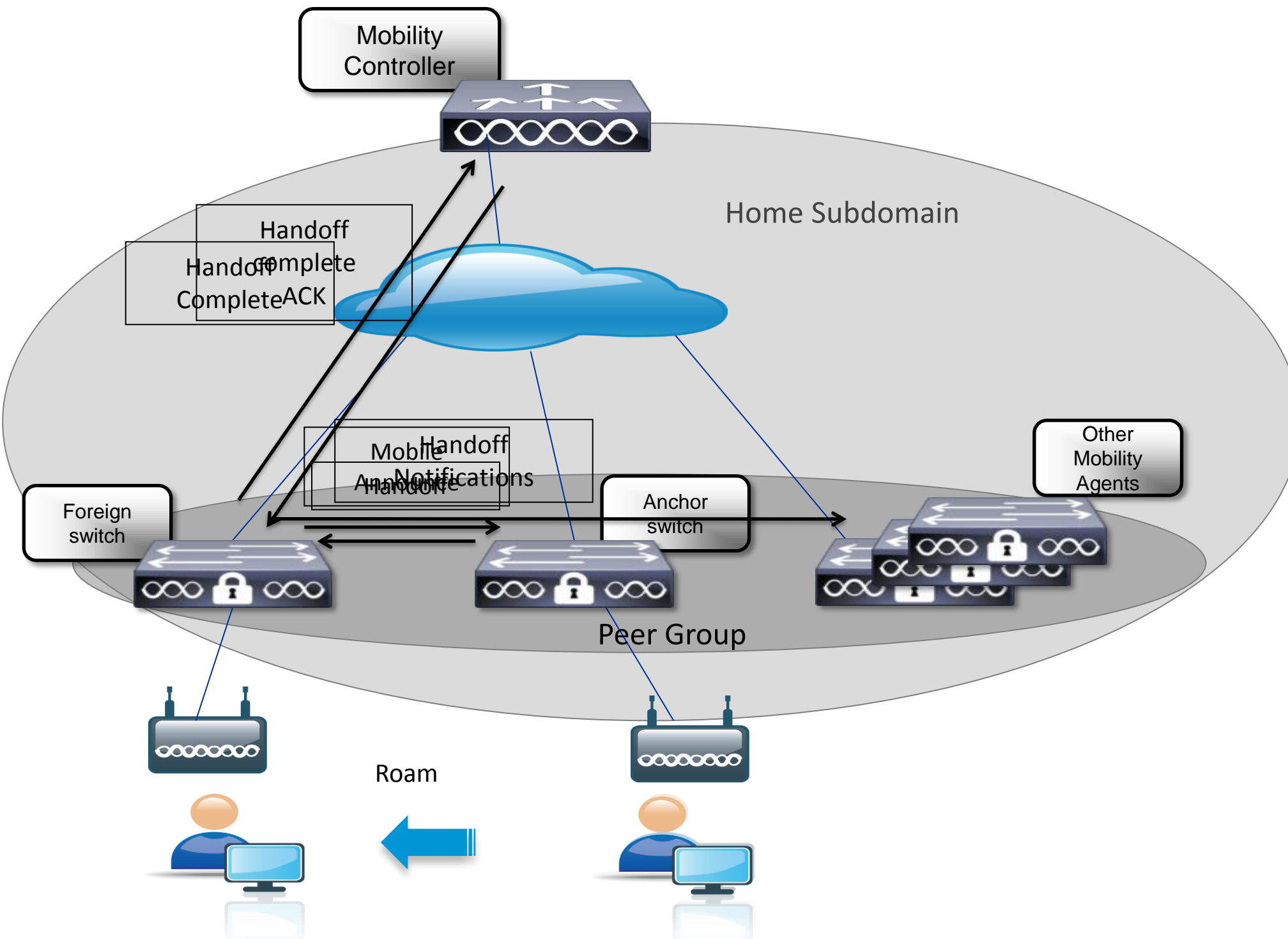
Intra Switch Roaming



1. Client roams
2. Internal database is updated
3. Mobility event is transparent to other members of the SPG and to MC

Intra Switch Peer Group (SPG) Roaming

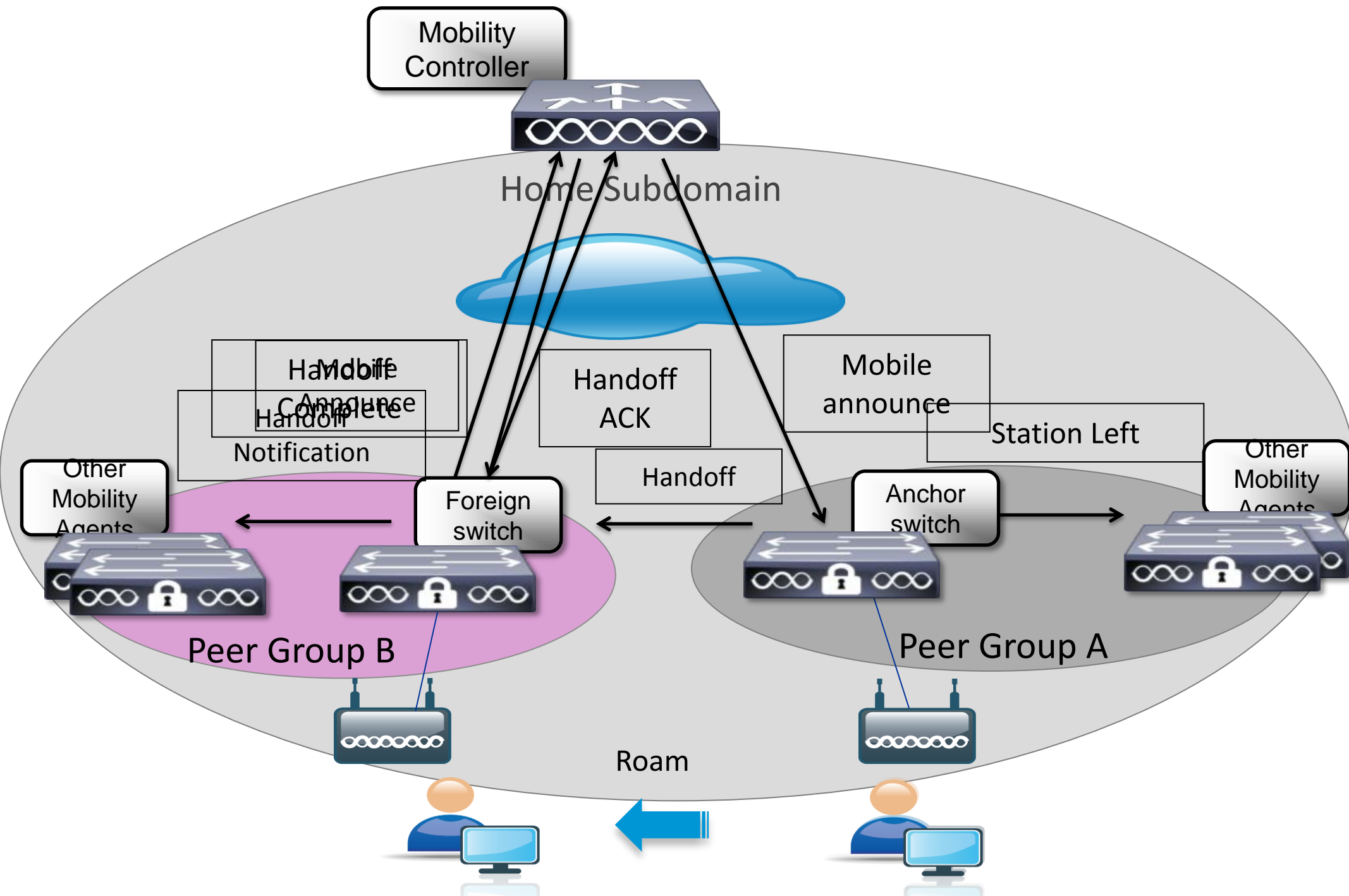
Control Plane



1. Client roams
2. Mobile Announce to Anchor MA
3. Handoff to Foreign
4. Handoff Complete to MC
5. Handoff Notifications sent to other MAs in the same SPG
6. Handoff Complete (ACK)
7. Note: messages to MC are kept to minimum, the roaming is faster

Inter SPG Roaming, same sub-domain

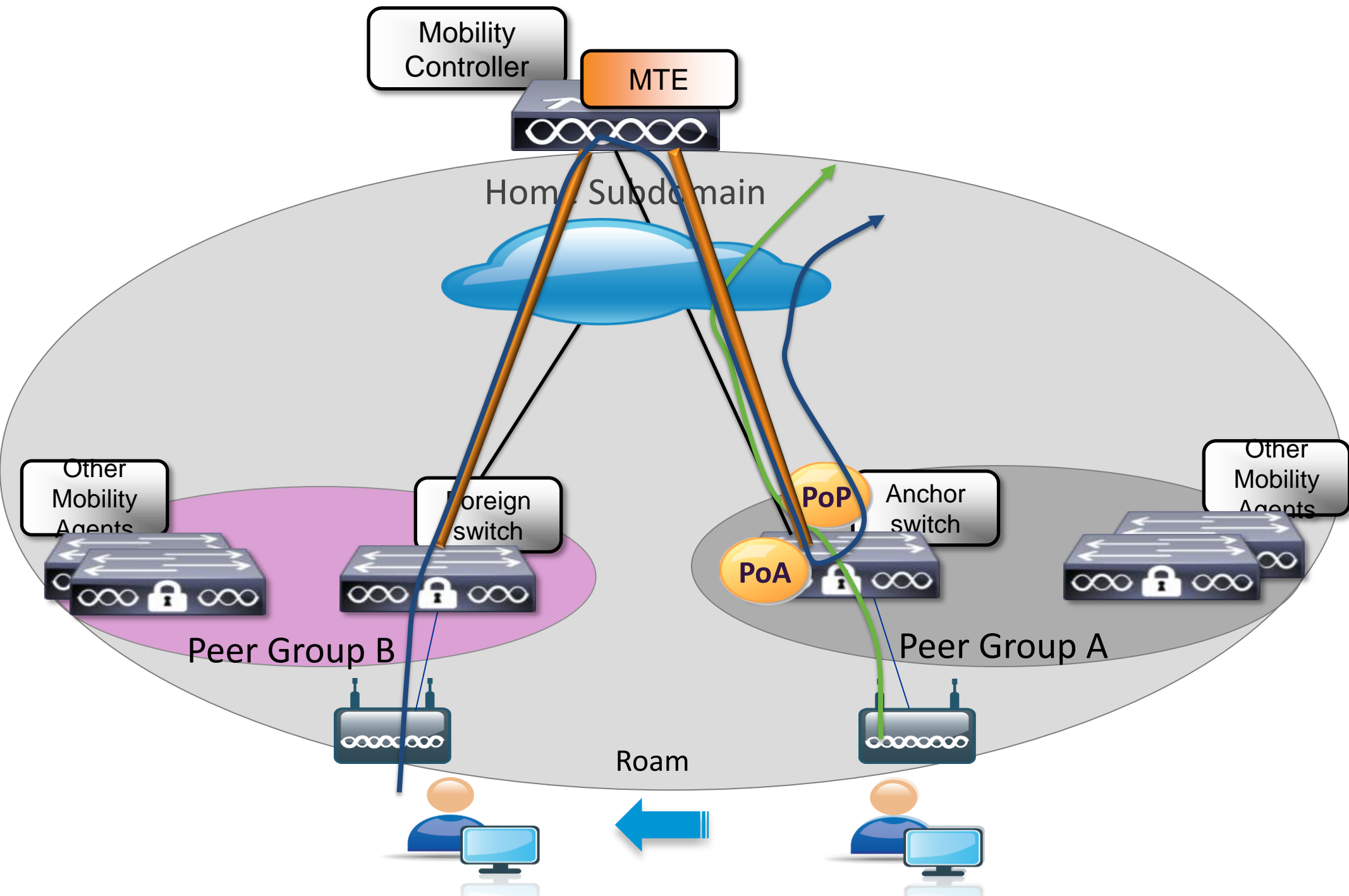
Control Plane



1. Client roams
2. Foreign has no info about the client: Mobile Announce to MC
3. Mobile Announce forwarded
4. Handoff to Foreign
5. Handoff complete to MC
6. Handoff Notification
7. Station Left message
8. Handoff ACK

Inter SPG Roaming, same sub-domain

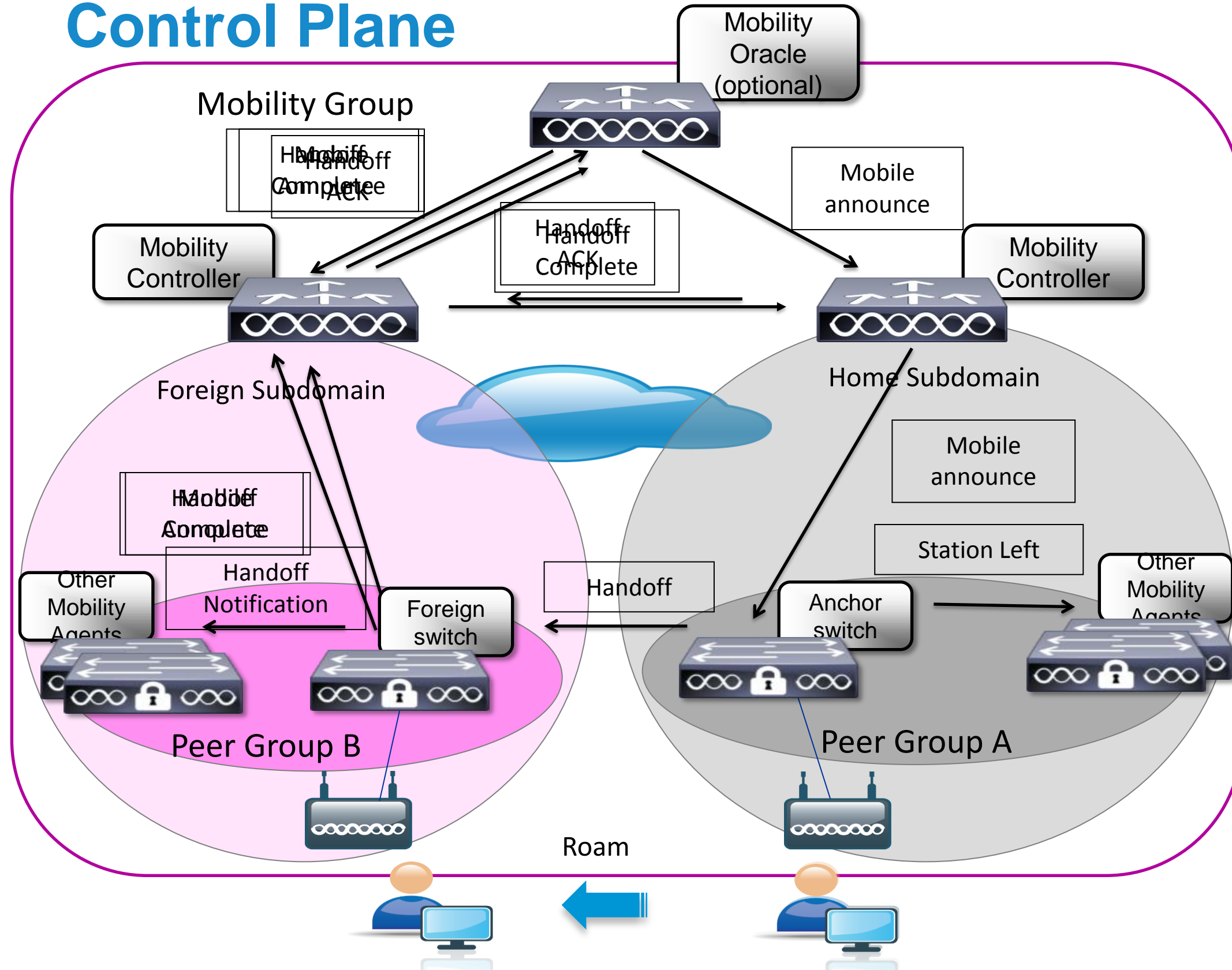
Data Plane



1. Client is at home switch
2. Traffic flows through PoP on anchor switch
3. Client roams
4. PoA moves to Foreign
5. PoP remains at anchor switch
6. MTE tunnelling functionality is used
7. Traffic flows as shown

Inter sub-domain roaming

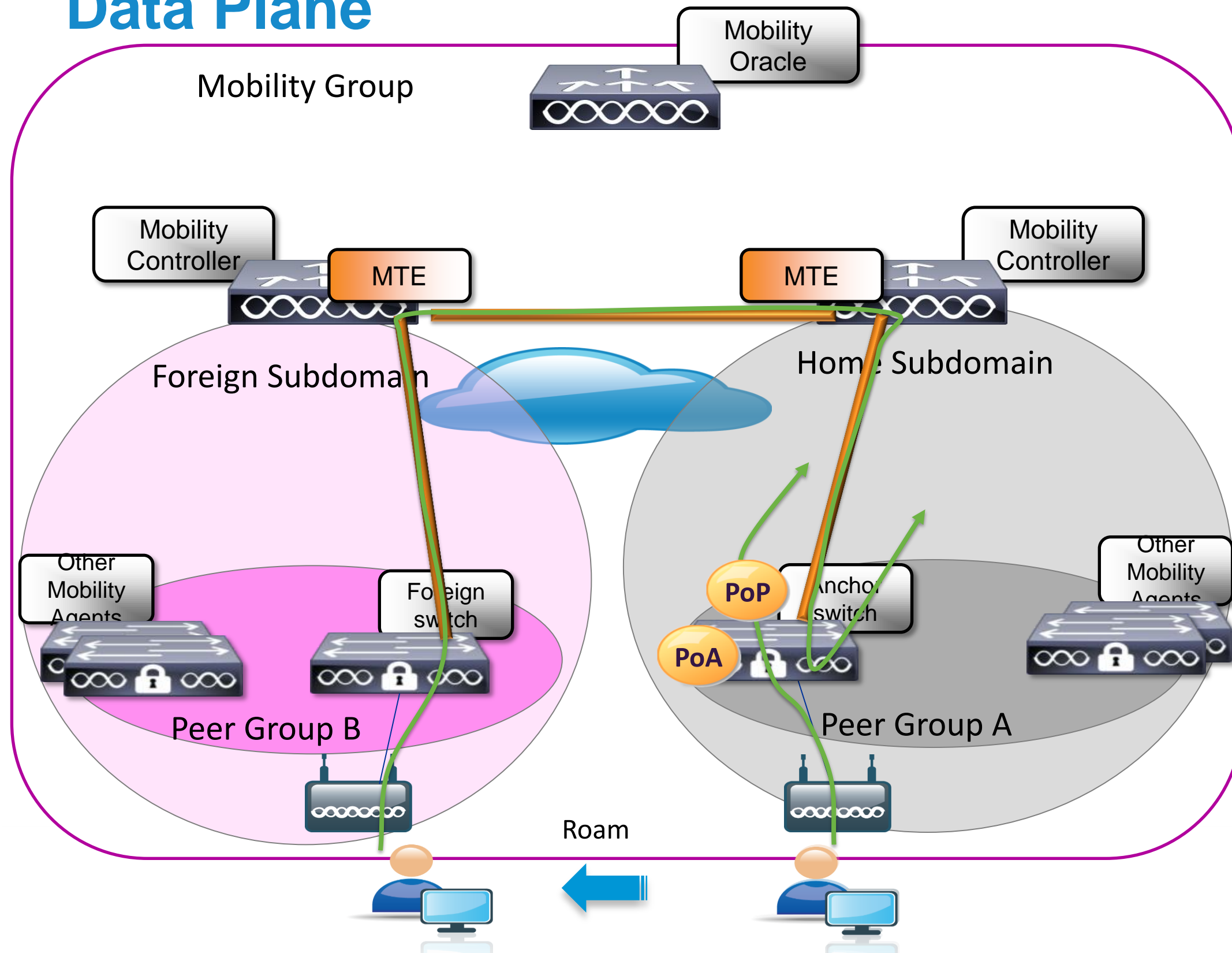
Control Plane



1. Client roams
2. Mobile Announce to MC
3. (Mobile Announce to MO)
4. Mobile Announce forwarded to Anchor through MC
5. Direct Handoff to Foreign
6. Handoff complete to MC
7. Station Left messages
8. Handoff Notifications
9. Handoff to other MCs (and MO)
10. Handoff ACKs

Inter sub-domain roaming

Data Plane



1. Client is at home switch
2. Traffic flows through PoP on anchor switch
3. Client roams
4. PoA moves to Foreign
5. PoP remains at anchor switch
6. MTE tunnelling functionality is used
7. Traffic flows as shown

Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- **Converged Access – IP Addressing**
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

Converged Access – IP Addressing – For Wireless Management / APs

Wireless LAN Management for directly-attached APs on Catalyst 3850

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

```
interface GigabitEthernet1/0/1
description to_AP
switchport access vlan 20
switchport mode access
```

```
interface Vlan20
ip address 10.0.20.1 255.255.255.0
!
wireless management interface Vlan20
```

If you do not define a wireless management VLAN on the 3850 (i.e. no “`wireless management interface vlan x`” in the config), the switch will then be transparent to AP attachment and everything will continue to operate as it does today on a 3750-X, i.e. AP attachment to centralised controller, DHCP option 43 controller assignment, etc.

- As soon as you define a «Wireless management interface VLAN», the Catalyst 3850 will intercept all incoming AP requests, and terminate / process them at the local CPU.

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)

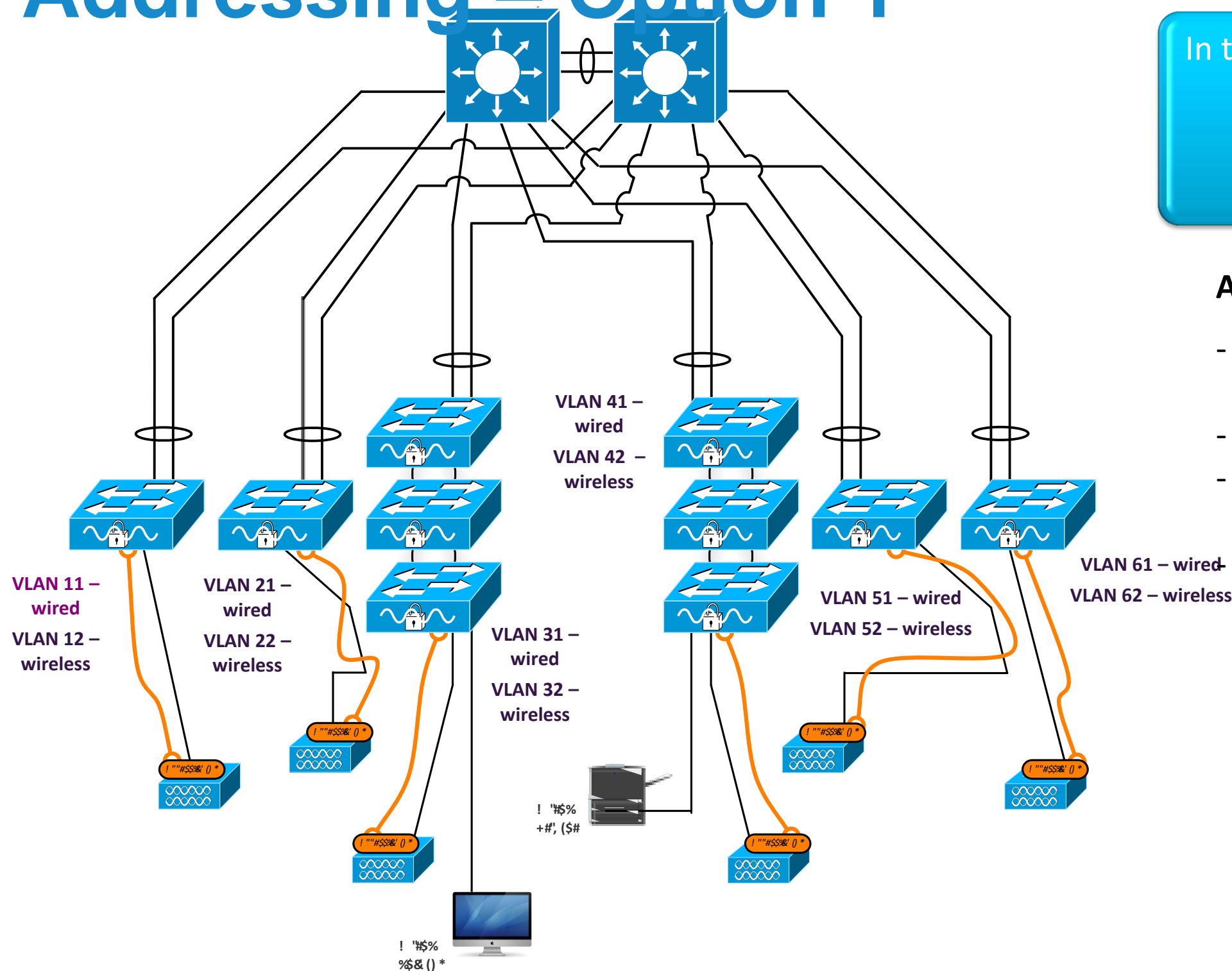
There are trade-offs between each of these IP addressing design models.

On the following slides, we have attempted to summarise some of the pluses and minuses of each of these IP addressing options. Prescriptive guidance for IP address deployment in Converged Access requires additional testing and validation.

Converged Access – IP Addressing – Option 1

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 customer 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

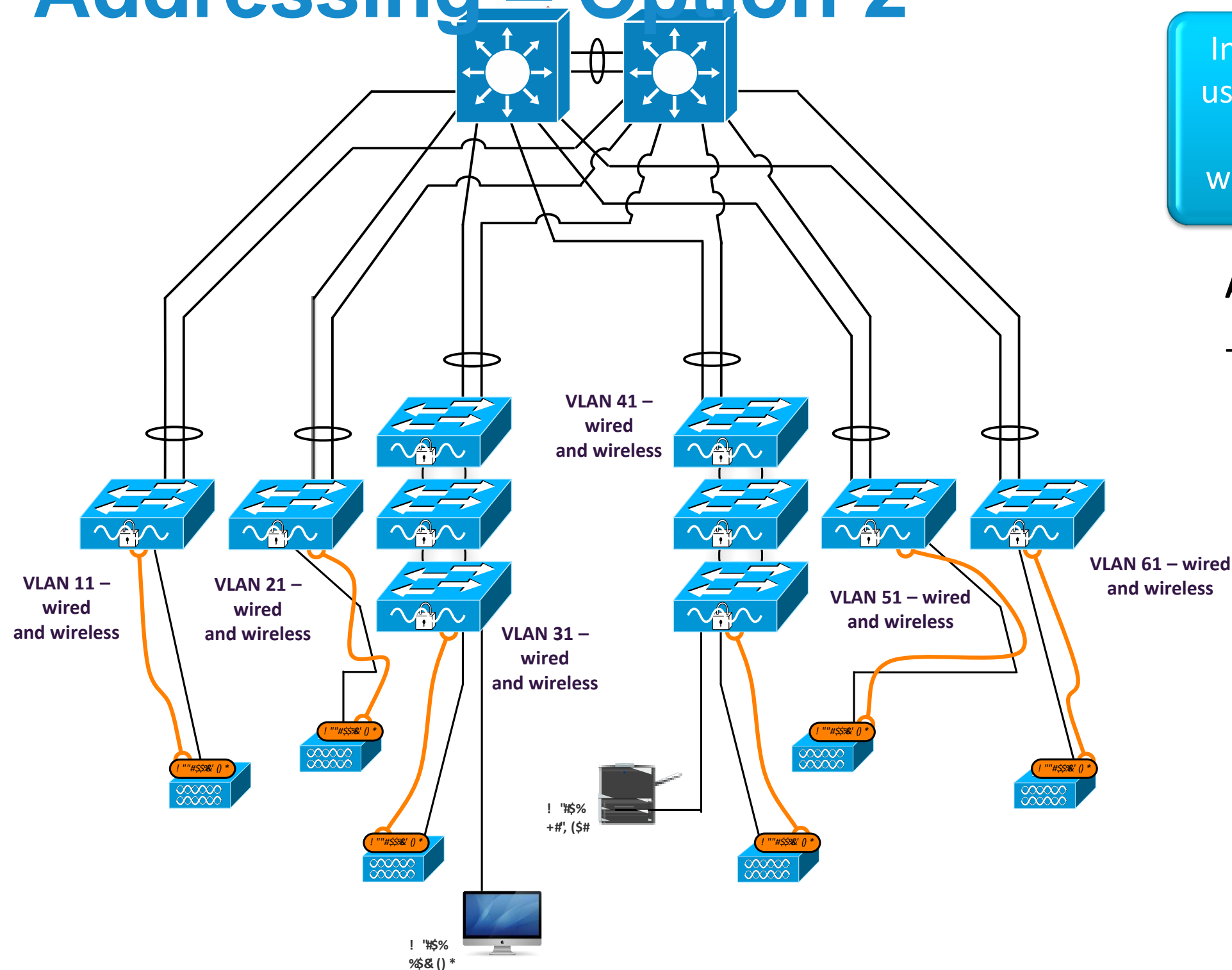
DRAWBACKS –

- 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

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. Opt. 1

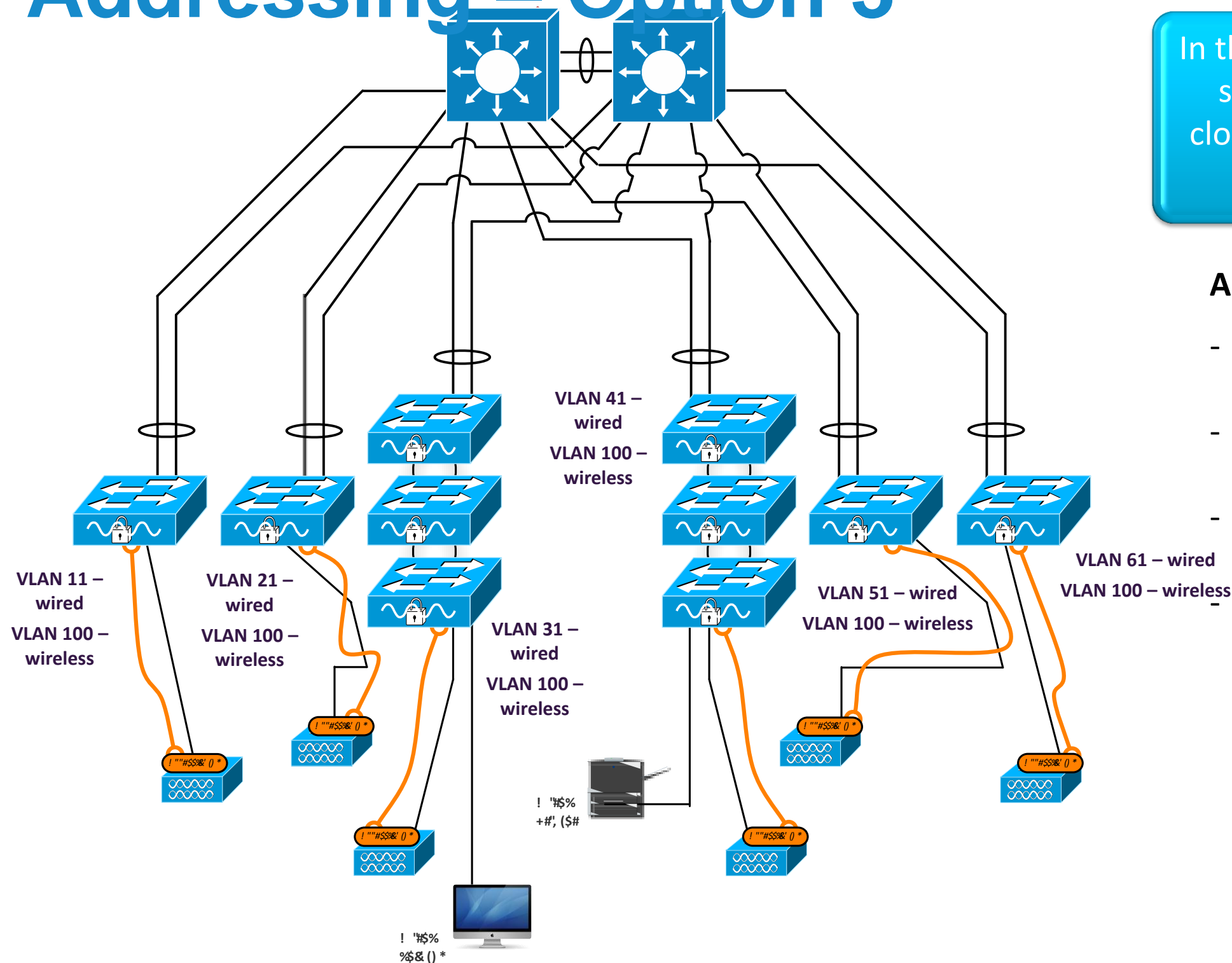
DRAWBACKS –

- 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. Opt 1)
- Possible DHCP contention, wired / wireless

Converged Access – IP Addressing – Option 3

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. Opt. 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)

DRAWBACKS –

- Optimised with VSS, or single-control-plane, at distribution (to avoid L2 loops)
- Topology differs, wired vs. wireless

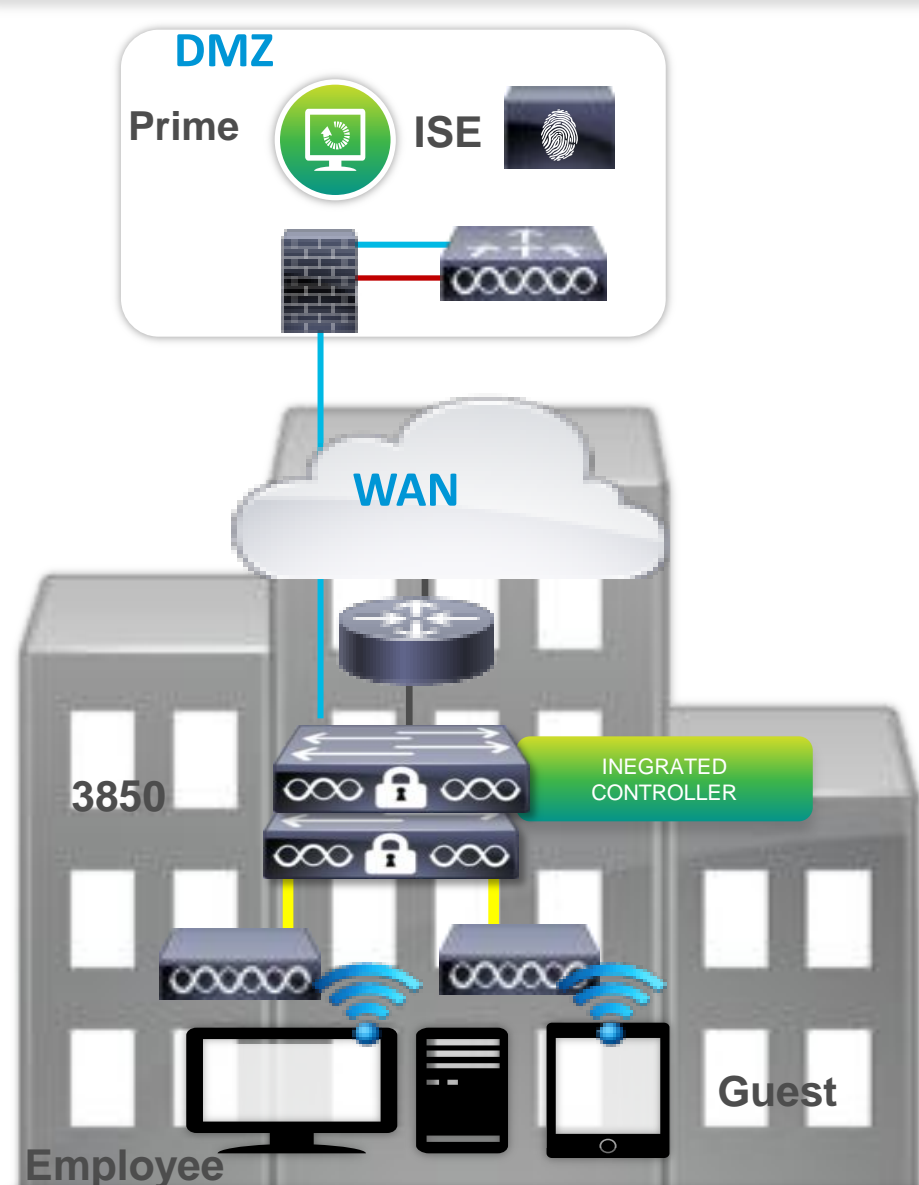
Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- **How to deploy a Converged Access network ?**
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

Converged Access Deployment Mode

Branch use case

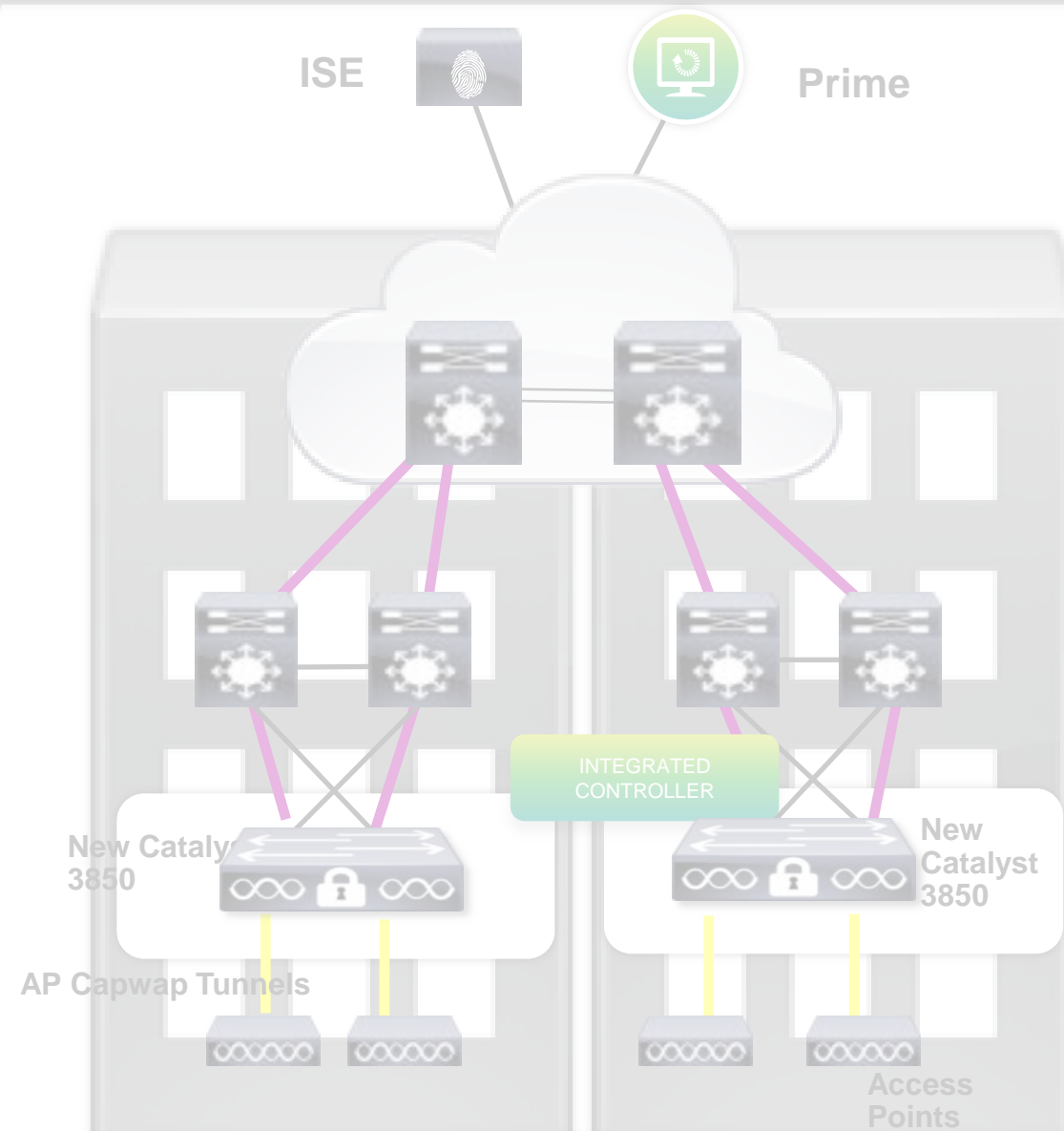
INTEGRATED CONTROLLER OPTIONS



BRANCH

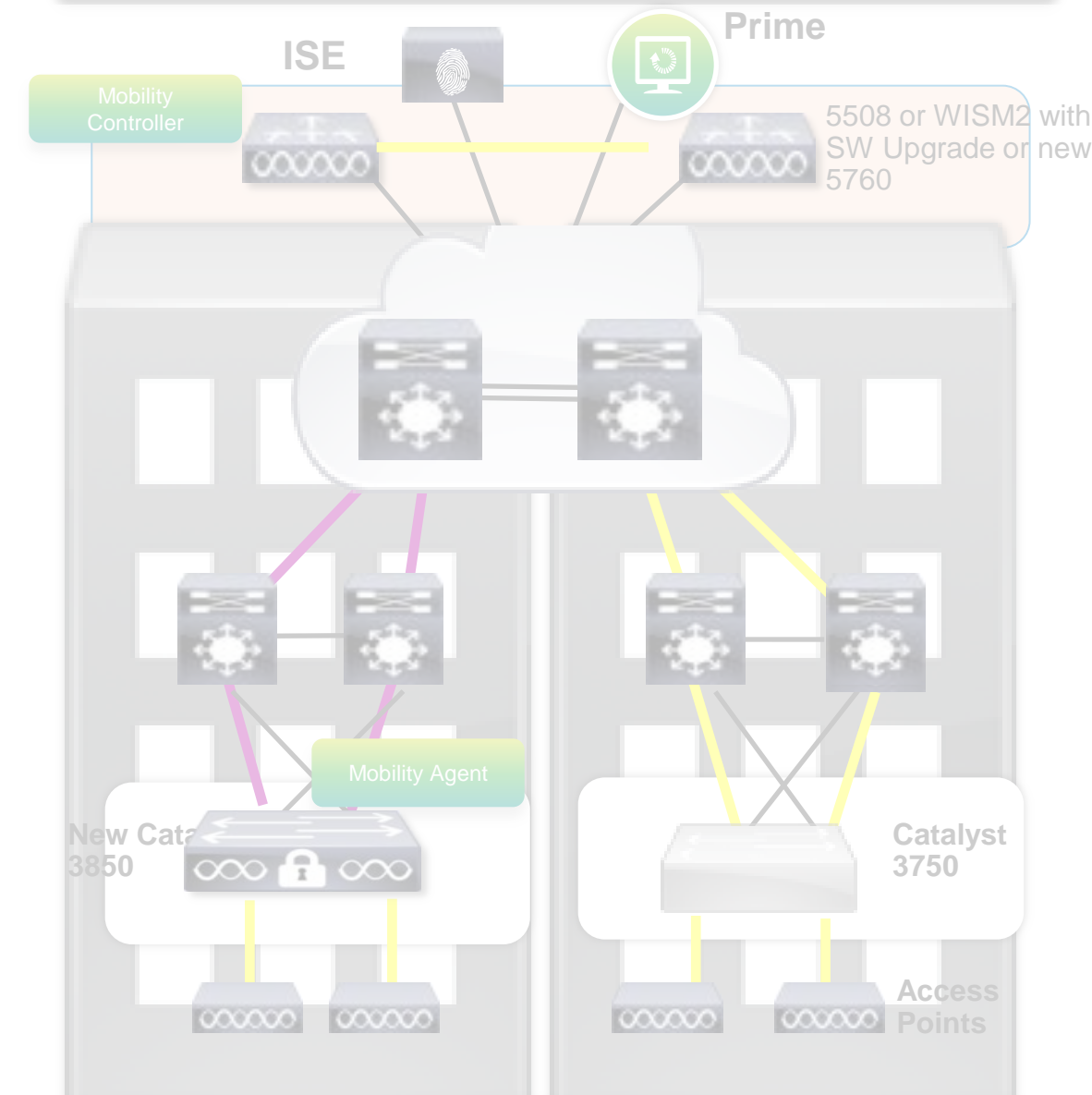
UP TO 50 ACCESS POINTS

EXTERNAL MOBILITY CONTROLLER NEEDED



SMALL CAMPUS

UP TO 250 ACCESS POINTS



LARGE CAMPUS

GREATER THAN 250 ACCESS POINTS

Capwap Tunnel

Standard Ethernet, No Tunnels

Guest Tunnel from Switch to DMZ Controller

Converged Access Deployment Mode Branch - Mobility Configuration

- Management VLAN Configuration

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

- SVIs for client VLANs defined locally on the switch

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

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

- Wireless Management Interface Configuration

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

```
3850#show wireless Interface summary
```

Wireless Interface Summary

AP Manager on management Interface: Enabled

Interface Name	Interface Type	VLAN ID	IP Address	IP Netmask	MAC Address
Vlan31	Management	31	192.168.31.42	255.255.255.0	2037.06ce.0a55

This activates the MA functionality



BRANCH

Converged Access Deployment Mode Branch - Mobility Configuration

Configuring Mobility Controller

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

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

```
3850#sh wireless mobility summary  
Mobility Controller Summary:
```

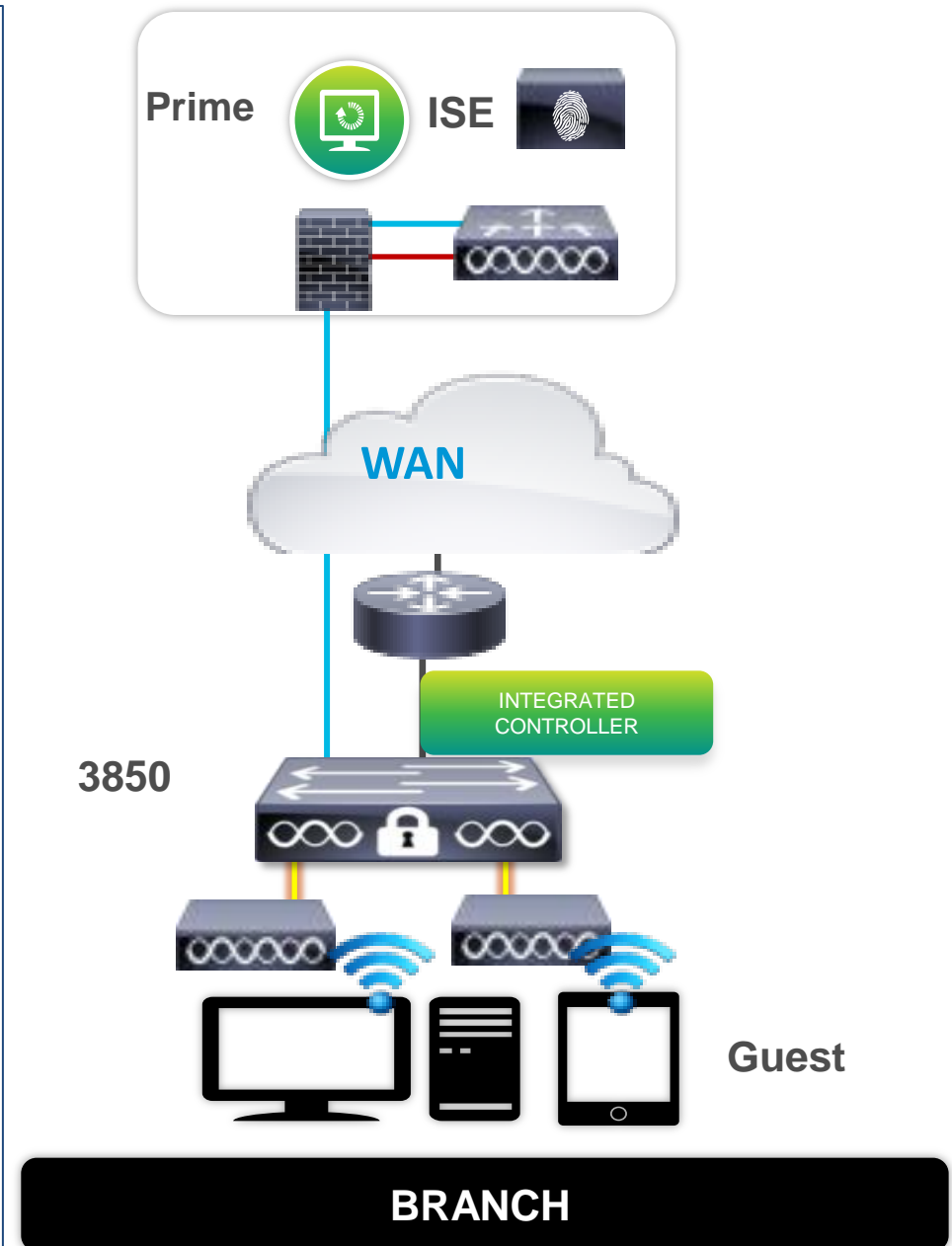
```
Mobility Role : Mobility Controller  
Mobility Protocol Port : 16666  
Mobility Group Name : default  
Mobility Oracle IP Address : 0.0.0.0  
DTLS Mode : Enabled  
Mobility Domain ID for 802.11r : 0xac34  
Mobility Keepalive Interval : 10  
Mobility Keepalive Count : 3  
Mobility Control Message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

Controllers configured in the Mobility Domain:

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

This activates the MC functionality

After reboot



Converged Access Deployment Mode Branch - Mobility Configuration

Access Point port configuration

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

Access Points need to be configured on Wireless Management VLAN

```
3850#show ap summary
Number of APs: 1
```

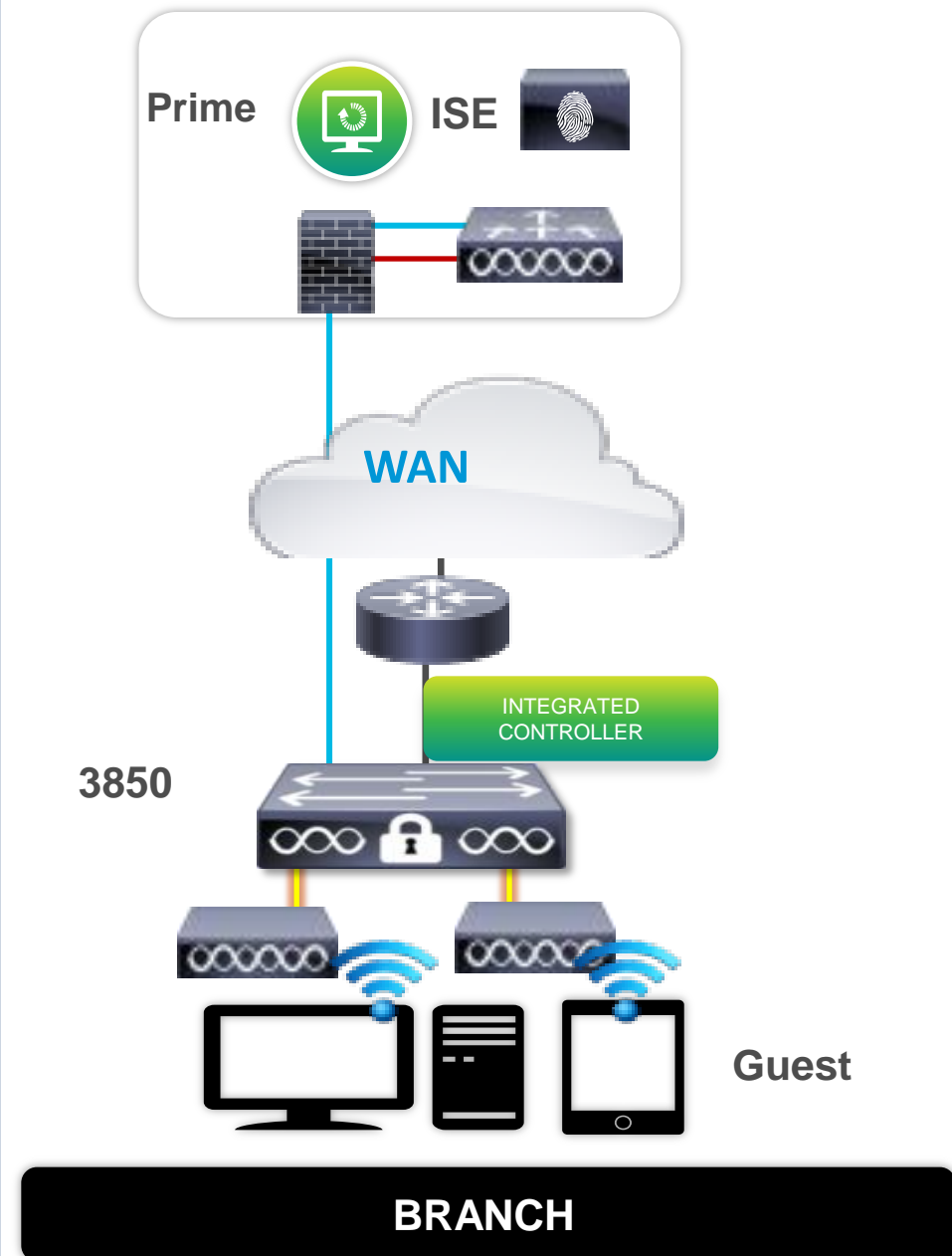
```
Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured
```

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

WLAN Configuration

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

WLAN sample configuration



Converged Access Deployment Mode Branch - Mobility Configuration

Client Connectivity

3850r#sh wireless client summary

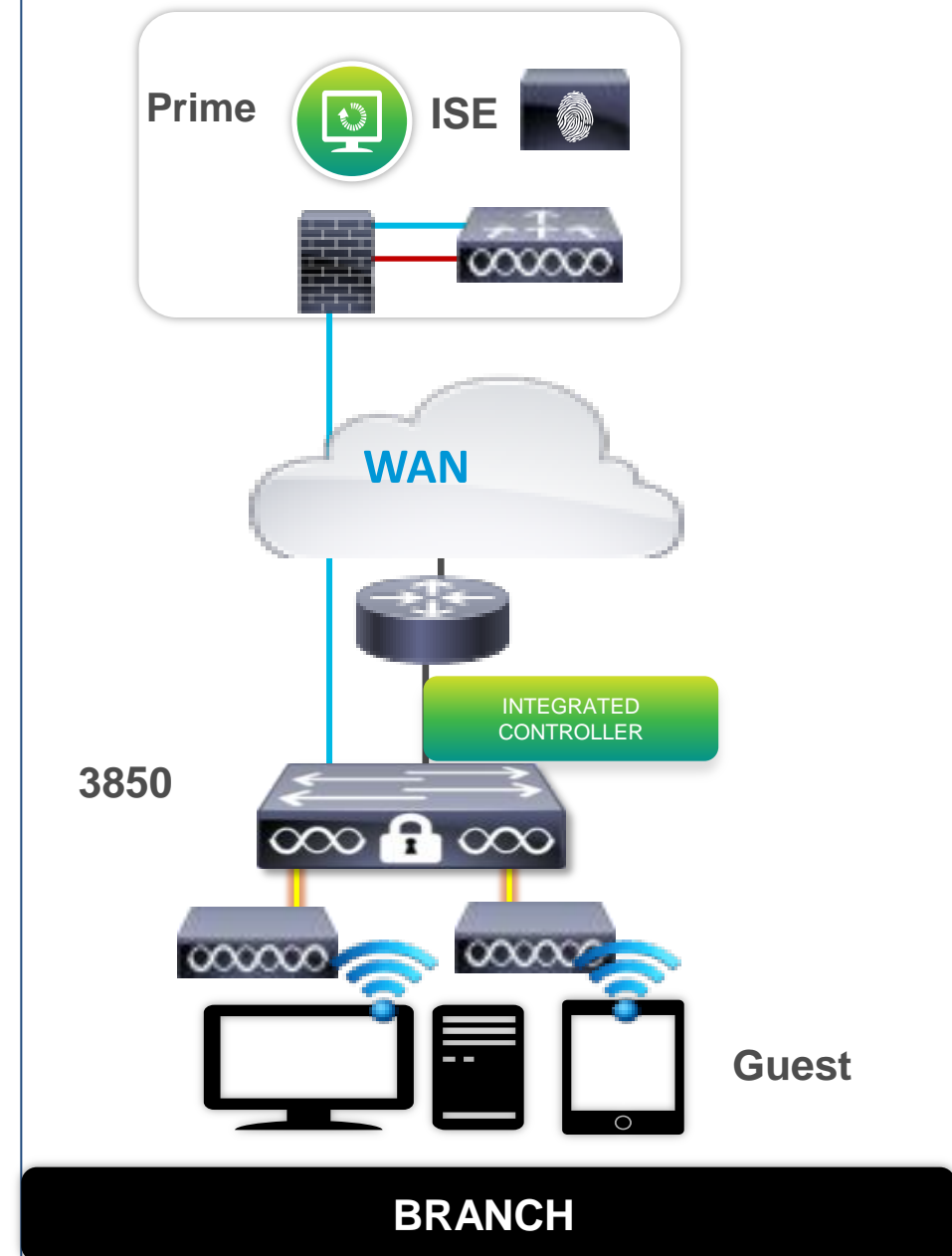
Number of Local Clients : 1

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

3850#sh wcdb database all

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

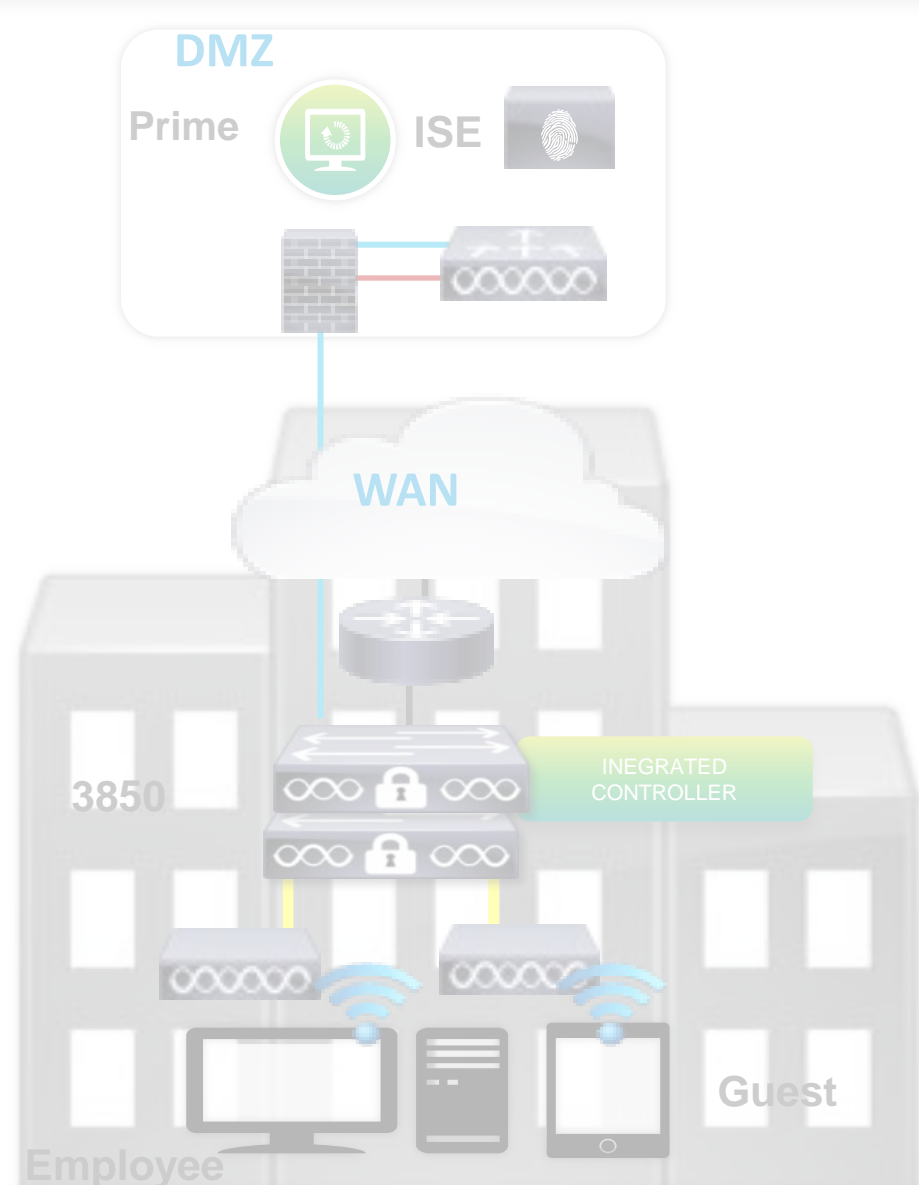
Mac Address	VlanId	IP Address	Src If	Auth	Mob
-----	-----	-----	-----	-----	-----
f81e.dfe2.e80e	32	192.168.32.57	0x00FF5BC000000011	RUN	LOCAL



Converged Access Deployment Mode

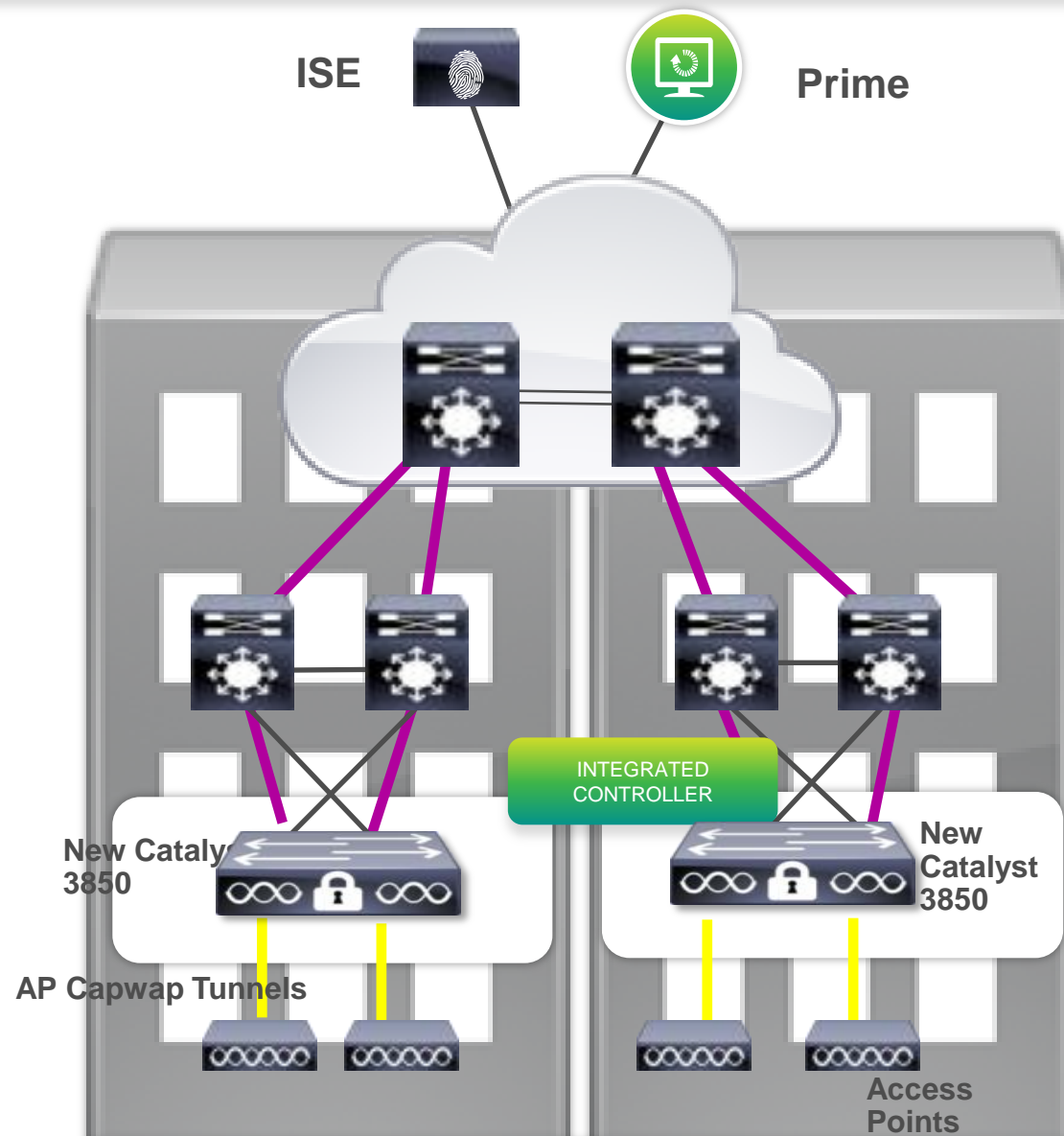
Small Campus use case

INTEGRATED CONTROLLER OPTIONS



BRANCH

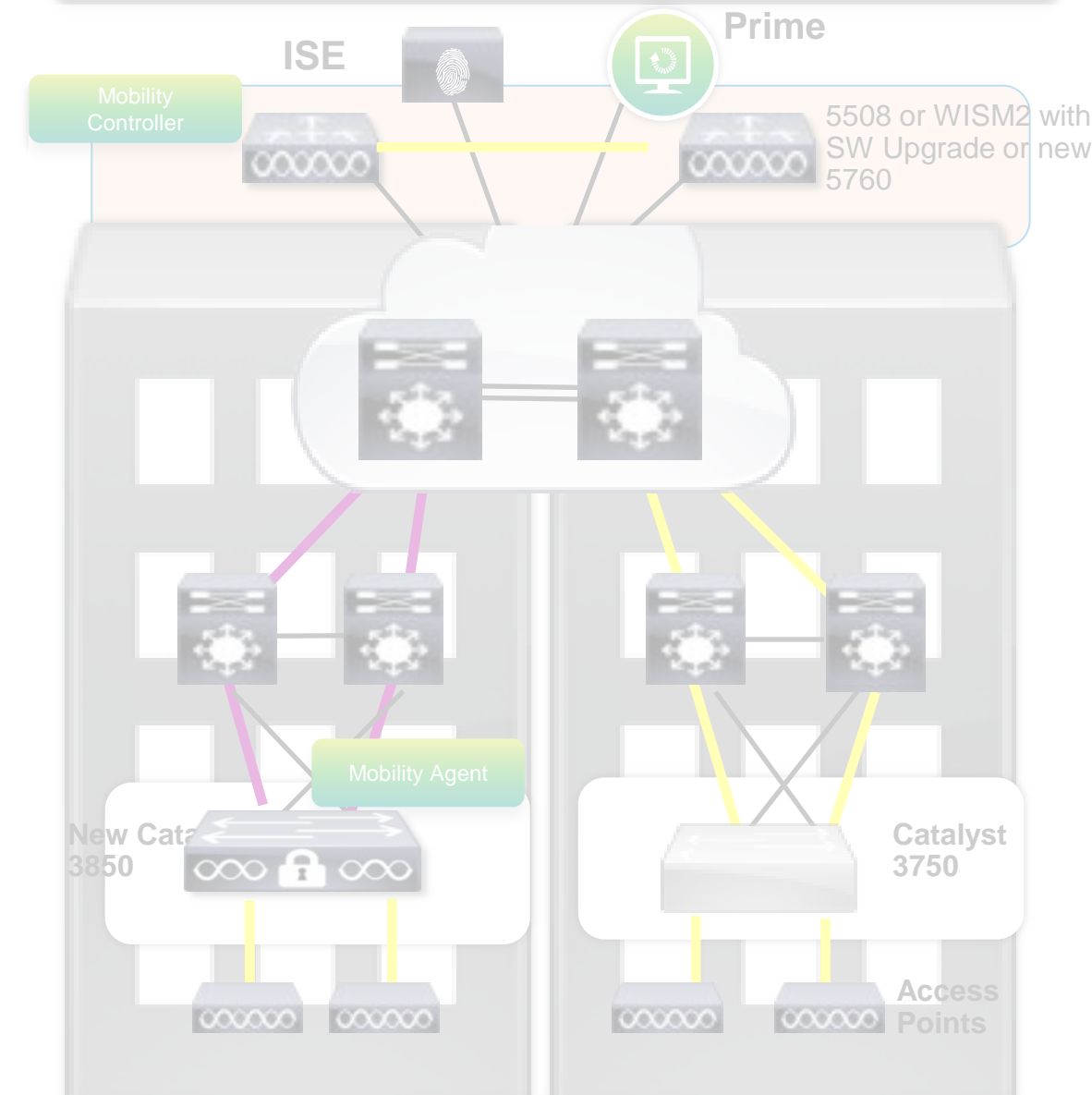
UP TO 50 ACCESS POINTS



SMALL CAMPUS

UP TO 250 ACCESS POINTS

EXTERNAL MOBILITY CONTROLLER NEEDED



LARGE CAMPUS

GREATER THAN 250 ACCESS POINTS

Capwap Tunnel

Standard Ethernet, No Tunnels

Guest Tunnel from Switch to DMZ Controller

Converged Access Deployment Mode Small Campus – SPG configuration

3850-MC#sh wireless mobility summary

Mobility Controller Summary:

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

Link Status is Control Path Status : Data Path Status

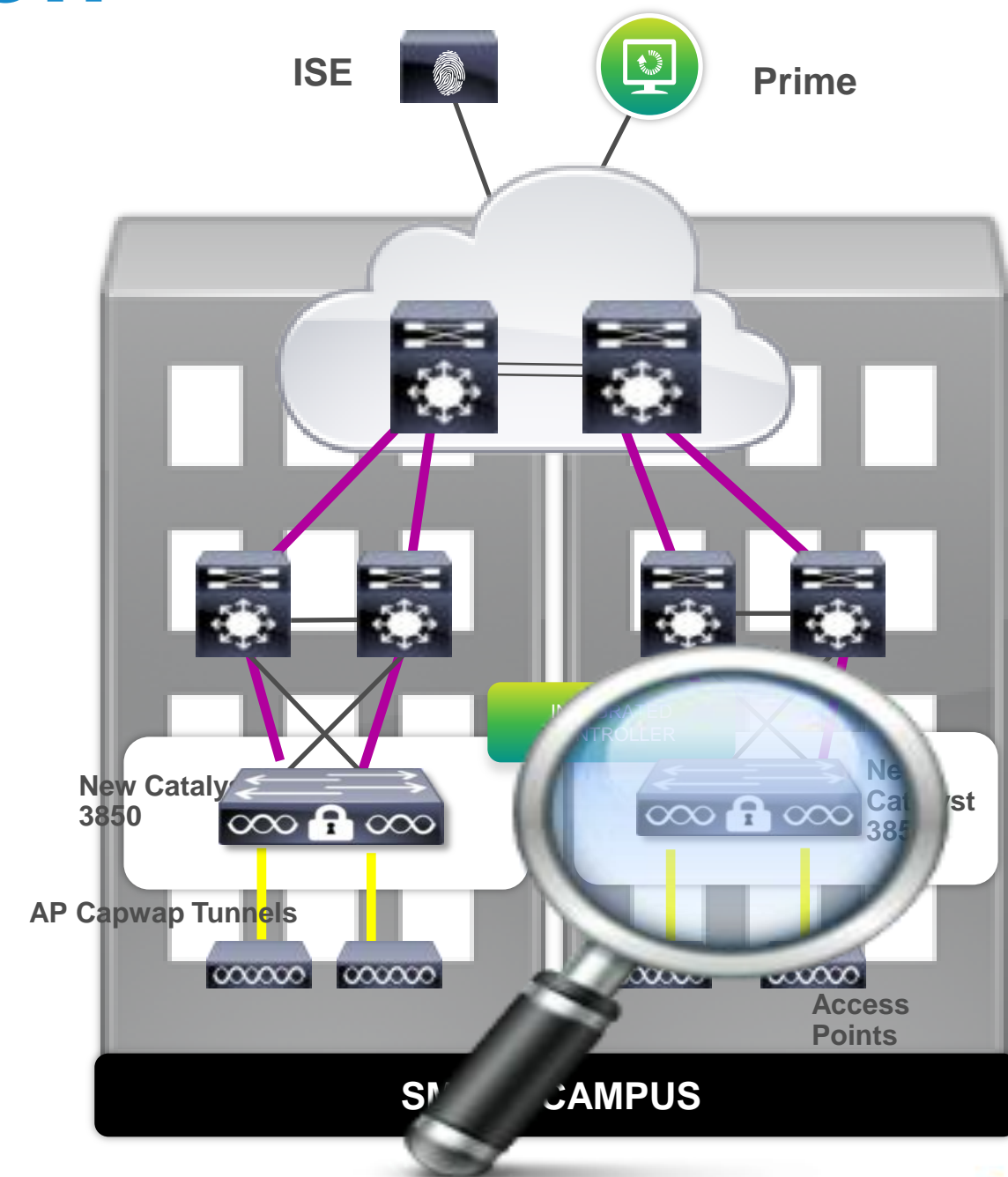
Controllers configured in the Mobility Domain:

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

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

IP	Public IP	Link Status
192.168.21.44	192.168.31.44	UP: UP

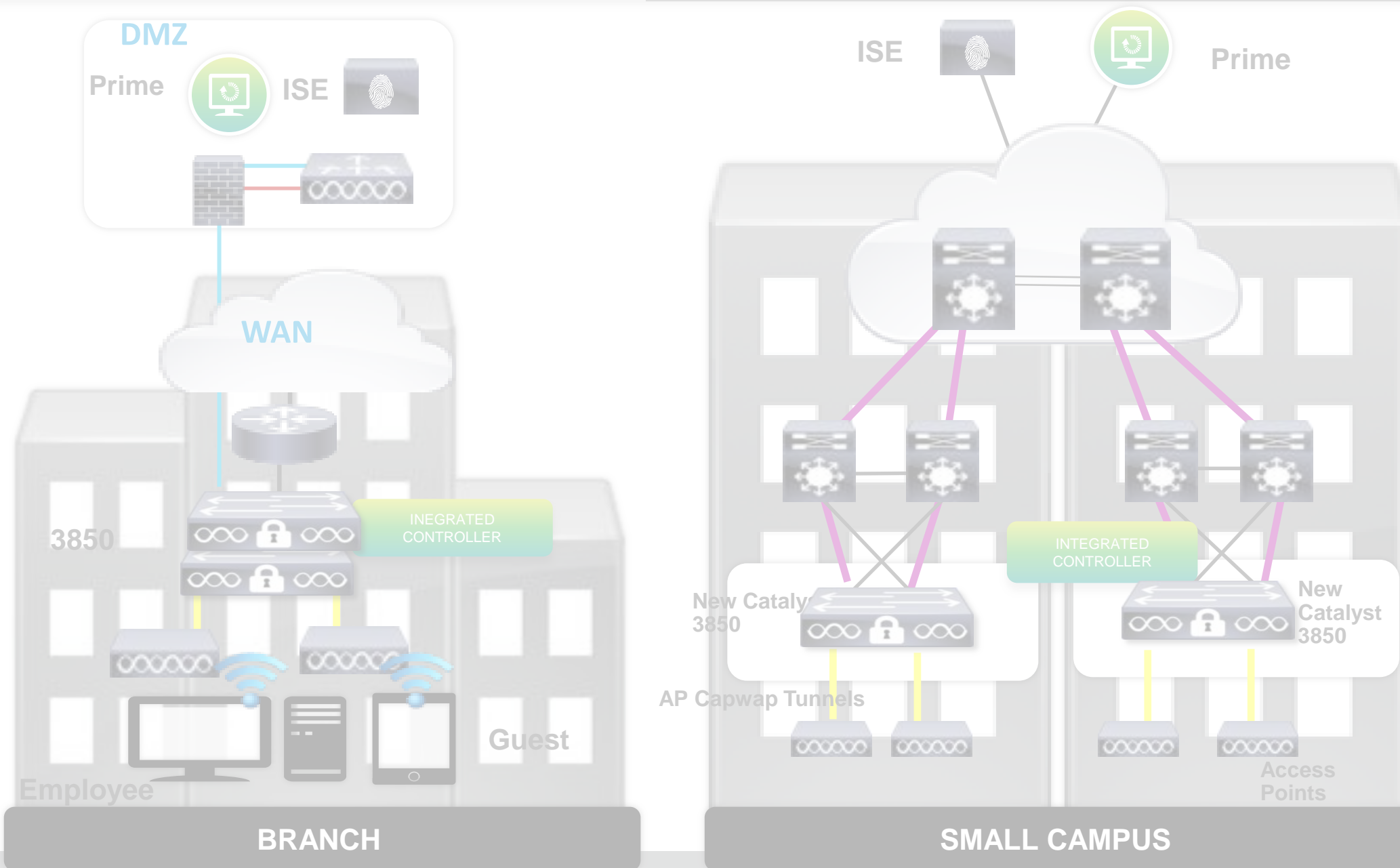
Both control and data plane needs to be UP



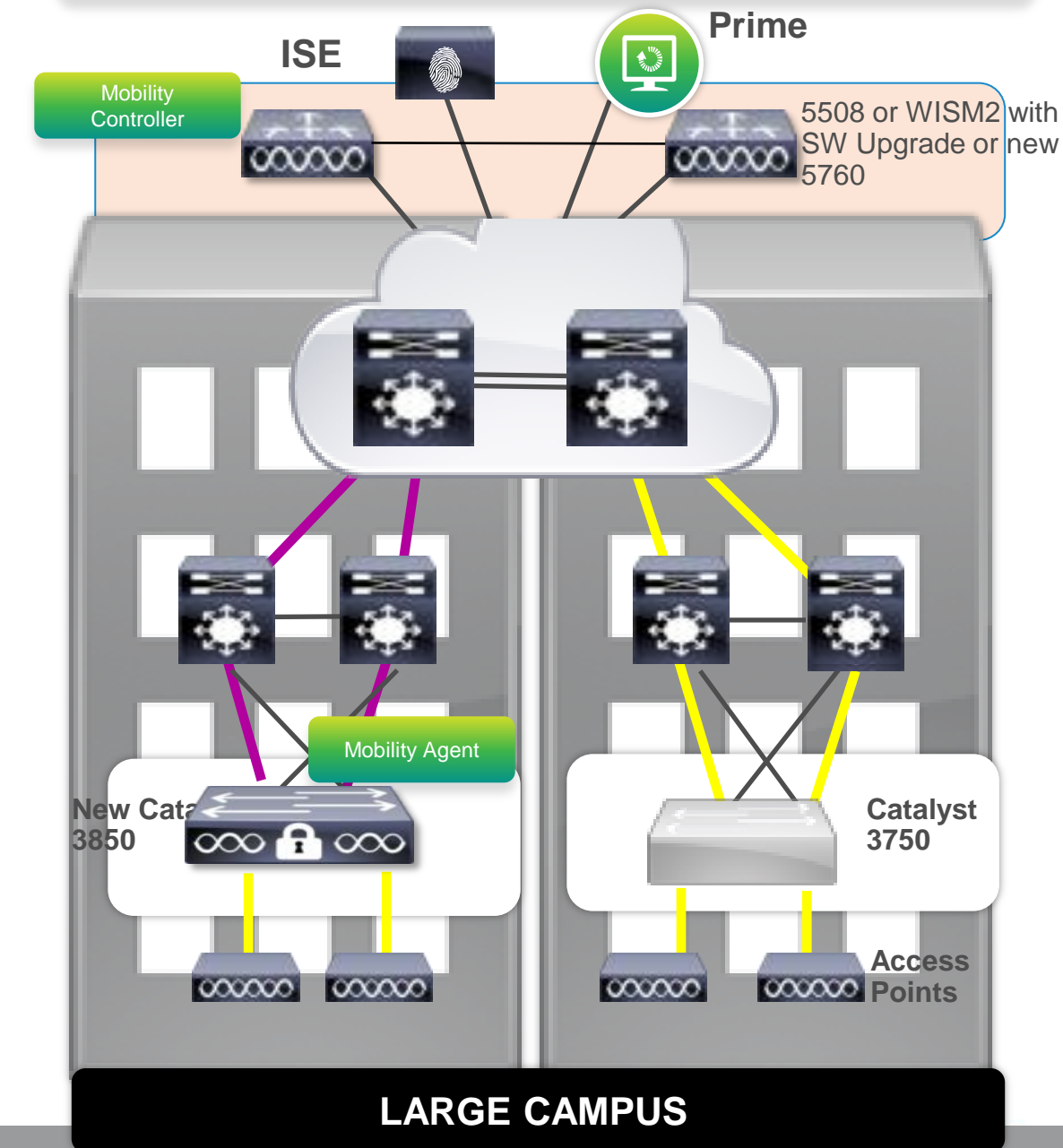
Converged Access Deployment Mode

Large Campus use case

INTEGRATED CONTROLLER OPTIONS



EXTERNAL MOBILITY CONTROLLER NEEDED



UP TO 50 ACCESS POINTS

UP TO 250 ACCESS POINTS

GREATER THAN 250 ACCESS POINTS

Capwap Tunnel

Standard Ethernet, No Tunnels

Guest Tunnel from Switch to DMZ Controller

Converged Access Deployment Mode Large Campus - Mobility Configuration

- Configure 5760 as MC and member of SPG

```
interface Vlan21
  description MANAGEMENT VLAN
  ip address 192.168.21.42 255.255.255.0
```

```
5760(config)#wireless management interface VLAN21
```

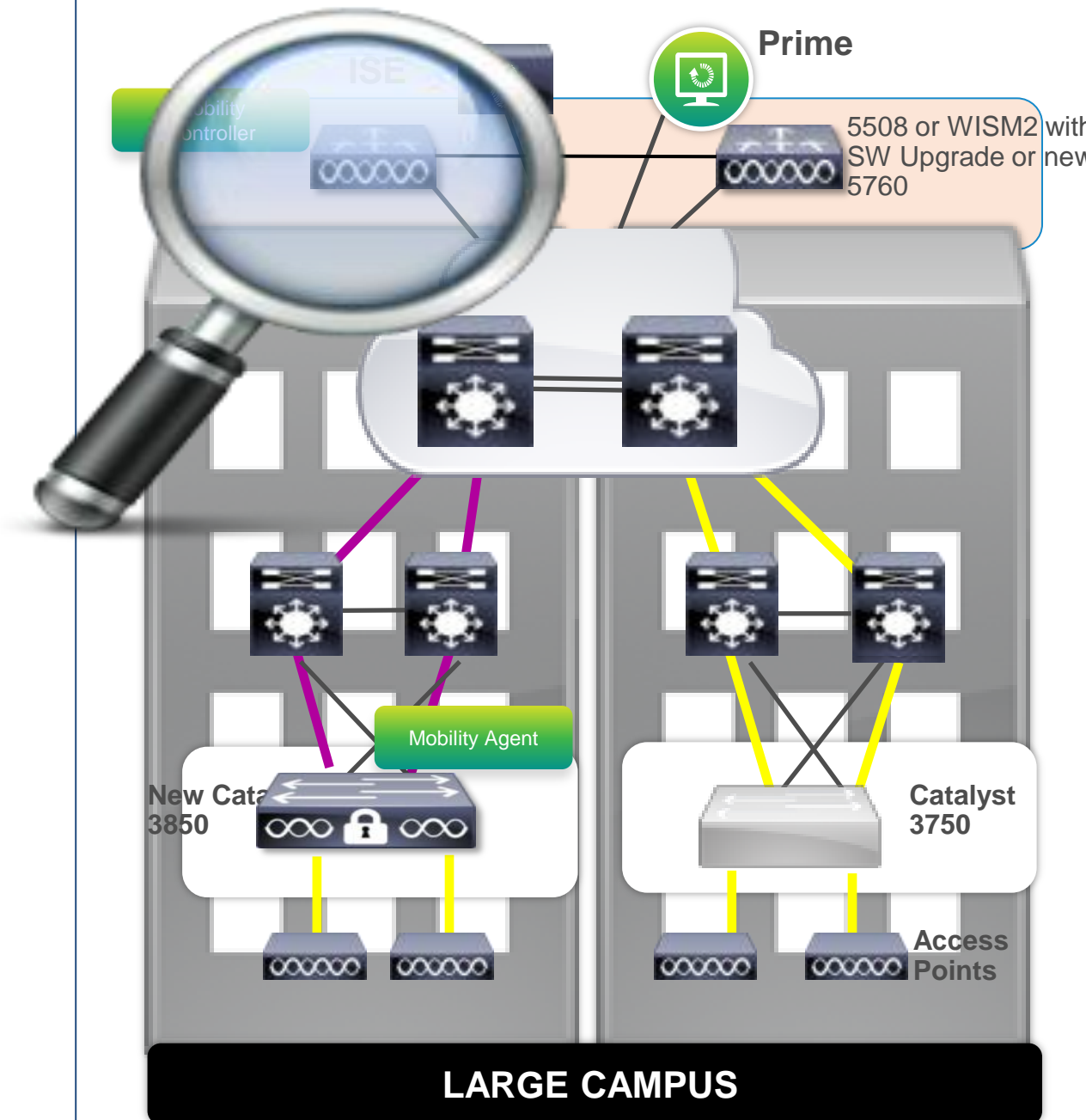
```
5760(config)#wireless mobility controller peer-group GroupABC
```

```
5760(config)#wireless mobility controller peer-group GroupABC member ip 192.168.21.44 public-ip
192.168.21.44
```

- Configure 3850 as MA

```
interface Vlan21
  description MANAGEMENT VLAN
  ip address 192.168.21.44 255.255.255.0
```

```
3850(config)#wireless mobility controller ip 192.168.21.42
```



Converged Access Deployment Mode Mobility Configuration – Large Campus

- Mobility Group configuration

```
5760(config)#wireless mobility group name sevt-lab
```

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

- Verify the configuration

```
5760-simo#sh wireless mobility summary
```

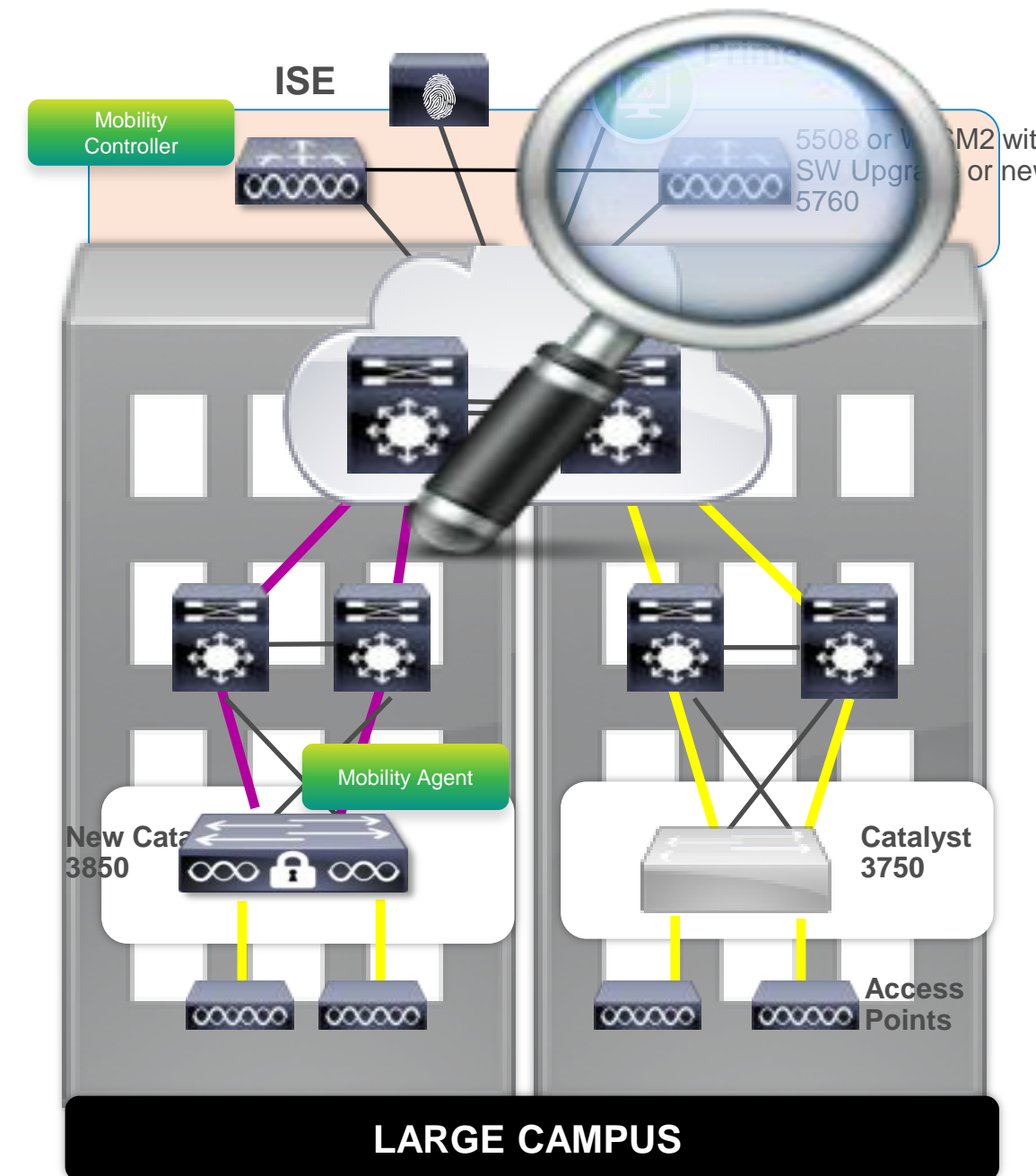
Mobility Controller Summary:

Controllers configured in the Mobility Domain:

IP Address	Public IP Address	Group Name	Multicast IP	Status
192.168.21.42	-	sevt-lab	0.0.0.0	UP
10.1.1.5	10.1.1.5	sevt-lab	0.0.0.0	UP

Switches configured in Group20 switch Peer Group: 1

IP Address	Public IP Address	Status
192.168.21.44	192.168.21.44	UP

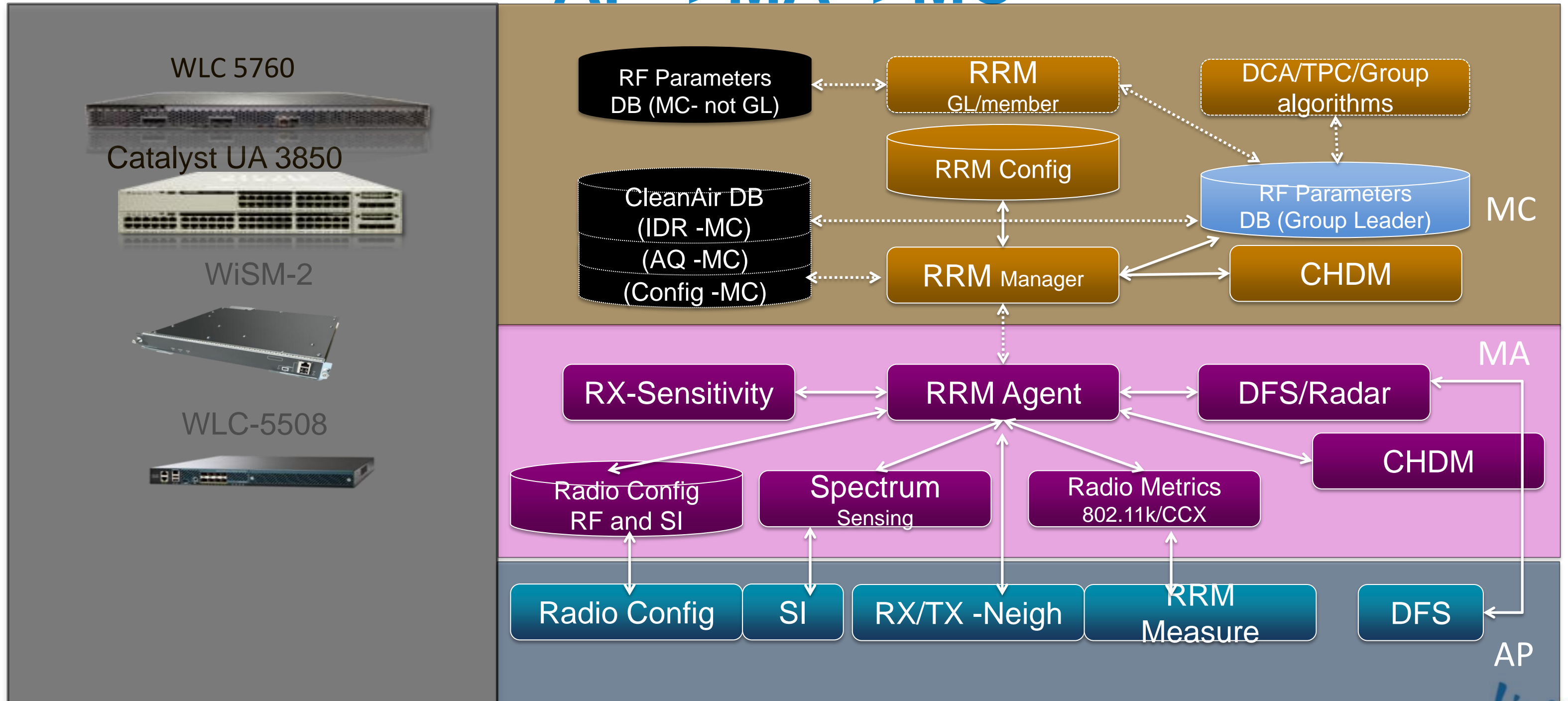


Agenda

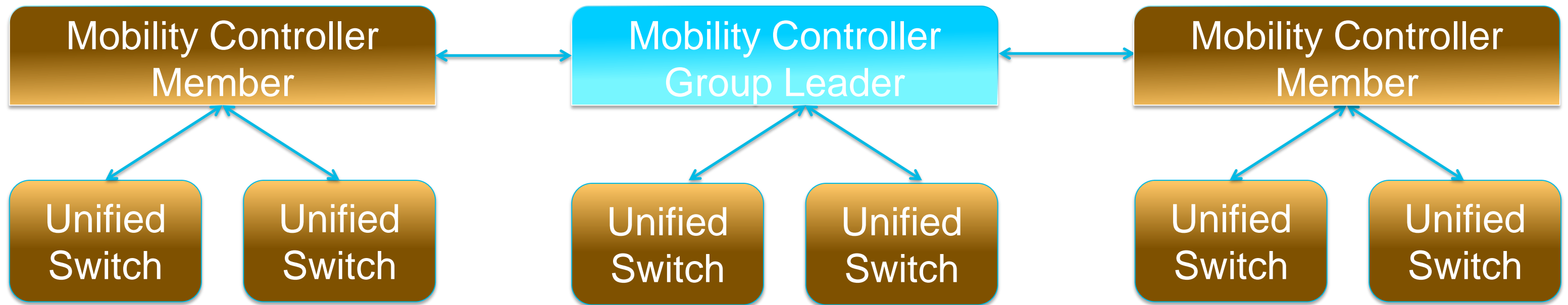
- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - **CleanAir & RRM**
 - WebAuth & Guest Anchor (GA)
 - Security Features
- Bringing Together Wired and Wireless

RRM-CleanAir Data in Converged Access

AP=>MA=>MC



RF Grouping and Distribution



- WLC version 7.3 MR1 supported for RRM with Converged Access
- NO RF Groups and Profiles at FCS -
- Static and Auto Grouping supported

Basic RRM Configuration Tips – Converged Access – what to expect

It's possible that you've not had a true default controller in a while, so check things you normally wouldn't after an upgrade – for instance 1 Mbps is the mandatory minimum data rate by default.

- *Sh tech-support wireless* on MC/RF Group leader
- Grouping Mode – Mind the previous discussion regarding compatibilities and group options – static leader is my preference for now – but automatic works
- Data Rates – will likely need to be touched and changed
- Channels – default's should be ok for most folks. Check and ensure that they match

Where to look for RRM information

- For AP specific RRM metrics – these can only be viewed on the MA (think of this as the local controller)
- For RRM RF Group functions Algorithm's such as Grouping, Channel, and Txpower – may be viewed on either MA or MC – but as with Unified Access – only devices having local AP's will show stats:

MA

```
edison#sh ap dot11 2 channel
Automatic Channel Assignment
Channel Assignment Mode      : AUTO
Channel Update Interval     : 600 seconds
Anchor time (Hour of the day) : 0
Channel Update Contribution  : SN.. [redacted]
Channel Assignment Leader   : katana (192.168.10.101)
```

```
DCA Sensitivity Level      : MEDIUM (10 dB)
Channel Energy Levels
  Minimum                  : -82
  Average                  : -82
  Maximum                  : -82
Channel Dwell Times
  Minimum                  : 4 hours 0 minutes 13 seconds
  Average                  : 4 hours 0 minutes 13 seconds
  Maximum                  : 4 hours 0 minutes 13 seconds
```

```
802.11b Auto-RF Channel List
802.11b Auto-RF Allowed Channel List : 1,6,11
Auto-RF Unused Channel List       : 2,3,4,5,7,8,9,10
```

MC – and RF GL

```
katana#sh ap dot11 2 channel
Automatic Channel Assignment
Channel Assignment Mode      : AUTO
Channel Update Interval     : 600 seconds
Anchor time (Hour of the day) : 0
Channel Update Contribution  : SN.. [redacted]
Channel Assignment Leader   : katana (192.168.10.101)
Last Run                    : 21 seconds ago
```

```
DCA Sensitivity Level      : MEDIUM (10 dB)
Channel Energy Levels
  Minimum                  : unknown
  Average                  : unknown
  Maximum                  : unknown
Channel Dwell Times
  Minimum                  : unknown
  Average                  : unknown
  Maximum                  : unknown
```

```
802.11b Auto-RF Channel List
802.11b Auto-RF Allowed Channel List : 1,6,11
Auto-RF Unused Channel List       : 2,3,4,5,7,8,9,10
```

Where to look for RRM information

- For AP specific RF configurations – these can be viewed on the MA (think of this as the local controller)
- For RRM RF Group functions Algorithm's such as Grouping, Channel, and Txpower – may be viewed on either MA or MC – but as with Unified Access – only devices having local AP's will show stats:

```
edison#sh ap dot11 2 group
Radio RF Grouping
802.11b Group Mode           : AUTO
802.11b Group Update Interval: 600 seconds
802.11b Group Leader        : katana (192.168.10.101)
802.11b Group Member        : Cisco_69:9a:64(192.168.10.8)
                             katana(192.168.10.101)
```

MC – and RF GL

MA

```
katana#sh ap dot11 2 group
Radio RF Grouping
802.11b Group Mode           : STATIC
802.11b Group Update Interval: 600 seconds
802.11b Group Leader        : katana (192.168.10.101)
802.11b Group Member        : katana(192.168.10.101)
                             Cisco_69:9a64(192.168.10.8)
                             edison(192.168.10.100) (*Not a
Manager)
802.11b Last Run             : 506 seconds ago

Mobility Agents RF membership information
-----
No of 802.11b MA RF-members : 1

MA Member name               IP address
-----
edison                        192.168.10.100
```

Sh tech-support wireless on the MC/RF Groupleader will save a lot of typing

Cisco *live!*

CleanAir – for Converged Access

- Works the same as it does in legacy Unified (yes really)
- Some defaults will need to be touched
- Requires PI 2.0 for any upper level display features – information is available for all functions from the command line
- SE Connect is supported – must be launched manually
- AQ, IDR, Convergence, security and Trap reporting all work well
- All CleanAir information only available at the MC level
- All Cleanair configurations @ MC not MA
- AP interface cleanair enable/disable on MA

CleanAir Mitigation

- All CleanAir configs generally fall under the CleanAir tag Except mitigation commands –
- EDRRM and PDA are CleanAir driven – but function through DCA

–katana(config)#ap dot11 2 rrm channel ?

– **cleanair-event** Configure cleanair event-driven RRM parameters

– **dca** Config 802.11b dynamic channel assignment algorithm parameters

– **device** Configure persistent non-WiFi device avoidance in the 802.11b channel assignment

– **foreign** Configure foreign AP 802.11b interference avoidance in the channel assignment

– **load** Configure Cisco AP 802.11b load avoidance in the channel assignment

– **noise** Configure 802.11b noise avoidance in the channel assignment

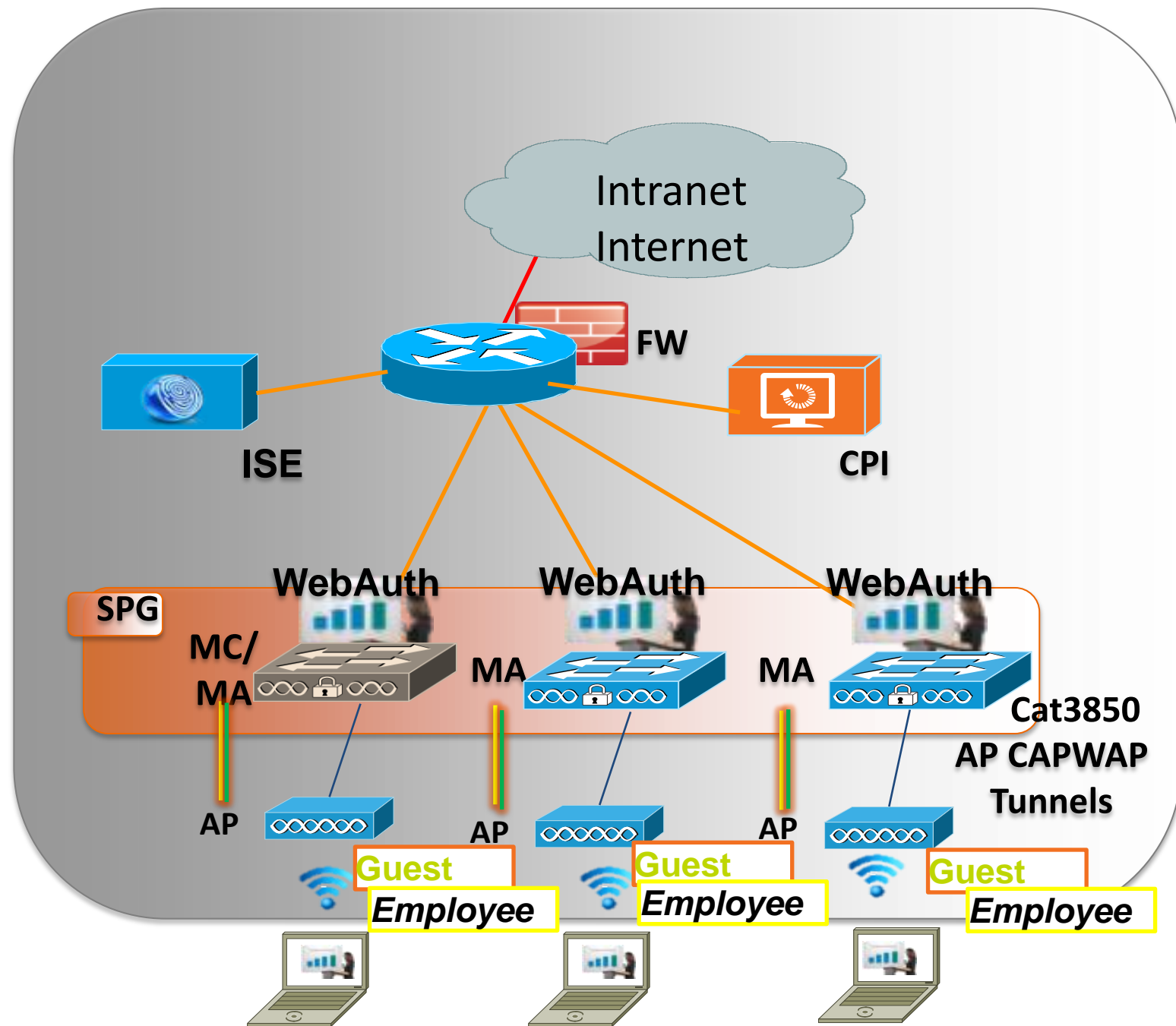
–**cleanair-event = EDRRM**

–**device = PDA**

Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - **WebAuth & Guest Anchor (GA)**
 - Security Features
- Bringing Together Wired and Wireless

Converged Access Deployment Mode Mobility Configuration – Large Campus

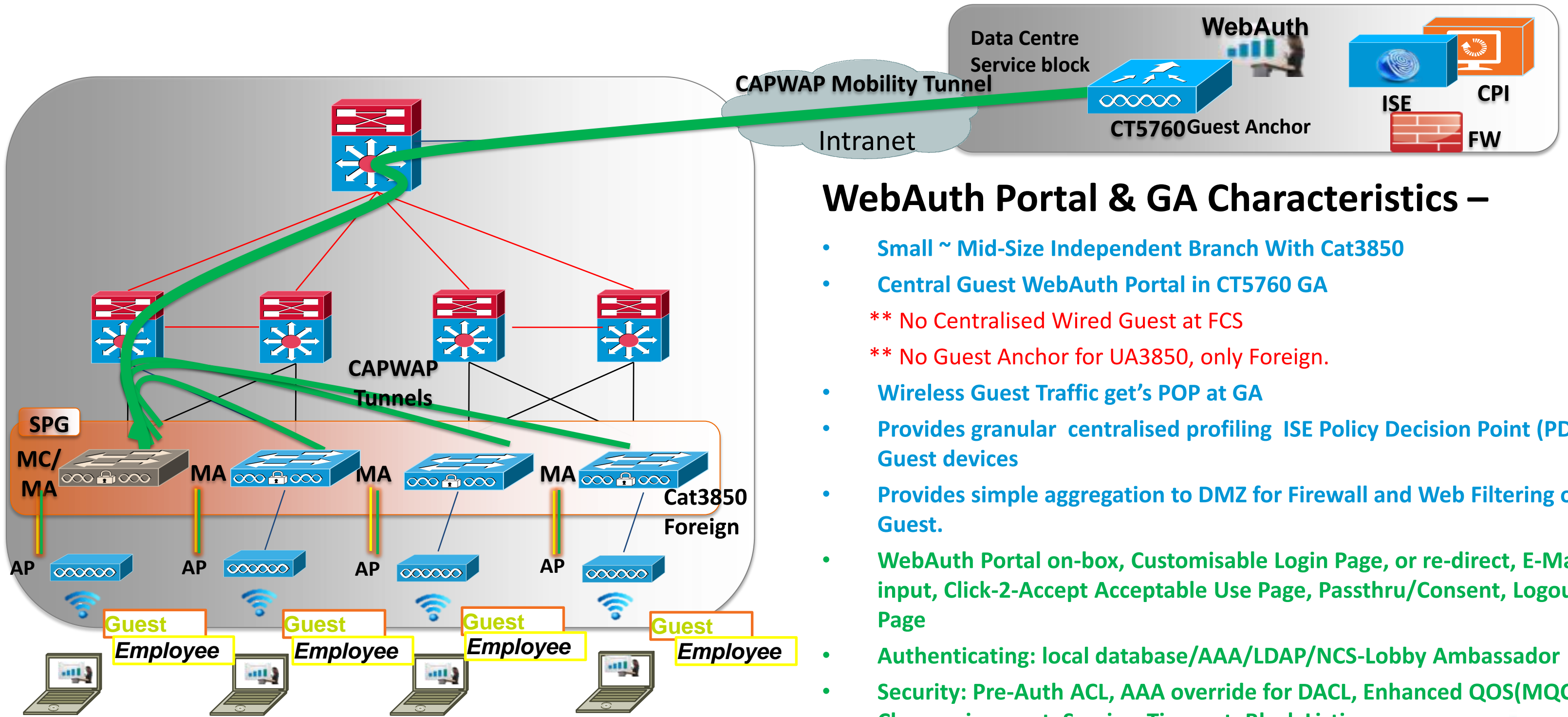


WebAuth Portal Characteristics –

- Small ~ Mid-Size Independent or Remote Branch
- Distributed Guest WebAuth Portal in each MA
- **** MC must be up in SPG for MA to WebAuth**
- Wireless Guest Traffic get's POP at MA
- WebAuth Portal on-box, Customisable Login Page, or re-direct, E-Mail input, Click-2-Accept Acceptable Use Page, Passthru/Consent, Logout Page
- Authenticating: local database/AAA/LDAP/NCS-Lobby Ambassador
- Security: Pre-Auth ACL, AAA override for DACL, Enhanced QOS(MQC) Class assignment, Session-Timeout, Black Listing
- Visibility: Netflow
- Seamless Mobility L2/L3 Roaming

CA Mid-Size & Small Branch

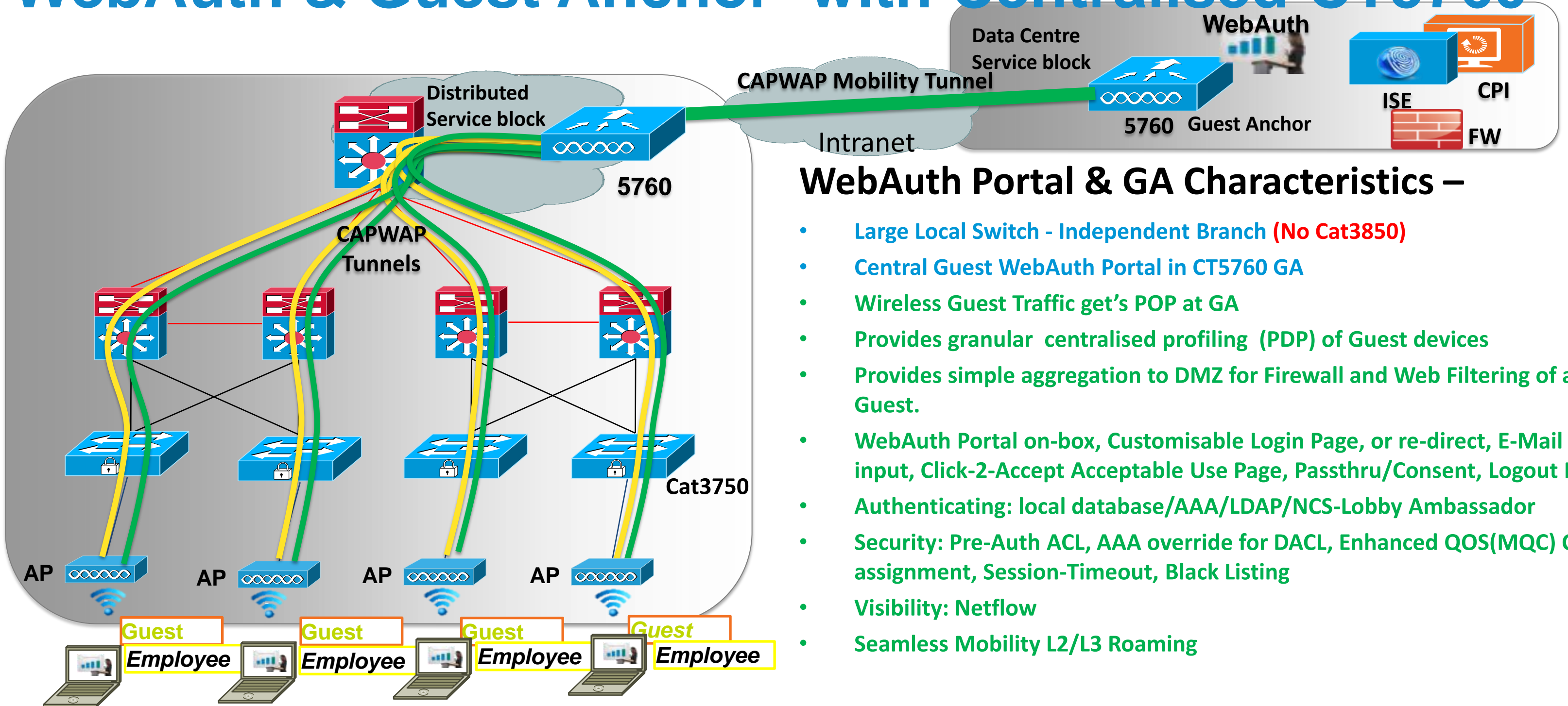
WebAuth & Guest Anchor with CT5760 & Cat3850



WebAuth Portal & GA Characteristics –

- Small ~ Mid-Size Independent Branch With Cat3850
- Central Guest WebAuth Portal in CT5760 GA
- ** No Centralised Wired Guest at FCS
- ** No Guest Anchor for UA3850, only Foreign.
- Wireless Guest Traffic get's POP at GA
- Provides granular centralised profiling ISE Policy Decision Point (PDP) of Guest devices
- Provides simple aggregation to DMZ for Firewall and Web Filtering of all Guest.
- WebAuth Portal on-box, Customisable Login Page, or re-direct, E-Mail input, Click-2-Accept Acceptable Use Page, Passthru/Consent, Logout Page
- Authenticating: local database/AAA/LDAP/NCS-Lobby Ambassador
- Security: Pre-Auth ACL, AAA override for DACL, Enhanced QOS(MQC) Class assignment, Session-Timeout, Black Listing
- Visibility: Netflow

CA Large Campus WebAuth & Guest Anchor with Centralised CT5760

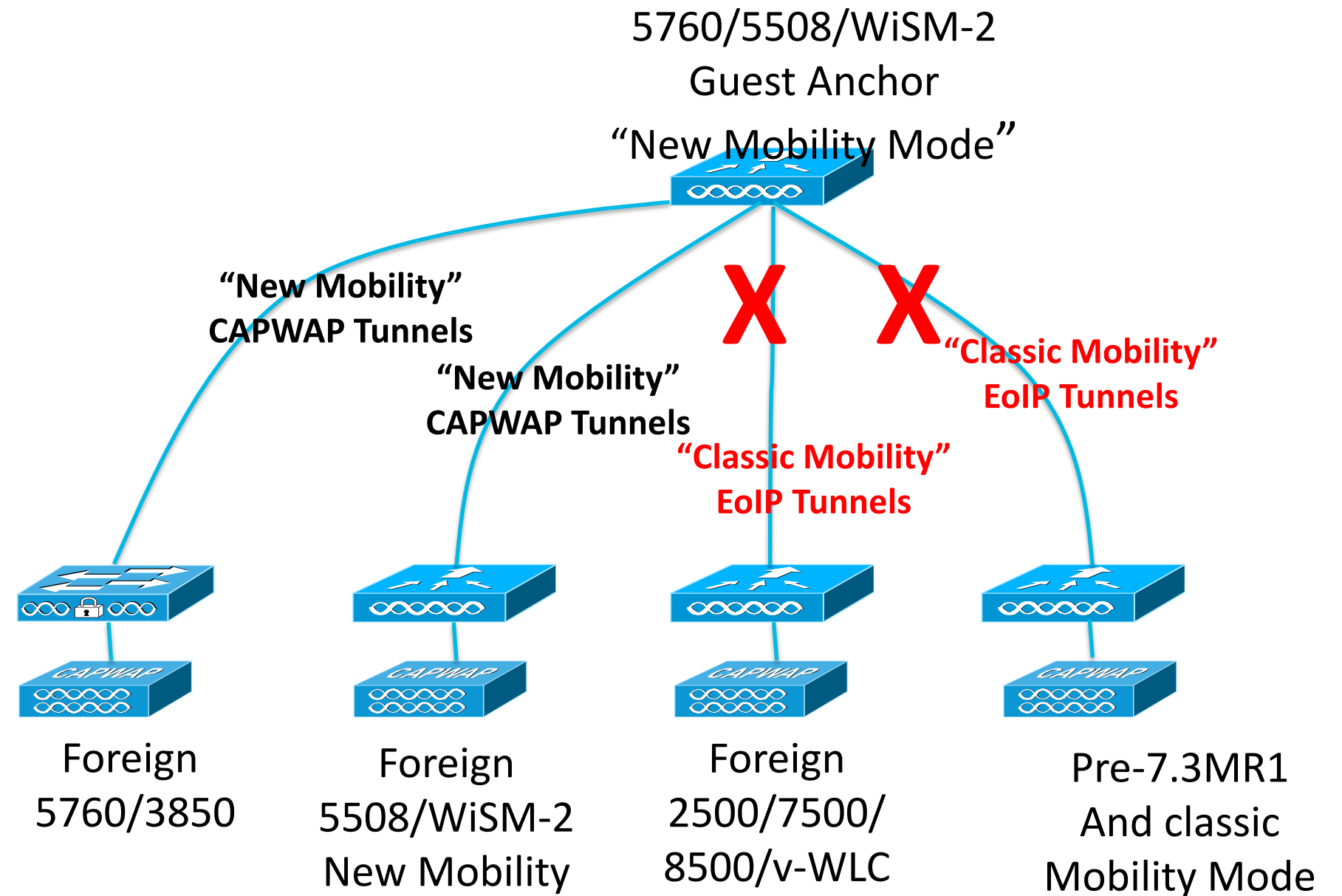


WebAuth Portal & GA Characteristics –

- Large Local Switch - Independent Branch (No Cat3850)
- Central Guest WebAuth Portal in CT5760 GA
- Wireless Guest Traffic get's POP at GA
- Provides granular centralised profiling (PDP) of Guest devices
- Provides simple aggregation to DMZ for Firewall and Web Filtering of all Guest.
- WebAuth Portal on-box, Customisable Login Page, or re-direct, E-Mail input, Click-2-Accept Acceptable Use Page, Passthru/Consent, Logout Page
- Authenticating: local database/AAA/LDAP/NCS-Lobby Ambassador
- Security: Pre-Auth ACL, AAA override for DACL, Enhanced QOS(MQC) Class assignment, Session-Timeout, Black Listing
- Visibility: Netflow
- Seamless Mobility L2/L3 Roaming

Converged Access Guest Anchor (GA) & IRCM Restrictions

- 5508/WiSM-2 as a Guest Anchor WLC for existing AireOS WLC you need to upgrade to 7.3MR1 & run “New Mobility Mode” (re-boot)
- All the controllers in the network must be reconfigured to operate in “New Mobility” mode, part of which changes EoIP to CAPWAP tunnels (re-boot)
- Any Foreign 5508/WiSM-2 needs to upgrade to 7.3MR1 and configured to operate in “New Mobility Mode”
- Foreign AireOS platforms (2500/7500/8500/v-WLC) do not support “New Mobility” mode and are not supported.



"New Mobility Mode" IRCM

- "New Mobility" Inter-Release Controller Mobility Compatibility Matrix



Converged Access Service "New Mobility"	AireOS 7.3MR1	IOS 10.0
Layer 2 and Layer 3 Roaming	X	X
Wireless Guest Anchor/Termination	2*	3*
Rogue Detection	X	X
Fast Roaming (CCKM) in a mobility group	X	X
Location Services	X	X
Radio Resource Management (RRM)	1*	1*
Management Frame Protection (MFP)	X	X
AP Failover	--	--

NOTES:

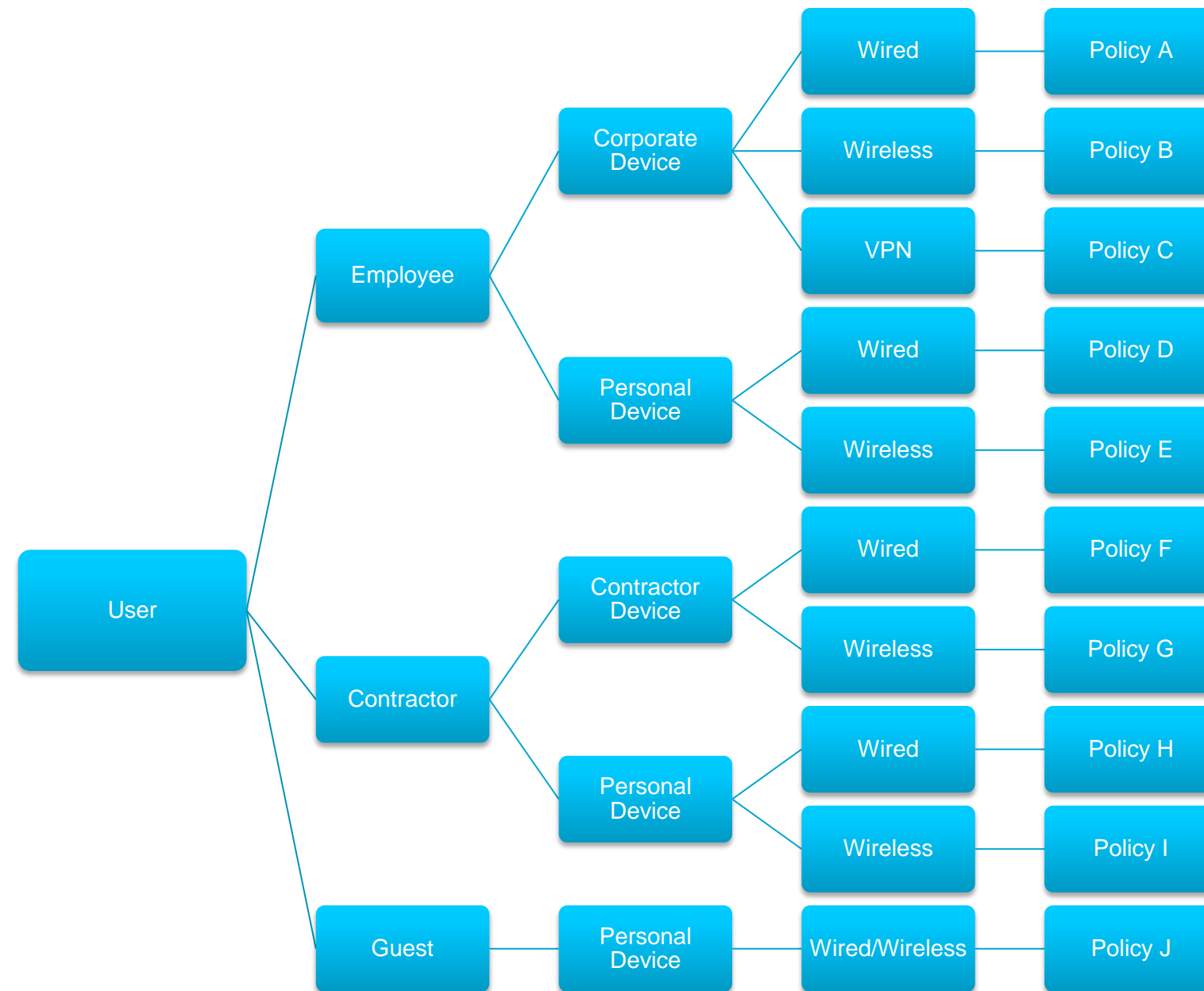
1. For RRM Converged Access is compatible with CUWN release 7.3 MR1 but **does not** support RF Profiles and Groups .
2. New Mobility is only supported on AireOS CT5508 & WiSM-2 platforms but **does not** for any IRCM or GA with CT2500/CT7500/CT8500/v-WLC
3. Guest Anchor Termination is only supported on CT5760/CT5508/WiSM-2. CT5760/CT5508/WiSM-2/Cat3850 all supported as a Foreign.

- New Mobility Mode enables compatibility with Converged Access
- Classic Mobility Mode **IS NOT** compatible with New Mobility Mode – No Simultaneous Support

Agenda

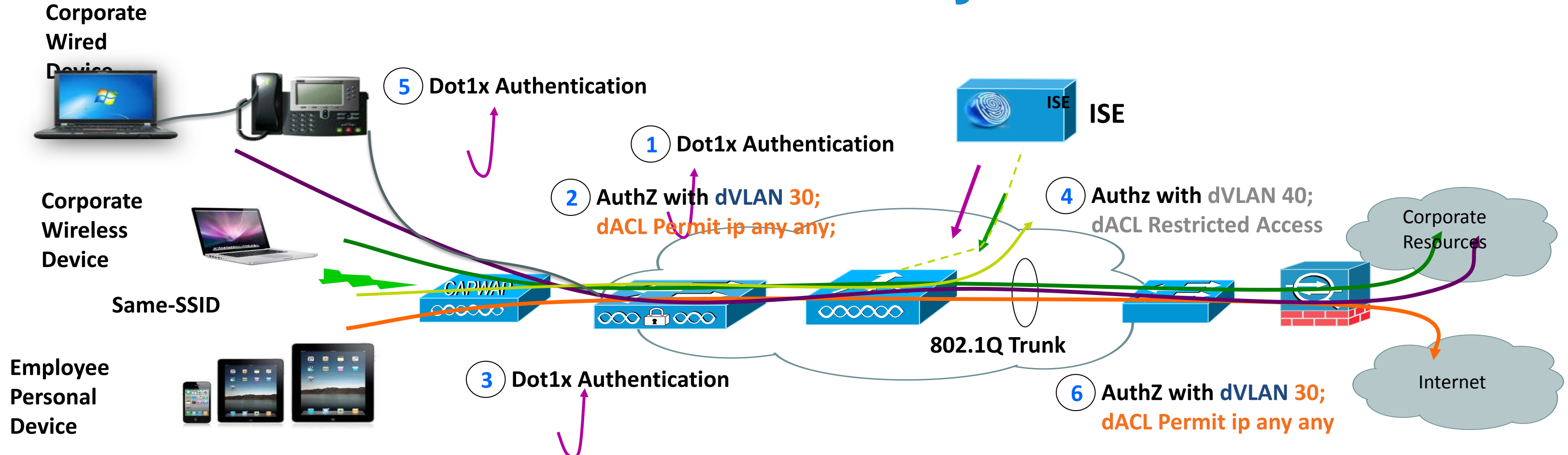
- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - **Security Features**
- Bringing Together Wired and Wireless

Need for Integrated One Policy



How do we make security policy consistent to every wired and wireless device?

Wired and Wireless One Policy



- 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

Personal Device

- Wired and Wireless authorisation policy for personal device

✓	Employee-Personal-Device	if RegisteredDevices AND (Radius-Service-Type-Frame AND <u>Wired-OR-Wireless-802.1x</u> 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:

Description:

*Condition Expression

Condition Name	Expression	Operator	Value
◇	Radius:NAS-Port-Type	Equals	Ethernet
◇	Radius:NAS-Port-Type	Equals	EEE 802.11

Submit Cancel

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

Corporate Device

- Wired and Wireless converged authorisation policy for Corporate device
- Check based corporate device MAC address in white list



Corporate-Device-policy

```
if Whitelist 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/Corp-User ) then Full-Access-Policy
```

EAP Chaining supported for user and device authentication



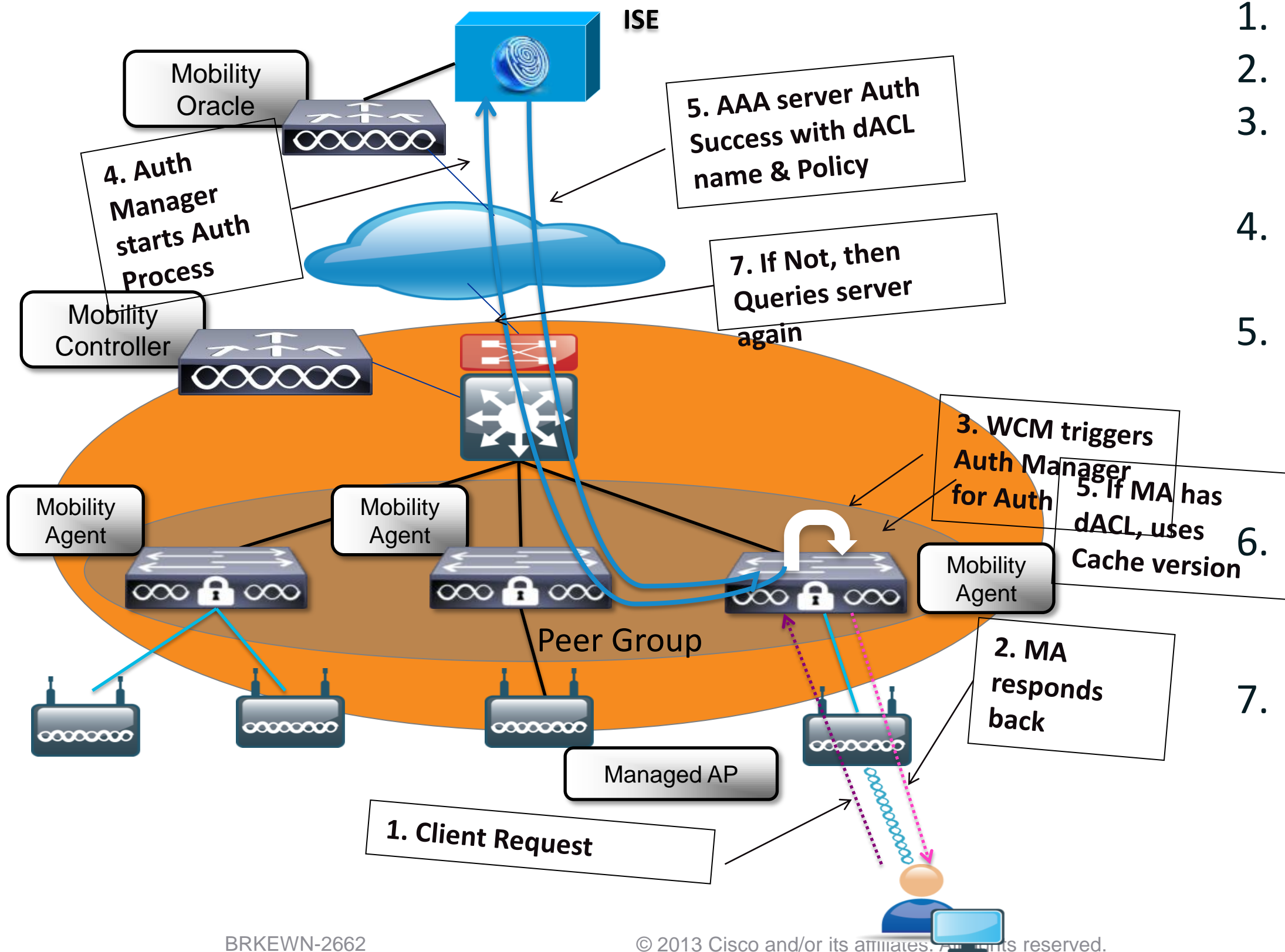
Corporate-user-device-policy

```
if (Radius-Service-Type-Frame AND Wired-OR-Wireless-802.1x AND Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS WS2008er2.corp1.rf-demo.com/Users/employee AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapChainingResult EQUALS User and machine both succeeded ) then Full-Access-Policy
```


Policy Enforcement on Converged Access

- Policy enforcement done in IOS for both wired & wireless
 - For wireless clients WCM will decide which policy to be applied
- Client Roaming:
 - L3 roam ACL policies will be applied on anchor switch
 - L2 Roam ACL polices handoff to newer switch
- ACL type supported
 1. Per-User ACL : - Highly centralised group-to-policy
 2. Filter-ID ACL :- Distributed group-to-policy.
 3. Downloadable ACL :- Optimised centralised group-to-policy. Group-specific ACL are defined on authentication server.
 4. Redirect ACL : URL redirection
 5. *PACL, RAACL, VACL* :- *ACL for routed ports and MAC, ACL for IPV4 and IPV6 traffic, ACL for VLAN.* Policy resides on the switch. Another distributed group-to-policy

Downloadable ACL



1. Wireless Client request Association
2. MA respond back with Association
3. WCM triggers IOS module to do authentication
4. Auth Manager starts authentication process for client with AAA server
5. AAA server respond with authentication success with dACL name and version number in policy attributes
6. If switch has downloaded this dACL previously and has current version it uses cache version
7. If switch does not have current version then it query server for latest dACL

Downloadable ACL

- Downloadable ACL can be defined for both Wired and Wireless client
- It provides network policy enforcement based on user/device authorisation profile
- Configuring dACL policy on the fly and it get pushed

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name

Description

* 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
```

BYOD Policy



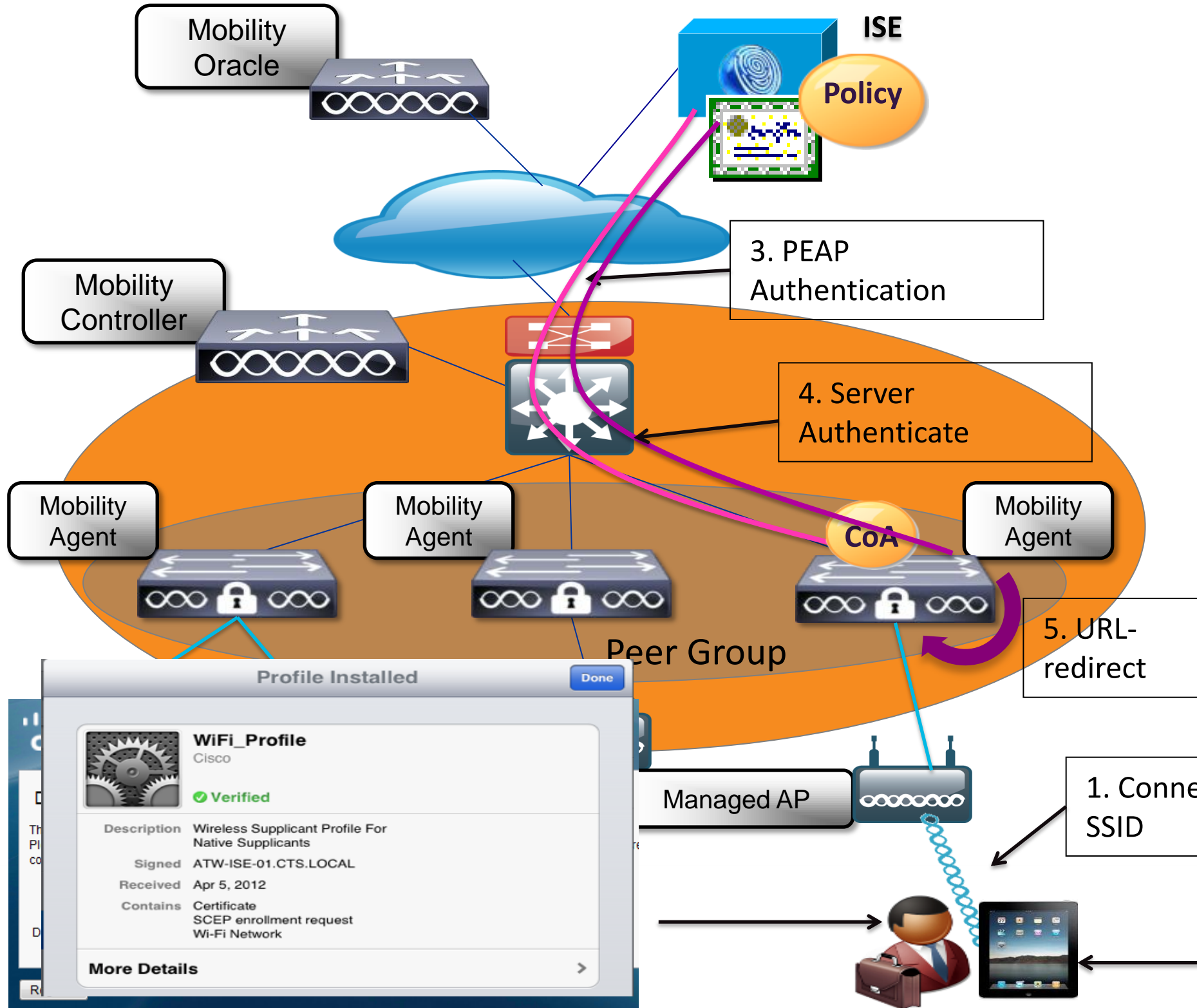
- dVLAN
- Cisco AV pair Qos policy push
- Profiling and posturing
- Guest Access

Attributes Details

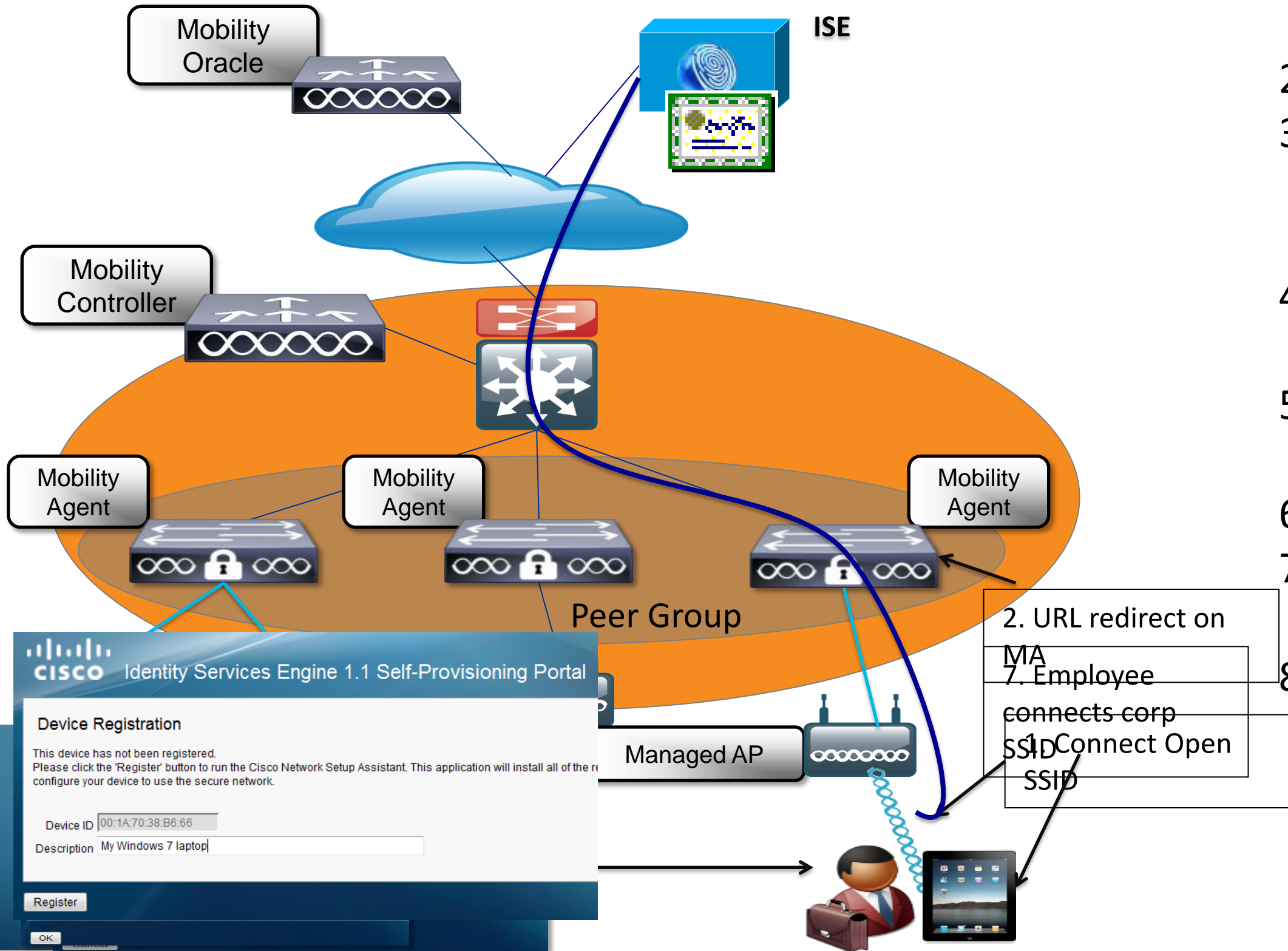
```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:100
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DAACL = corp-policy-1
Airespace-ACL-Name = NSP-ACL
cisco-av-pair = url-redirect-ac=NSP-ACL
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp
cisco-av-pair = ip:sub-qos-policy-in=Standard-Employee
cisco-av-pair = ip:sub-qos-policy-out=Standard-Employee
```


Device Enrollment and Provisioning Use case 1: Single SSID-Employee Access

1. Employee associates to BYOD-Secure SSID
2. Employee enters username and password
3. MA does PEAP authentication
4. Server authenticate
5. MA does client URL redirection
6. Device registration page load & MAC get prepopulated
7. Employee registers device
8. Supplicant Provisioned and certificate installed
9. CoA occurs and supplicant authenticate using EAP-TLS
10. dVLAN, dACL, QoS policy for Employee pushed to MA



Device Enrollment and Provisioning Use case 2: Dual SSID-Employee & Guest



1. User(Employee or Guest) associates to BYOD-Open SSID
2. User redirected to CWA guest portal
3. Based on credential user redirect to guest or employee registration portal
4. Mac address pre-populated user registers device
5. Supplicant gets provisioned & certificate installed
6. Employee disconnect Open SSID
7. Employee associates corp SSID get corp vlan, dACL, QoS
8. Guest in Guest VLAN, Internet only ACL, Guest QoS

BYOD Single And Dual SSID Configuration on Converged Access

Secure Corporate Access SSID

```
wlan BYOD-Dot1x 10 BYOD-Dot1x
aaa-override
accounting-list Cisco
client vlan 118
ip access-group NSP-ACL
nac
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
wlan BYOD-Open 11 BYOD-Open
aaa-override
client vlan 70
ip access-group Guest-ACL
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list Cisco
no shutdown
```

Guest Access SSID

Wired port Configuration

```
interface GigabitEthernet1/0/10
switchport access vlan 118
switchport mode access
ip access-group NSP-ACL in
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
```

BYOD Single And Dual SSID

Authentication, Authorisation and Accounting profile

```
aaa new-model
!
!
aaa group server radius Cisco
 server 10.1.172.36 auth-port 1812 acct-port 1813
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa authorization auth-proxy default group Cisco
aaa accounting network default start-stop group Cisco
!
```

Dot1x enable

```
dot1x system-auth-control
```

Change of Authorisation

```
aaa server radius dynamic-author
 client 10.1.172.36 server-key cisco123
 auth-type any
```

Radius server attributes 6,8,25 are attributes for Service-type, framed-IP and class.

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 10 tries 3
radius-server host 10.1.172.36 auth-port 1812 acct-port 1813 key cisco123
radius-server deadtime 5
!
radius server Cisco
```

URL Redirection

- User connects to provisioning SSID and gets redirected to Guest Portal after launching browser

```
NG3K48P-MA#show access-session interface capwap 0 details
  Interface: Capwap0
    IIF-ID: 0xFF8CC0000000F9
  MAC Address: 00f4,b916,f98b
  IPv6 Address: Unknown
  IPv4 Address: 172,20,228,54
  User-Name: byod
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: ac14e42b504dd9e2000000d8
  Acct Session ID: Unknown
  Handle: 0x610001A2
  Current Policy: (No Policy)

Server Policies (priority 100)
  URL Redirect: https://wnbutme-ise.cisco.com;8443/guestportal/gateway?
sessionId=ac14e42b504dd9e2000000d8&action=nsp
  URL Redirect ACL: NSP-ACL
  Filter-ID: NSP-ACL

Method status list:
  Method      State
  dot1x      Authc Success
```



Rogue AP/Client Management Phases

There are three main phases of rogue AP/Client management in the Unified Access solution:

1. Detection

- Listen for non-infrastructure access points, clients and ad-hocs
- 11n rogue considerations

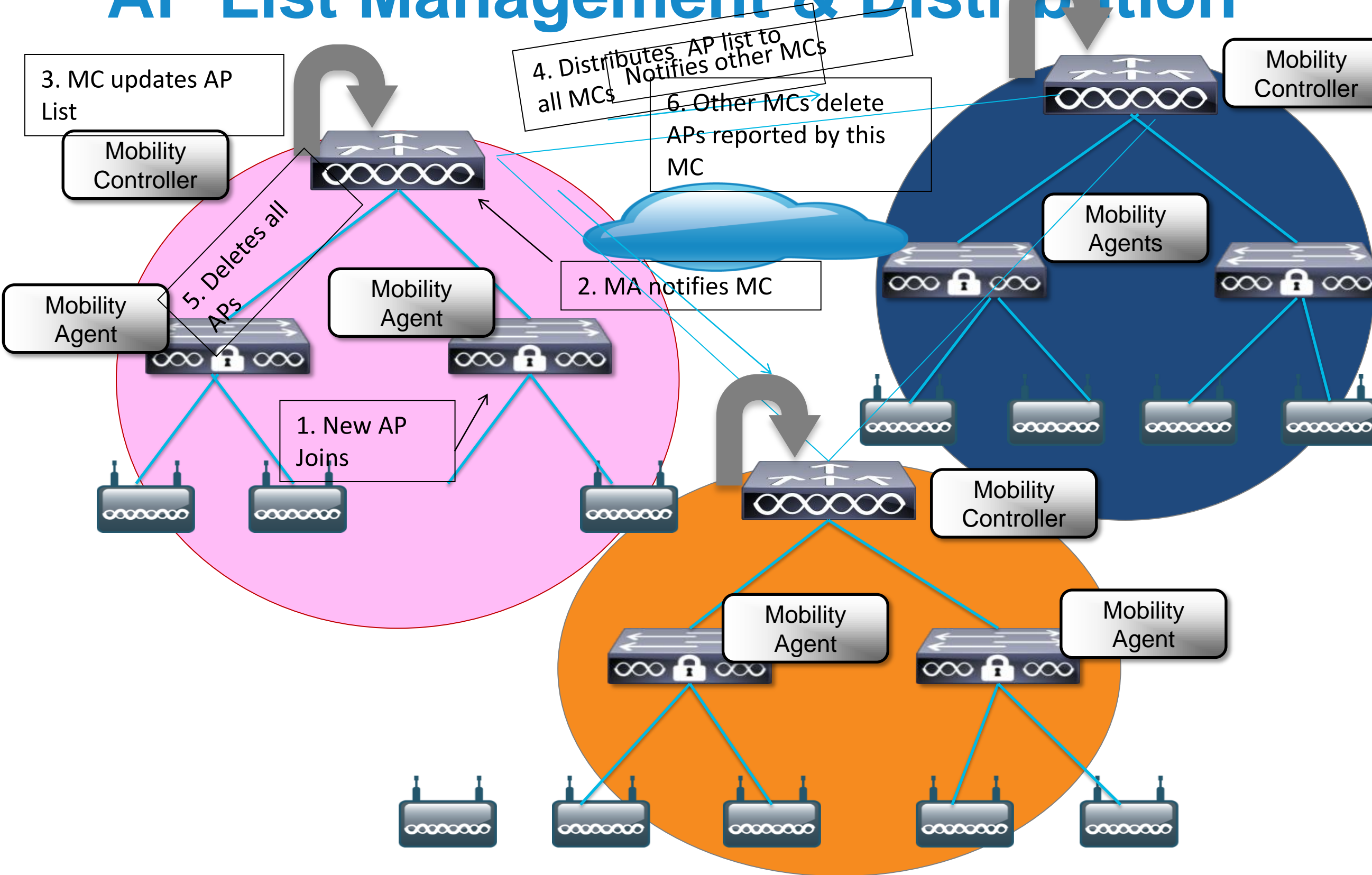
2. Classification

- Rogue rules based on RSSI, SSID, Clients, etc.
- Assessing if rogue is on wired infrastructure

3. Mitigation

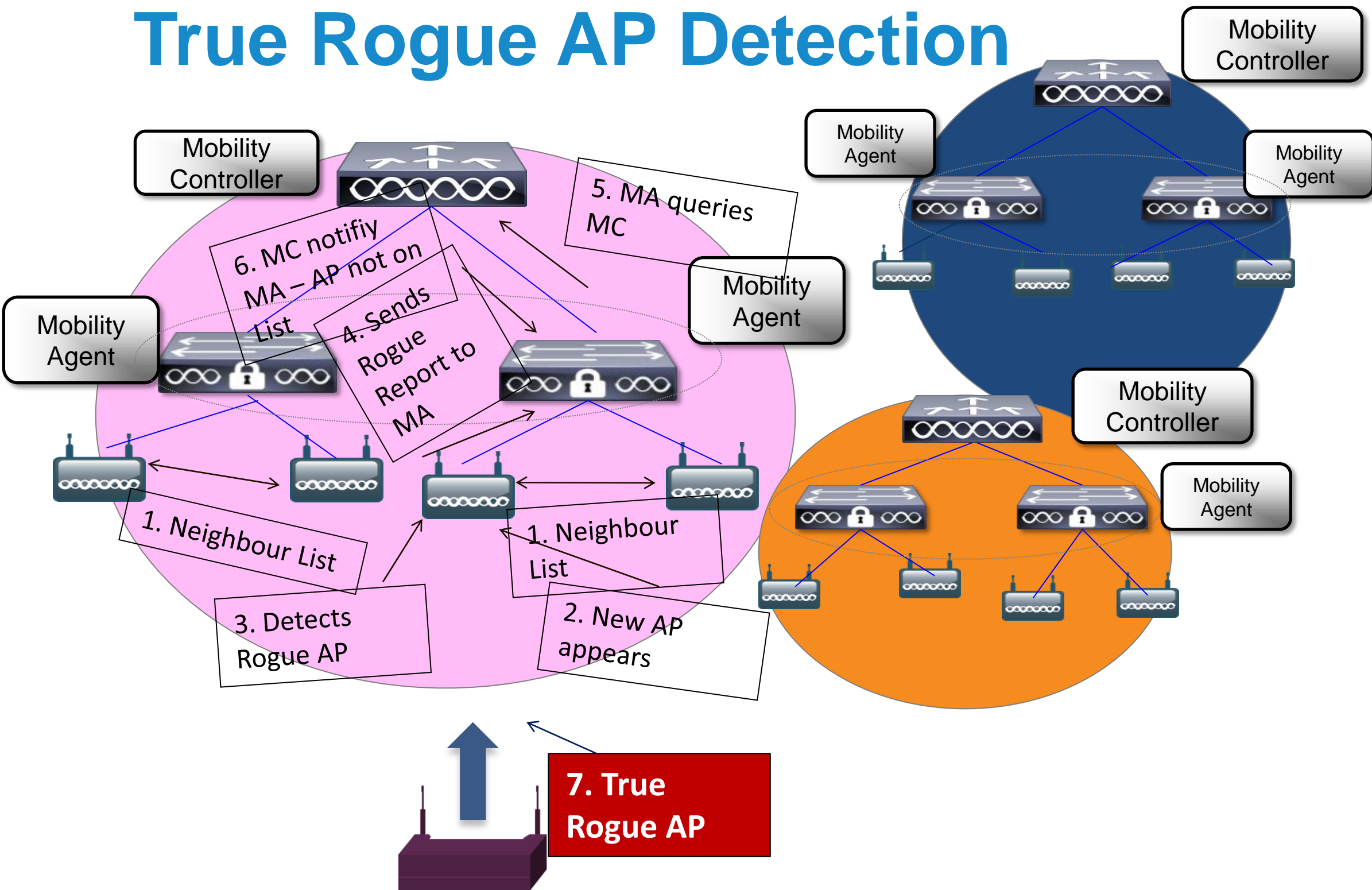
- Switch port shutting
- Location pin-pointing
- Over the air containment

AP List Management & Distribution



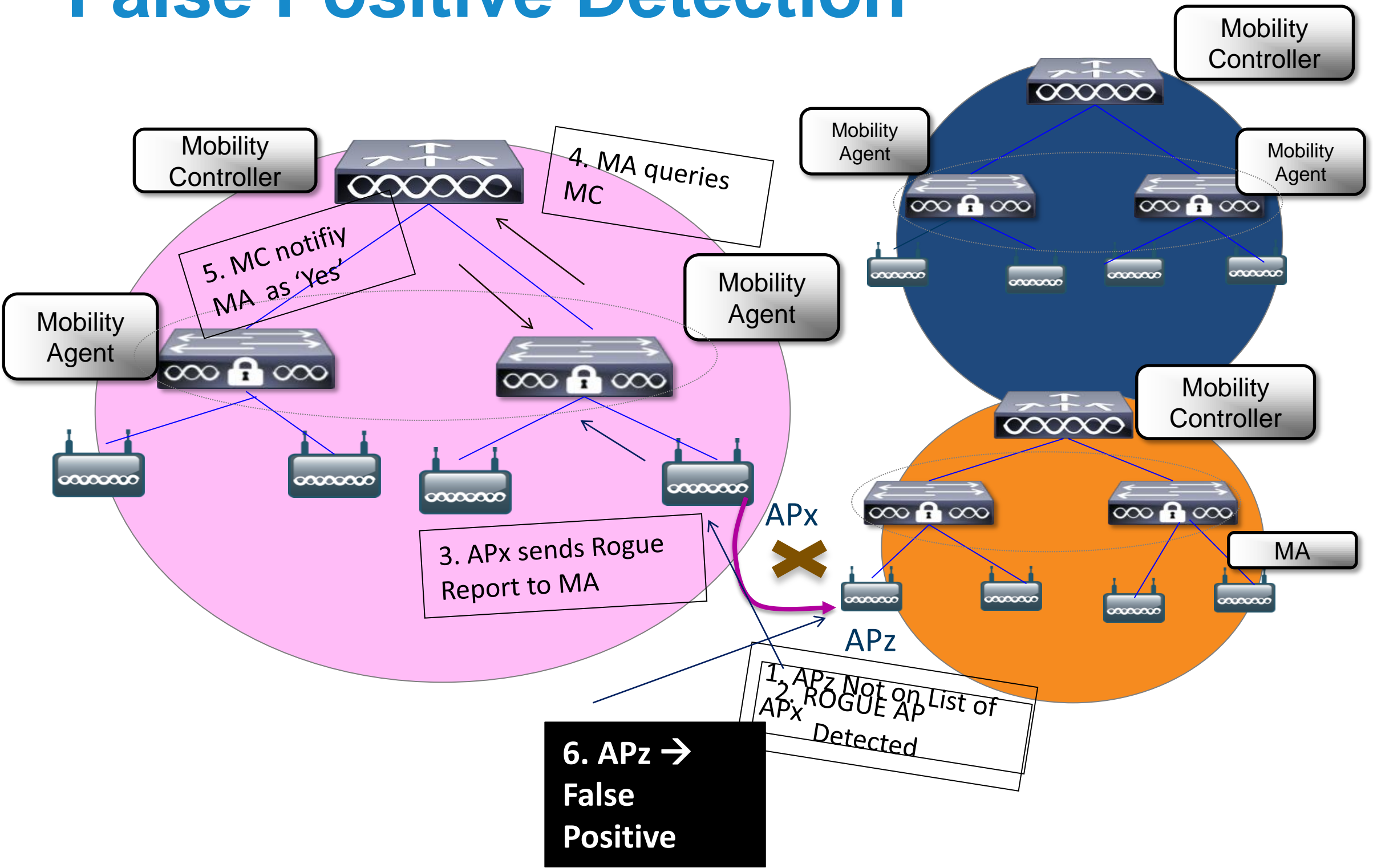
1. New AP joins successfully
2. MA notifies MC in its domain
3. MC updates AP list
4. Distributes List to all MCs in same domain
5. When MA gone - its MC deletes all APs & notifies other MCs
6. When MC gone - all other MCs delete APs reported by this MC

True Rogue AP Detection



1. Each AP maintains its Neighbour (N) List
2. New AP appears
3. AP detects Rogue AP (Not in N List)
4. Sends Rogue Report to MA
5. MA queries MC to check New AP on Global AP List
6. MC notifies MA - AP Not on Global List
7. New AP → True ROGUE AP

False Positive Detection



1. For some reason, APz Not on Neighbour List of APx
2. APz detected as Rogue AP
3. APx sends Rogue Report to MA
4. MA queries MC about APz on Global AP List
5. MC notifies MA as 'Yes'
6. So, APz is a False Rogue AP

6. APz → False Positive

1. APz Not on List of APx
2. ROGUE AP Detected

Rogue Classification Rules

Rule Name: Corporate
 Type: Malicious
 Match Operation: Match All Match Any
 Enable Rule:

Conditions
 Minimum RSSI(-95 to -50): -70 dBm
 Managed SSID:

Rule Name	Type	Status
Corporate	Malicious	Enabled
Starbucks	Friendly	Enabled

Rule Name: Starbucks
 Type: Friendly
 Match Operation: Match All Match Any
 Enable Rule:

Conditions
 Minimum RSSI(-95 to -50): -80 dBm

User configured SSID: tmobile

Detected as Rogue

Rogue Rule:
SSID: Starbucks;
RSSI: -80dBm

Marked as Friendly

Rogue Rule:
SSID: Corporate;
RSSI: -70dBm

Marked as Malicious

No matching
Rogue Rule

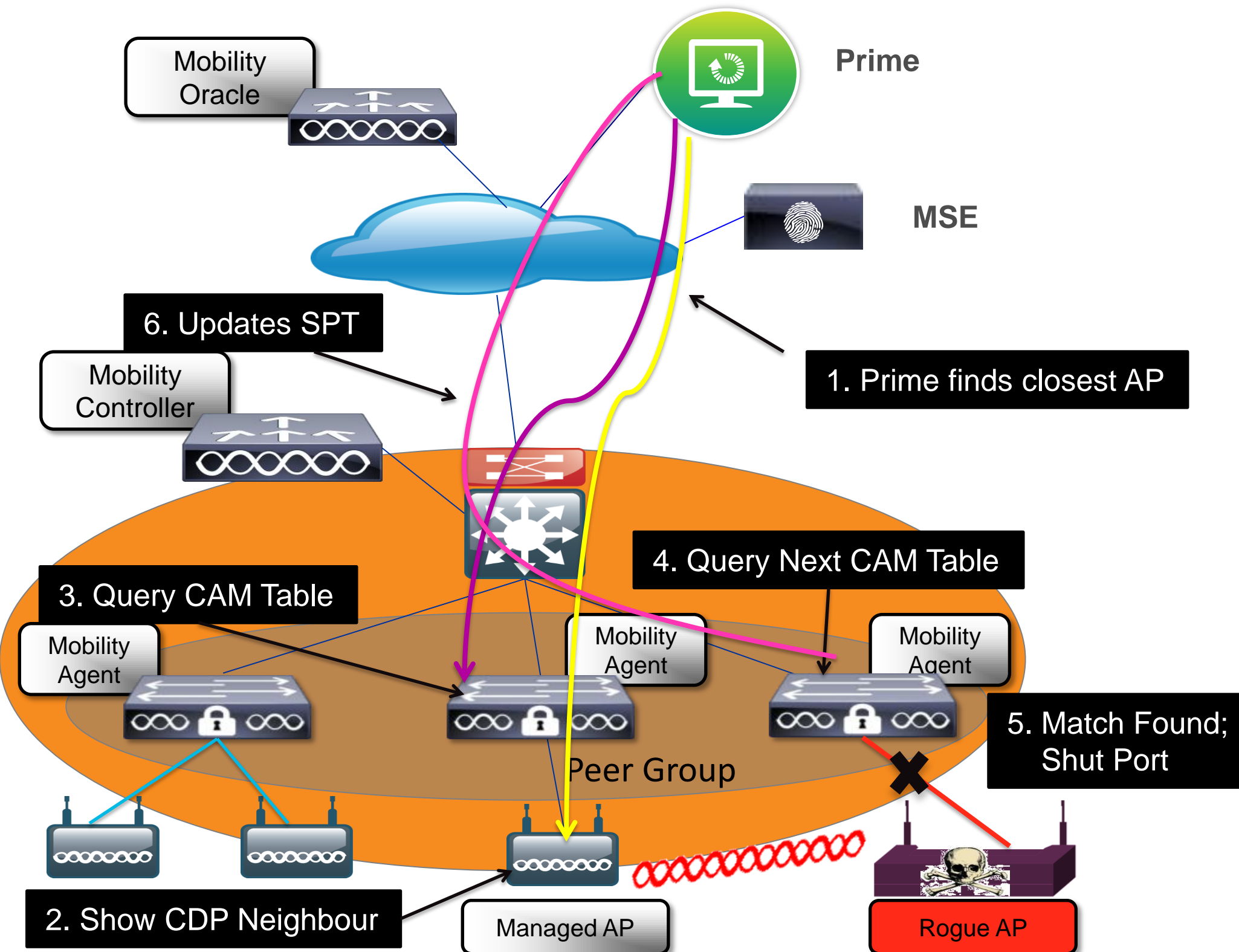
Marked as Unclassified

```

wireless wps rogue rule malicious priority 1
classify malicious
condition duration 120
condition encryption off
condition rssi -70
condition ssid corp
match all
wireless wps rogue rule friendly priority 2
classify friendly
condition duration 20
condition rssi -80
condition ssid Starbucks
match all
  
```

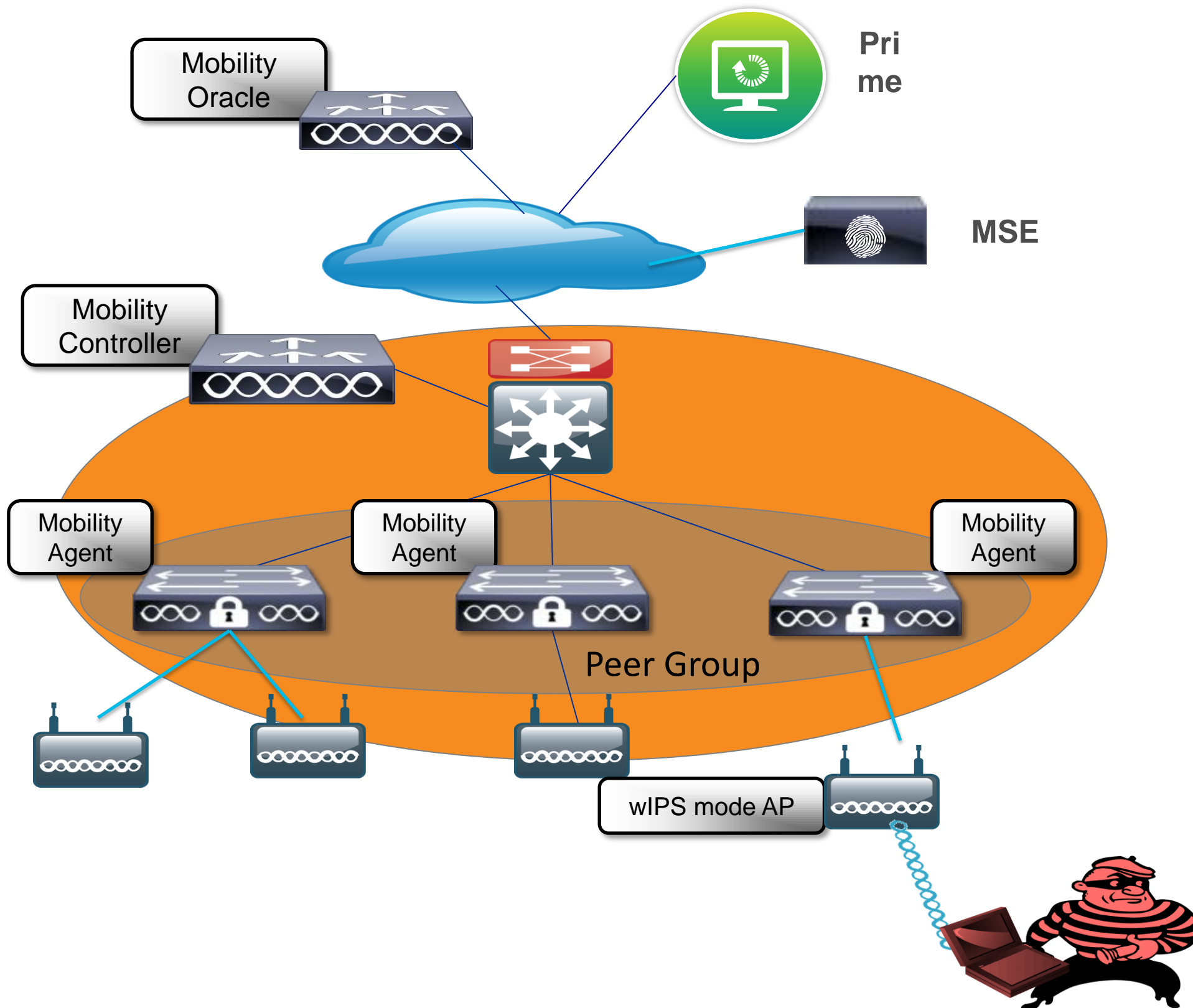


Switch Port Tracing



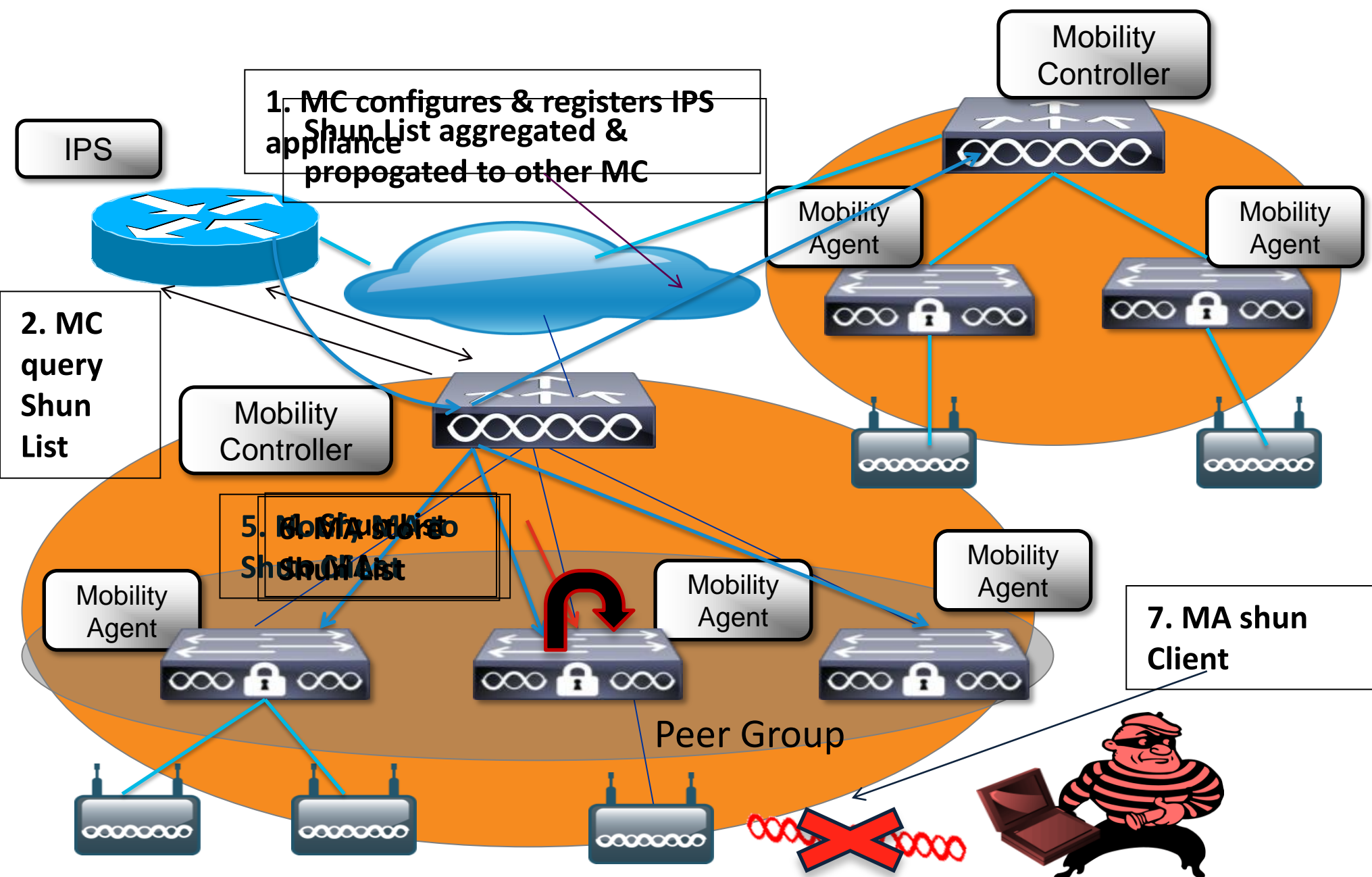
1. Prime finds closest AP detecting Rogue
2. AP retrieves its CDP Neighbours
3. Prime uses SNMP to query nearest MA CAM table:
 - Match Rogue AP MAC by +/-1 & +/-2 AND by OUI
4. If no match found query next hop
5. If match found eliminate managed device & eliminate by location
6. Update SPT status on Prime

wIPS



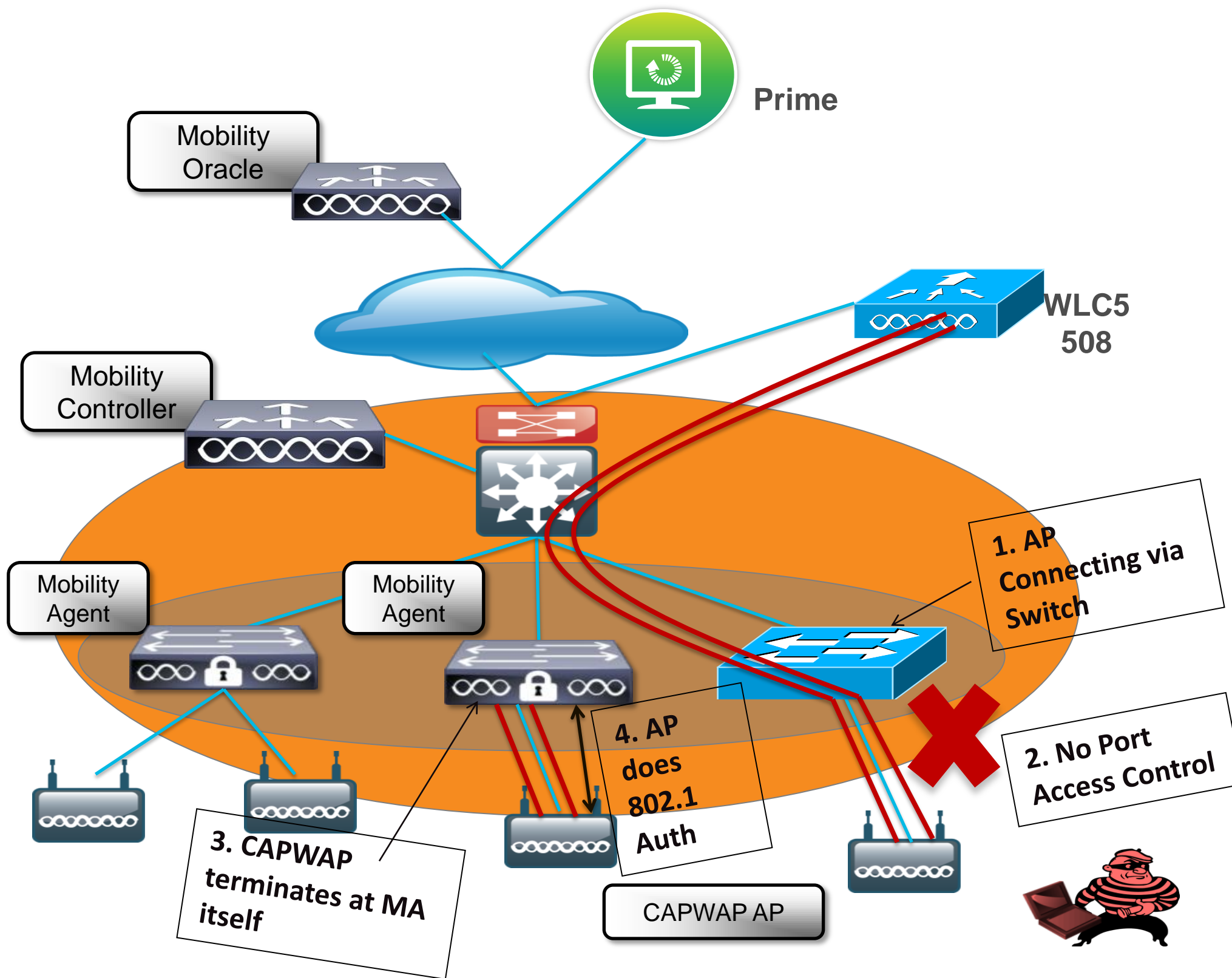
1. Attack Launched against Corporate Infrastructure
2. Detected on AP
3. CAPWAP AP Communicated to MA
4. Passed transparently to MSE via NMSP
5. Logged into wIPS Database on MSE, sent to Prime via SNMP traps
6. Display on Prime
7. Feature parity with CUWN architecture

CIDS



1. MC Configures and registers IPS Appliance
2. MC query Shun list from IPS Sensor via HTTPS
3. MC aggregate Shun List and Propagate to other MC in same mobility group
4. Pushes Shun list to MA
5. Notify MA to Shun Client on list
6. MA receive and store Shun list
7. MA Shun client on list

AP Dot1x



1. In earlier Architecture, CAPWAP AP connect to WLC via Switch
2. No Port Access Control
3. In Converged Access, CAPWAP tunnel terminates at MA itself
4. AP does the 802.1x Auth

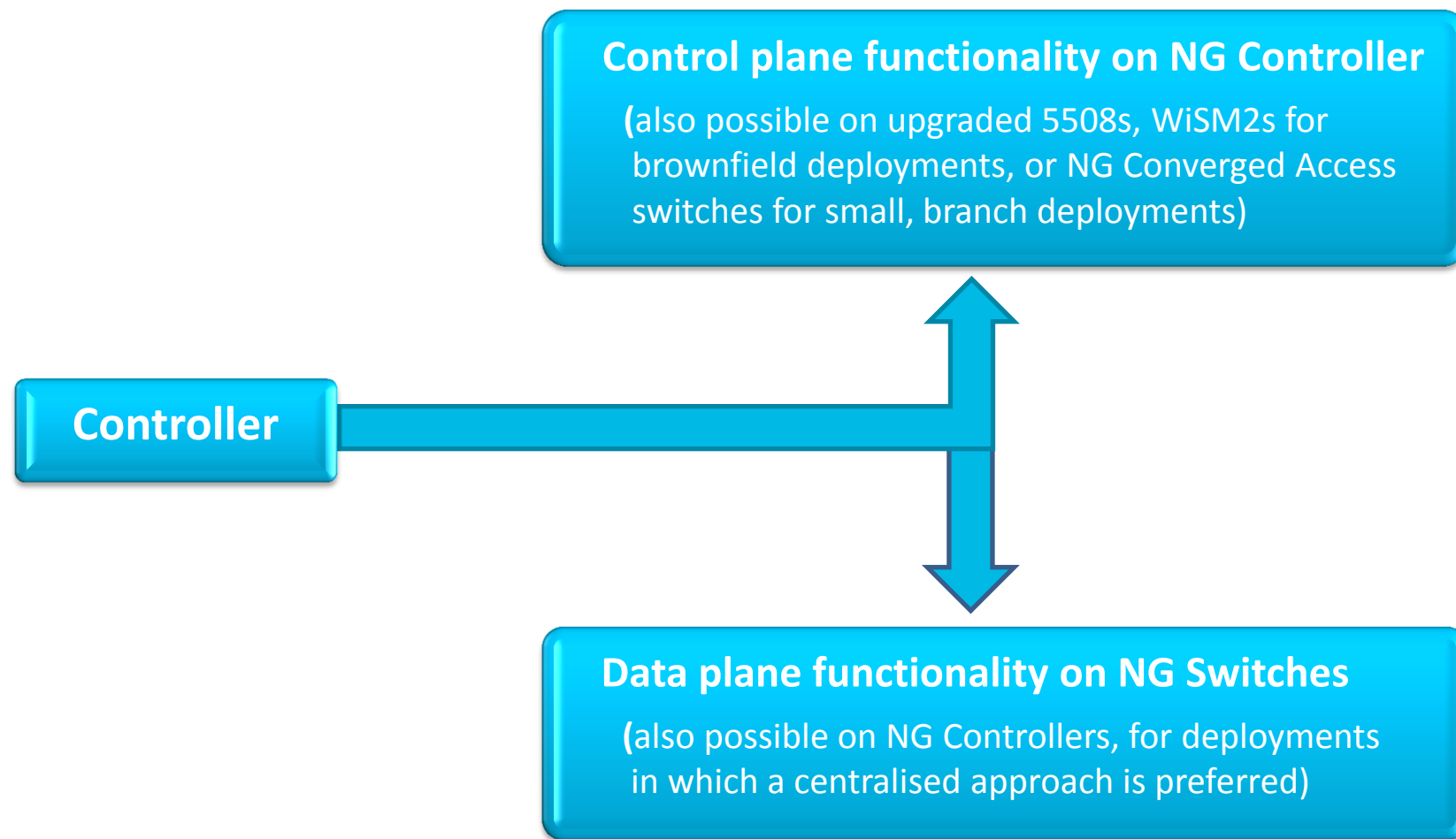
Advantages:

1. Protect network against physical tapping
2. No NEAT support needed

Agenda

- What is Converged Access ?
- Deploying One Network: Converged Access
- Wireless Deployment Options
- The new Converged Access Mobility Architecture
- Converged Access – IP Addressing
- How to deploy a Converged Access network ?
 - CleanAir & RRM
 - WebAuth & Guest Anchor (GA)
 - Security Features
- **Bringing Together Wired and Wireless**

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

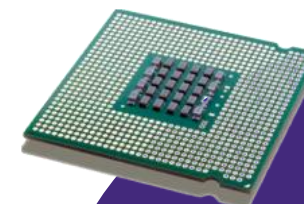


Next-Generation WLAN Controller (5760)



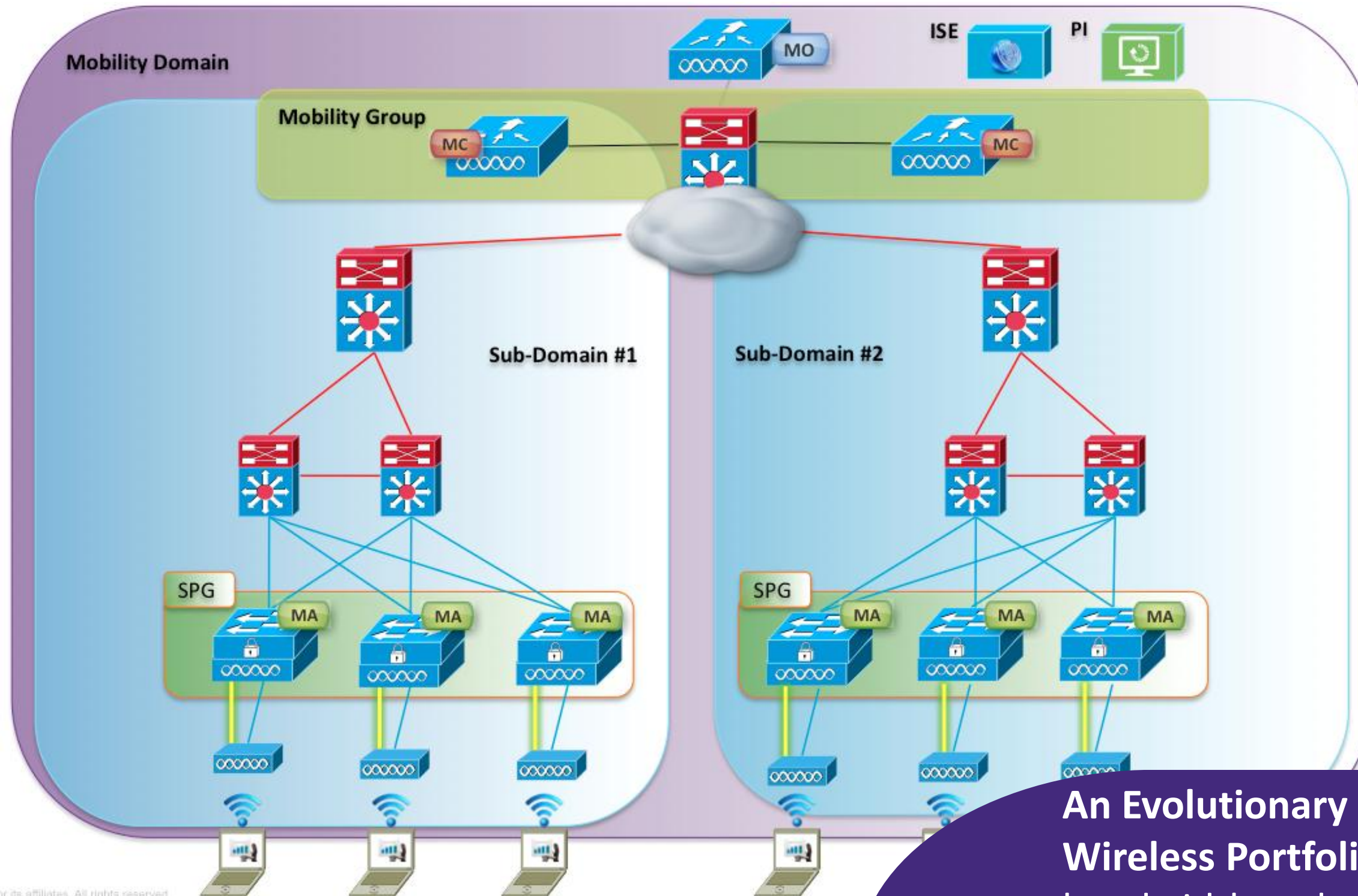
Next-Generation Switches (Catalyst 3850s)

Enabled by Cisco's strength in Silicon and Systems ... Doppler 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

Q & A



Complete Your Online Session Evaluation

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

Complete your Overall Event Survey and 5 Session Evaluations.

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

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



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.wv

Cisco *live!*



Sh tech-support wireless - MA

```
edison#sh tech-support wireless
*** show ap capwap timers ***
```

```
Cisco AP CAPWAP timers
```

```
AP Discovery timer      : 10
AP Heart Beat timeout   : 30
```

```
*** show ap capwap retransmit ***
```

```
Global control packet retransmit interval : 3
```

```
Global control packet retransmit count : 5
```

```
AP Name                      Retransmit Interval          Retransmit Count
-----
```

```
AP0022.bd18.87c0             3                             5
```

```
*** show ap dot11 24ghz cleanair air-quality summary ***
```

```
% This is command is not available on Mobility Agent
```

```
*** show ap dot11 24ghz cleanair air-quality worst ***% This is command is not available on Mobility Agent
```

```
*** show ap dot11 24ghz cleanair config ***
```

```
% This is command is not available on Mobility Agent
```

```
*** show ap dot11 24ghz cleanair device type all ***
```

```
% This is command is not available on Mobility Agent
```


Unified CleanAir - Getting Started

- MA ap interface level commands

- edison#sh ap sum (use sh ap dot11 24Ghz/5GHz to see interfaces)

```
-Number of APs: 1
-Global AP User Name: cisco
-Global AP Dot1x User Name: Not configured
-AP Name          AP Model  Ethernet MAC   Radio MAC      Port
-----
-AP0022.bd18.87c0  3502E    0022.bd18.87c0  0022.bdcc.d570  Gi1/0/1
```

- ap name AP0022.bd18.87c0 dot11 24ghz/5ghz cleanair (cr) - *enable interface 2.4/5 GHz*

- ap name AP0022.bd18.87c0 **no** dot11 5ghz cleanair (cr) *to disable*

- MC – all cleanair config commands are processed on MC – and passed to MA

```
-katana#sh ap dot11 2 cleanair config
-Clean Air Solution..... : Disabled
-Air Quality Settings:
- Air Quality Reporting..... : Disabled
- Air Quality Reporting Period (min)..... : 15
- Air Quality Alarms..... : Enabled
- Air Quality Alarm Threshold..... : 35
```

- At the MC config prompt

-(config)# ap dot11 24Ghz cleanair - *enable cleanair globally for the device*

-(config)# **no** ap dot11 24Ghz cleanair – *disable cleanair globally for the device*

CleanAir – Getting information from the MC

■katana#sh ap dot11 24Ghz cleanair ?

- air-quality no description
- config Displays CleanAir Configuration for 2.4GHz band
- device no description

■katana#sh ap dot11 24Ghz cleanair device type ?

- all Displays all CleanAir Interferers for 2.4GHz band
- bt-discovery Displays CleanAir Interferers of type BT Discovery for 2.4GHz band
- bt-link Displays CleanAir Interferers of type BT Link for 2.4GHz band
- <snip>

■katana#sh ap dot11 24Ghz cleanair air-quality summary/**worst**

-AQ = Air Quality

-DFS = Dynamic Frequency Selection


-AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
----------	---------	--------	--------	-------------	-----

-AP0022.bd18.87c0	11	99	99	0	No
-------------------	----	----	----	---	----

Spectrum Expert Connect

- Version 4.1.11 of SE the opening splash screen adds the remote sensor option
- You will need the IP address of the AP you just configured
- You will need the NSI Key
- You will need to select the radio you wish to view

Connect to Sensor



Sensor Card with Internal Antenna

Sensor Card with External Antenna

Remote Sensor:

IP Address

Radio b/g/n a/n

Key

Open Spectrum Capture File:

Automatically use this sensor next time

Some sensor cards may select external vs. internal antenna automatically in lieu of above setting.

```
edison#sh ap name AP0022.bd18.87c0 config dot11 24 | include IP
IP Address Configuration          : DHCP
IP Address                       : 192.168.10.150
IP Netmask                       : 255.255.255.0
Gateway IP Address               : 192.168.10.1
edison#sh ap name AP0022.bd18.87c0 config dot11 24 | include CleanAir
CleanAir Management Information
CleanAir Capable                 : Yes
CleanAir Management Admin State  : Enabled
CleanAir Management Operation State : Up
CleanAir NSI Key                 : 3E3717CCEB38ABFE01C0AE10E0423E42
CleanAir Sensor State            : Configured
```

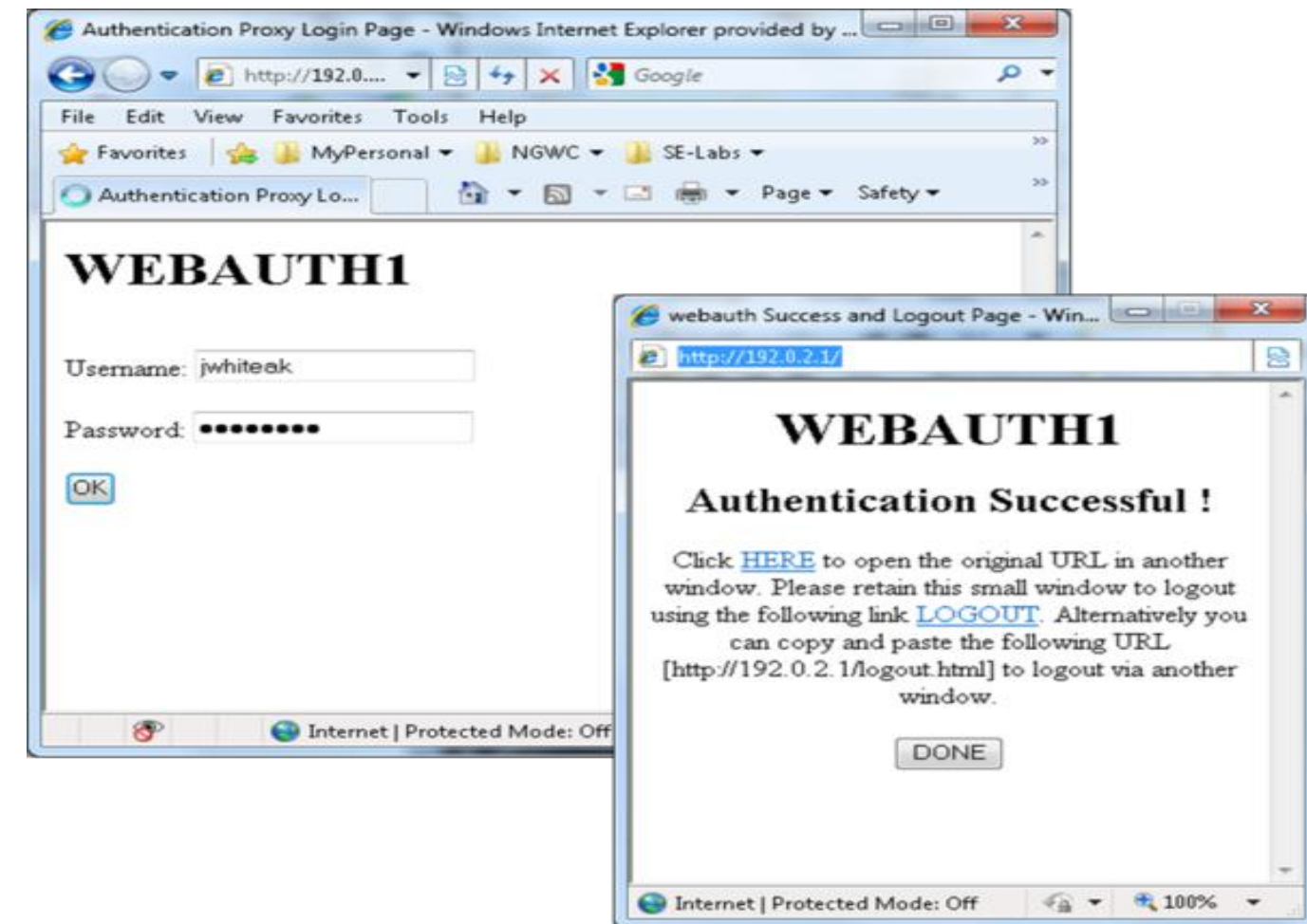
Spectrum Connect to CleanAir

- All versions/modes of Spectrum Expert connect rely on the NSI protocol for connection
- Network Spectrum Interface (NSI) is a proprietary protocol using the TCP transport directly between the AP and the Spectrum Expert console.
- The AP becomes the server, and the client (Spectrum Expert) initiates the connection



Wireless WebAuth – Local WebAuth Solutions (LWA)

- Converged Access Cat3850 and CT5760 both support consistent CUWN - LWA models as AireOS 7.0 release features
- For LWA in Campus with or without using Guest Anchor, within a SPG the MC must be active
- Central WebAuth (CWA) integration with ISE will be covered in separate session



Wireless WebAuth – Sample Config CLI

! First section is to define our global values and the internal Virtual Address.

! This should be common across all WCM nodes.

```
parameter-map type webauth global
```

```
virtual-ip ipv4 192.0.2.1
```

! This is for generic WebAuth and will authenticate against internal user database

```
parameter-map type webauth webauth1
```

```
type webauth
```

```
banner text ^C WEBAUTH1^C
```

! This is for generic WebAuth with Consent form Click-2-Accept, no Authentication

```
parameter-map type webauth webconsent
```

```
type webconsent
```

```
banner text ^C WEBCONSENT^C
```

! Configure http server in global config. These are needed to enable Web Services in IOS

```
ip http server
```

```
ip http secure-server
```

```
ip http active-session-modules none
```

```
!
```

Wireless WebAuth – Sample Config CLI (cont)

! This WLAN “ua-web1” will advertise an SSID called “ua-web1”,

! Place the user in VLAN 21,

! Disable default WPA authentication and Enable web-auth security

! Use wcm_local authentication for this security from global AAA Setup

! Associate earlier defined parameter-map “webauth1”

!

```
wlan ua-web1 11 ua-web1
```

```
client vlan 21
```

```
no security wpa
```

```
security web-auth
```

```
security web-auth authentication-list wcm_local
```

```
security web-auth parameter-map webauth1
```

```
no shutdown
```

!

! Sample AAA Global setup for wcm_local

!

```
username abc password 7 08204E4D
```

```
aaa new-model
```

```
aaa local authentication wcm_local authorization wcm_author
```

!

```
aaa user profile local
```

!

```
aaa authentication login wcm_local local
```

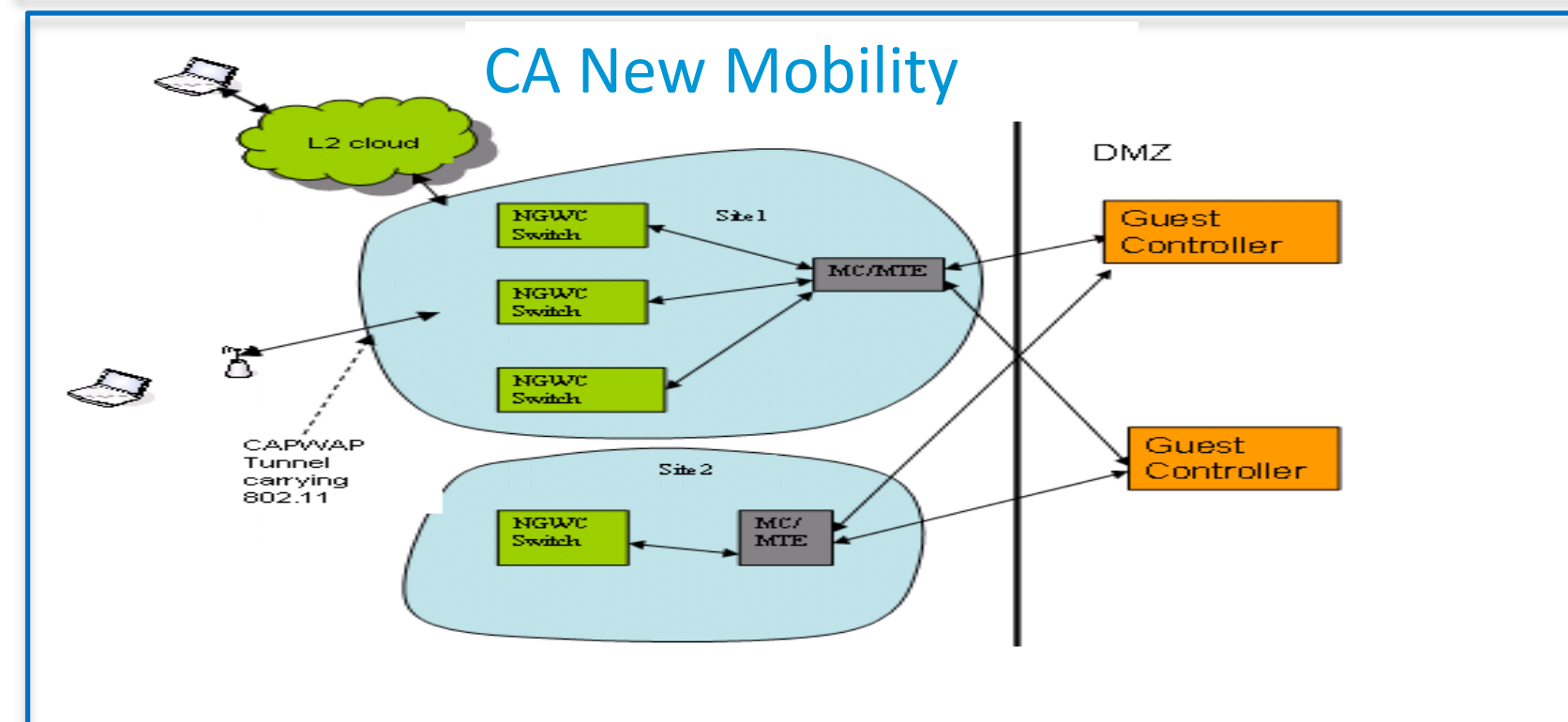
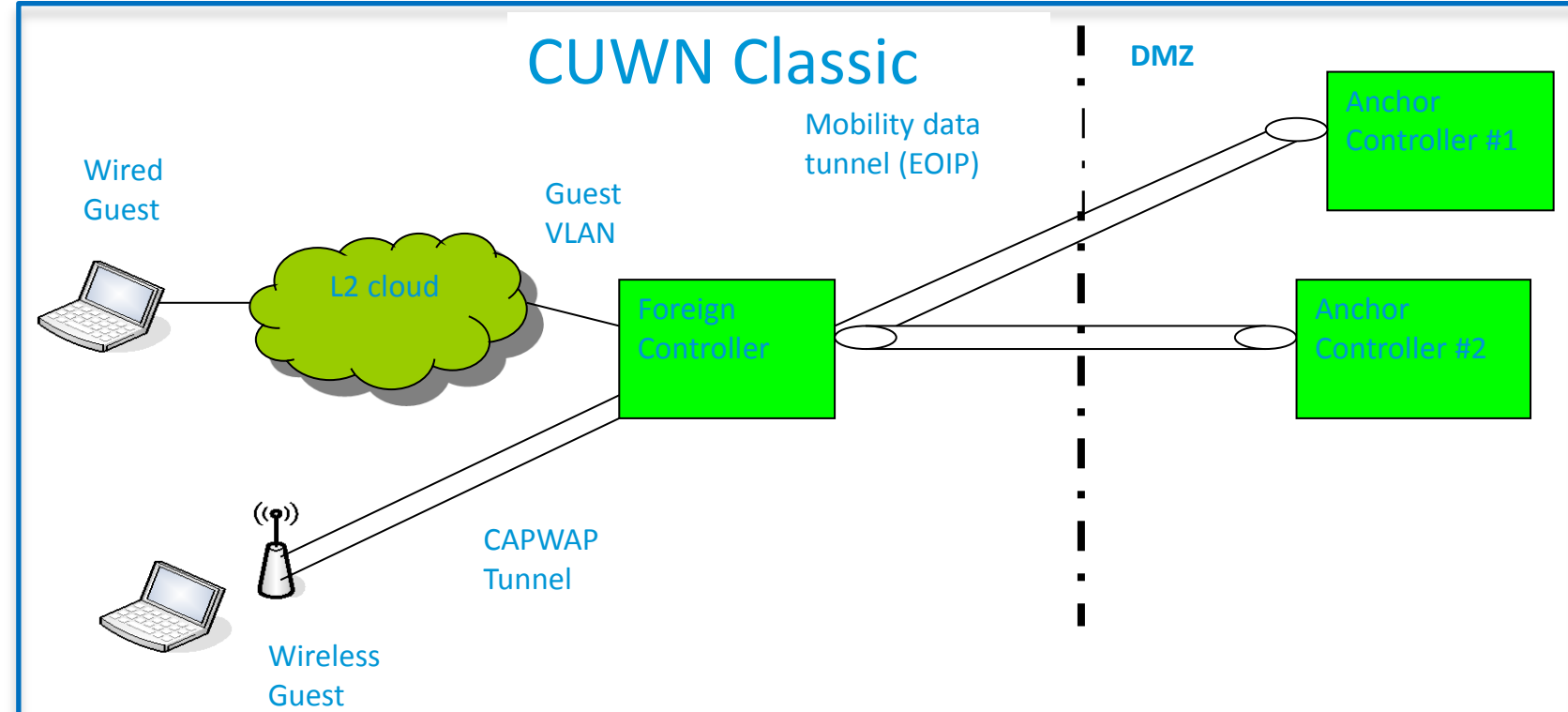
```
aaa authentication dot1x wcm_local local
```

```
aaa authorization network wcm_local local
```

!

Guest Anchor (GA)

- Converged Access Cat3850 and CT5760 both support consistent CUWN - GA modes as AireOS 7.0 release features
- Anchor roles are supported on CT5760 and also CT5508/WiSM-2 running New Mobility modes only.
- Foreign Role is supported on Cat3850/CT5760/CT5508/WiSM-2
- Authentication Methods:
 - L3 Methods (WebAuth)
 - ❖ L3 Authentication happens at Anchor / L2 at Foreign



Wireless GA – Sample Config CLI

```
! Config on Foreign MC/MA (192.168.21.44)
! All Mobility Group Configuration must be completed prior to these steps
! Place the user in dummy VLAN 1 and establish (GA) Tunnel
! to Anchor (GA) controller (192.168.21.43) , Disable Snooping on foreign VLAN
! Disable default WPA authentication and Enable web-auth security
! Use wcm_local authentication for this security from global AAA Setup.
! Associate earlier defined parameter-map "webauth1"
!
no ip dhcp snooping vlan 1
wlan ua-web1 11 ua-web4
  client vlan 1
  mobility anchor 192.168.21.43
  no security wpa
  security web-auth
  security web-auth authentication-list wcm_local
  security web-auth parameter-map webauth1
  no shutdown
!
```

Wireless GA – Sample Config CLI

```
! Config on Anchor GA (192.168.21.43)
! All Mobility Group Configuration must be completed prior to these steps
!
! Place the user in VLAN 24 and establish (GA) Tunnel to a local GA controller (192.168.21.43)
! Disable default WPA authentication and Enable web-auth security
! Use wcm_local authentication for this security from global AAA Setup.
! Associate earlier defined parameter-map "webauth1"
!
wlan ua-web1 11 ua-web4
  client vlan 24
  mobility anchor 192.168.21.43
  no security wpa
  security web-auth
  security web-auth authentication-list wcm_local
  security web-auth parameter-map webauth1
  no shutdown
!
```