


ArchitecturingNetwork for Branch Offices with Cisco FlexConnect
使用思科FlexConnect技术构建分支机构WLAN网络

- 张国敏
- Customer Support Engineer

Objectives

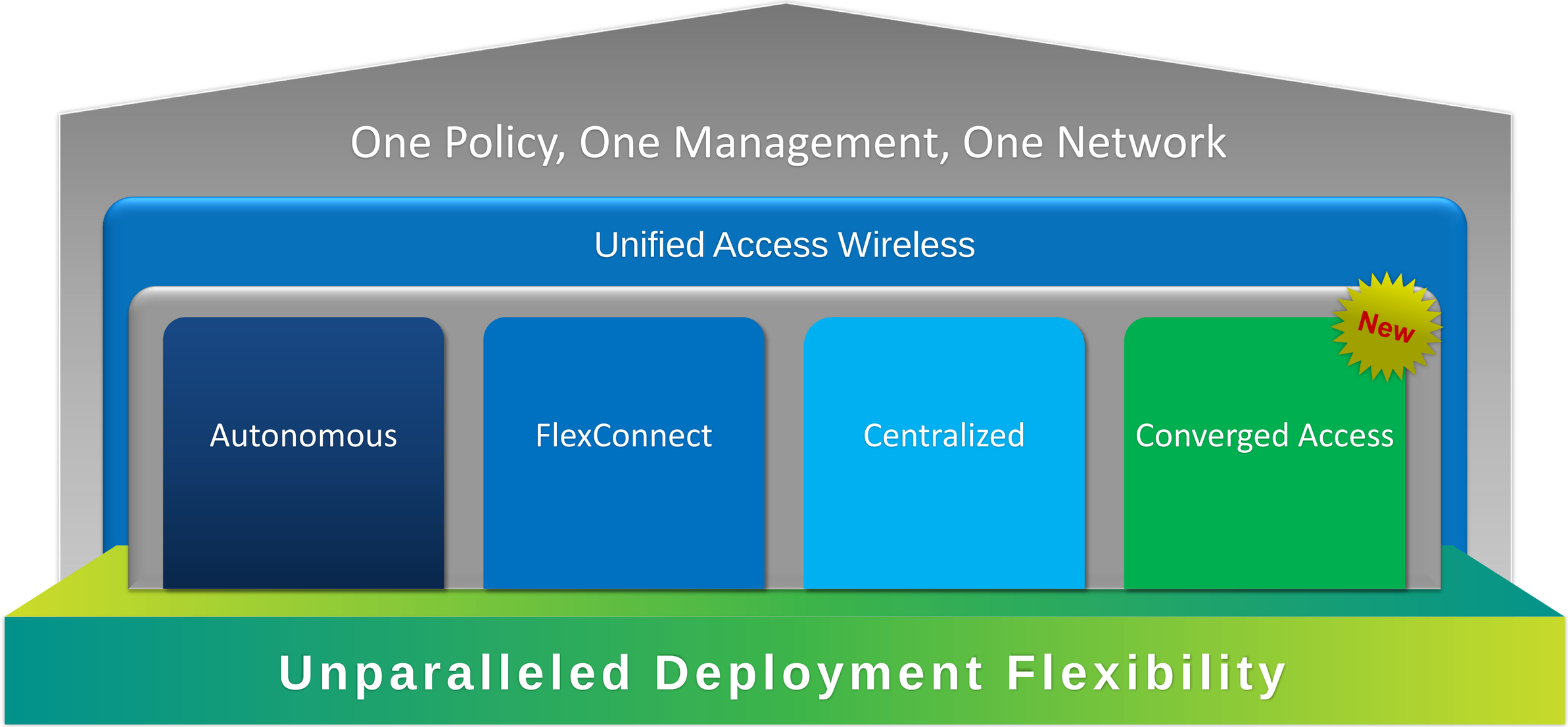
Design & Deploy Branch Network That Increases Business Resiliency

Agenda

- Learn Cisco Unified Wireless LAN Principles **(Reminder)**
- Understand Wireless Branch Deployment Options
- Evaluate FlexConnect Architectural Requirements
- Identify the need for FlexConnect & AP Groups
- Design a Resilient Branch Network
- Design Secure & BYOD enabled Branch Network
- How to operate Wireless Branch efficiently over WAN

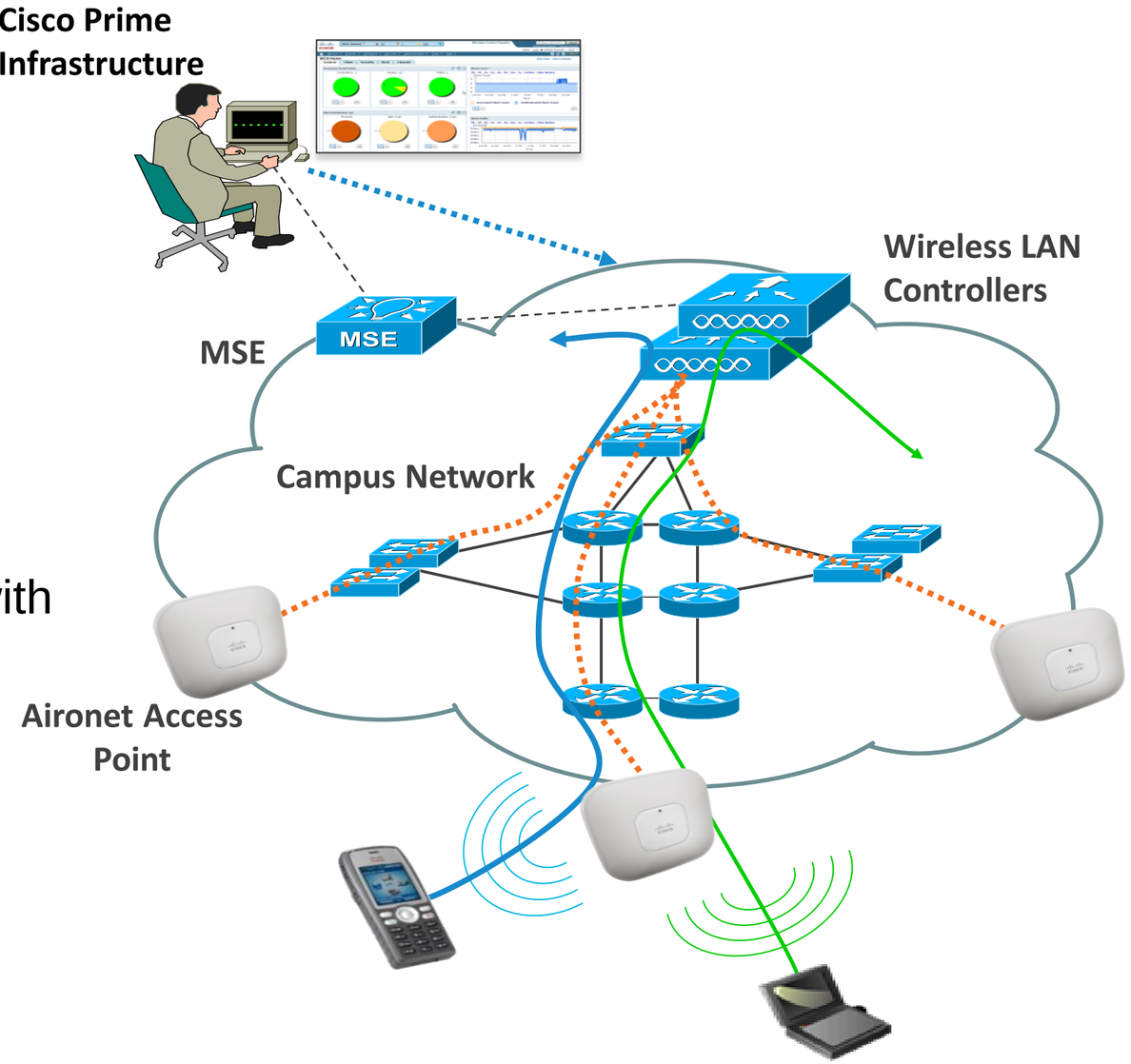
Cisco Unified Wireless LAN Principles

Cisco One Network : Wireless Deployment Modes



Cisco Unified Wireless Principles

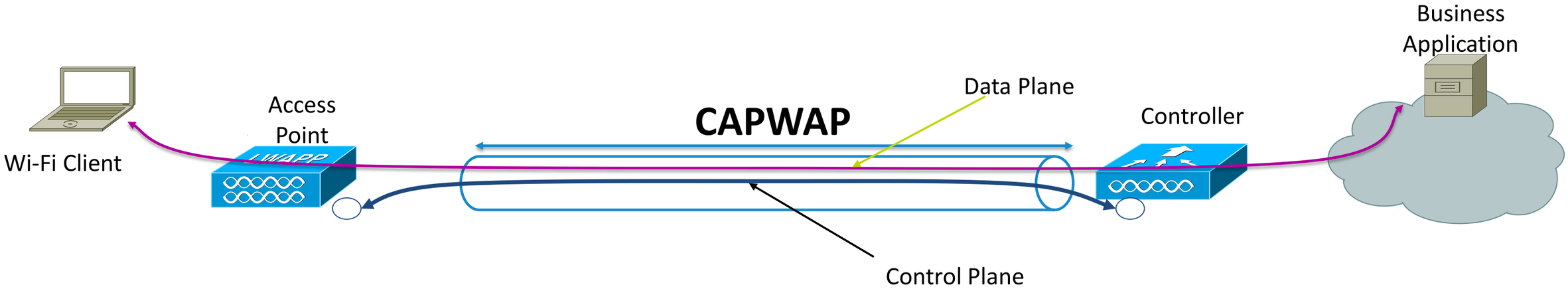
- Components
  - Wireless LAN controllers
  - Aironet access points
  - Management (Prime Infrastructure)
  - Mobility Service Engine (MSE)
- Principles
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC



CAPWAP Overview

Control and Provisioning of Wireless Access Point

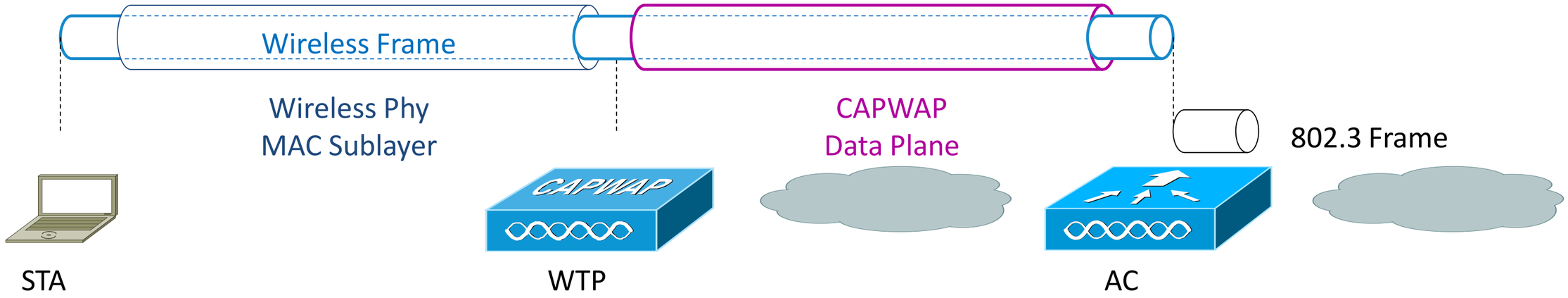
- CAPWAP is a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs)
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (optional)
- CAPWAP supports only Layer 3 mode deployments



CAPWAP Modes

Split MAC

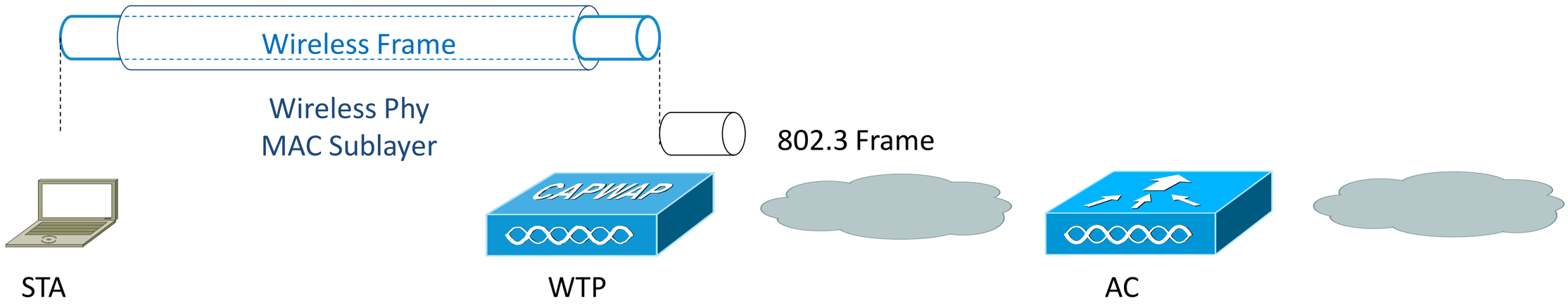
- The CAPWAP protocol supports two modes of operation
  - Split MAC (Centralized Mode)
  - Local MAC (H-REAP/FlexConnect)
- Split MAC



CAPWAP Modes

Local MAC

- Local MAC mode of operation allows for the data frames to be either locally bridged or tunneled as 802.3 frames
- Locally bridged

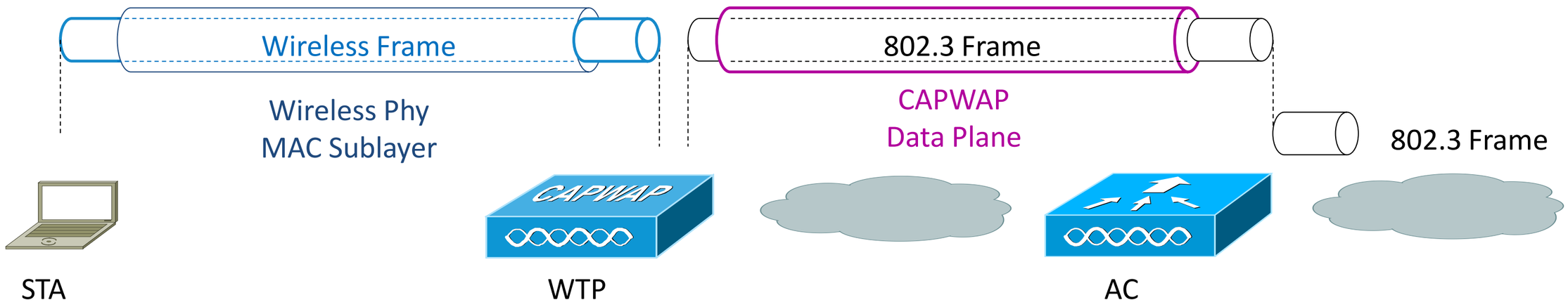


- **FlexConnect support locally bridged MAC and split MAC per SSID**

CAPWAP Modes

Local MAC

- Local MAC mode of operation allows for the data frames to be either locally bridged or tunneled as 802.3 frames
- Tunneled as 802.3 frames



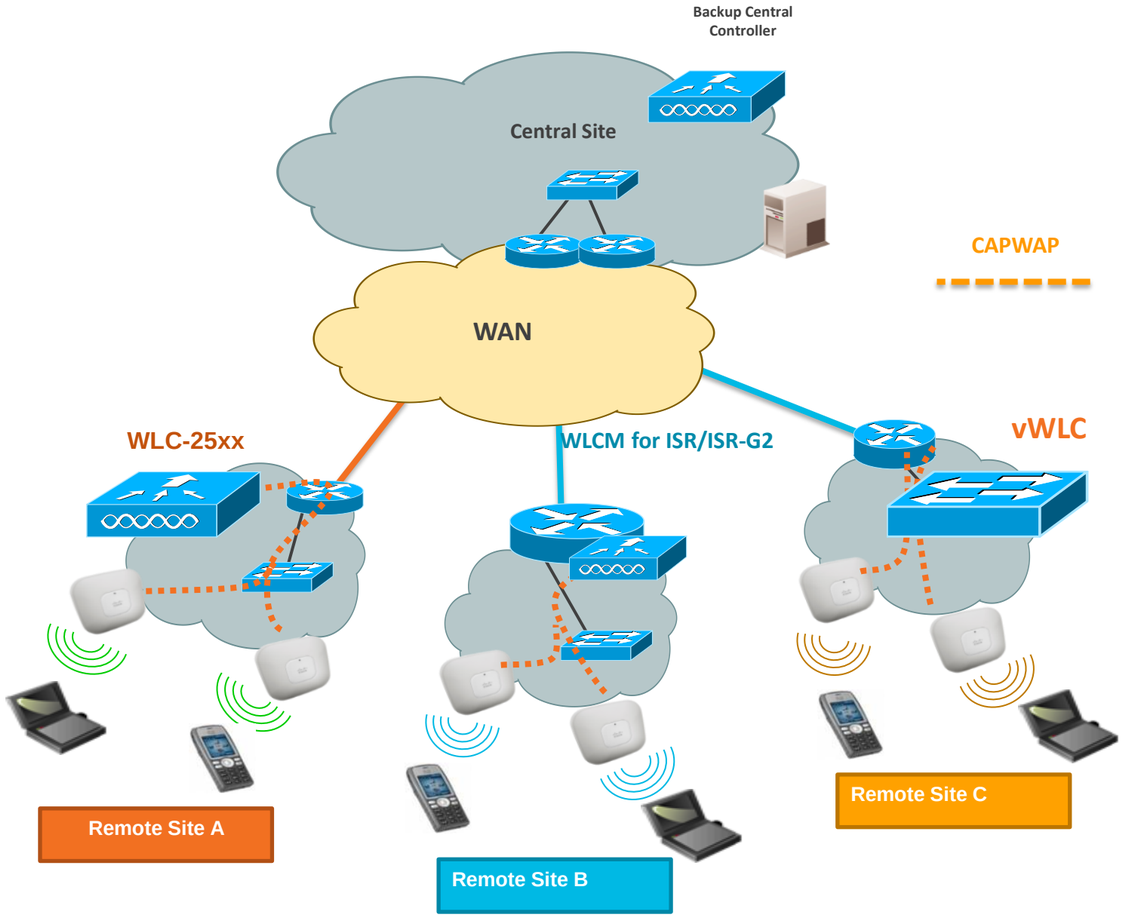
- Tunneled local MAC is not supported by Cisco

Wireless Branch Deployment Options

Branch Office with Local WLAN Controller

Overview

- Branches can also have local remote controllers
- Small form factors WLC are available to have « small campus » :
  - CT-2504,
  - Integrated controller modules in ISR/ISR-G2
  - vWLC
- High-availability design with central backup controller is supported; WAN limitations may apply



Branch Office with Local WLAN Controller

Advantages

- Cookie cutter configuration for every branch site
- Layer-3 roaming within the branch
- Reliable Multicast (filtering)
- IPv6 L3 Mobility
- IPv6 ACL

Note: If you have ISR/ISR G2 at branch site then it is recommended to use the IOS Firewall at edge for unified access policies.

Branch Office Deployment

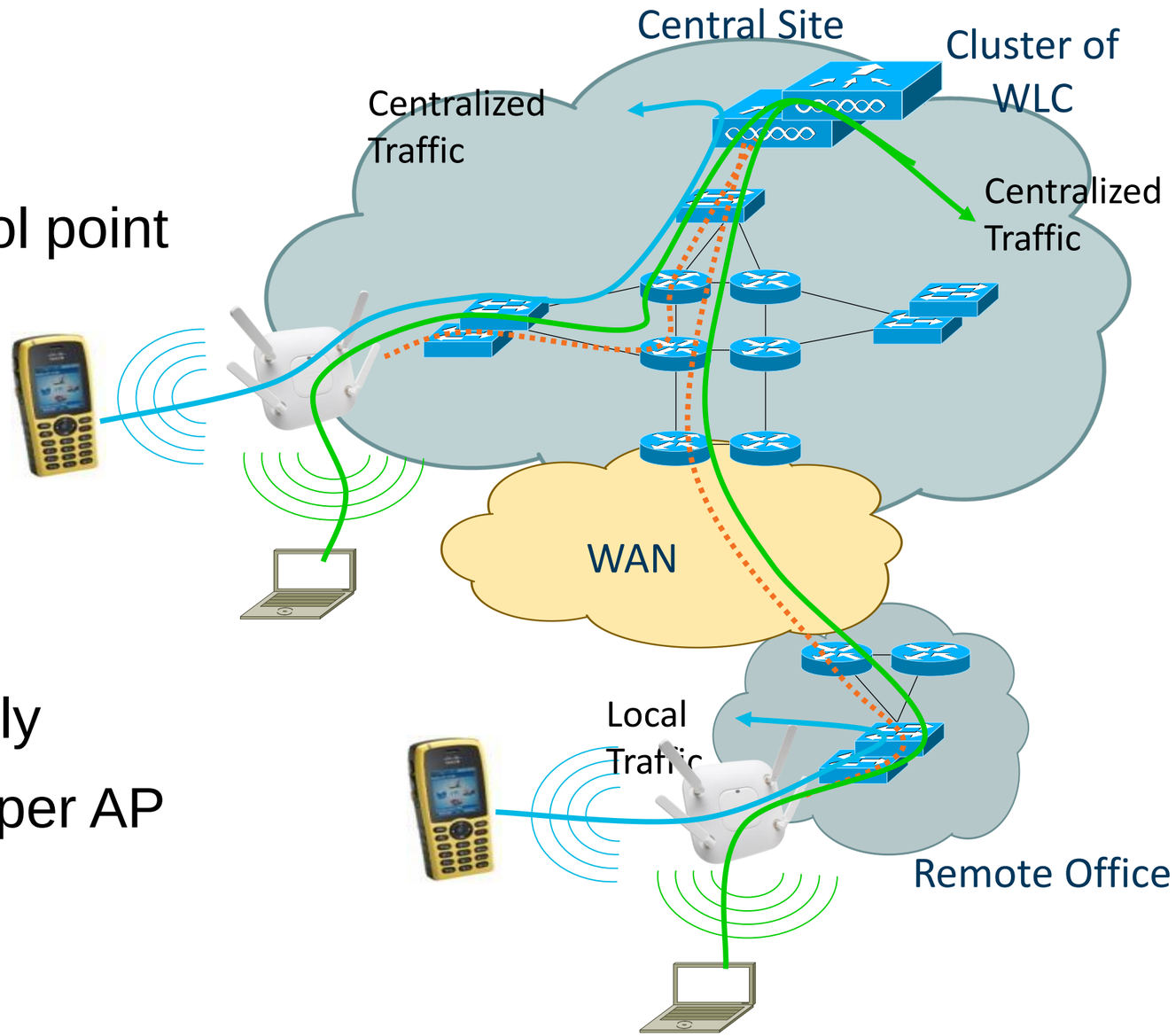
FlexConnect (HREAP)

- Hybrid architecture
- Single management and control point
- Data Traffic Switching

  Centralized traffic (split MAC)

  or

  Local traffic (local MAC)
- HA will preserve local traffic only
- Traffic Switching is configured per AP and per WLAN (SSID)



FlexConnect Glossary

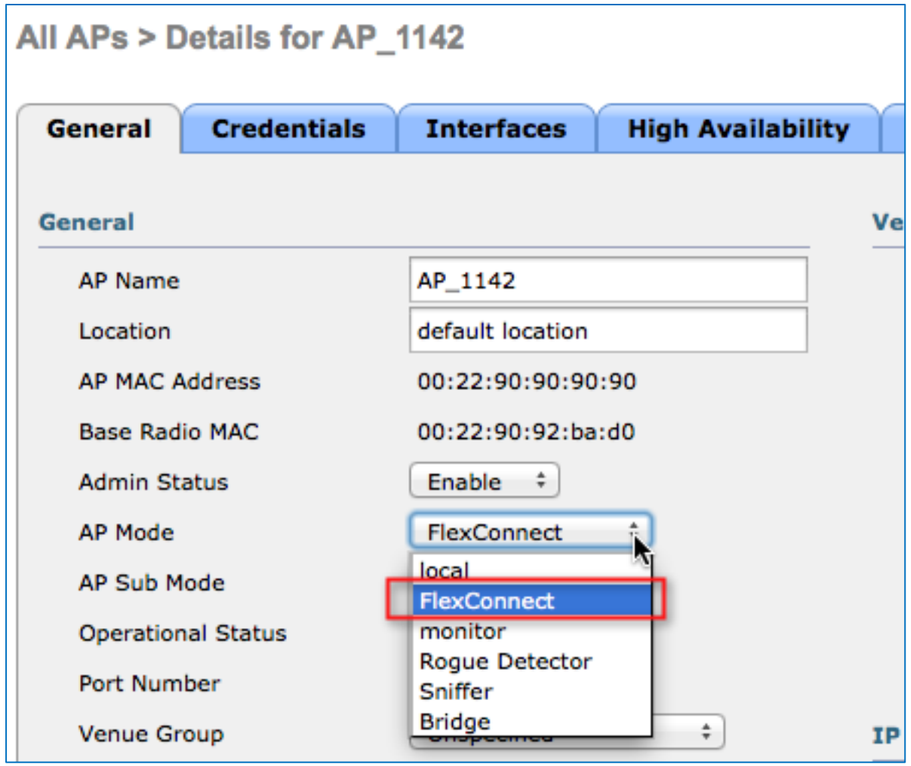
- **Connected Mode** – When FlexConnect can reach Controller (connected state), it gets help from controller to complete client authentication.
- **Standalone mode** – When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.

- **Local Switching** – Data traffic switched onto local VLANs for an SSID
- **Central Switching** – Data traffic tunneled back to WLC for an SSID

Configure FlexConnect Mode

Step 1: Configure Access Point Mode

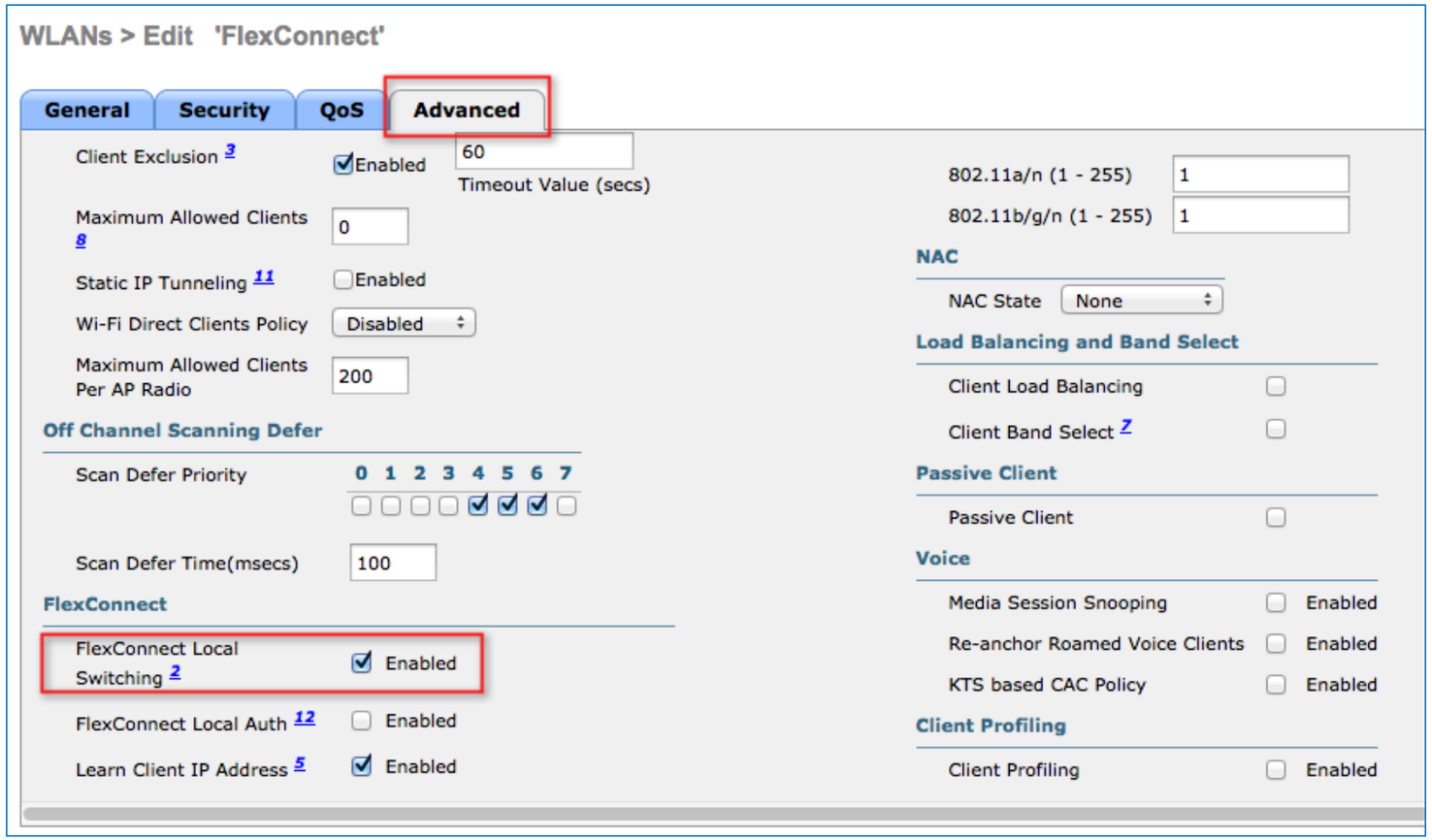
- Enable FlexConnect mode per AP
- Supported AP: AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600 , AP-2600 , AP-3600, AP-3700, AP-1520, AP-1530, AP-1550



Configure FlexConnect Local Switching

Step 2: Enable Local Switching per WLAN

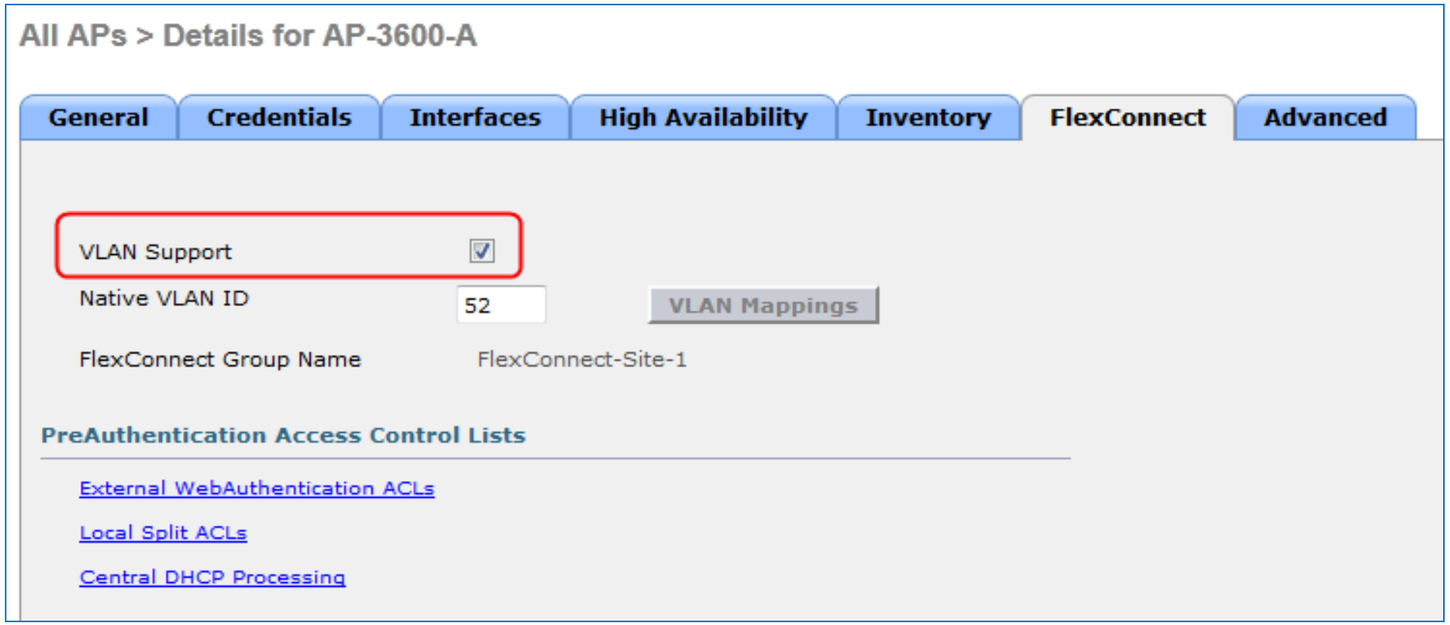
- Only WLAN with “FlexConnect Local Switching” enabled will allow local switching on the FlexConnect AP



Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

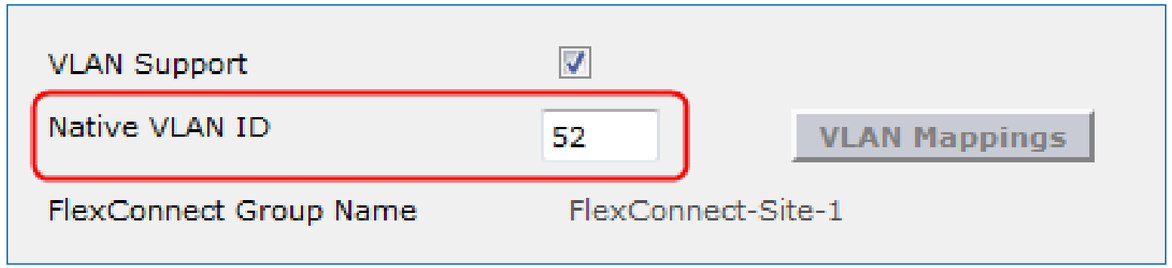
- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN Support provides the ability to configure remote VLAN to WLAN mappings. VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using NCS templates



Configure FlexConnect VLAN Mapping

Step 4: FlexConnect Specific Configuration – Native Vlan

- When connecting with Native VLAN on AP, L2 switchport must also match with corresponding Native VLAN configuration
- Each corresponding SSID that is allowed to be locally switch should be allowed on the corresponding switchport.

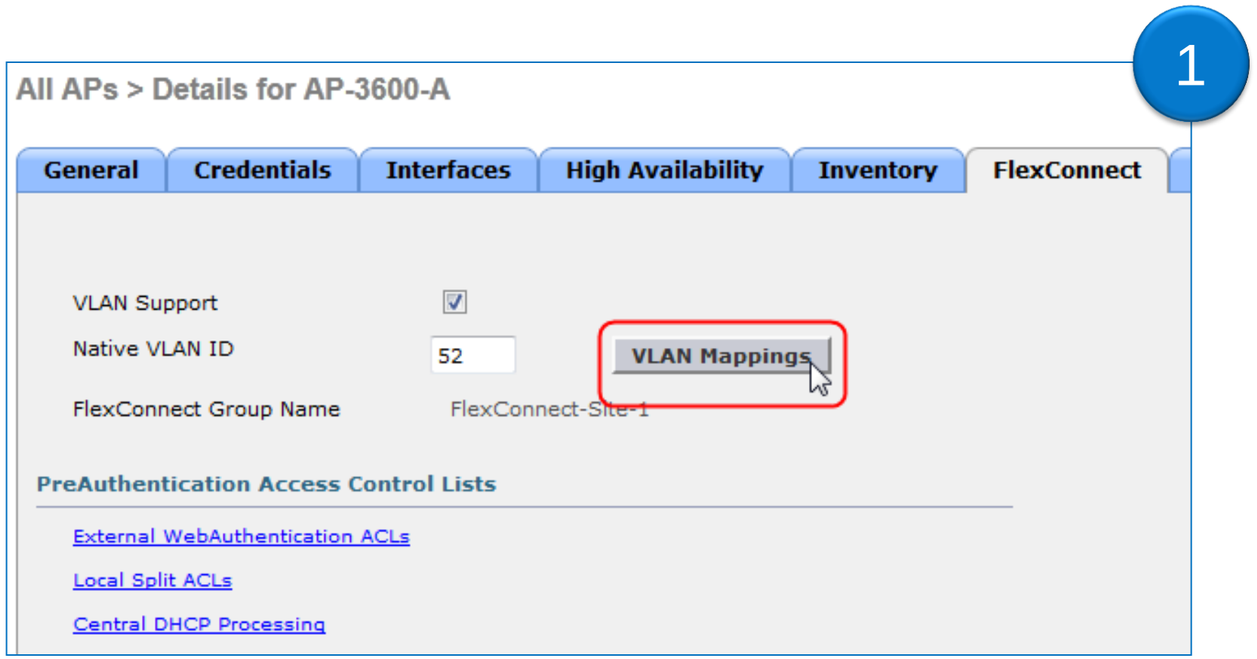


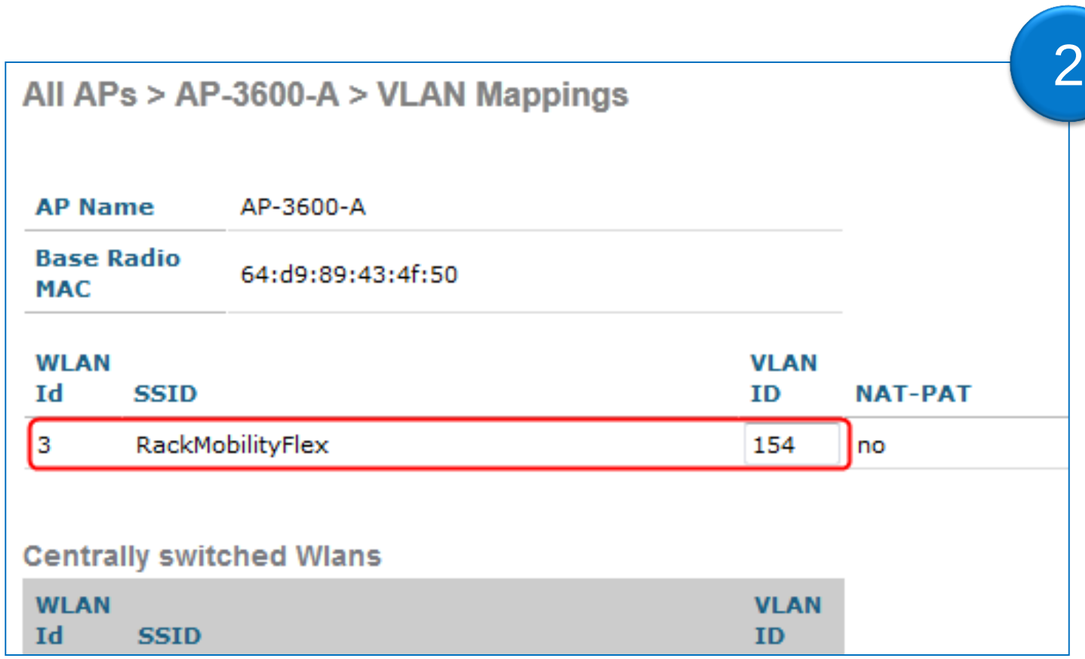

```
!
interface GigabitEthernet0/1
 switchport access vlan 52
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 52
 switchport trunk allowed vlan 52,154,155
 switchport mode trunk
 spanning-tree portfast
!
```

Configure FlexConnect VLAN Mapping

Step 5: Per AP SSID to VLAN Mapping

- Mapping of SSID to 802.1Q VLAN is done per FlexConnect AP



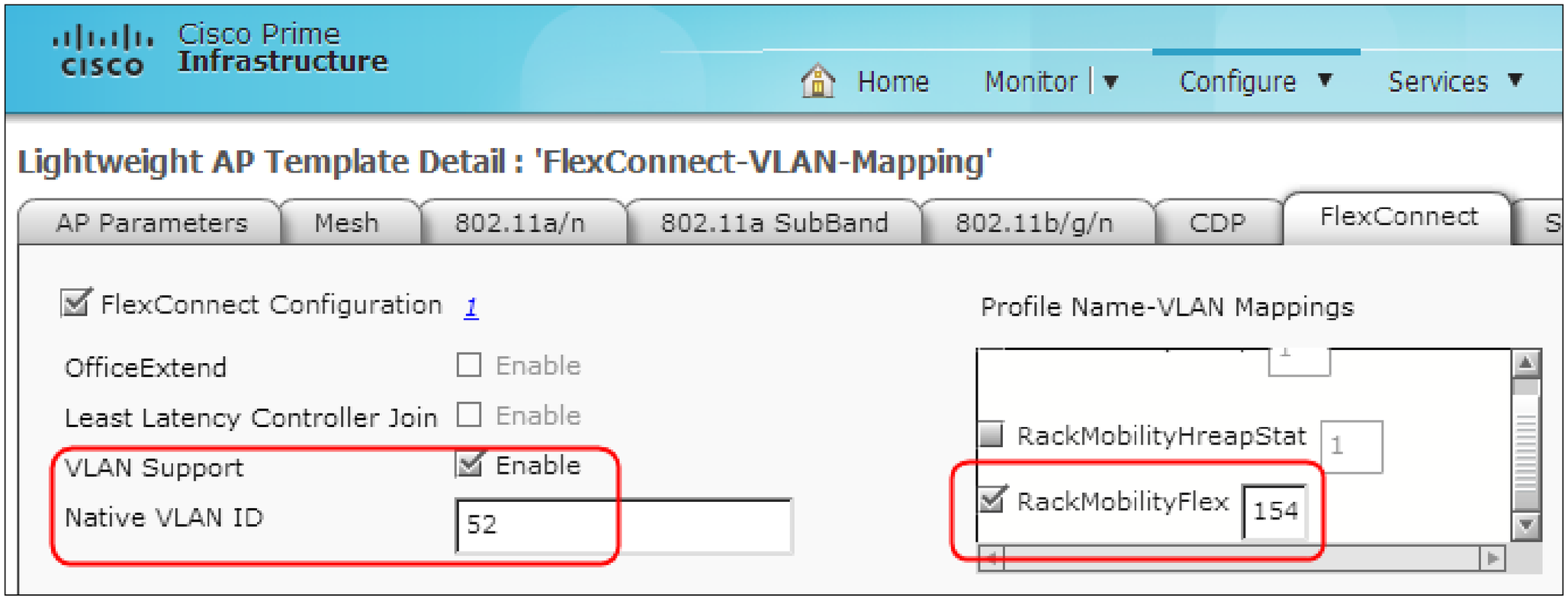


- Or the use of Prime Infrastructure (NCS) via configuration templates

Configure FlexConnect VLAN Mapping

Step 6: Using Cisco Prime Infrastructure

- Prime Infrastructure provides simplified configuration to all FlexConnect APs with one Lightweight AP Template



Evaluate FlexConnect Architectural Requirements

FlexConnect Design Considerations

For Your Reference

WAN Limitations Apply

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	128 kbps	300 ms	5	25
Data+Voice	128 kbps	100 ms	5	25
Data	128 kbps	1 sec	1	1
Monitor	128 kbps	2 sec	5	N/A
Data	1.44 Mbps	1 sec	50	1000
Data+Voice	1.44 Mbps	100 ms	50	1000
Monitor	1.44 Mbps	2 sec	50	1000

FlexConnect Design Considerations

Feature Limitations Apply

- Some features are not available in standalone mode or in local switching mode
  - MAC/Web Auth in Standalone Mode
  - VideoStream
  - IPv6 L3 Mobility
  - SXP TrustSec
  - See full list in « FlexConnect Feature Matrix »

  http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080b3690b.shtml

Economies of Scale For Lean Branches

Flex 7500 Wireless Controller

Access Points	300-6,000
Clients	64,000
Branches	2000
Access Points / Branch	100
Deployment Model	FlexConnect
Form Factor	1 RU
IO Interface	2 x 10GE
Upgrade Licenses	100, 200, 500, 1K RTU Licenses

Key Differentiation

- WAN Tolerance
  - High Latency Networks
  - WAN Survivability
- Security
  - 802.1x based port authentication
- Voice support
  - Voice CAC
  - OKC/CCKM

Cisco 8510 series Controller

Optimized for high scale deployments

Access Points	300-6,000
Clients	64,000
Branches/locations	6,000 (2000 groups)
Access Points per FlexConnect group	100
Deployment types	Local (centralized), FlexConnect and mesh
Form Factor	1 RU
IO Interface and redundancy	Dual redundant 10GE ports with LAG*
Power options	AC and DC*
Power redundancy	Dual redundant power supplies installed*

- High scale

  ** Indicates unique 8500 features*

  - 4K vlans*
  - 6000 local mode APs and 64,000 clients in 1RU*
- Rich Features with deployment flexibility
  - High Availability with Sub-second Stateful Switchover of Aps to standby in case of primary WLC outage.
  - Outdoor AP support
  - FlexConnect, Local mode and mesh support for 6000APs and 64,000 clients*
  - Right to use (with EULA) for ease of license enablement*
  - 3G Packet core integration: PMIPv6 MAG solution with ASR5K (LMA)
  - FlexConnect with HS2.0 for 3G offload
  - Other key features:

  802.11r fast roaming,

  Rate limit traffic flows,

  Video Stream for rich media flows

Flex 7500 Scale & Feature Update - 7.0.116.0 vs. 7.4

Scalability	7.0.116.0	7.4
Total APs	2000	6000
Total Clients	20,000	64,000
Total FlexConnect Group	500	2000
Support for OEAPs	No	Yes
Central Switching BW Limit	~250 Mb	~1 Gb
Data DTLS Support	No	Yes
Central Switching 802.1x	No	Yes

History of Flexconnect

- The REAP feature is supported up to WLC Release 3.2.215. From WLC Release 4.0.155.5, this functionality is called Hybrid REAP (H-REAP) with few enhancements until 7.0.x.x. From 7.2.103 release, this feature is called FlexConnect.

- REAP restriction ?
- H-REAP restriction?

FlexConnect Improvements in 7.2 – 7.5

7.2

- Smart AP Image Upgrade
- ACL's on FlexConnect AP
- AAA Over-ride of VLAN - dynamic VLAN assignment for locally switched clients
- FlexConnect Re-branding
- Fast Roaming for Voice Clients
- Peer to Peer Blocking

7.3 & 7.4

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

7.5

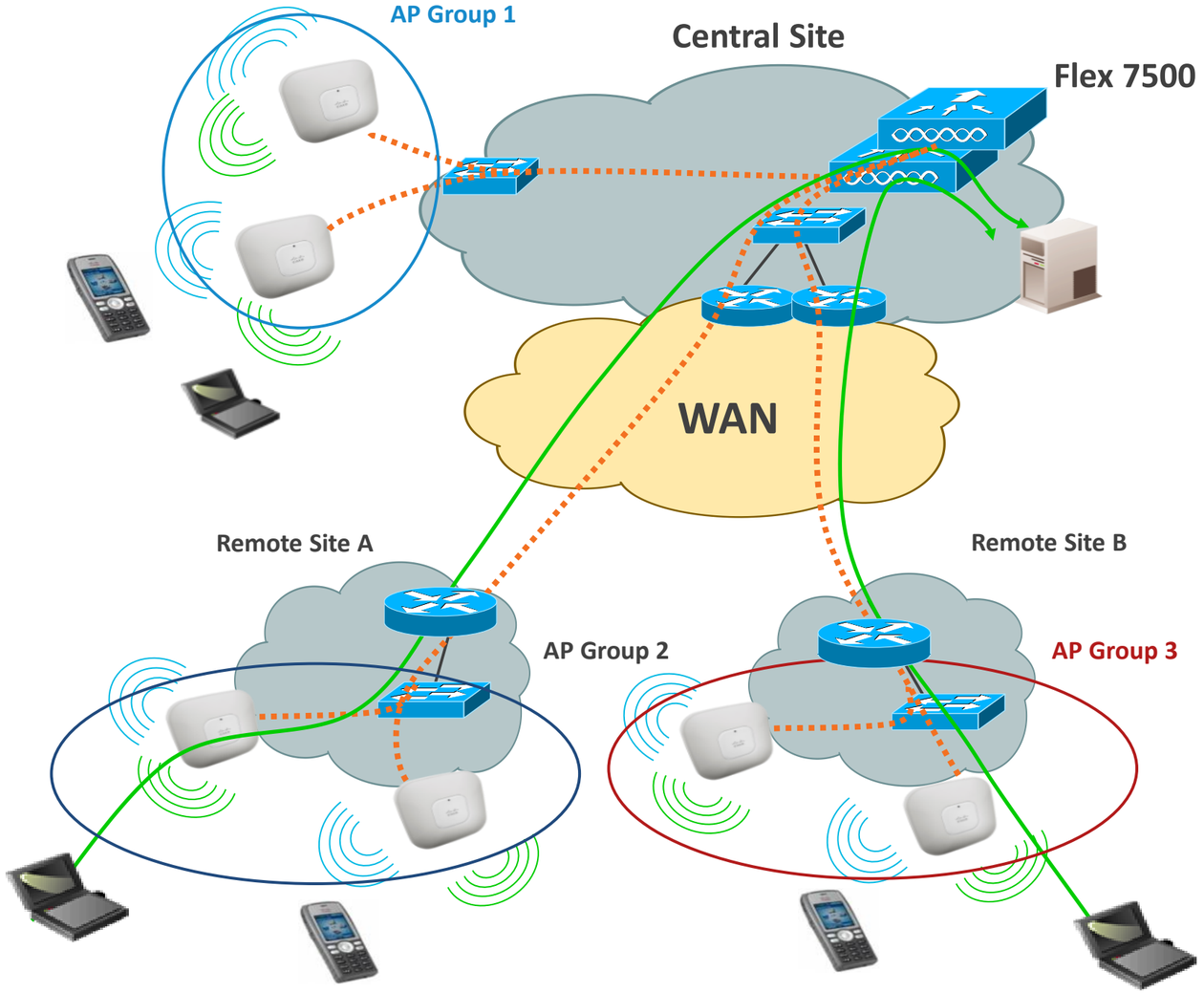
- PEAP and EAP-TLS Support
- FlexConnect Group specific WLAN-VLAN mapping
- AAA Client ACL

Why do we need FlexConnect & AP Groups?

Understanding AP Groups

Overview

- AP Groups is a logical concept of grouping AP's which deliver similar Wi-Fi services; these services can be:
  - By physical location, and/or
  - By functional services (data, voice, guest, …)
- Same AP groups need to be defined in all WLC's of a mobility



Scaling	Flex 7500	CT-5508	WiSM-2	CT-2504	vWLC
# AP Groups	6000	500	1000	30	200
# WLAN (SSID)	512	512	512	16	512
# VLAN (Interfaces)	4095	512	512	16	512

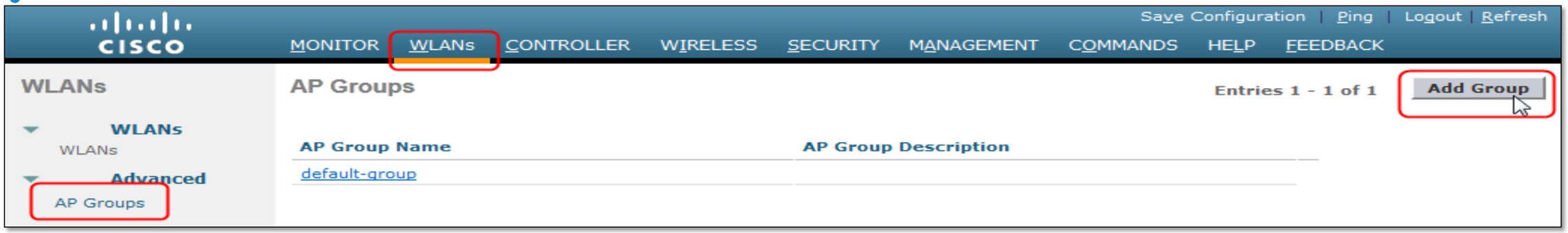
Understanding AP Groups

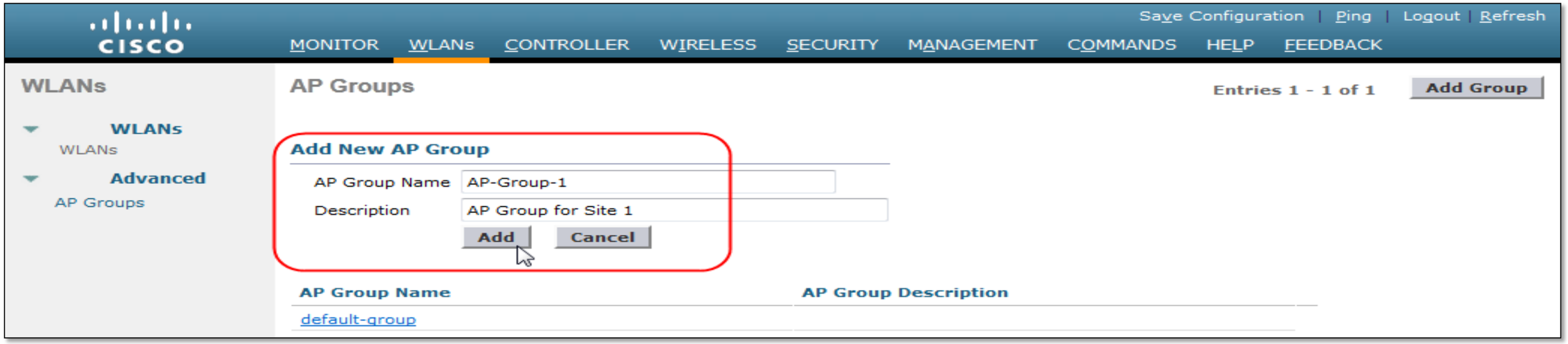
Rules to Know

- **Rules to know**
  - One AP can be in only one AP Group
  - One WLAN(SSID) can be in several AP Groups
  - WLAN with ID 1-16 can not be removed from the ‘default-group’
  - WLAN with ID greater than 16 will never be part of the ‘default-group’
  - All AP with no AP Group name or an unknown AP Group name will be part of the ‘default-group’
- **Well known mistakes**
  - Create no AP group, but create a WLAN with ID 17+.
  - Having AP groups defined, Create WLAN with ID 17+ but never map the WLAN to any AP Group.

AP Groups

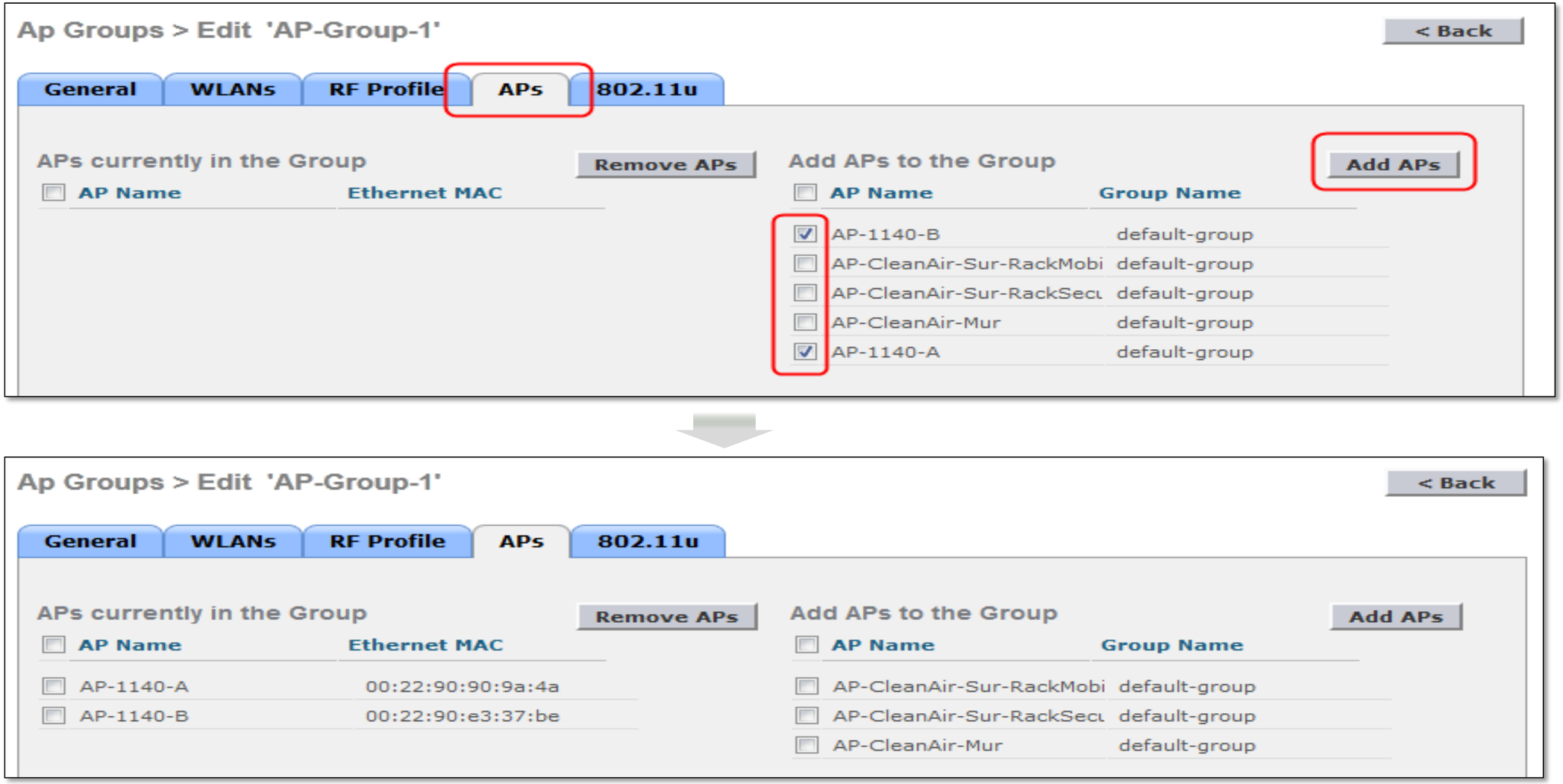
Configuration: Create a New Group





AP Groups

Configuration: Add AP or APs to Group



AP Groups Usage

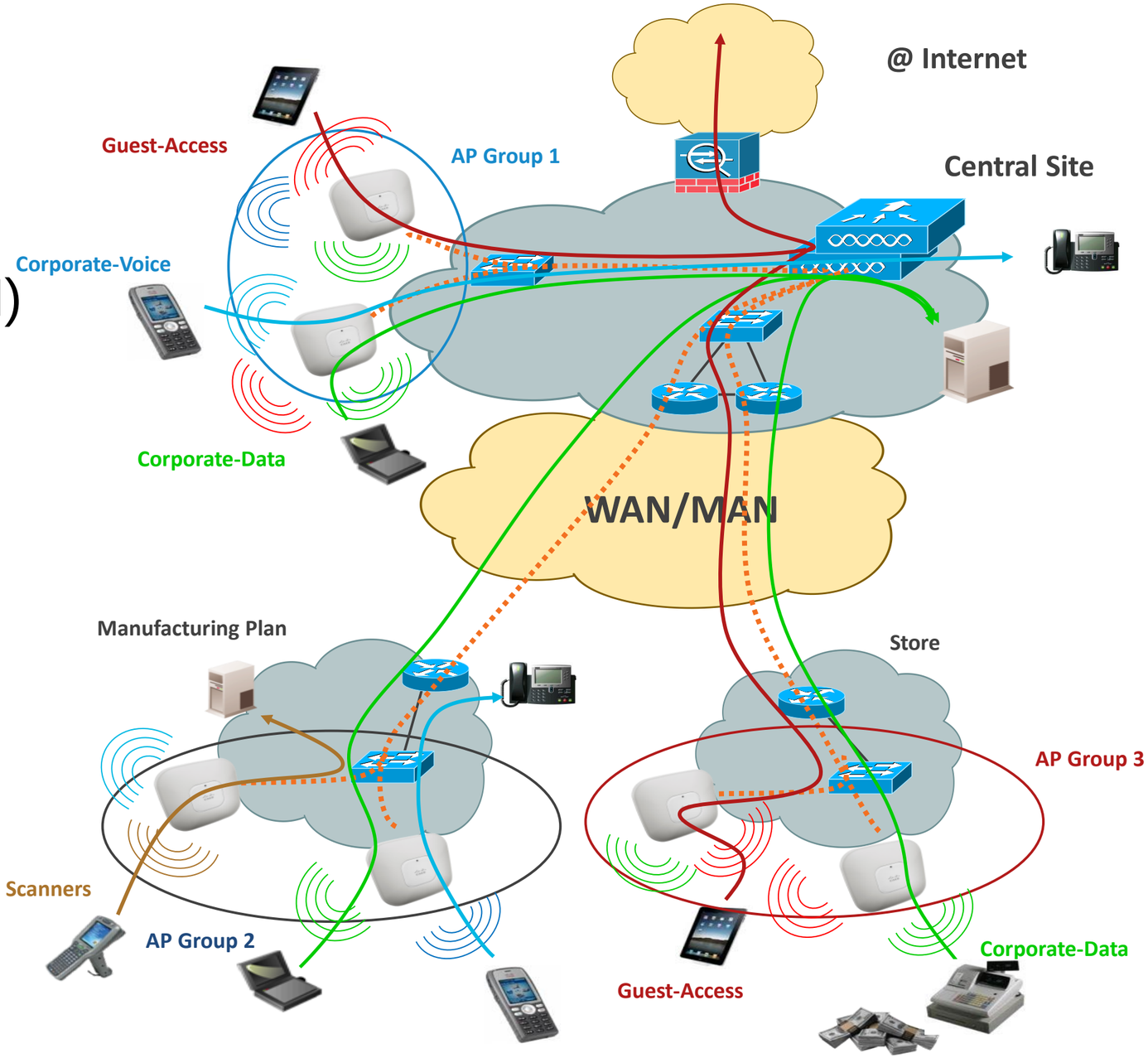
Per Location SSID

- AP groups give the ability to enable Wi-Fi Services (WLAN) based on physical location
- Example
  - **Central Site**

    Corporate-Voice, Corporate-Data, Guest-Access
  - **Manufacturing Plan**

    Corporate-Voice, Corporate-Data, Scanners
  - **Store**

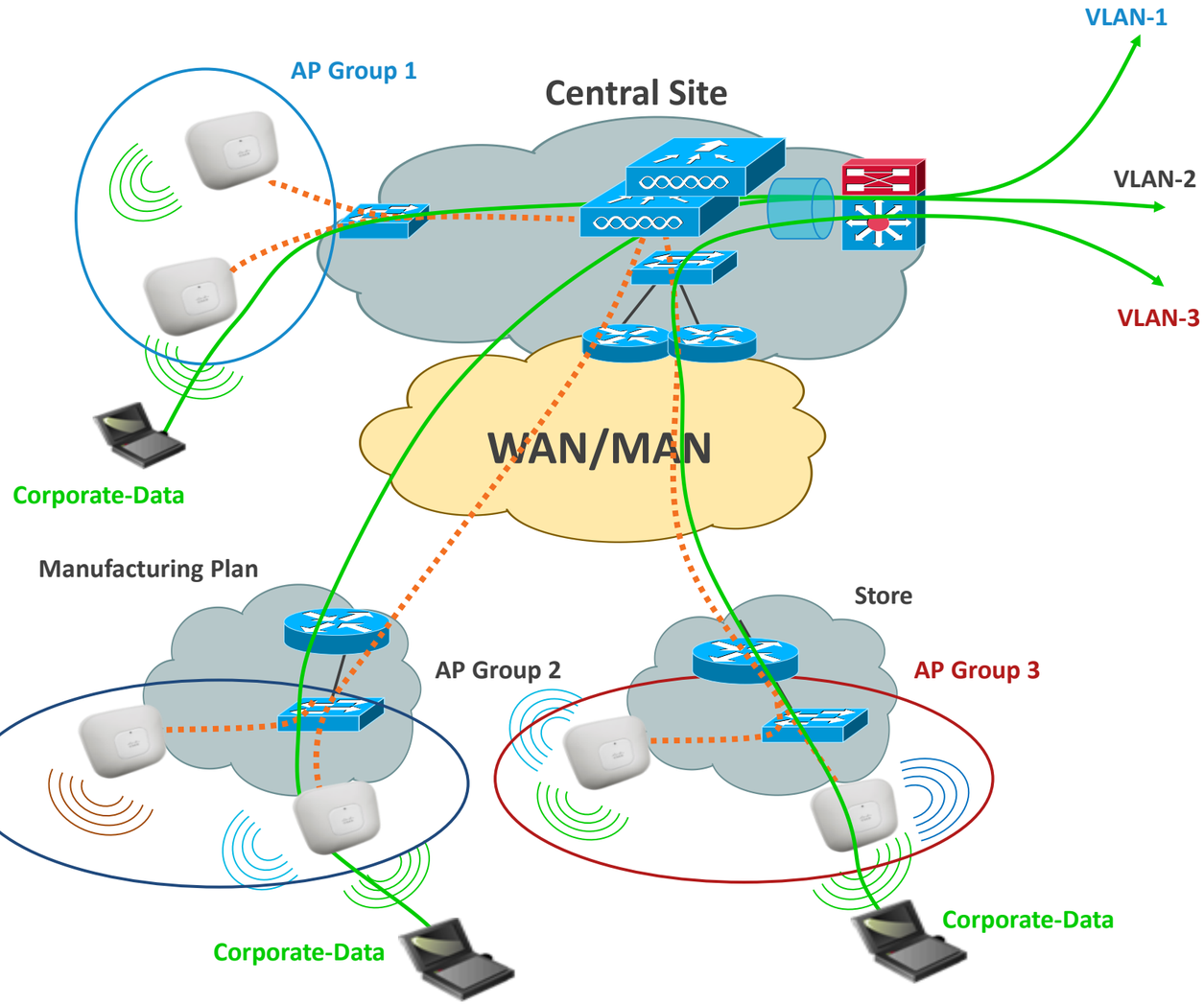
    Corporate-Data, Guest-Access



AP Groups Usage

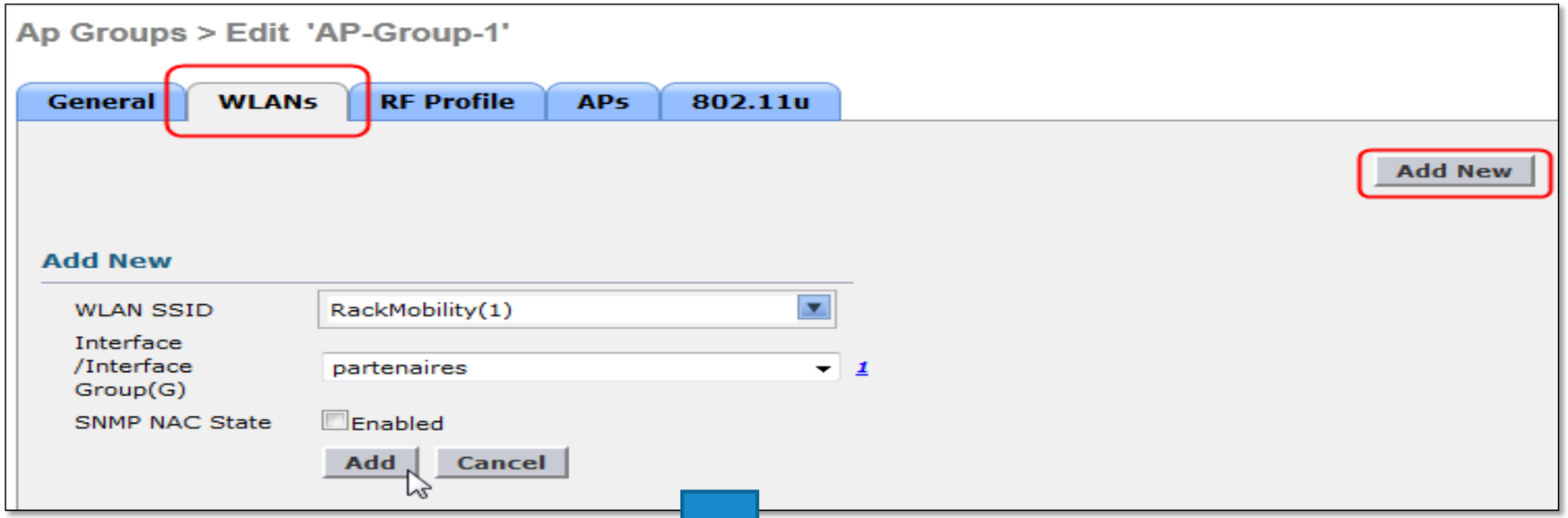
Per AP Group SSID to VLAN Mapping

- AP groups give the ability to statically map Wi-Fi service (WLAN) to VLAN based on physical location
- Users see the same Wi-Fi service on all sites but IP@ can be used for monitoring or filtering
- Can also be used to have smaller Wi-Fi subnets
  - For example per floor subnets in a building.



AP Groups

Configuration/VLAN Mapping

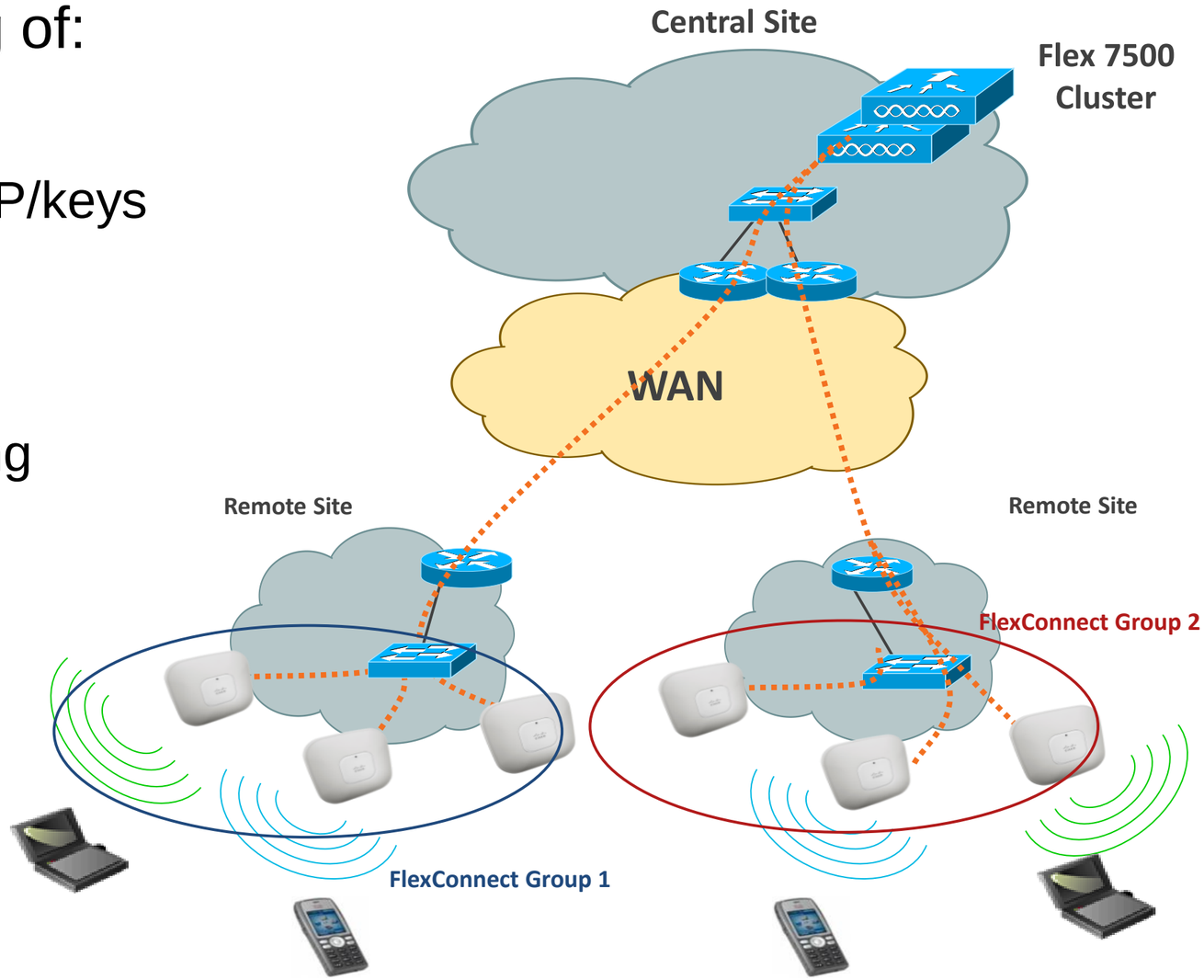


Understanding FlexConnect Groups

Overview

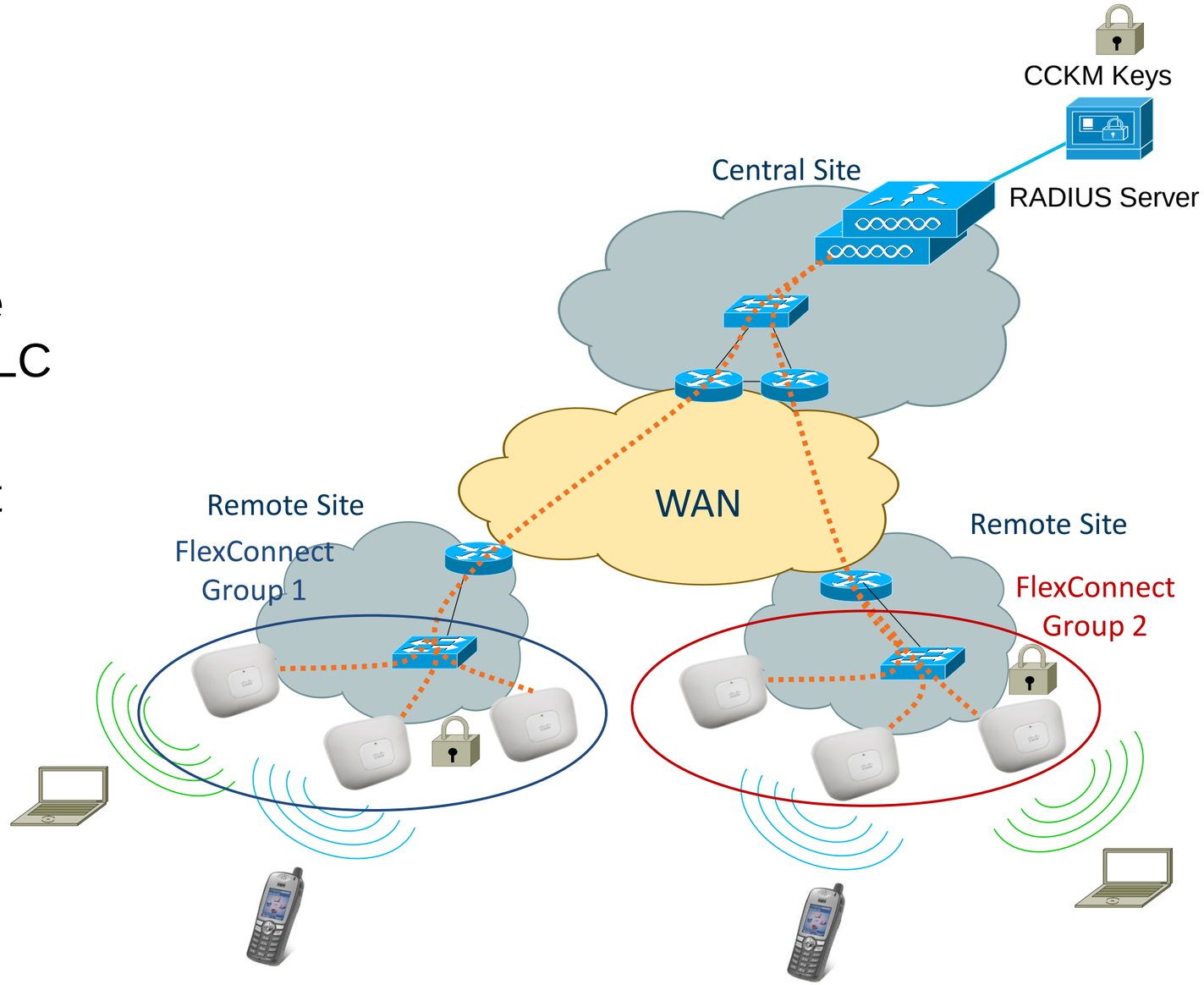
- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade
- Scaling information

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504	vWLC
FlexConnect Groups	2000	100	100	30	200
AP per Group	100	25	25	25	100



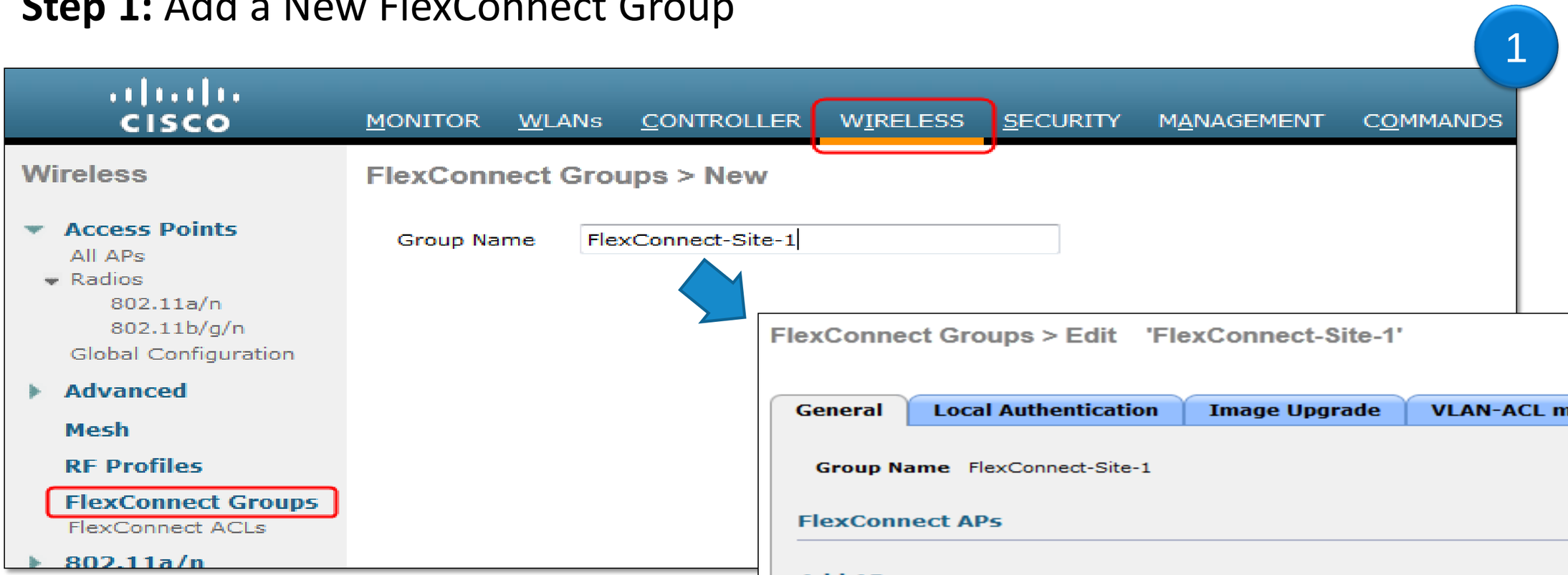
FlexConnect Groups and CCKM/OKC Keys

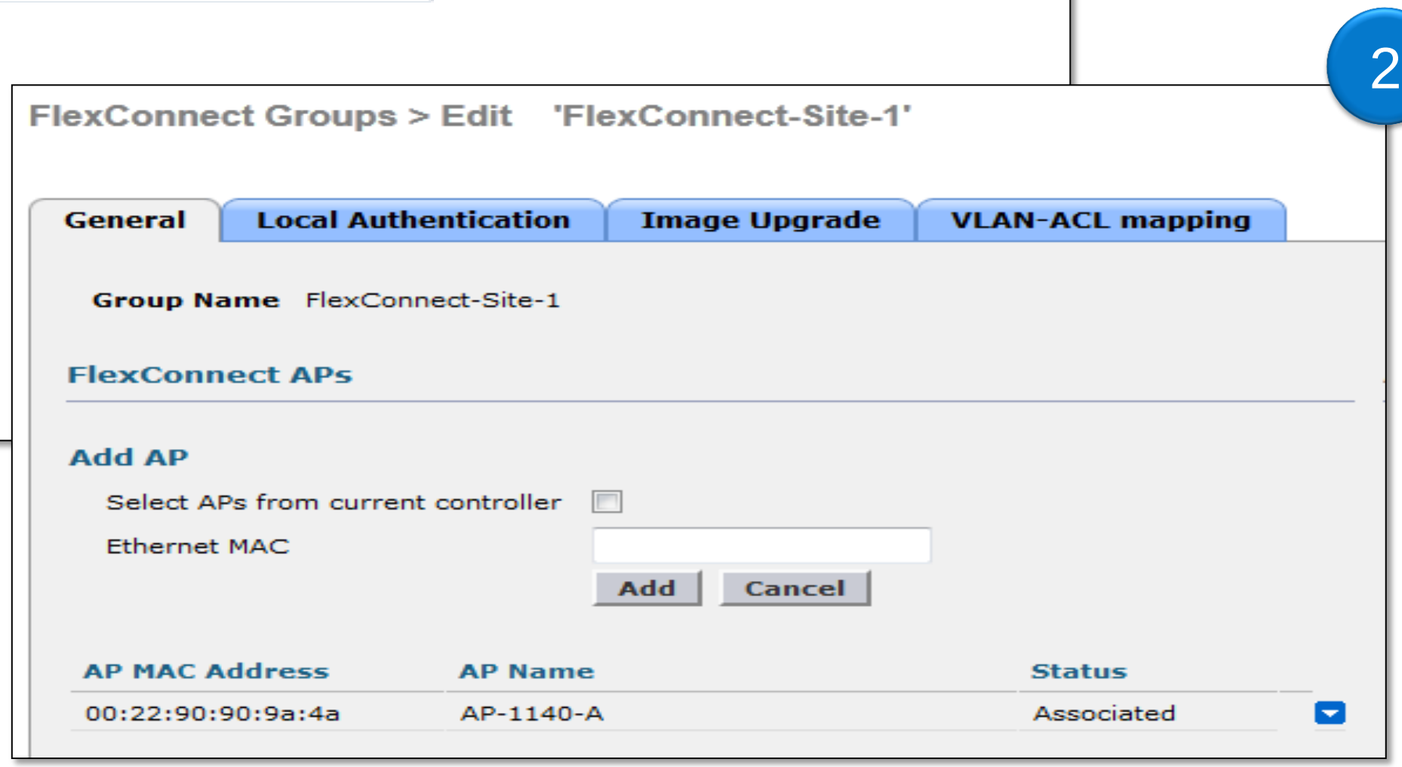
- CCKM/OKC keys are stored on FlexConnect APs for Layer 2 fast roaming
- The FlexConnect APs will receive the CCKM/OKC keys from the WLC
- If a FlexConnect AP boots up in standalone mode, it will not get the OKC/CCKM keys from the WLC and fast roaming will not be supported
- 802.11r Fast Transition is on FlexConnect APs in central and locally switched WLANs



FlexConnect Groups Creation

Step 1: Add a New FlexConnect Group





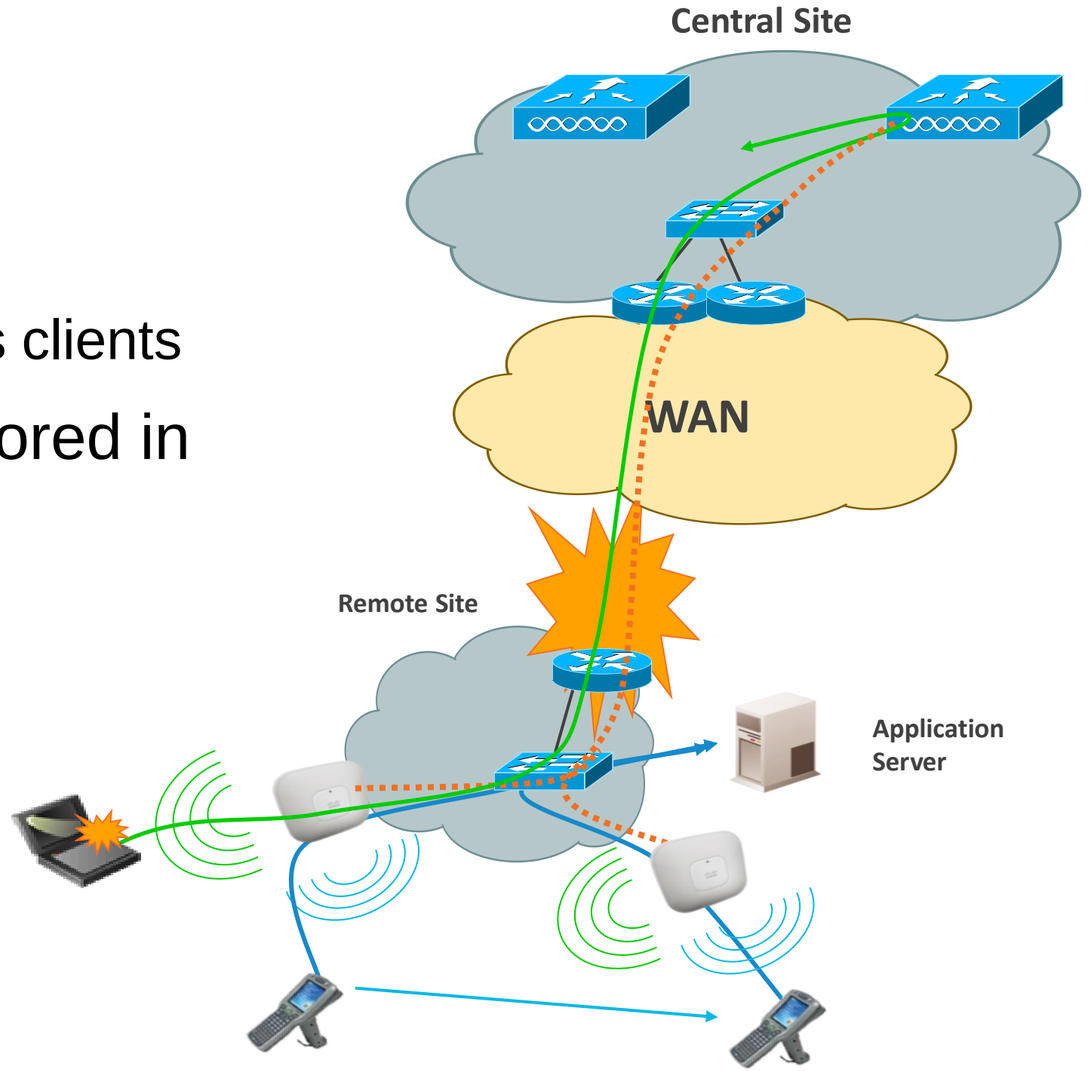
Step 2: Add APs to the FlexConnect Group

Design Wireless Branch
Designing a Resilient Network

FlexConnect Backup Scenario

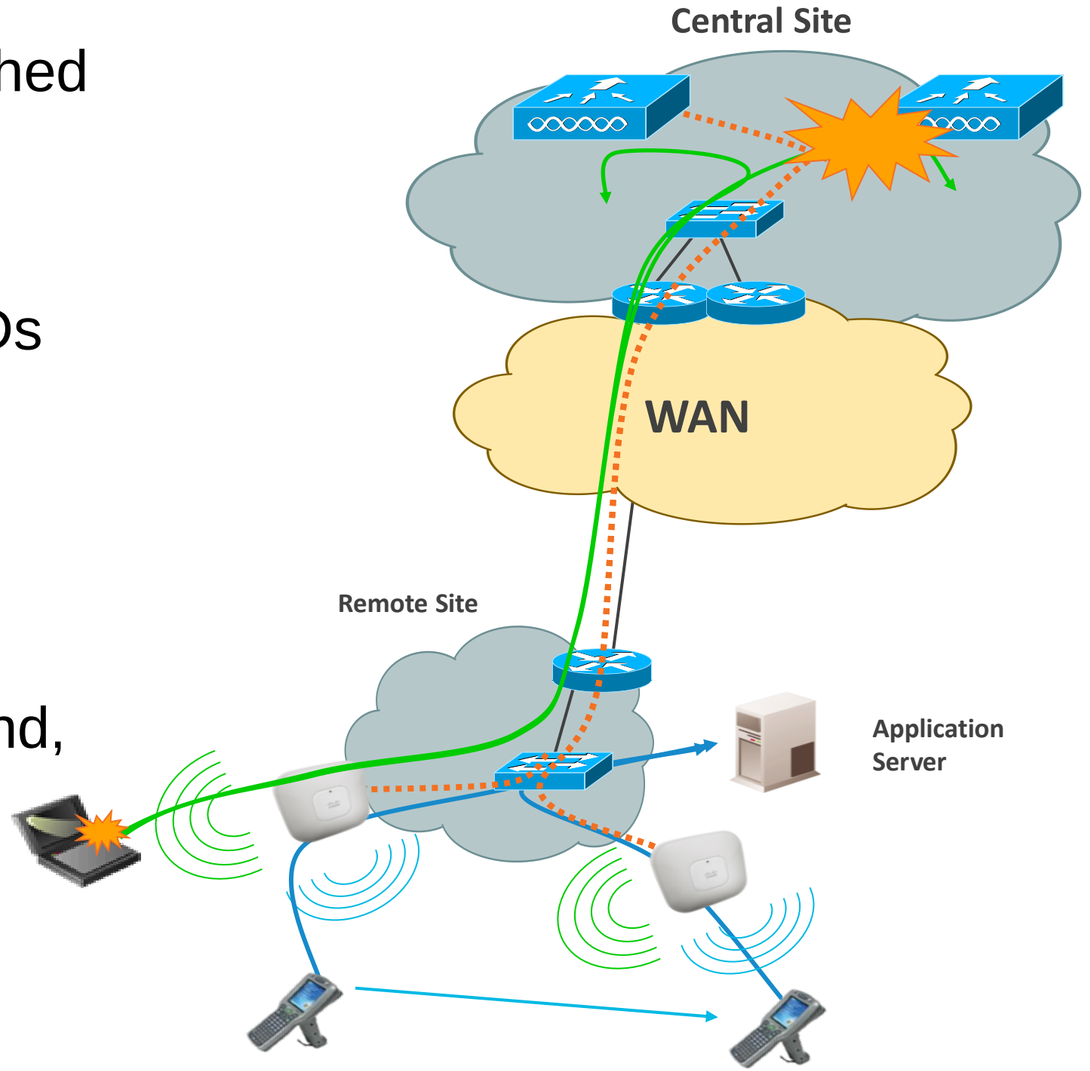
WAN Failure

- FlexConnect will backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- Static authentication keys are locally stored in FlexConnect AP
- Lost features
  - RRM, WIDS, location, other AP modes
  - Web authentication, NAC



FlexConnect Backup Scenario - *WLC Failure*

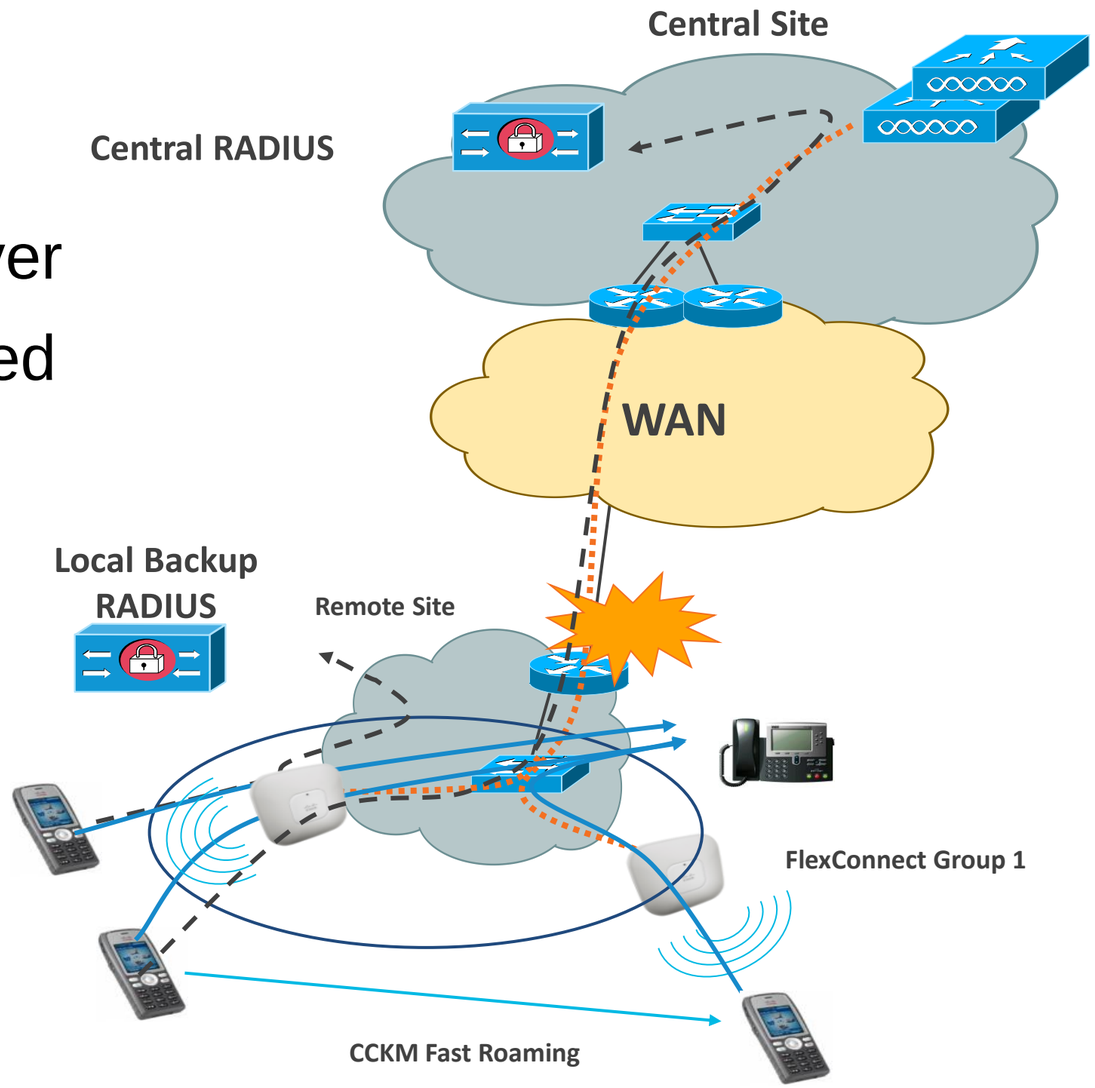
- FlexConnect will first backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with WLC and resume client sessions with central traffic.
- Client sessions with Local Traffic are not impacted during resync with Backup WLC.



FlexConnect Group: Local Backup RADIUS

Backup Scenario

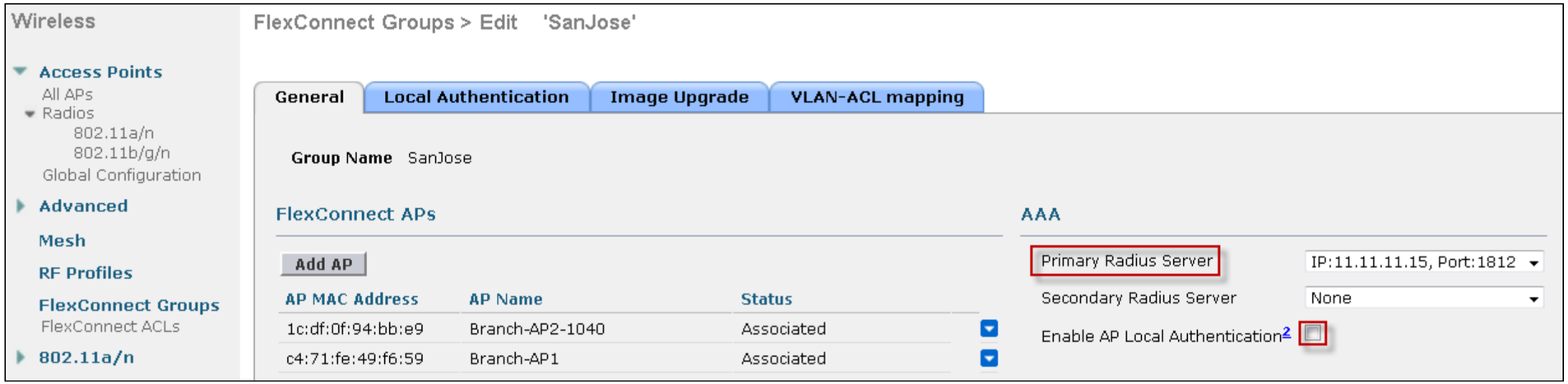
- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with locally defined RADIUS server
- Existing connected clients stay connected
- Clients can roam with
  - CCKM fast roaming, or
  - Reauthentication



FlexConnect Group: Local Backup RADIUS

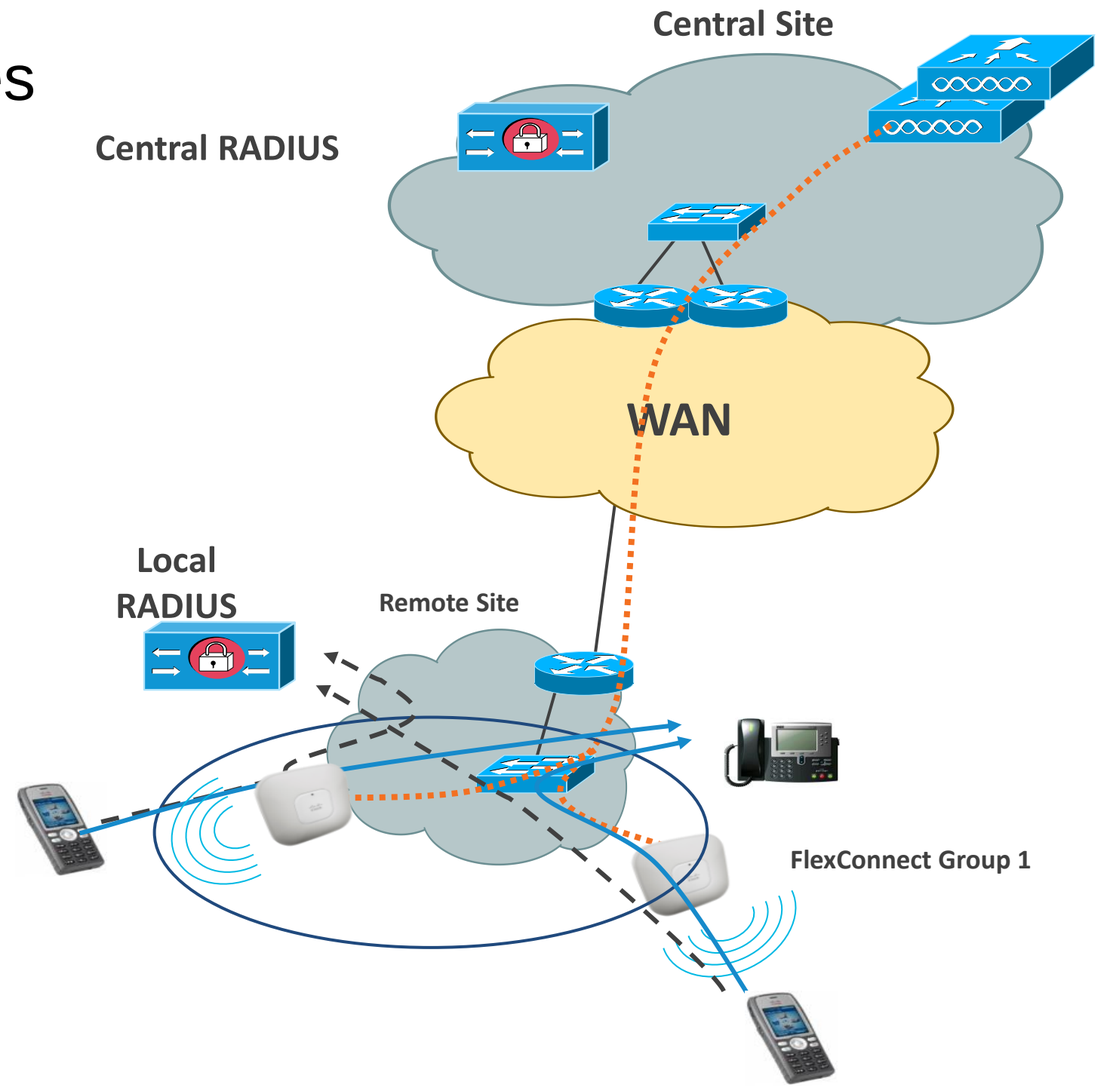
Configuration

- Define primary and secondary local backup RADIUS server per FlexConnect group



Local Authentication

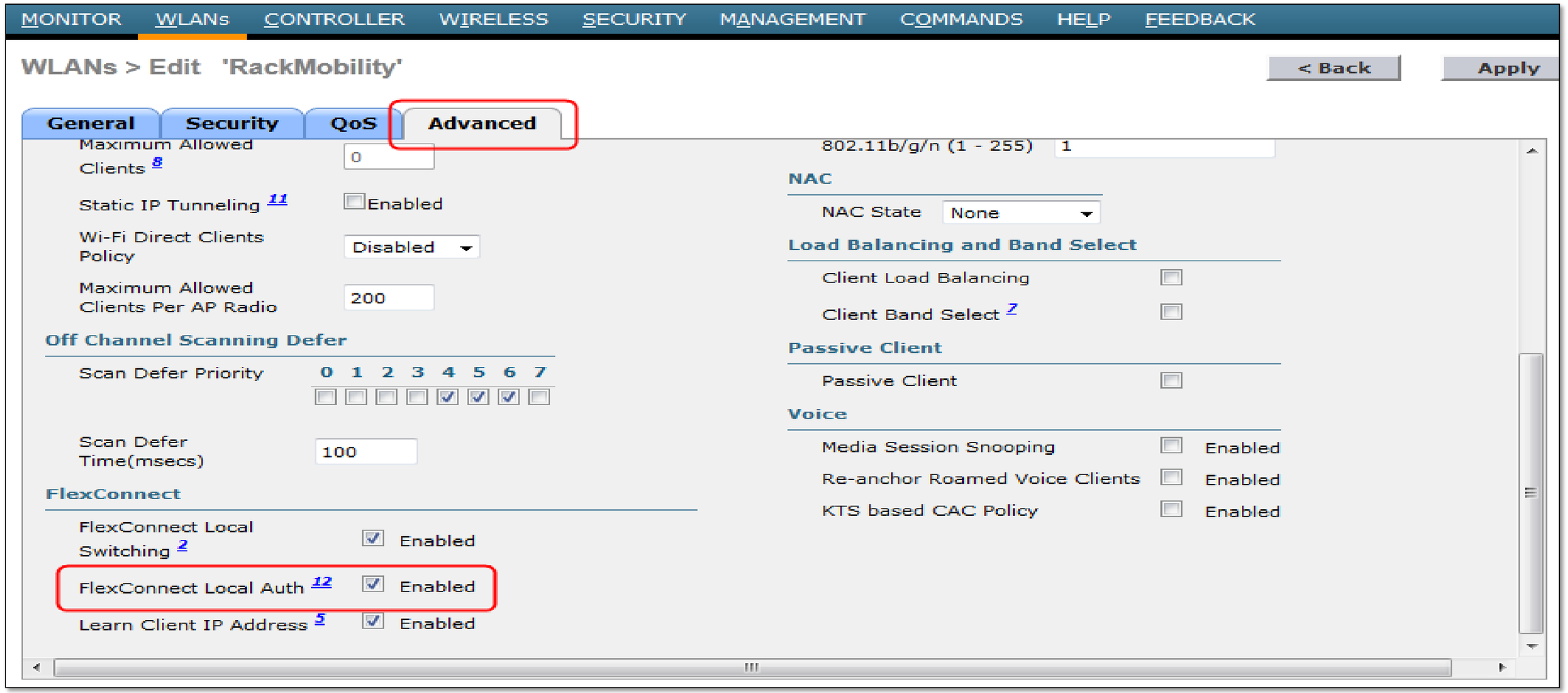
- By default FlexConnect AP authenticates clients through central controller
- Local Authentication allow use of local RADIUS server directly from the FlexConnect AP



New in 7.0.116

Local Authentication

Configuration



FlexConnect Group: Local Backup Authentication

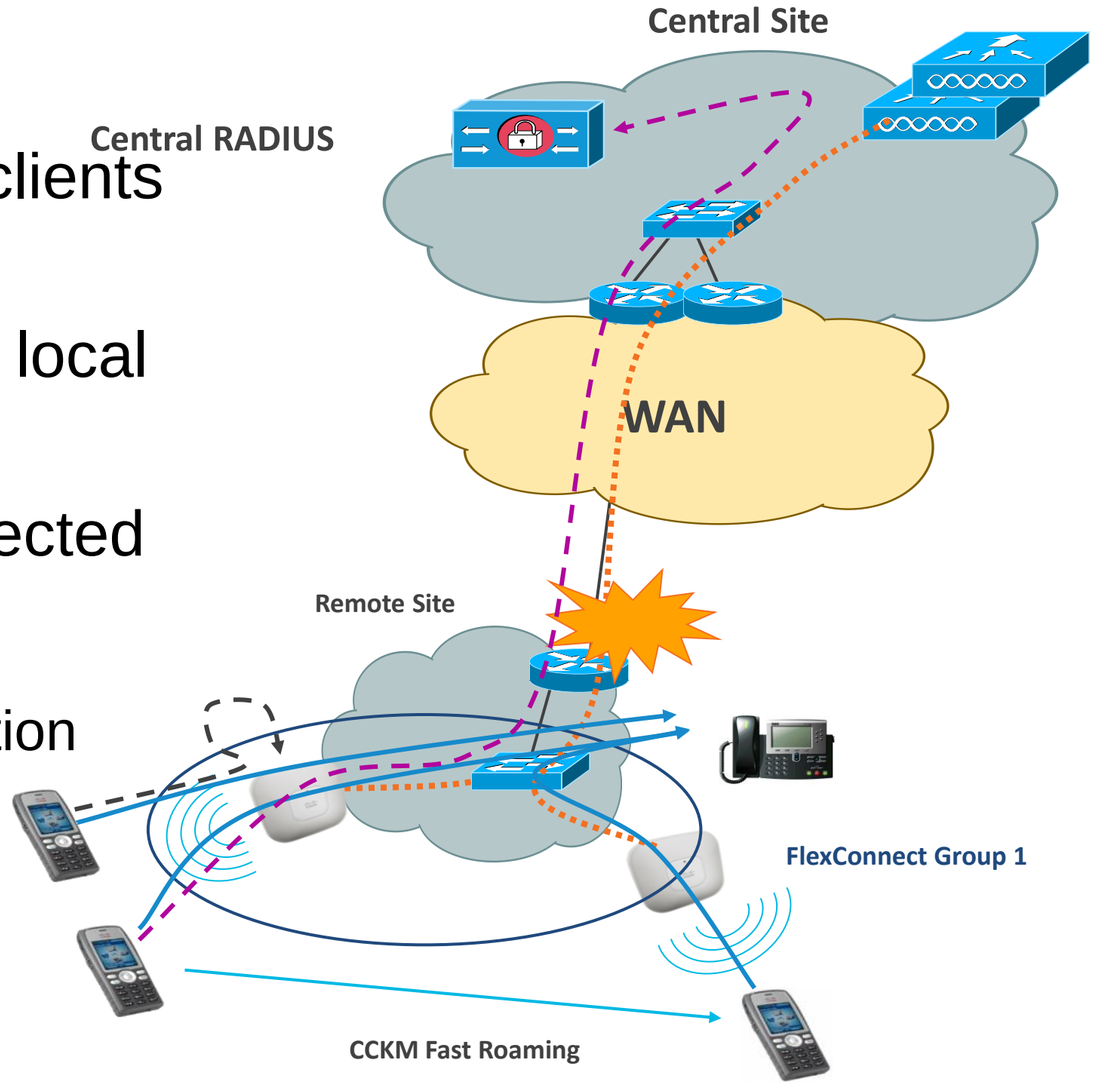
Backup Scenario

- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with its local database
- Each FlexConnect AP has a copy of the local user DB
- Existing authenticated clients stay connected
- Clients can roam with:

  CCKM fast roaming, or Local re-authentication

Supported Security Types	Release Version
LEAP	6.0
EAP-FAST	6.0
PEAP	7.5
EAP-TLS	7.5

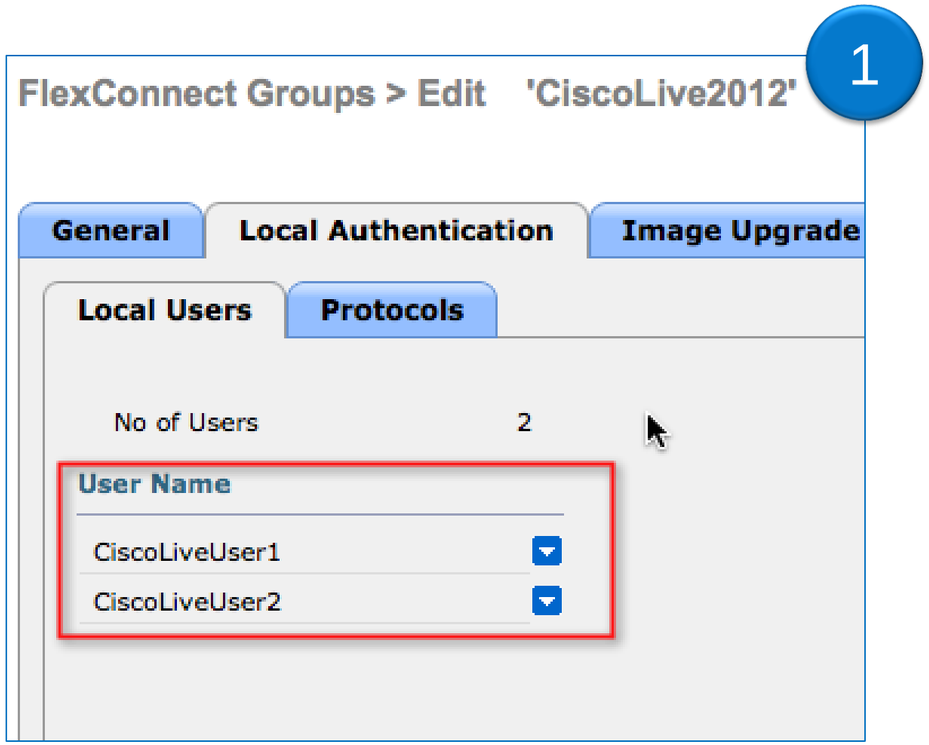
New

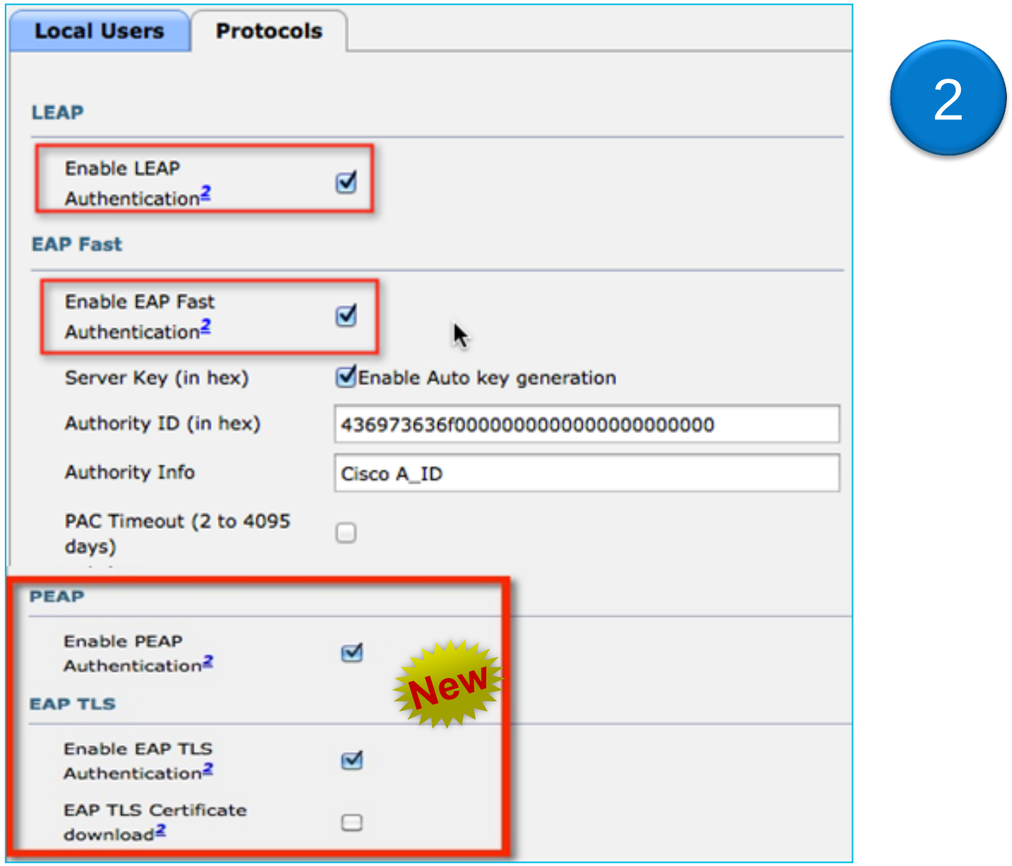


FlexConnect Group: Local Backup Authentication

Configuration

- Define users (max 100) and passwords
- Define EAP parameters (LEAP or EAP-FAST)





FlexConnect Backup Scenario

WAN Down Behavior (Bootup Standalone Mode)

- Central Switched WLANs will shutdown
- Web-auth WLANs will shutdown
- Local Switched WLANs will be up :
  - Only Open, Shared and WPA-PSK are allowed.
  - Local 802.1x allowed with local authentication or local RADIUS
- Unsupported features
  - RRM, CCKM, WIDS, Location, Other AP Mode, NAC.

Designing Secure & BYOD Enabled Branch Network

Understanding FlexConnect Access Lists

Overview

FlexConnect ACL are ACL that are applied at the FlexConnect AP level

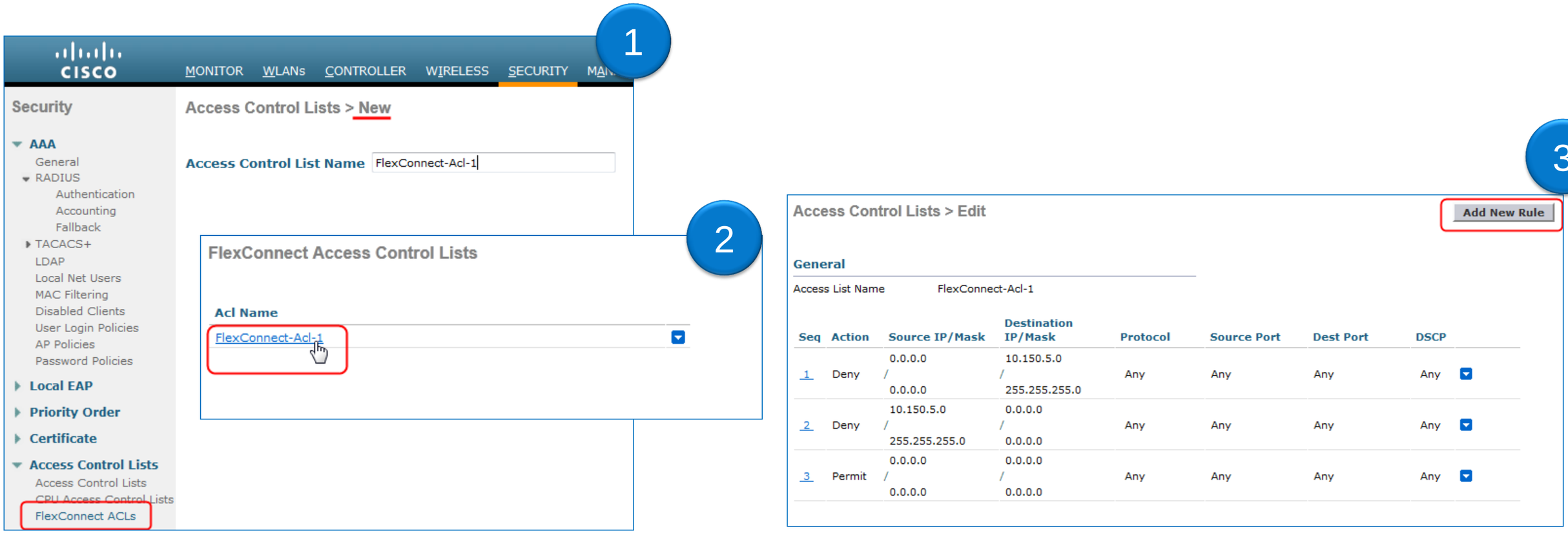
- 4 FlexConnect ACL usages :
  - ACL mapped to local VLAN per AP or FlexConnect Group
  - ACL used for NAT/PAT Split tunneling
  - ACL used for External WebAuthentication
  - ACL used for Web Policies (ISE policies)

- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 ACL

FlexConnect Access Lists

Configuration – Create FlexConnect ACL

- FlexConnect ACL are not the same as ACL for Local Mode AP
- FlexConnect ACL rule creation is similar to rule creation for Local Mode AP

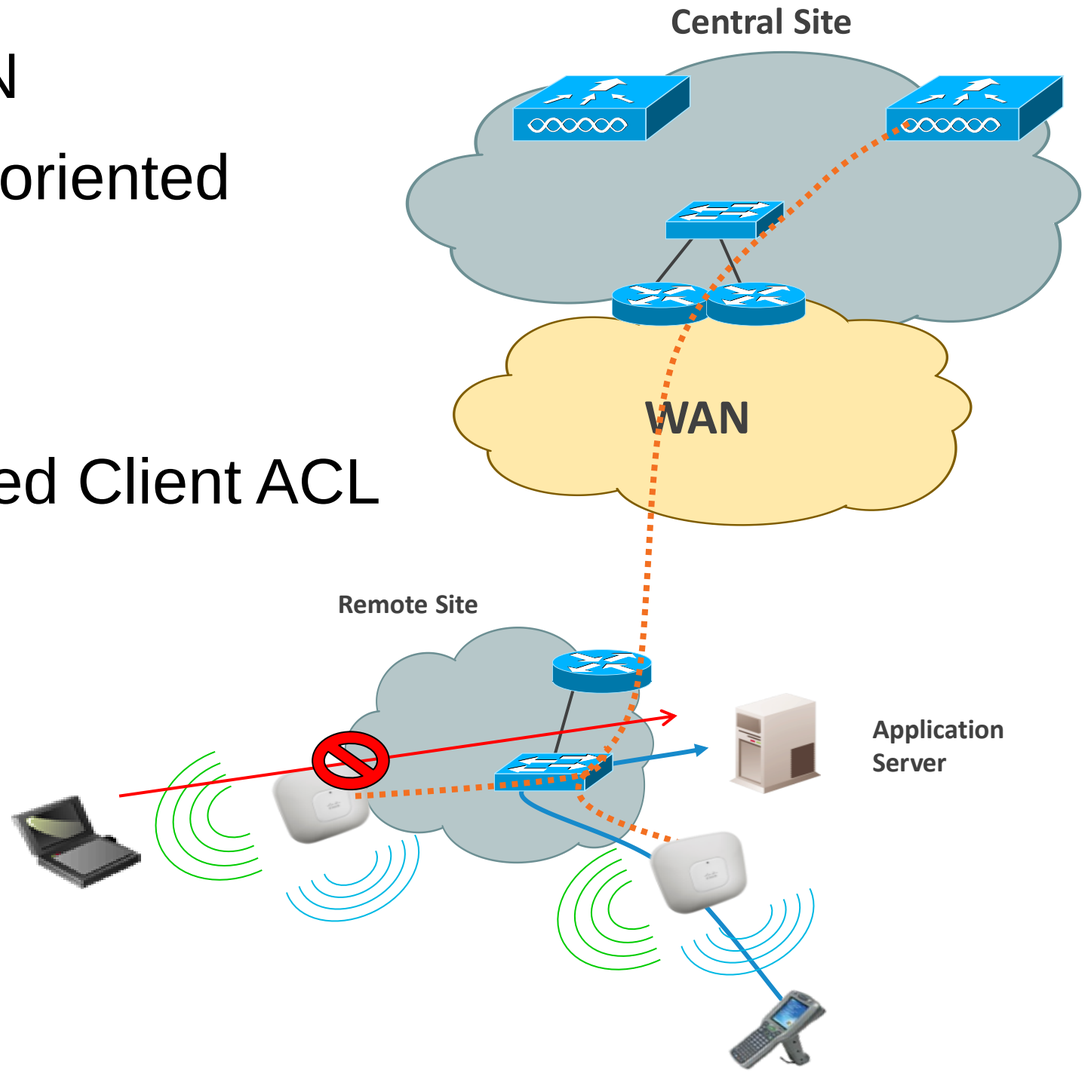


FlexConnect ACL – VLAN Mapping

Overview

- FlexConnect ACL are applied per VLAN
- FlexConnect ACL are Ingress / Egress oriented

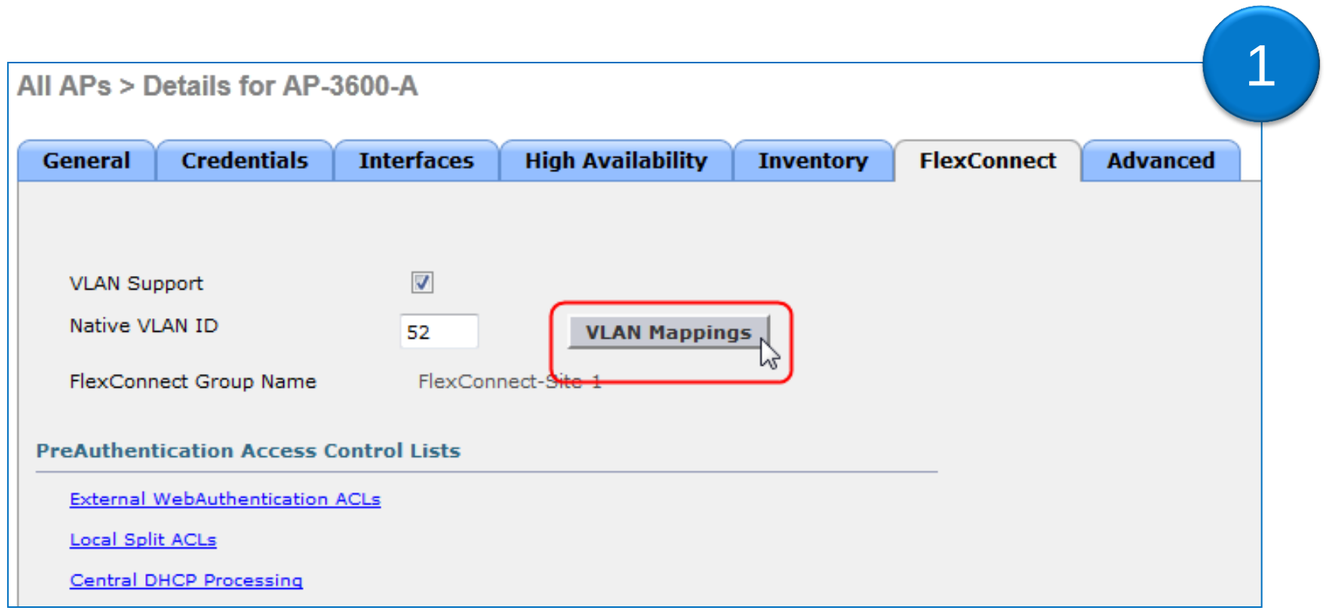
- Starting from 7.5 New
- FlexConnect ACL support AAA-returned Client ACL

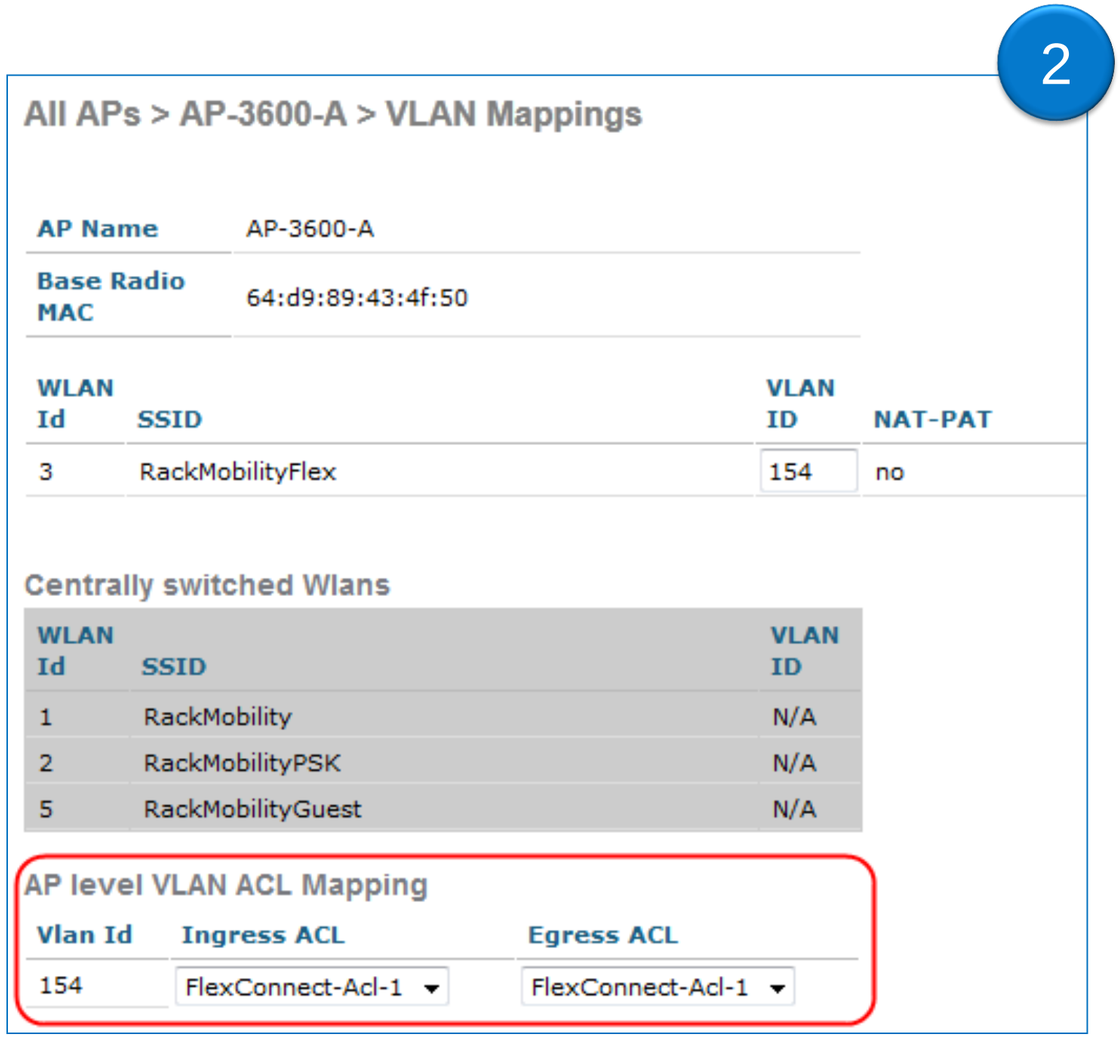


FlexConnect ACL – VLAN Mapping

Configuration – FlexConnect ACL per AP

- FlexConnect ACL can be applied per AP using VLAN Mappings configuration

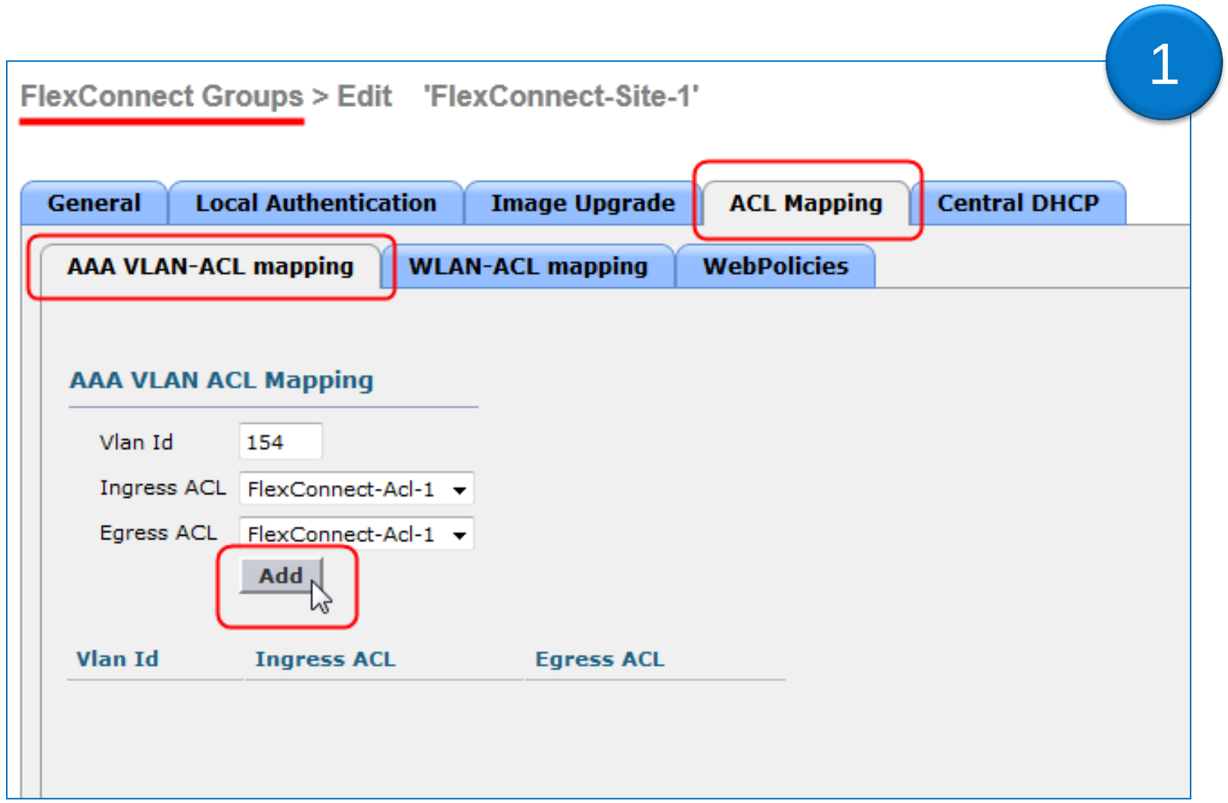


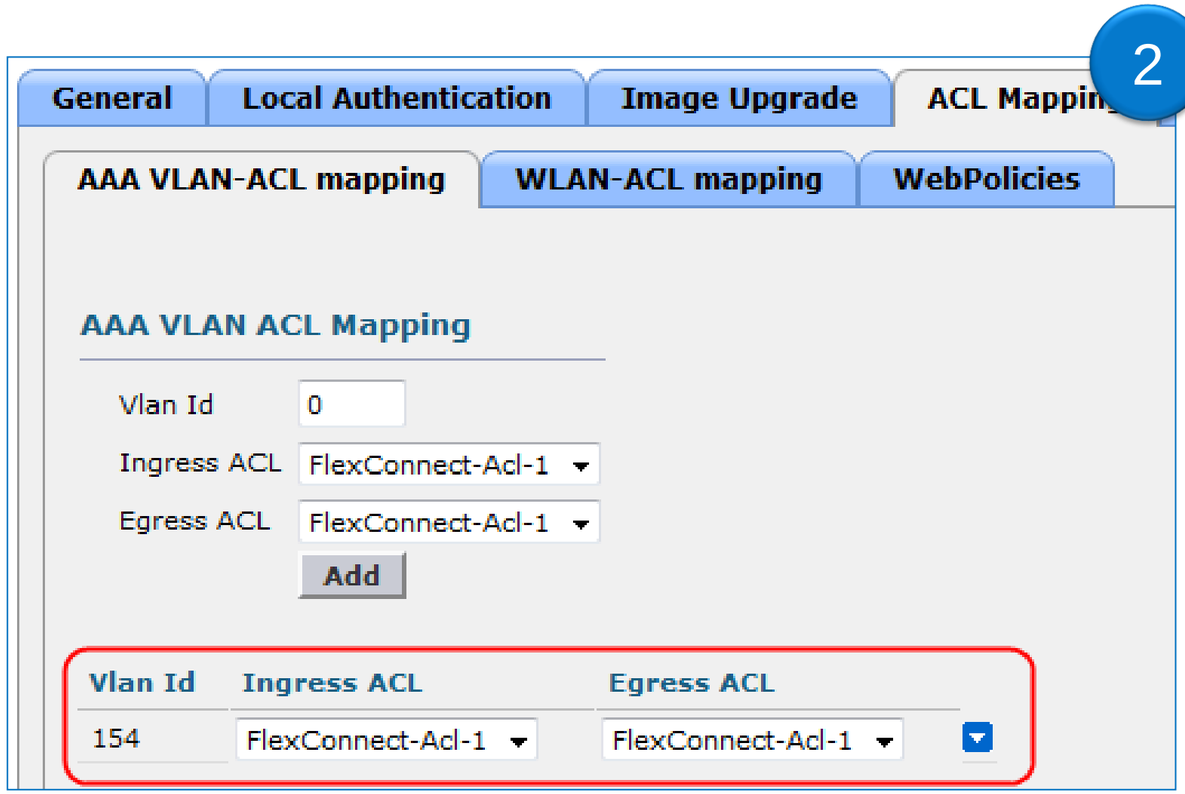


FlexConnect ACL – VLAN Mapping

Configuration –FlexConnect ACL per FlexConnect Group

- FlexConnect ACL can be applied per FlexConnect Groups per VLAN in the ACL Mapping tab.





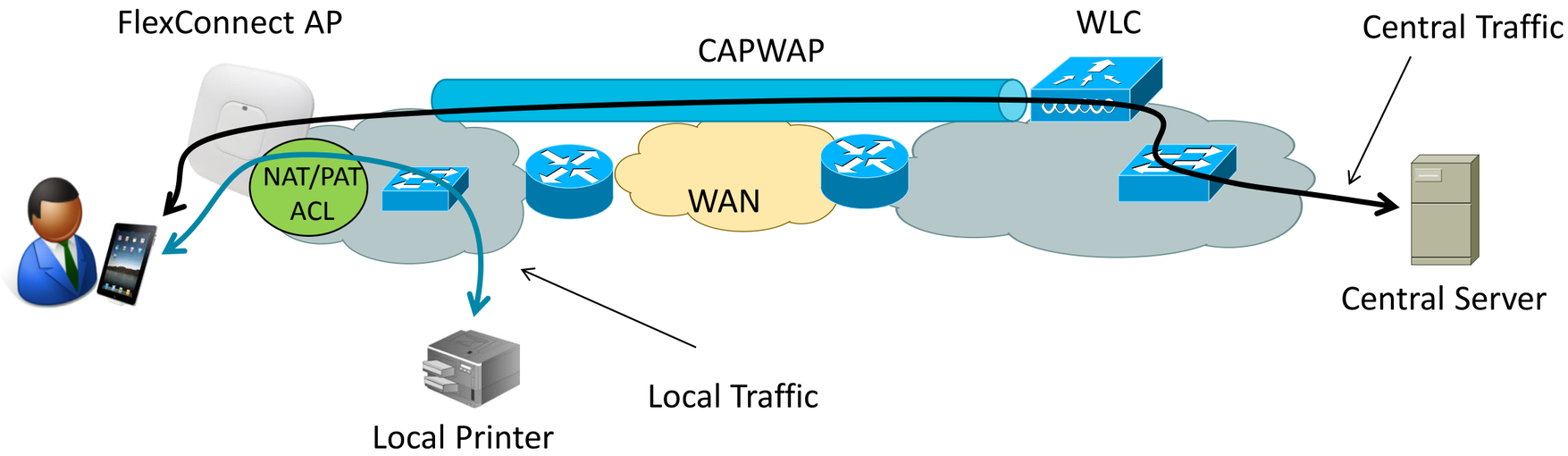
FlexConnect Split Tunneling

(Using FlexConnect Split ACL)

FlexConnect ACL – Split Tunneling

Overview

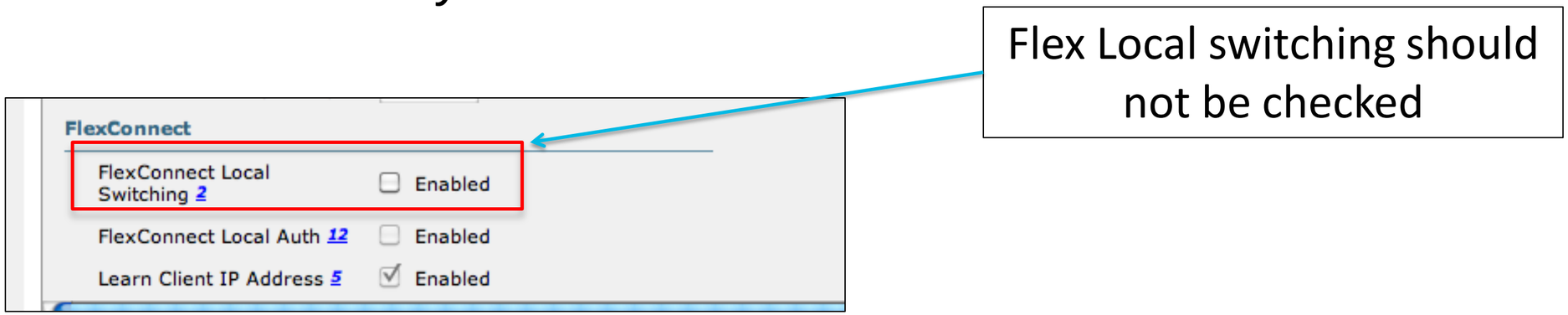
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP@ for the NAT/PAT feature



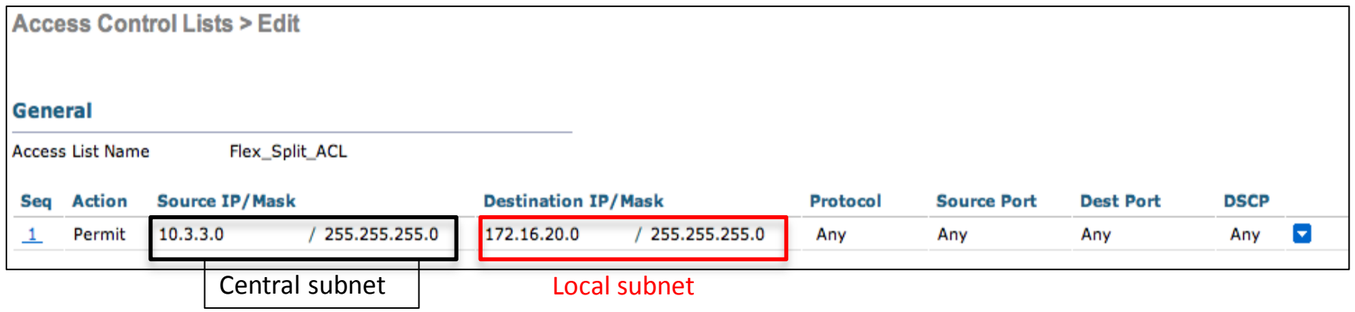
FlexConnect ACL – Split Tunneling

Configuration

- Create a centrally switched WLAN

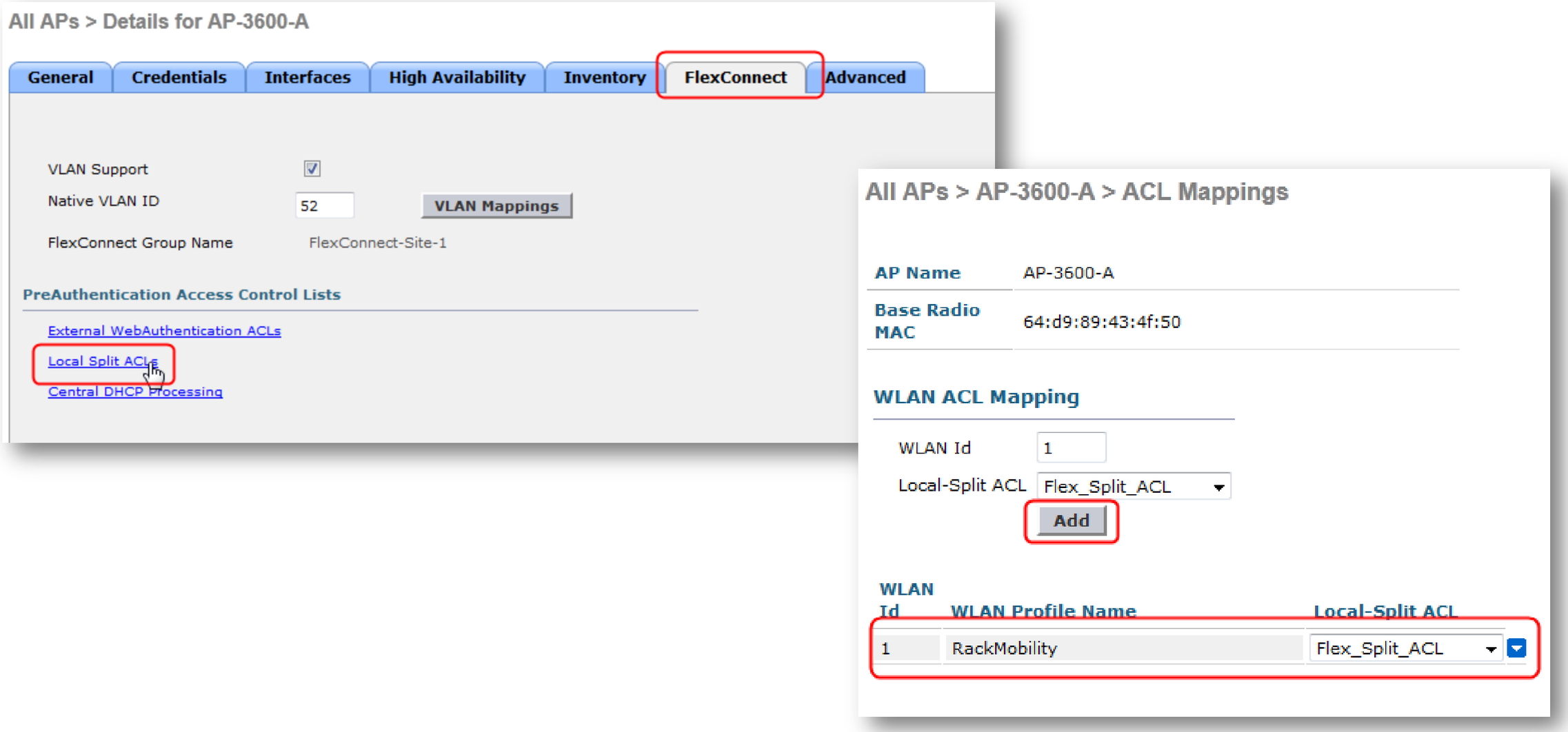


- Define Flex ACL to match traffic to be locally switched



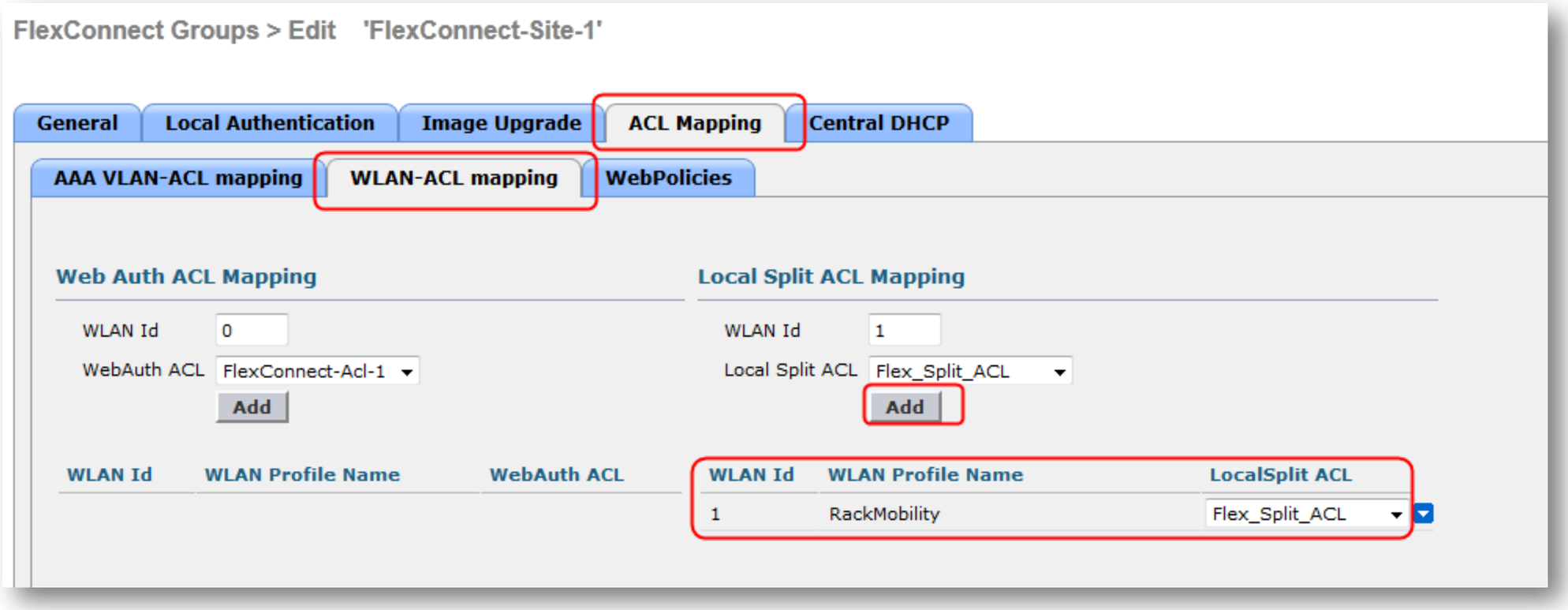
FlexConnect ACL – Split Tunneling

Configuration – Access Point



FlexConnect ACL – Split Tunneling

Configuration – FlexConnect Group



Deploying External WebAuth with FlexConnect and Local Switching

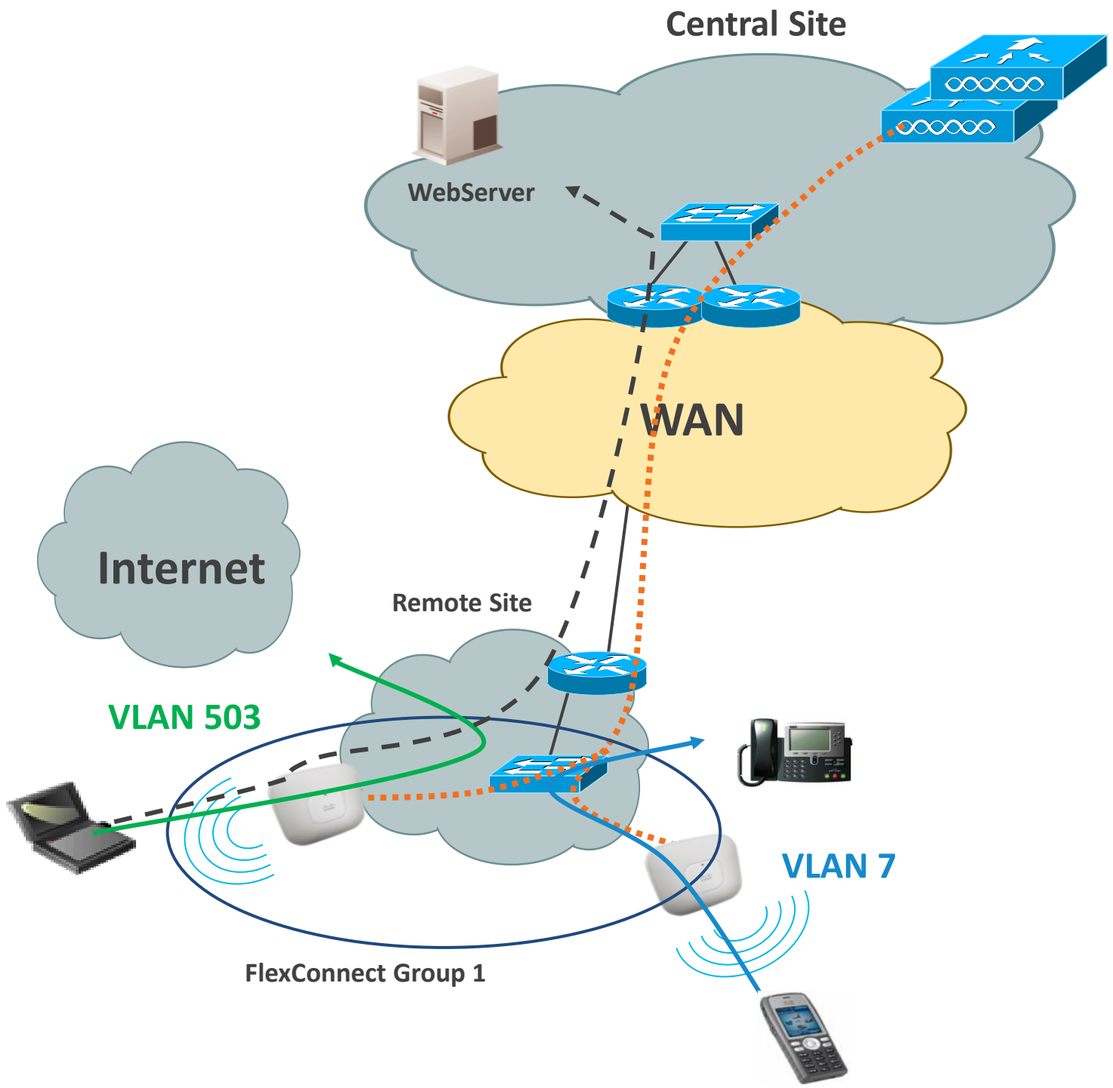
(Using FlexConnect WebAuth ACL)

External WebAuth with Local Switching

New in 7.2.110

Description

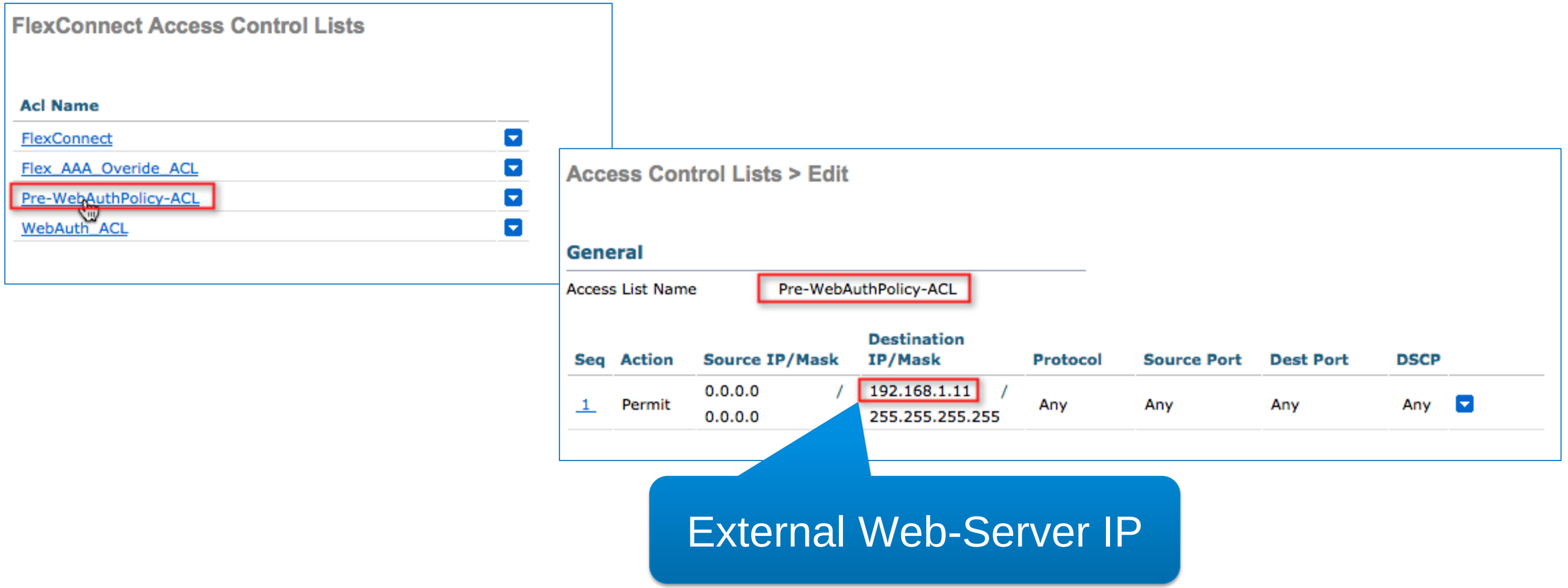
- Provides L3 Web Redirect from locally switched vlan
- Reduces WAN traffic by locally switching guest traffic
- Flexible and centralized web portal creation for multiple sites
- Provides flexible use of Conditional and Splash Page Web Redirect
- FlexConnect AP must be in Connected state with Centralized Controller to work



External WebAuth with Local Switching

Configuration

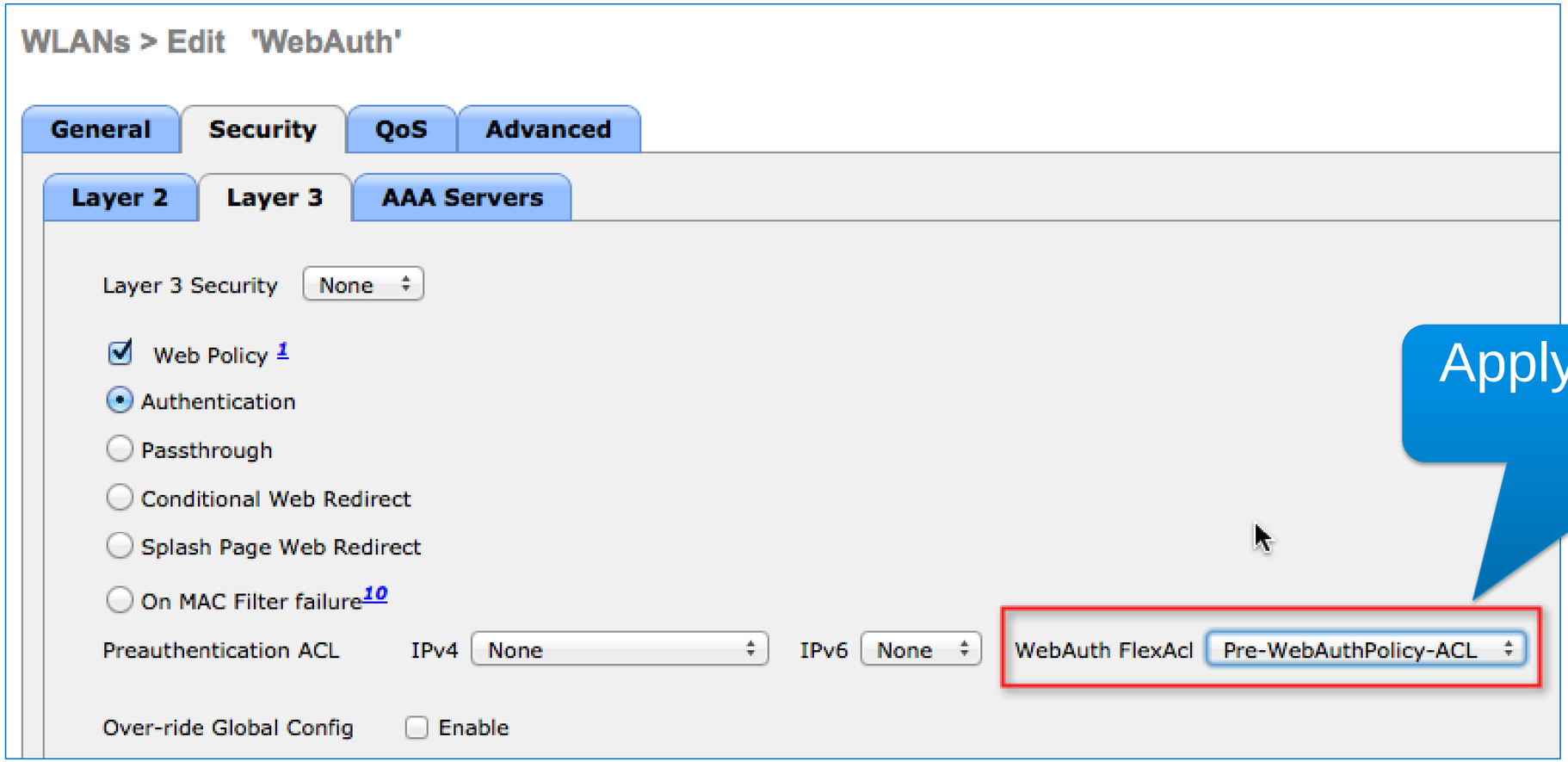
Step 1: Configure Pre-Auth ACL that will be applied to FlexConnect Group, AP or WLAN



External WebAuth with Local Switching

Configuration

Step 2: Apply Pre-Auth ACL to WLAN

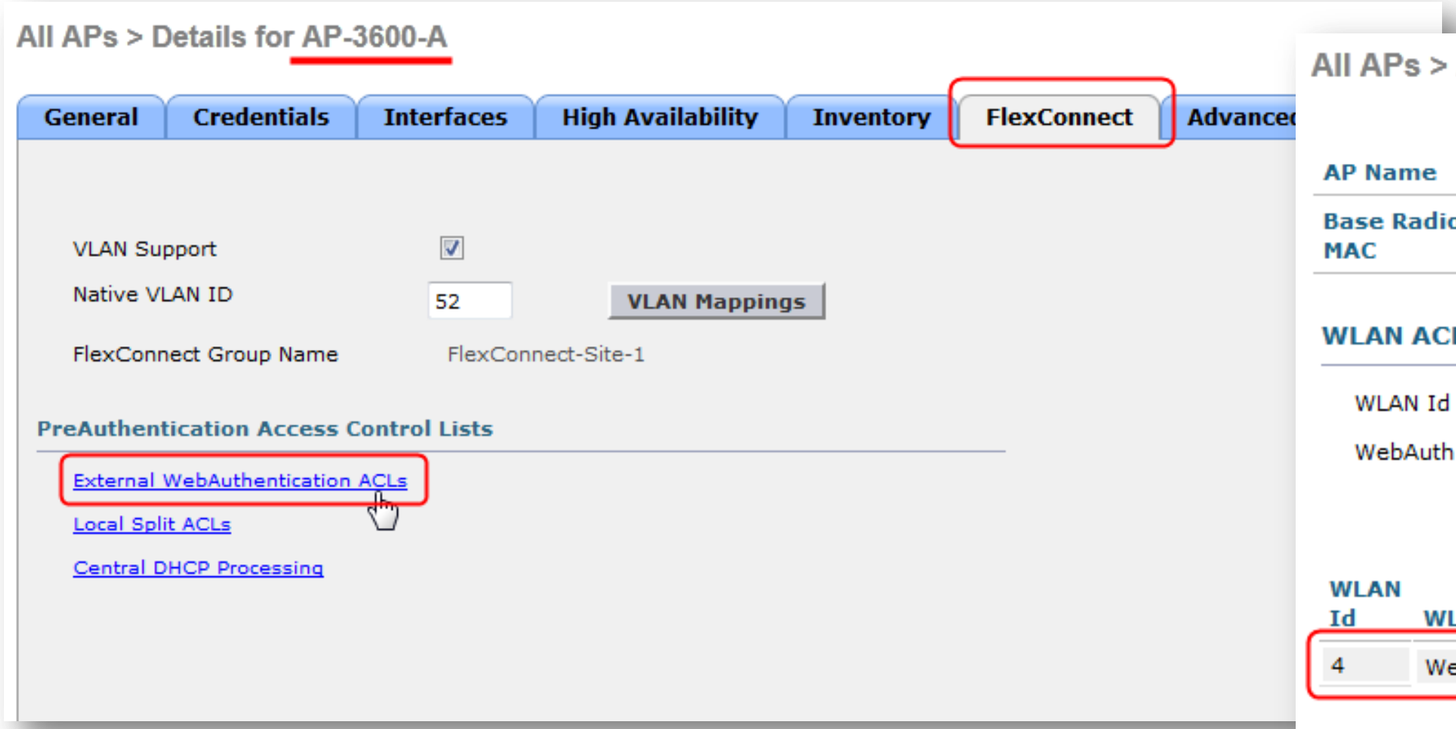


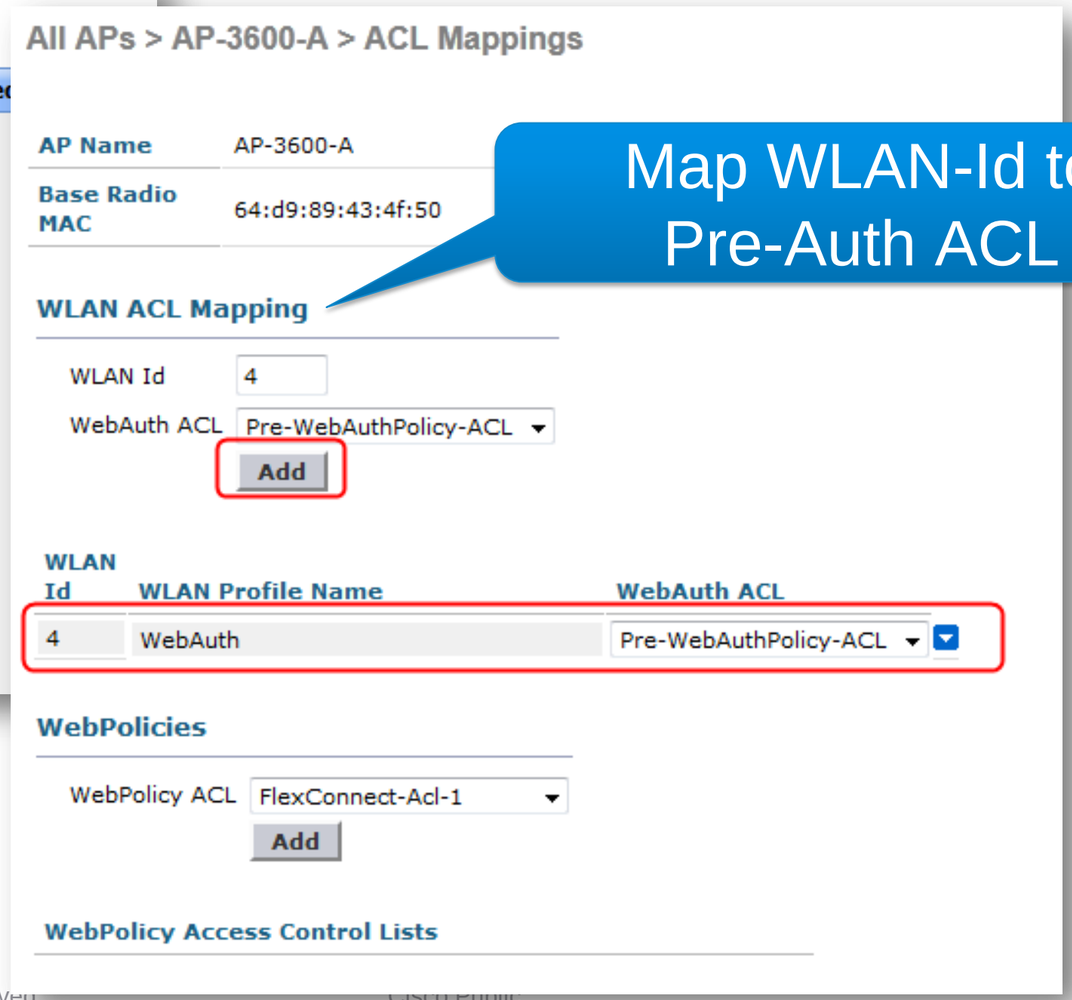
Apply Pre-Auth ACL to WLAN

External WebAuth with Local Switching

Configuration

Step 3: Apply Pre-Auth ACL to FlexConnect AP

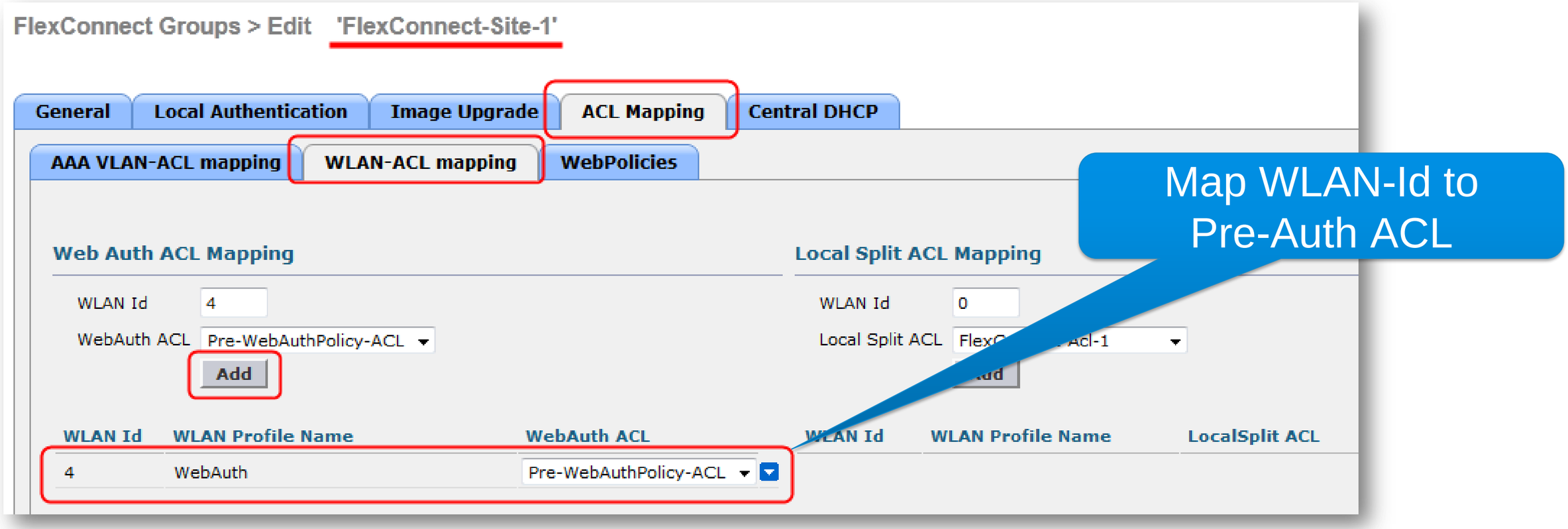




External WebAuth with Local Switching

Configuration

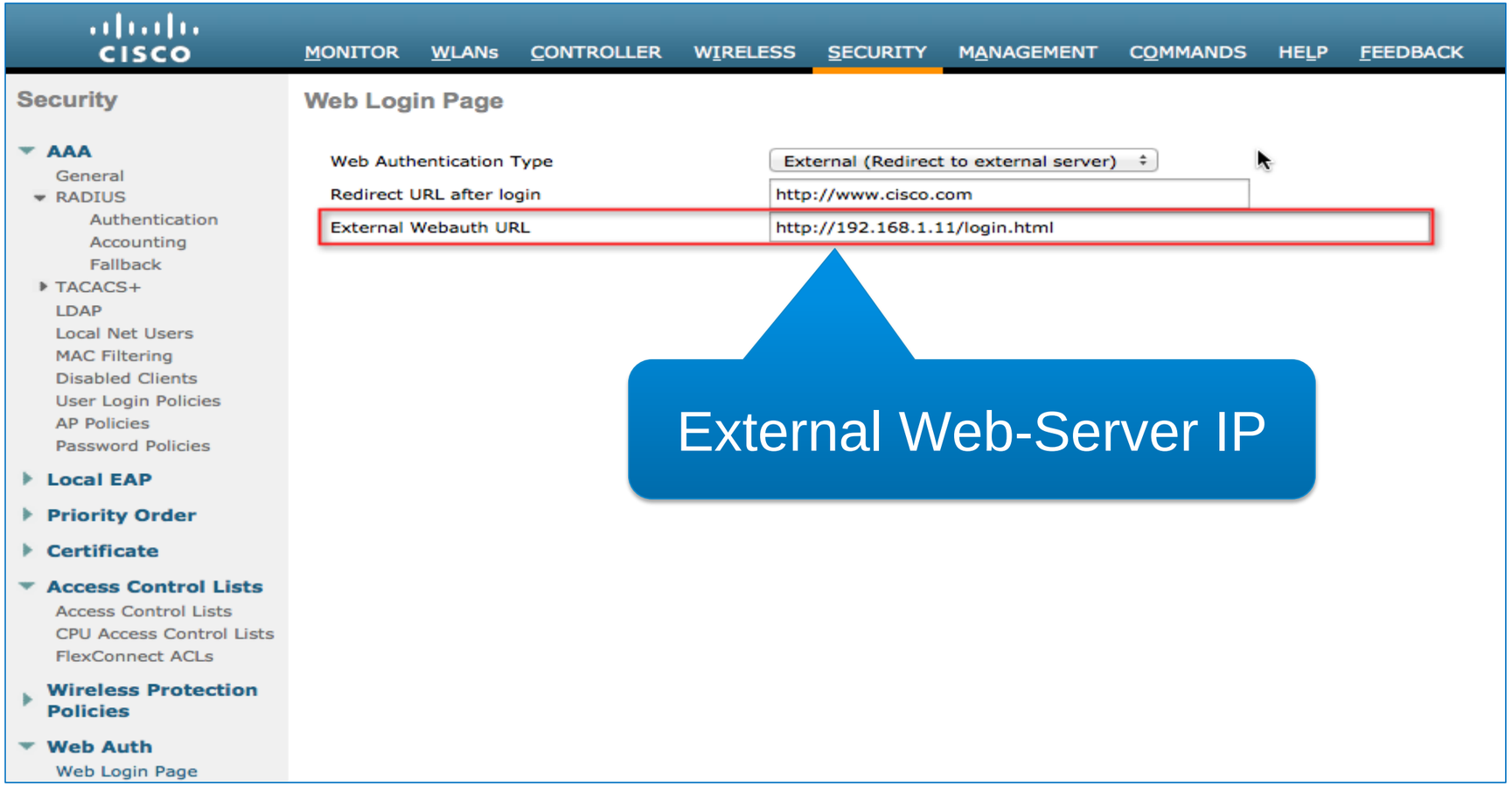
Or Step 3: Apply Pre-Auth ACL to FlexConnect Group



External WebAuth with Local Switching

Configuration

Step 4: Configure External Web Server



FlexConnect AAA VLAN Override

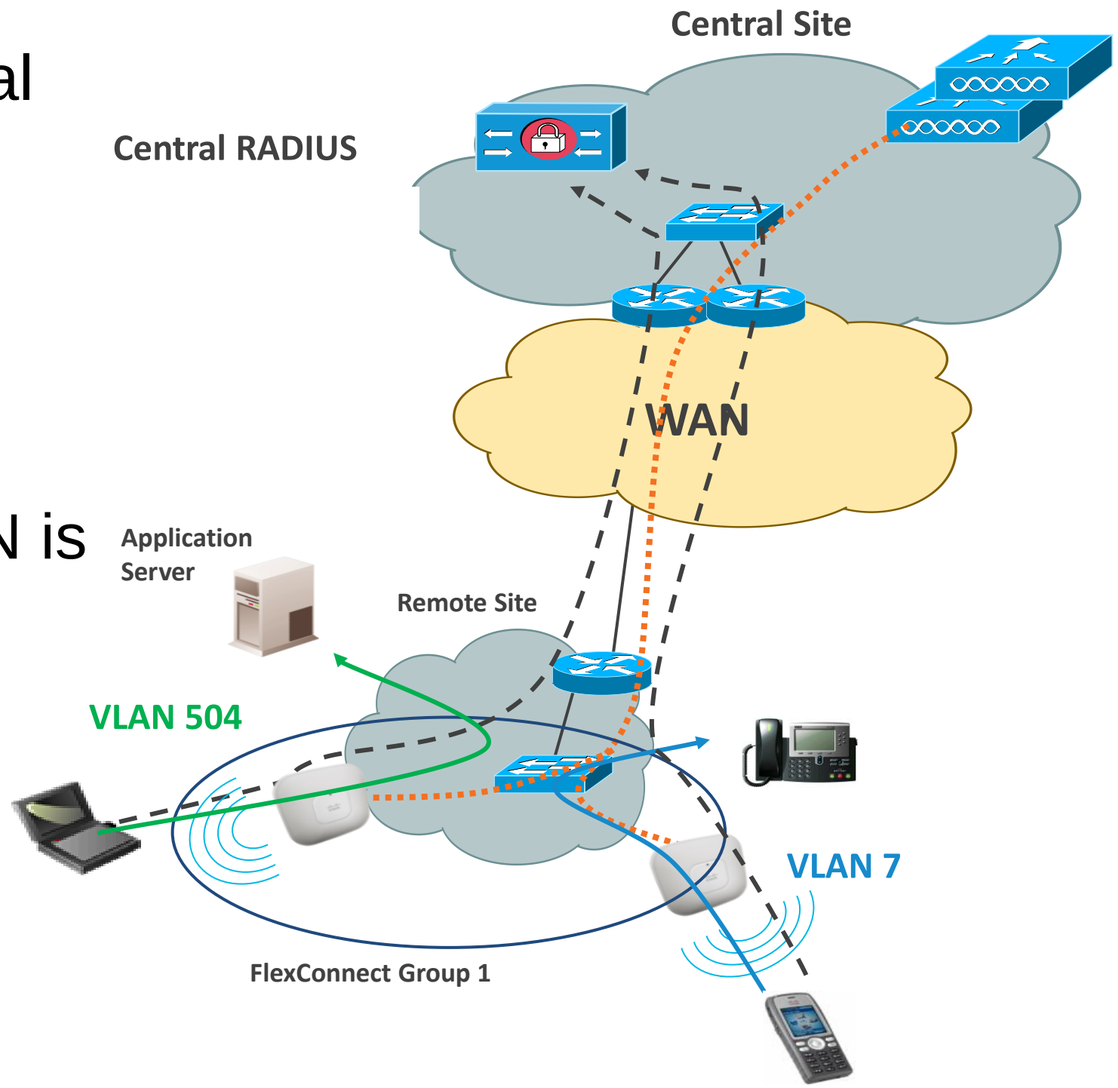
FlexConnect AAA VLAN Override

New in 7.2

Description

- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used, unless « VLAN Based Central Switching » enabled
- Starting from 7.5 New

  QoS and ACL Override is supported.

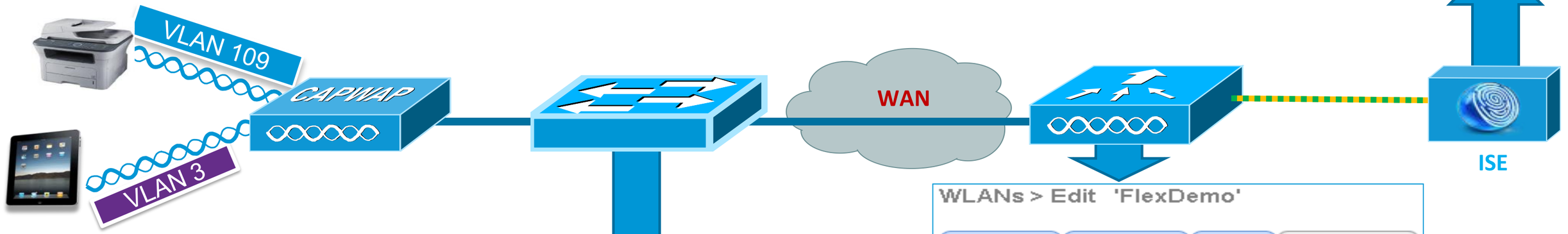


FlexConnect AAA VLAN Override

Configuration

For Your Reference

	Attribute	Type	Value
IETF 65 IETF 64 IETF 81	Tunnel-Medium-Type	Tagged Enum	[T:1] 802
	Tunnel-Type	Tagged Enum	[T:1] VLAN
	Tunnel-Private-Group-ID	Tagged String	[T:1] 3




```
interface GigabitEthernet1/0/4
 description AP-3600-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

WLANs > Edit 'FlexDemo'

General | Security | QoS | Advanced

Allow AAA Override ☑ Enabled

FlexConnect Groups > Edit 'SanJose'

General | Local Authentication | Image Upgrade | VLAN-ACL mapping

VLAN ACL Mapping

Vlan Id 3

Ingress ACL none

Egress ACL none

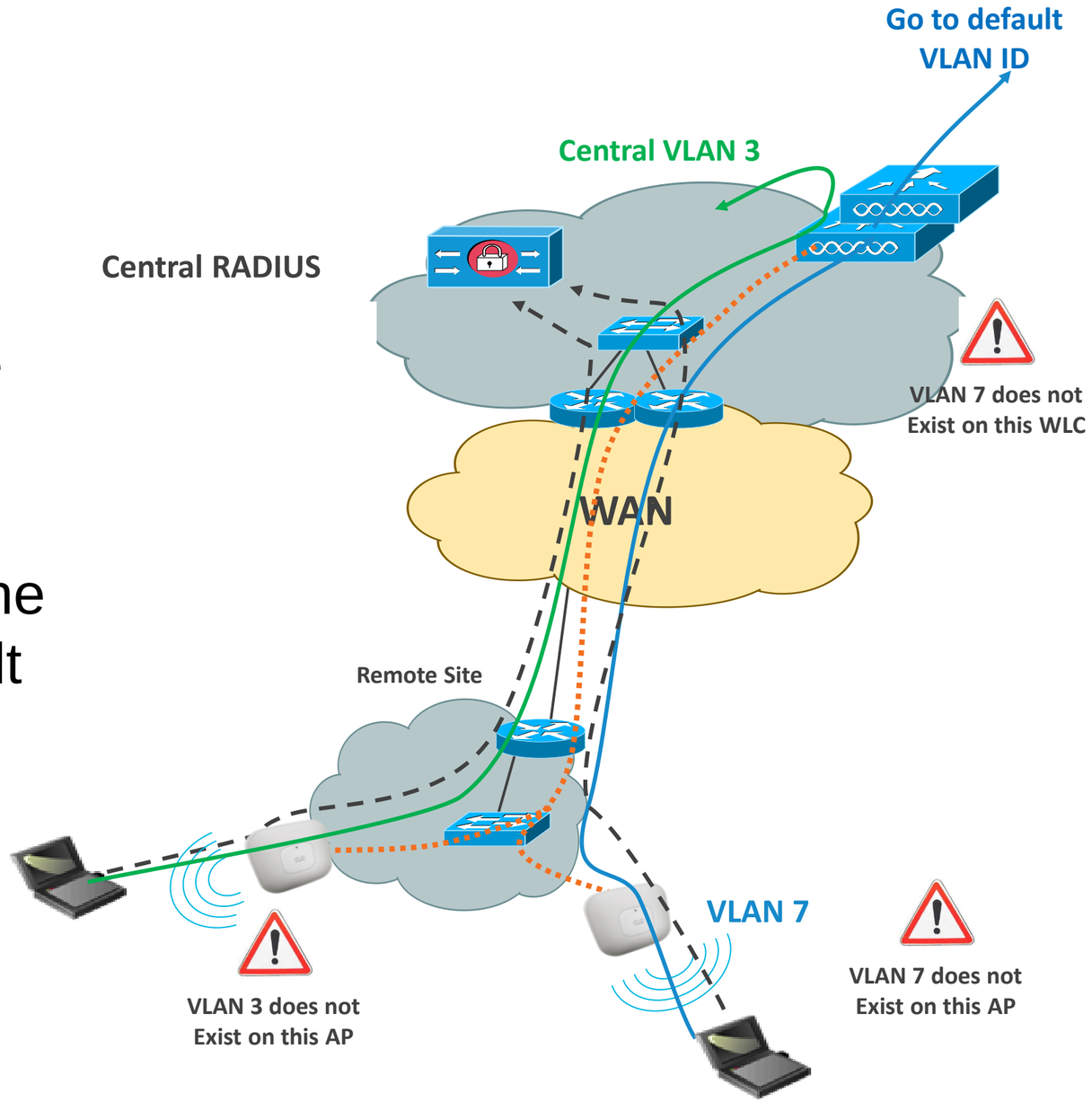
Add

Create Sub-Interface on FlexConnect AP

VLAN Based Central Switching

Overview

- While doing AAA VLAN Override with local switching :
- If VLAN ID does not exist at the AP, the traffic is central switched to the central VLAN ID
- If the central VLAN ID does not exist, the traffic is centrally switched to the default VLAN ID of the WLAN



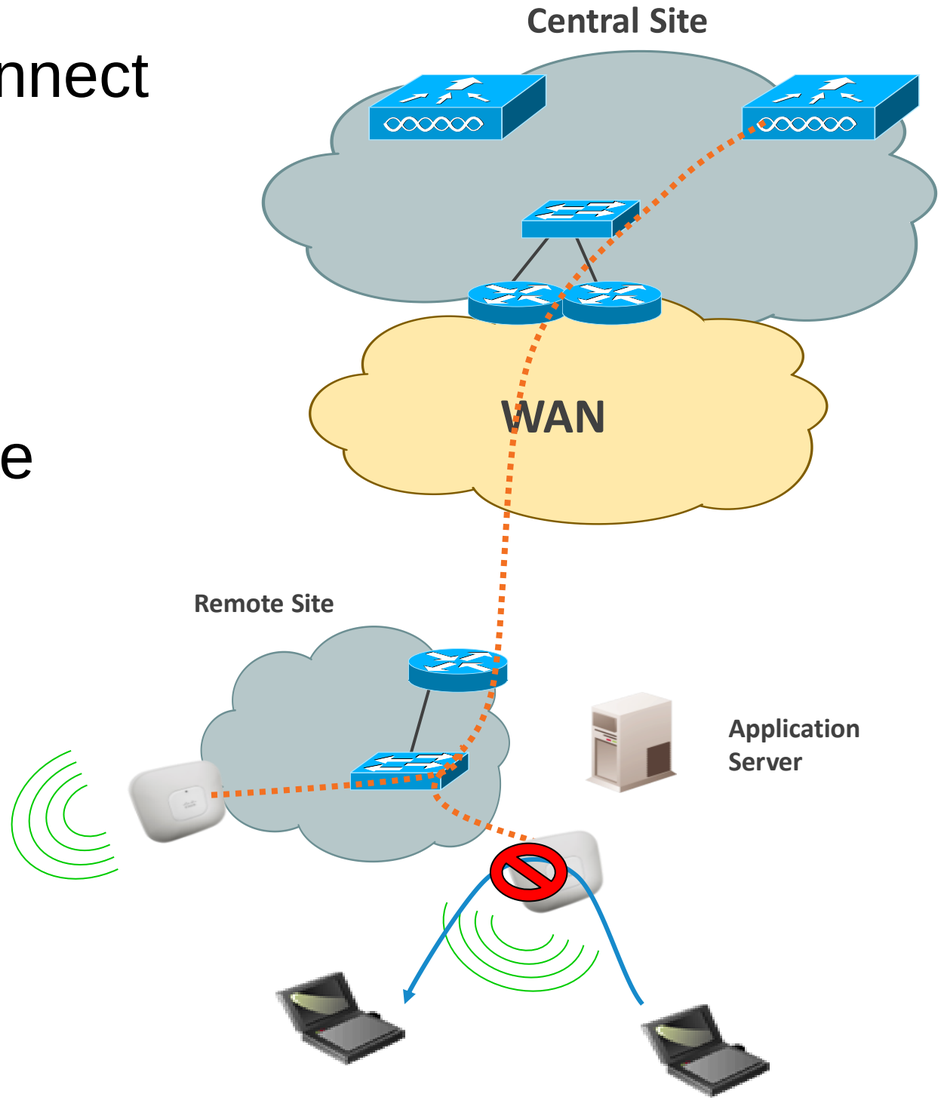
FlexConnect Peer-to-peer Blocking

Local Switching Peer-to-peer Blocking

New in 7.2

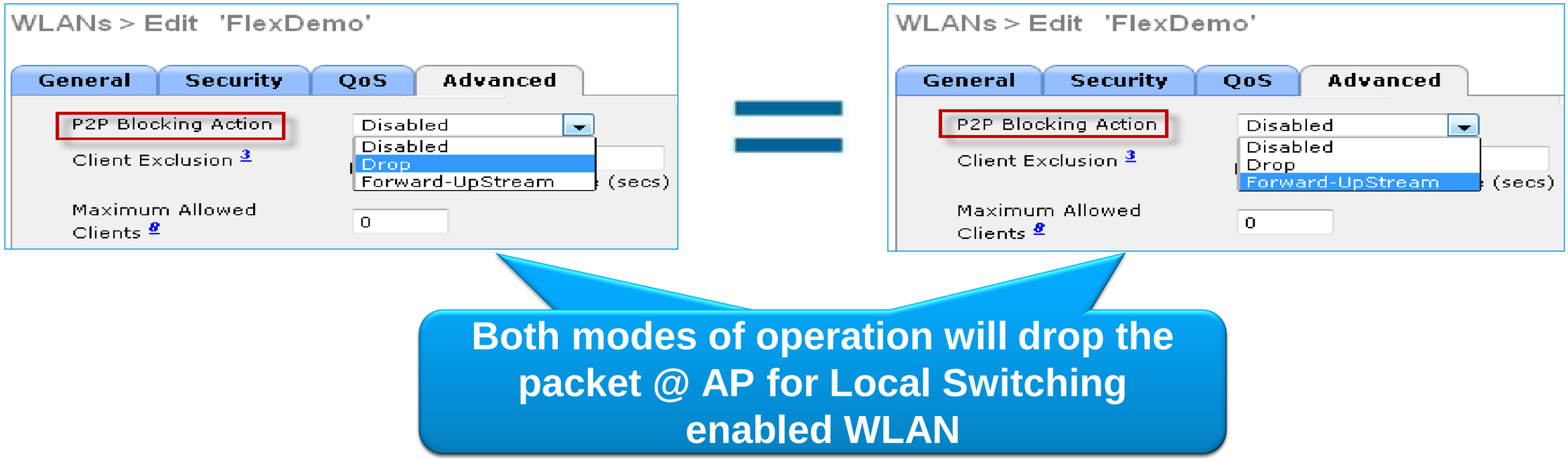
Description

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



Local Switching Peer-to-peer Blocking

Configuration



* Central Switching WLAN will support “Forward - UpStream” and will send the packet to the next upstream node connected to WLC

Operating Wireless Branch
Smart Upgrade over WAN

Upgrading a FlexConnect Deployment

Concerns

- Sites using FlexConnect AP are usually sites with low WAN bandwidth
- Each site may have small number of AP, but an enterprise may have a lot of branches
- Upgrading ~2000 AP through a low bandwidth WAN is a challenge :
  - Time needed to download all the AP firmware
  - Exhaust of the WAN link
  - Risk of failures during the download
- Release 7.2 introduce “Smart AP Image Upgrade”

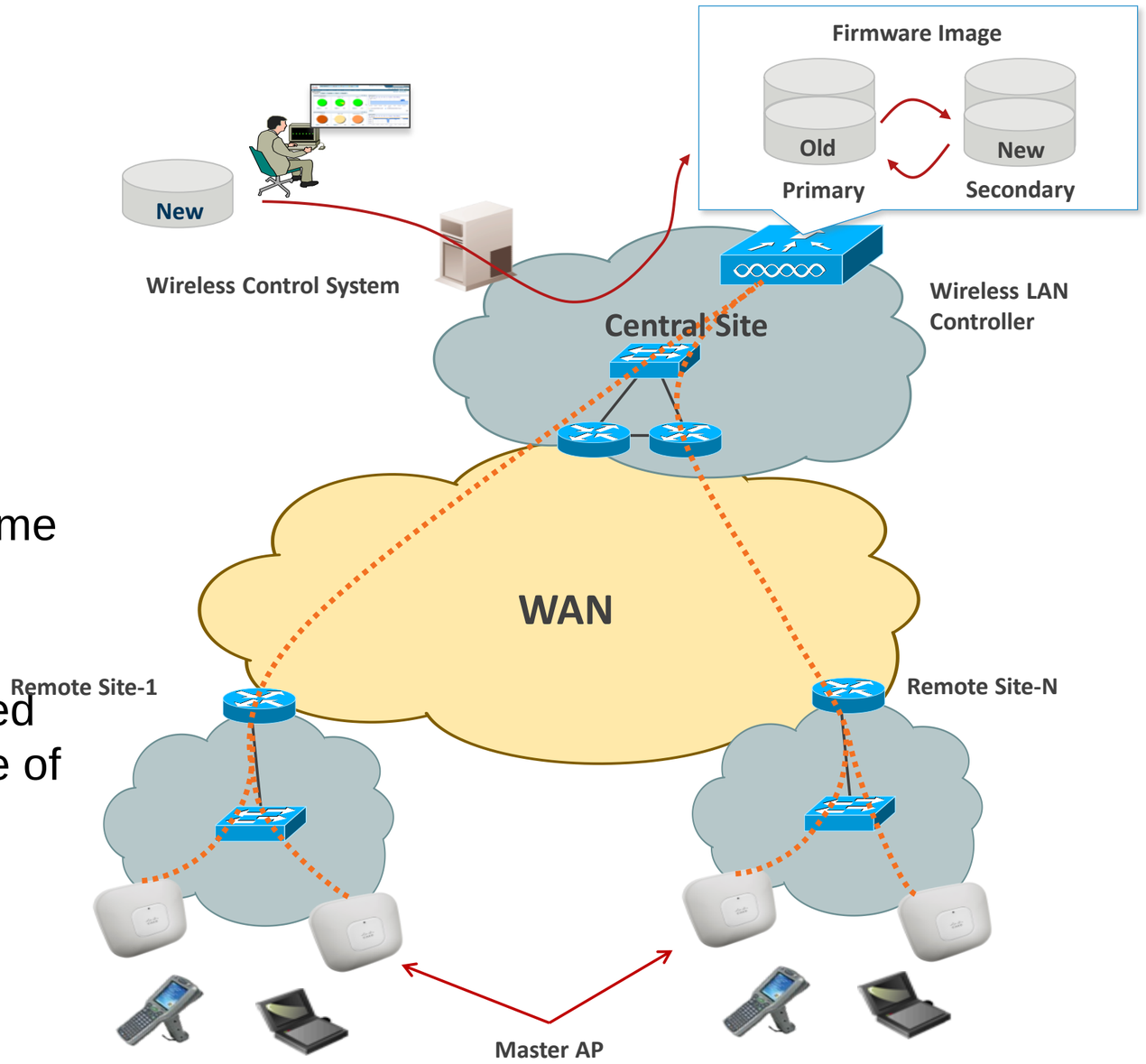
FlexConnect Smart AP Image Upgrade

Overview

Smart AP Image Upgrade use a « master » AP in each FlexConnect Group to download the code.

Other FlexConnect AP download the code from the master locally

1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)

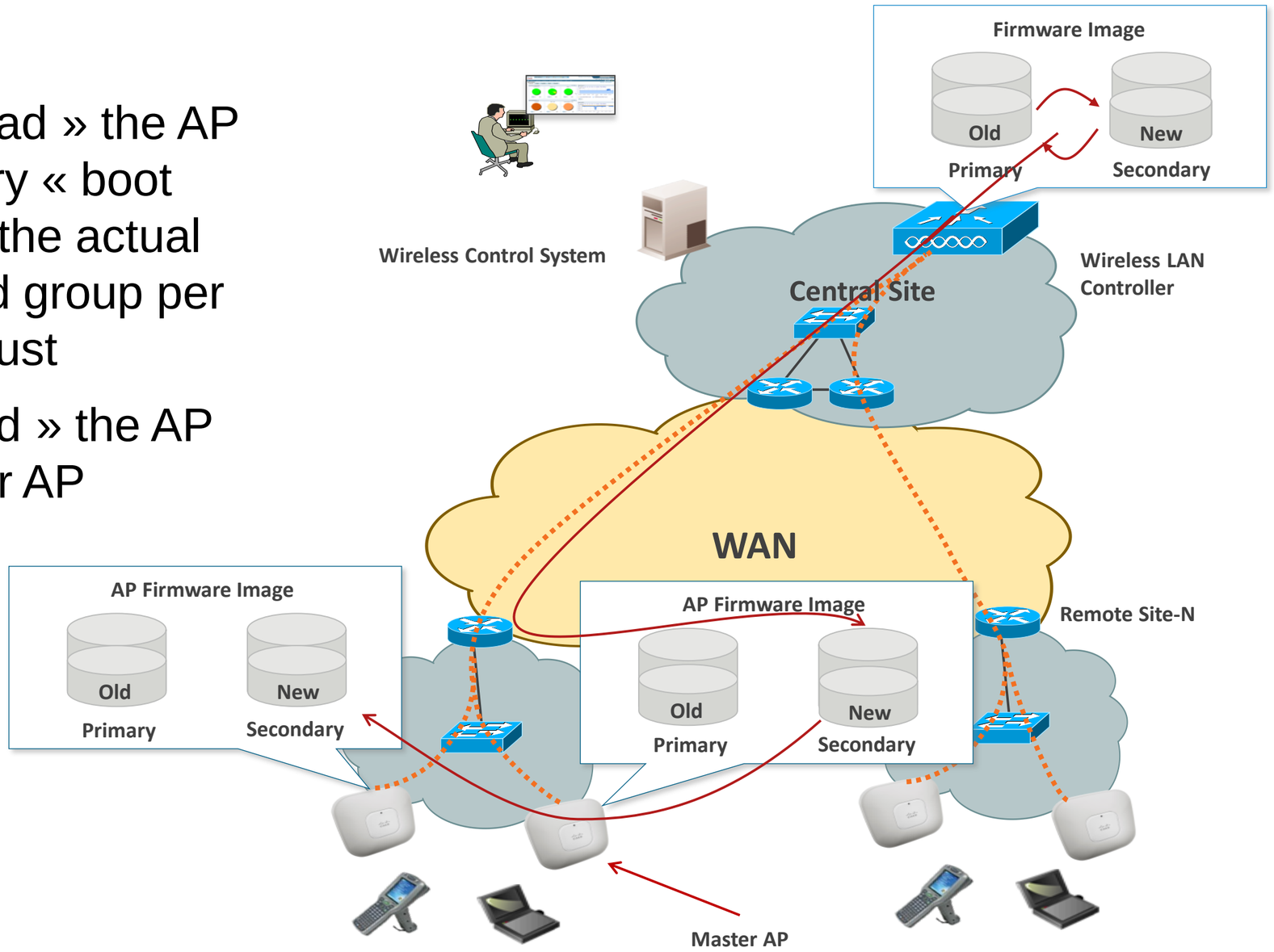


New in 7.2

FlexConnect Smart AP Image Upgrade

Description (Cont…)

4. Master AP « Pre-download » the AP firmware in the secondary « boot image » (will not disrupt the actual service)—Can be started group per group to limit WAN exhaust
5. Slave AP « Pre-download » the AP firmware from the Master AP
6. Change the « boot image » of the WLC to the new image
7. Reboot the controller



FlexConnect Smart AP Image Upgrade

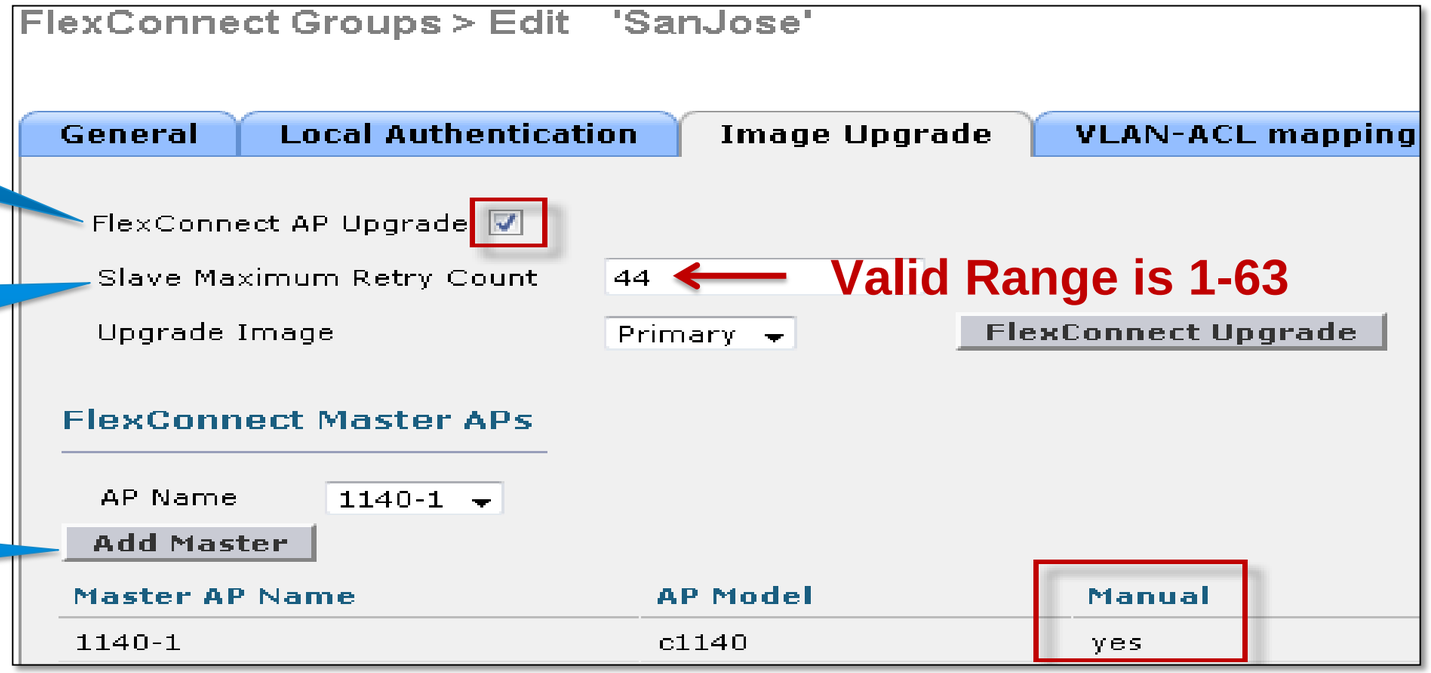
For Your Reference

Configuration

Enable Efficient AP Image Upgrade

Random Backoff Interval (100-300sec) between each retry

Master AP Selection is Optional

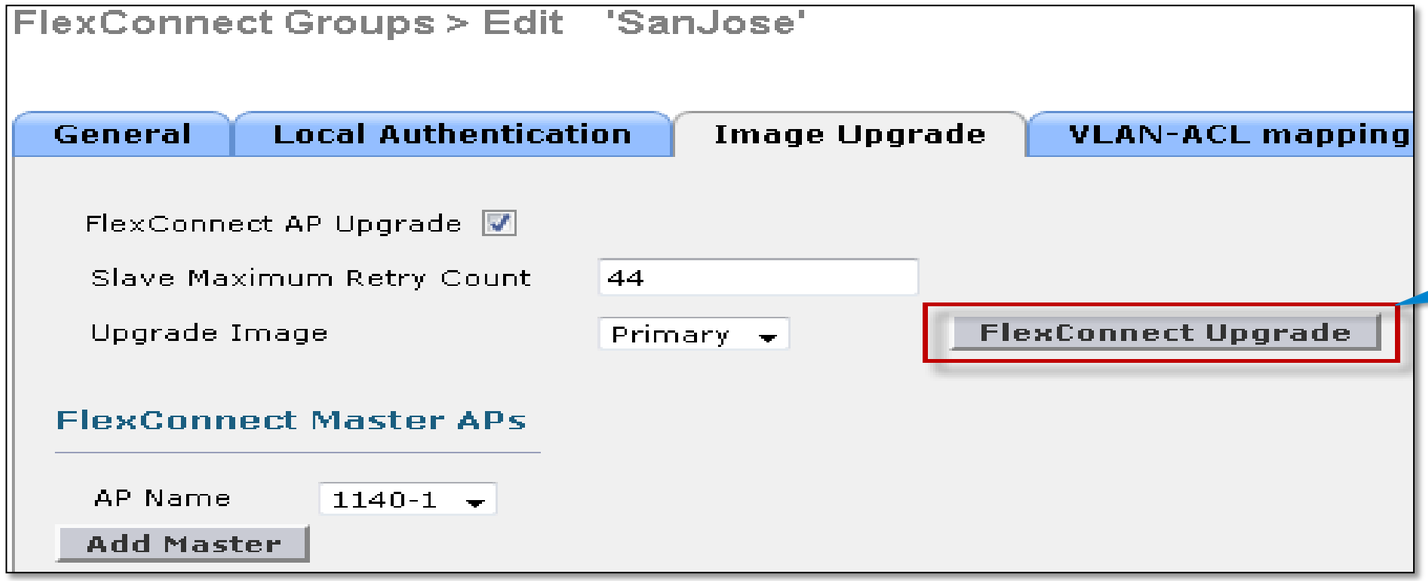


- "FlexConnect AP Upgrade" checkbox has to be enabled for each FlexConnect Group.
- By default, Master AP for each FlexConnect Group is selected using Lower-MAC algorithm.
- One Master select per AP type.

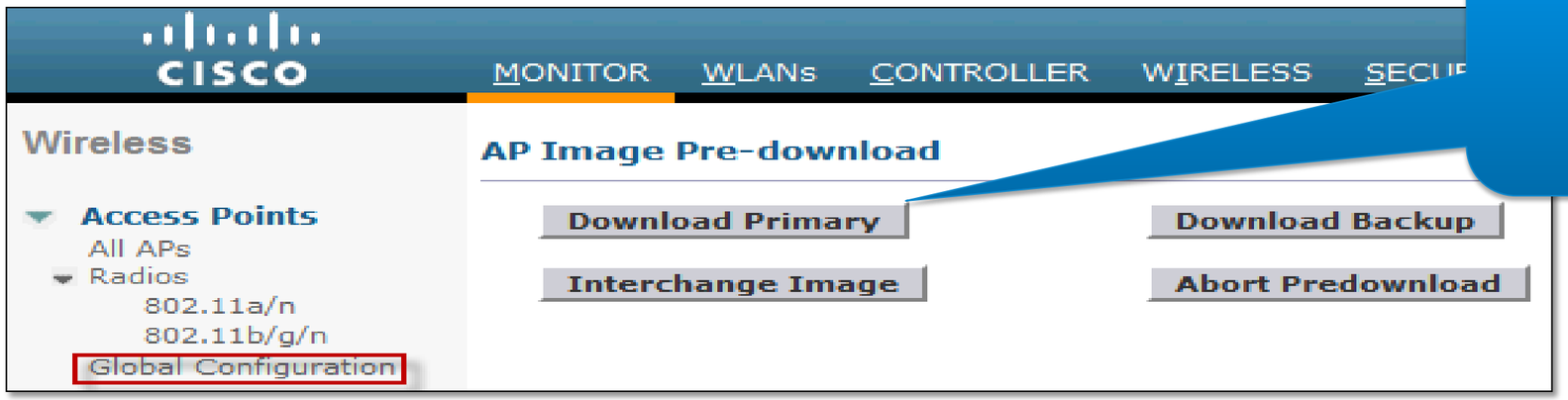
FlexConnect Smart AP Image Upgrade

Configuration (Cont)

For Your Reference



Per Branch or FlexConnect Group Upgrade



Upgrade across all Branches or FlexConnect Groups whose "FlexConnect AP Upgrade" checkbox is set

Deploying BYOD with FlexConnect and Local Switching

(Using FlexConnect WebPolicies ACL)

BYOD Device On-Boarding in FlexConnect

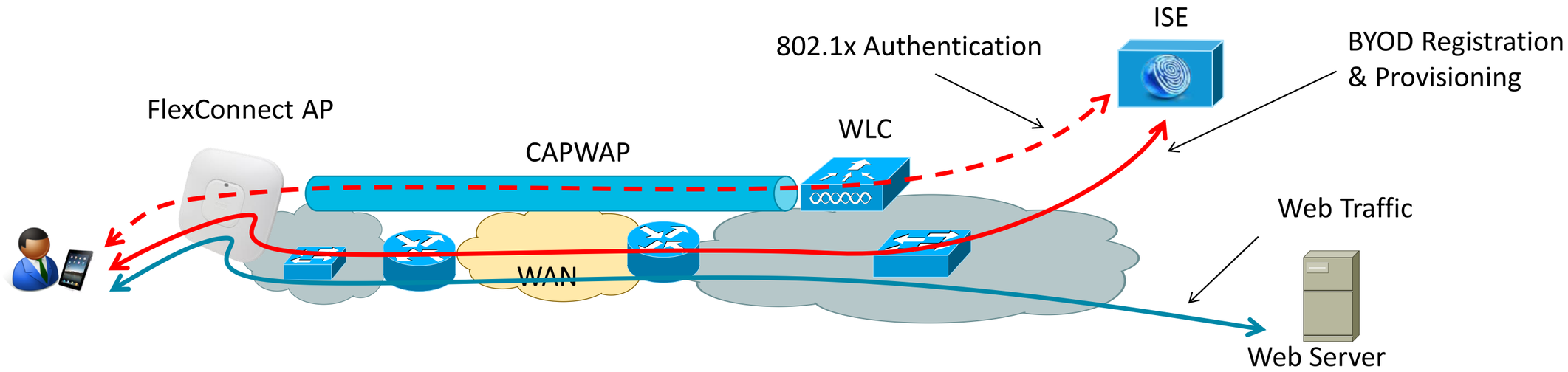
Example: Apple iOS Device Provisioning

Starting from 7.4

Deploying BYOD with FlexConnect and Local Switching

What's different for BYOD with FlexConnect ?

- No difference for centrally switched traffic.



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

Deploying BYOD with FlexConnect Wireless

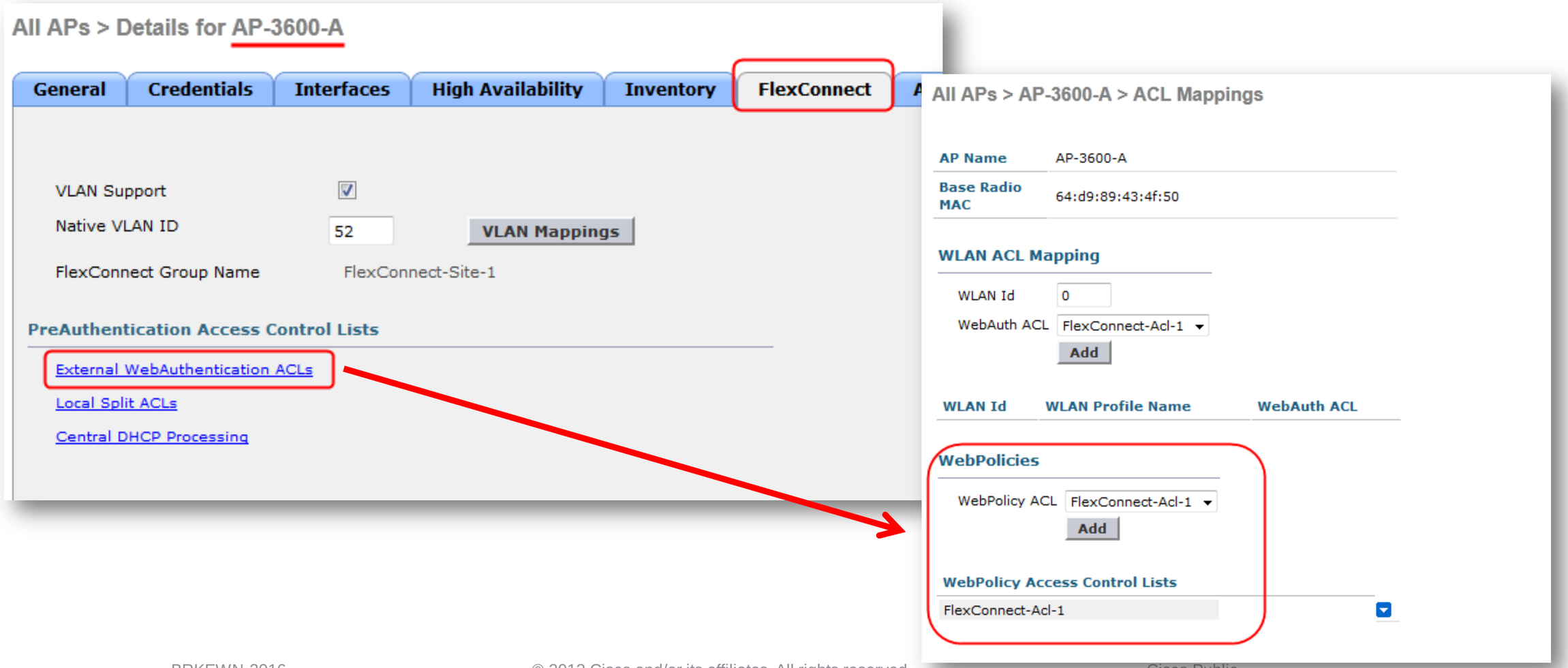
FlexConnect Features for BYOD

- AAA override feature allows Cisco ISE to tell WLC the enforcement actions to be taken for a client on a FlexConnect AP :
  - Dynamic VLAN association (Optional)
  - FlexConnect Web Policy ACL for URL Redirection
  - URL Redirection (WebAuth)
- CoA (Change of Authorization) Support
- Profiling Sensor : DHCP Sensor – Need Central DHCP Processing

FlexConnect Web Policy ACL

Configure Web Policy ACL per FlexConnect AP

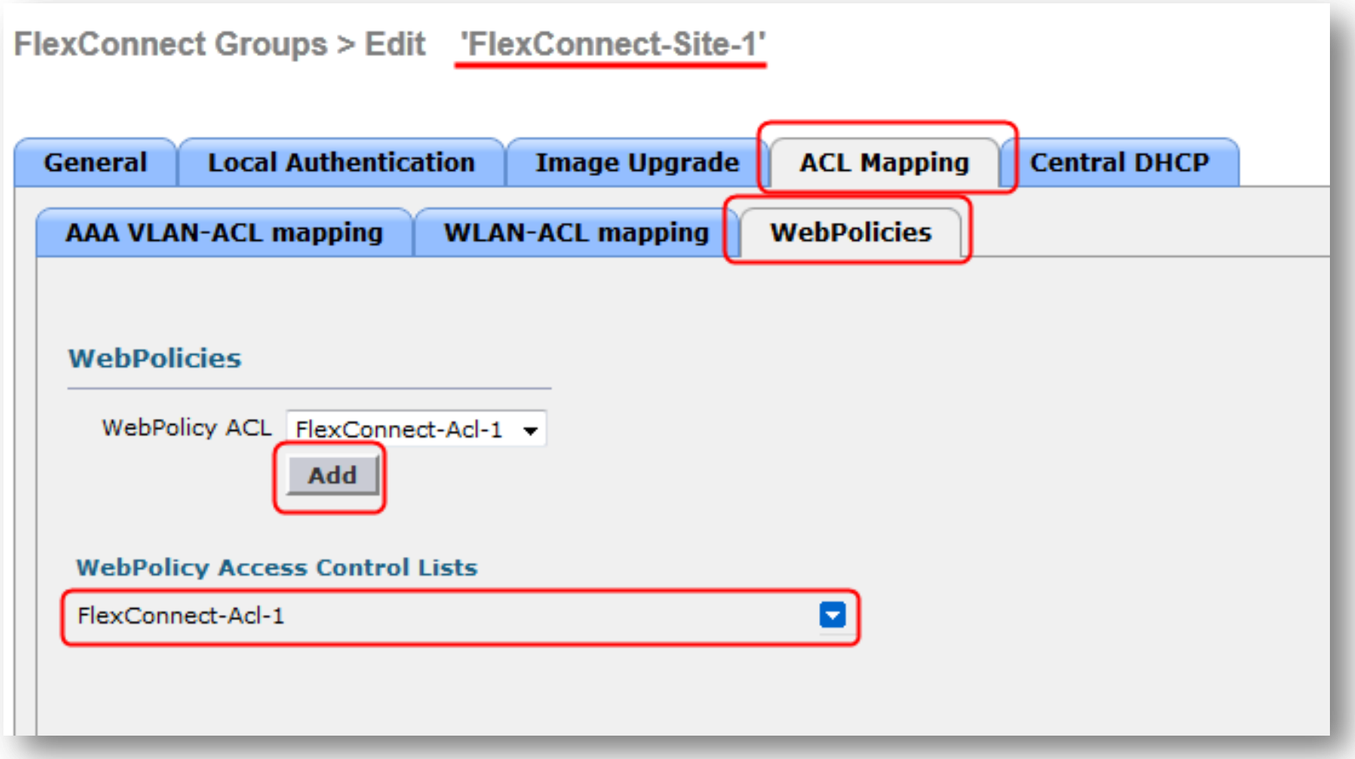
- ACL Mapping can be configured per FlexConnect AP



FlexConnect Web Policy ACL

Configure Web Policy ACL per FlexConnect Group

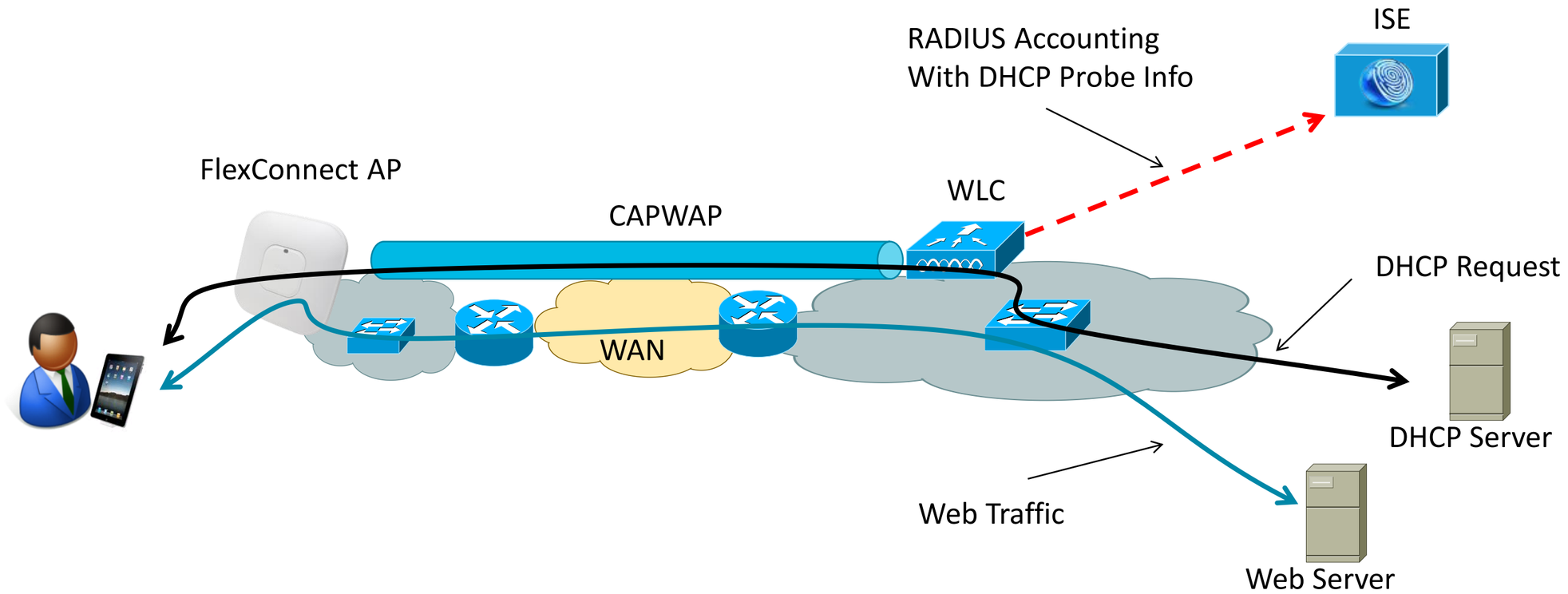
- Use ACL Mapping tab in FlexConnect Group configuration
- WebPolicies ACL are not the same as VLAN ACL or WebAuthentication ACL.



Cisco Wireless DHCP Profiling Probe

Understand Central DHCP Processing

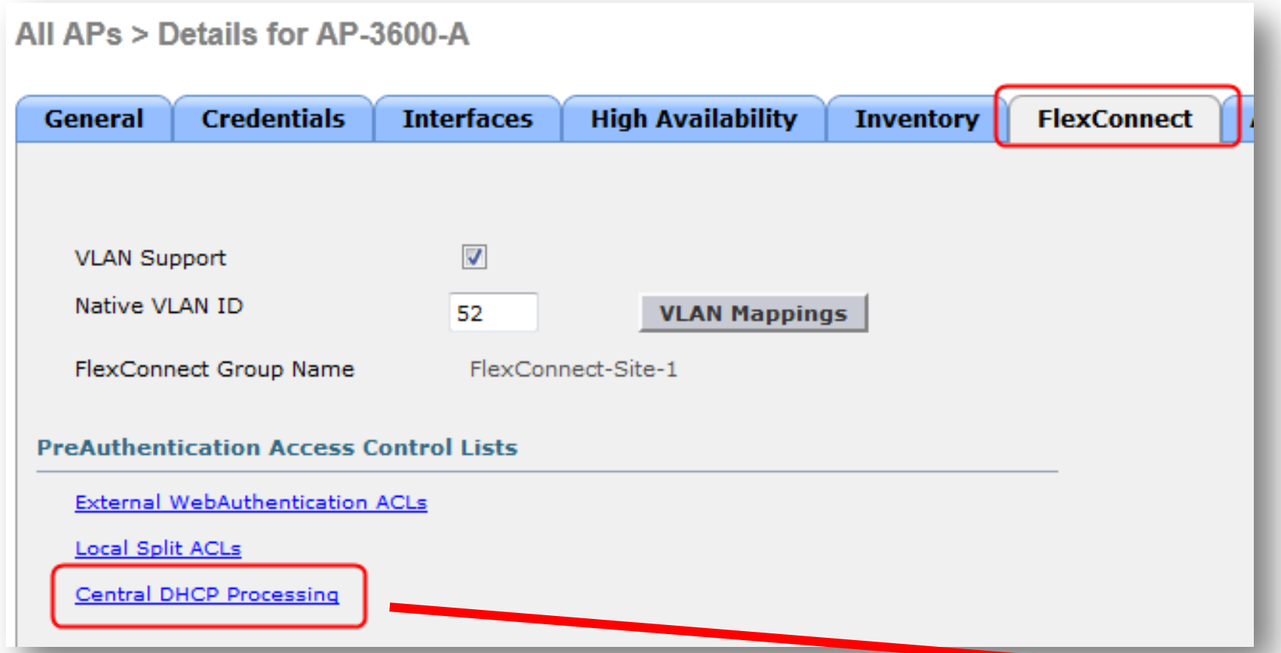
- By default DHCP request are locally switched
- To support DHCP Profiling Probe at WLC, Central DHCP Processing is enabled.

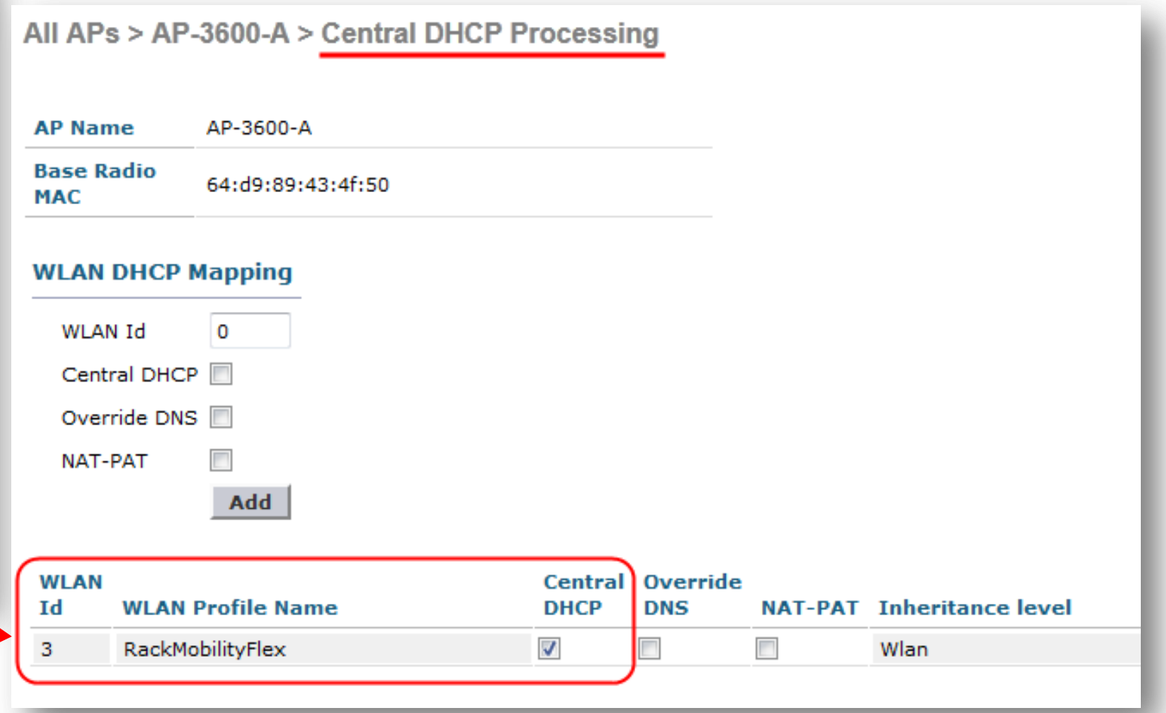


Cisco Wireless Central DHCP Processing

Configuration

- To support DHCP Profiling Probe with FlexConnect, DHCP request must be sent to WLC. This is done by the « Central DHCP Processing » configuration.





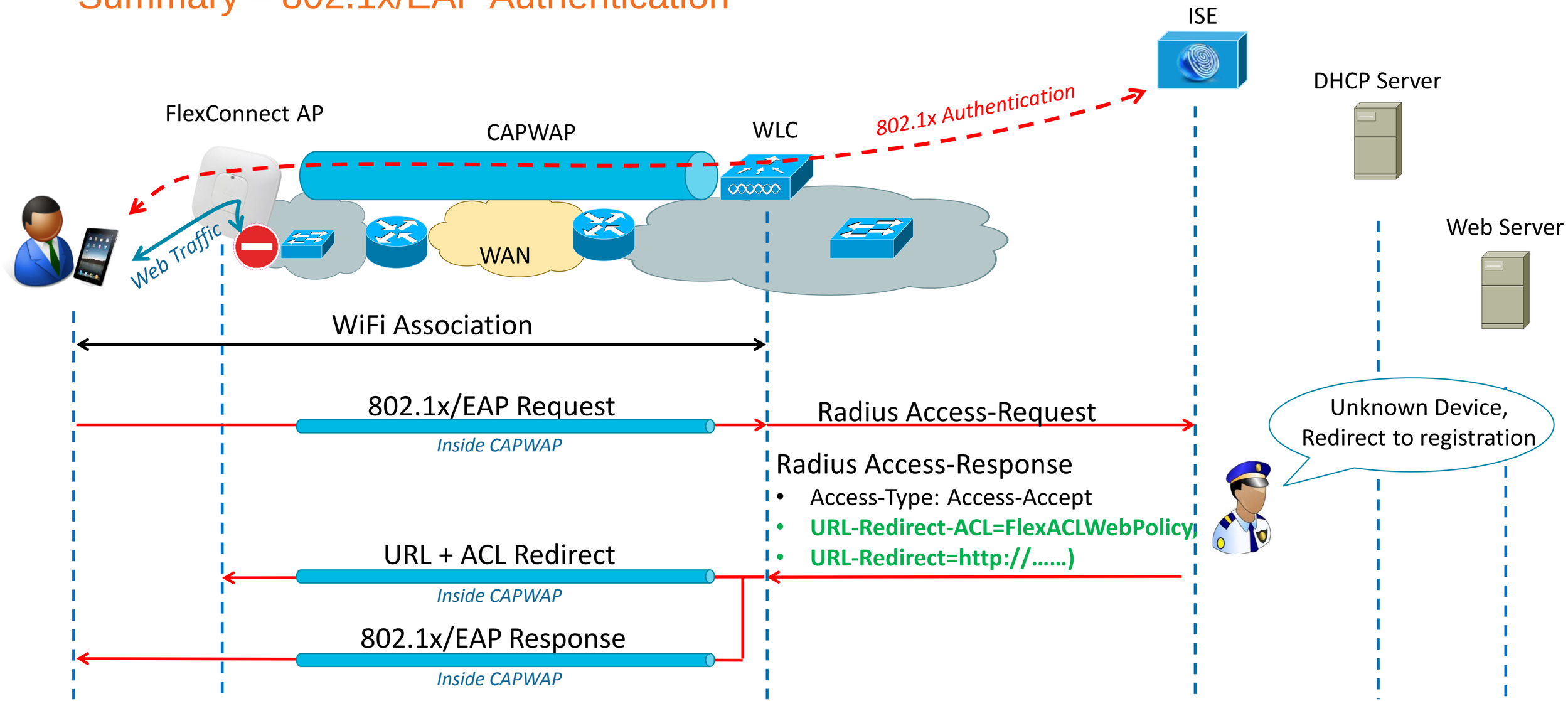
Deploying BYOD with FlexConnect Wireless

Summary

1. Device Association, Authentication & Authorization
2. URL and ACL redirection for device registration & provisioning
3. DHCP Profiling
4. Device registration & provisioning
5. Change-of-Authorization
6. Device Re-Association, Authentication & Authorization
7. Device Access

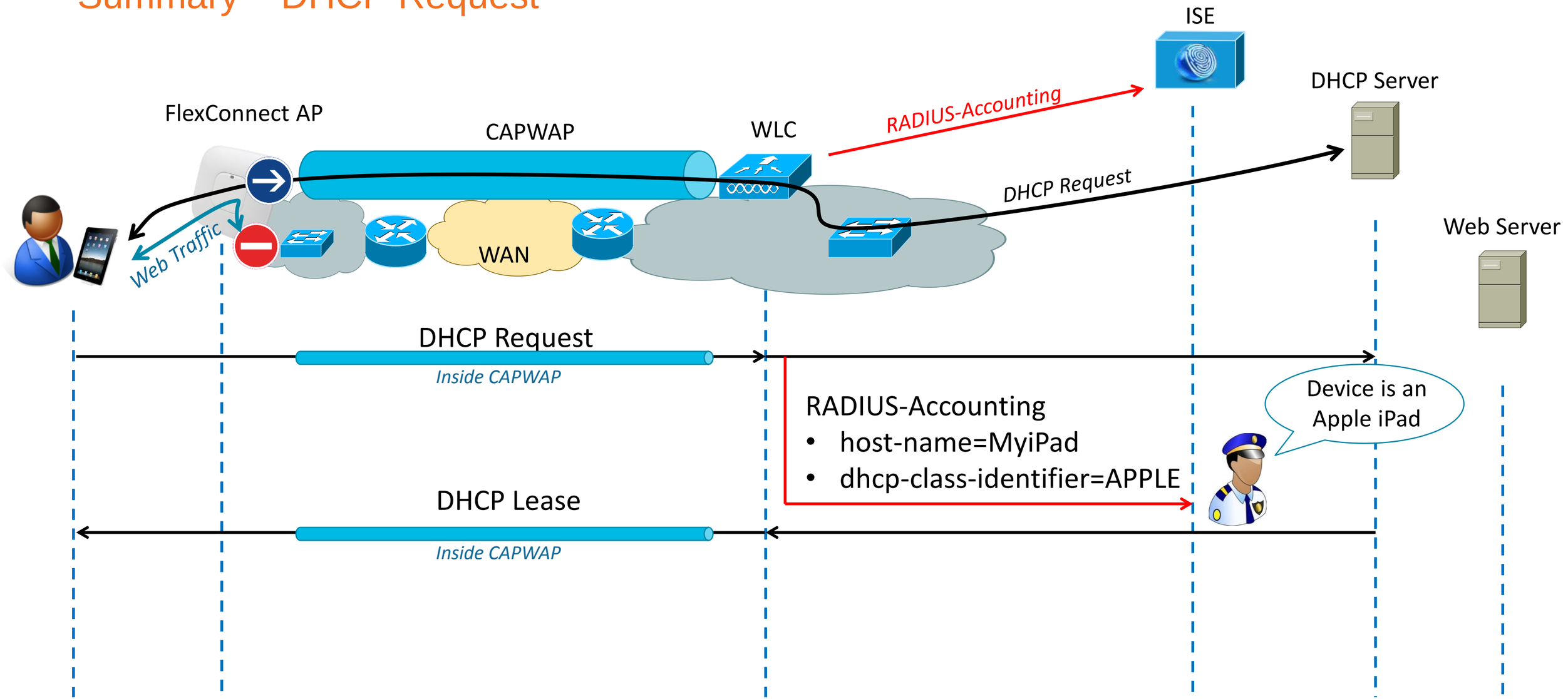
Deploying BYOD with FlexConnect Wireless

Summary – 802.1x/EAP Authentication



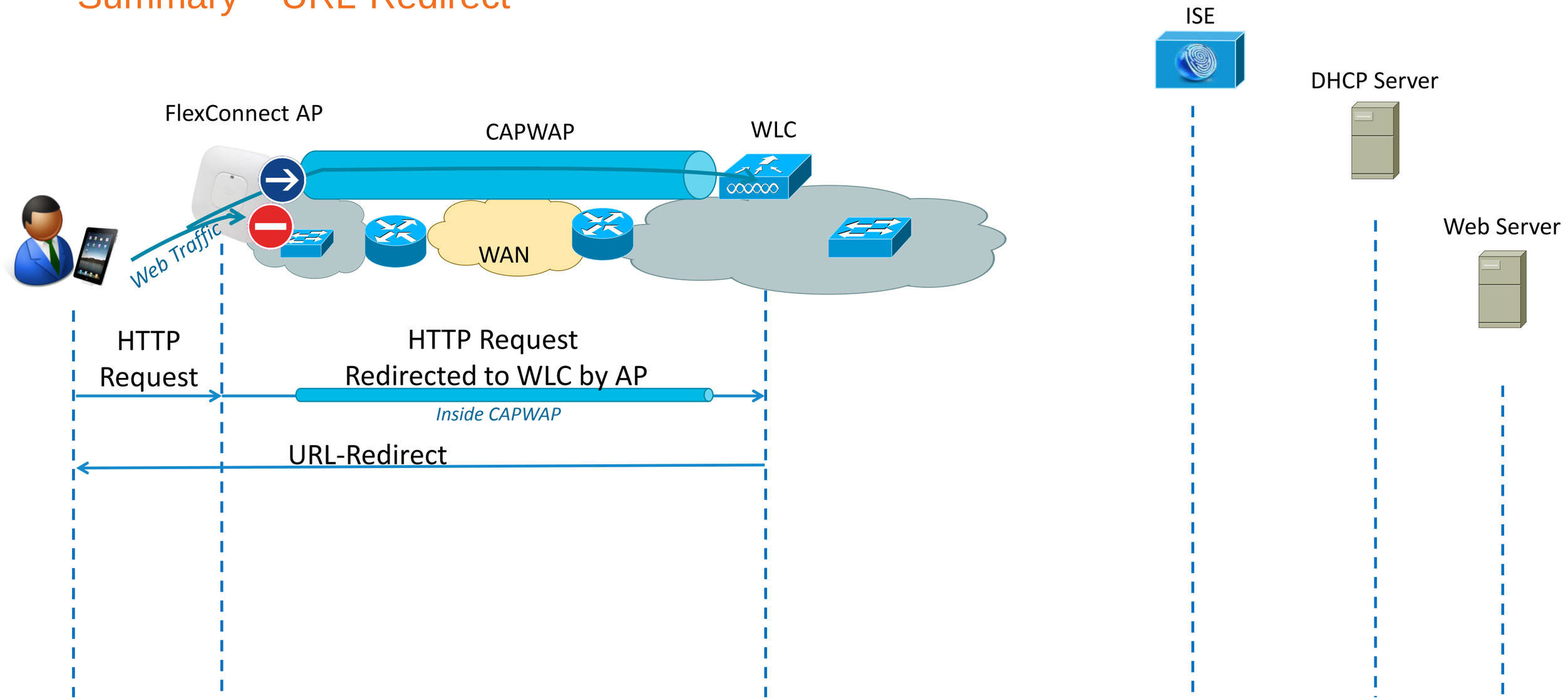
Deploying BYOD with FlexConnect Wireless

Summary – DHCP Request



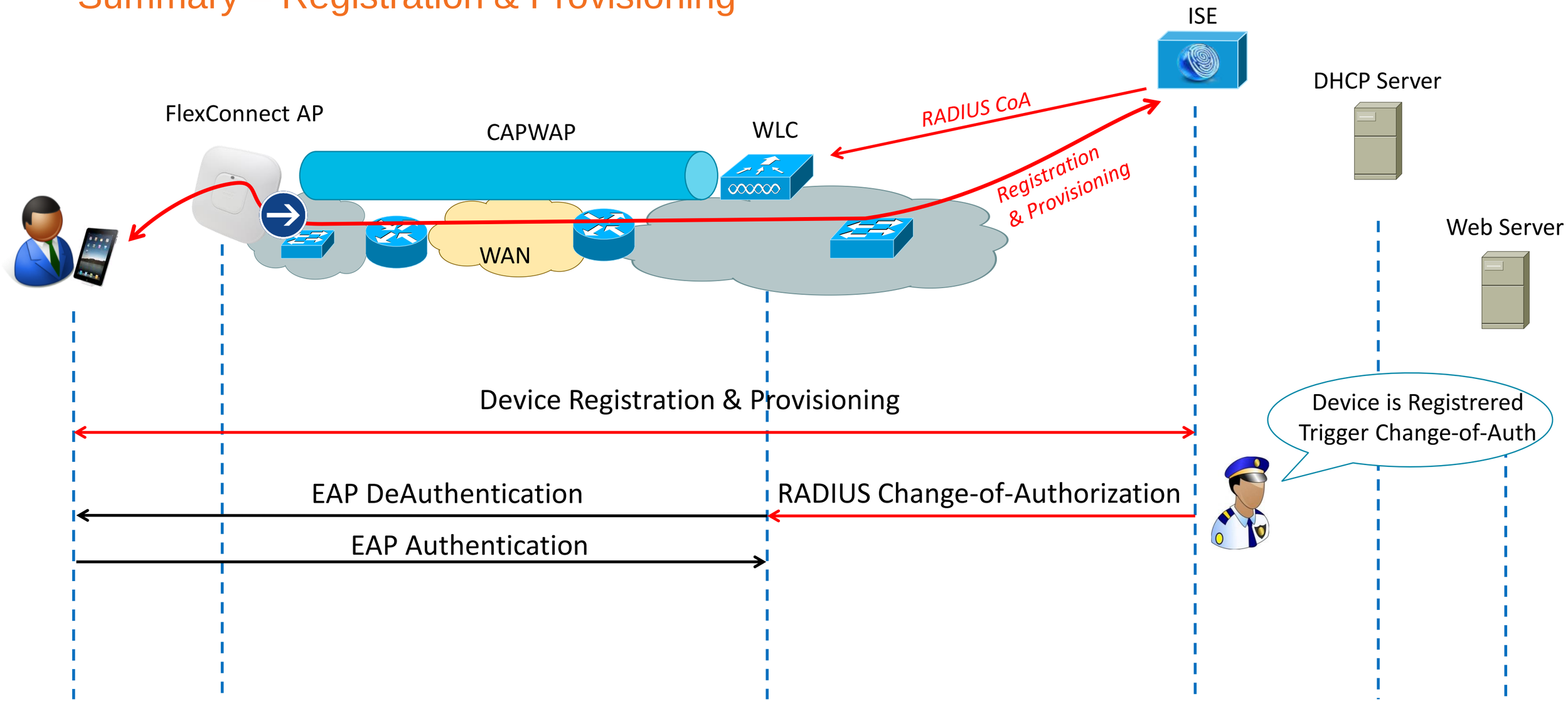
Deploying BYOD with FlexConnect Wireless

Summary – URL-Redirect



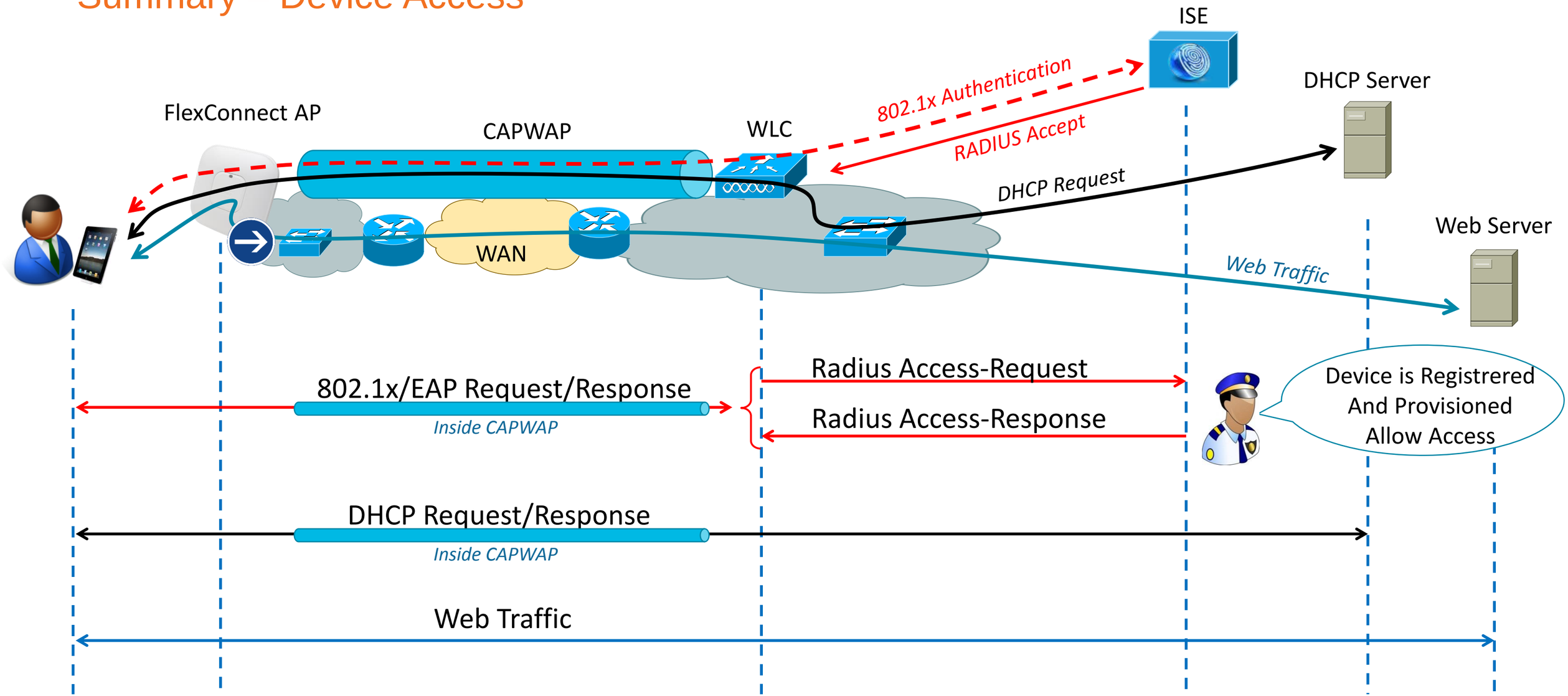
Deploying BYOD with FlexConnect Wireless

Summary – Registration & Provisioning



Deploying BYOD with FlexConnect Wireless

Summary – Device Access



Summary

Summary

- Cisco Unified Wireless Network based on Controllers deliver Wireless Branch Solution
- FlexConnect is the feature designed to solve remote connectivity and WAN constraints
- Several Failover Scenario are targeted to offer Survivability of Small Remote Sites
- FlexConnect Branch Controller Deployment Guide: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

Deploying Cisco's FlexConnect in Branches Increases Business Resiliency


CISCO