Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Branch Office Wireless LAN Design

BRKEWN-2016

TOMORROW starts here.

Abstract

- This session focuses on the architecture concepts of the branch office WLAN deployments, emphasising the core technologies that drive and enable mobility in retail, banking, education, entreprise or managed wlan services. Topics covered include in-depth protocol description of H-Reap/FlexConnect, all deployment options in practice, and are based on customer case studies for their application into the branch environment.

Objectives

Design & Deploy Branch Network That Increases Business Resiliency

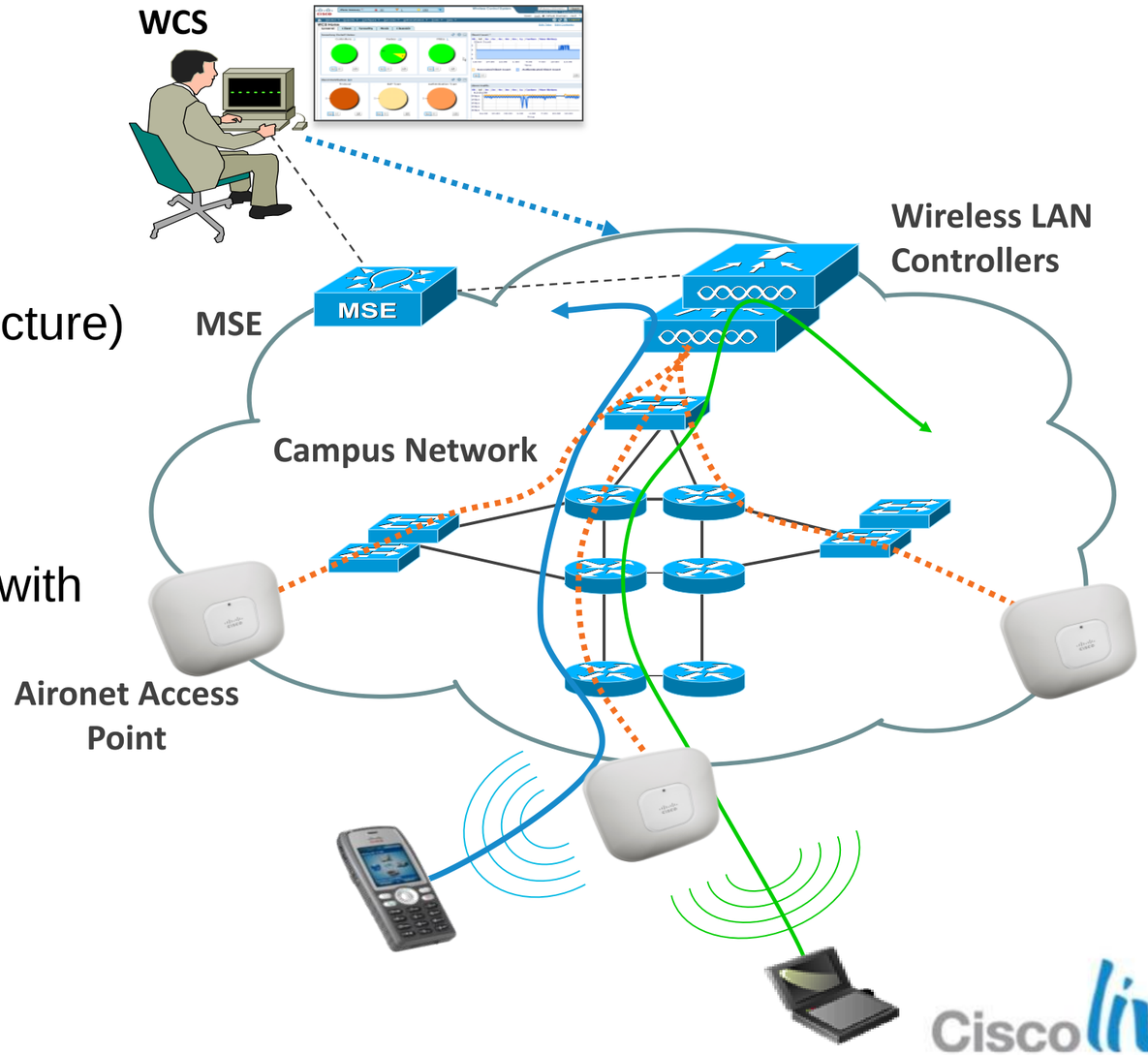
Agenda

- 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 Unified Wireless Principles

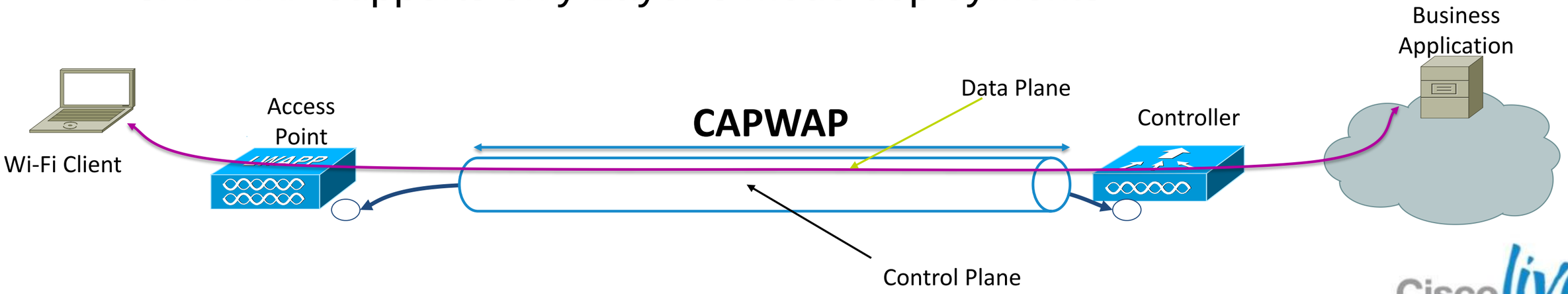
- Components
  - Wireless LAN controllers
  - Aironet access points
  - Management System (Prime Infrastructure)
  - Mobility Service Engine (MSE)
- Principles
  - AP must have CAPWAP connectivity with WLC
  - Configuration downloaded to AP by WLC
  - All Wi-Fi traffic is forwarded to the WLC



CAPWAP Overview

Control and Provisioning of Wireless Access Point

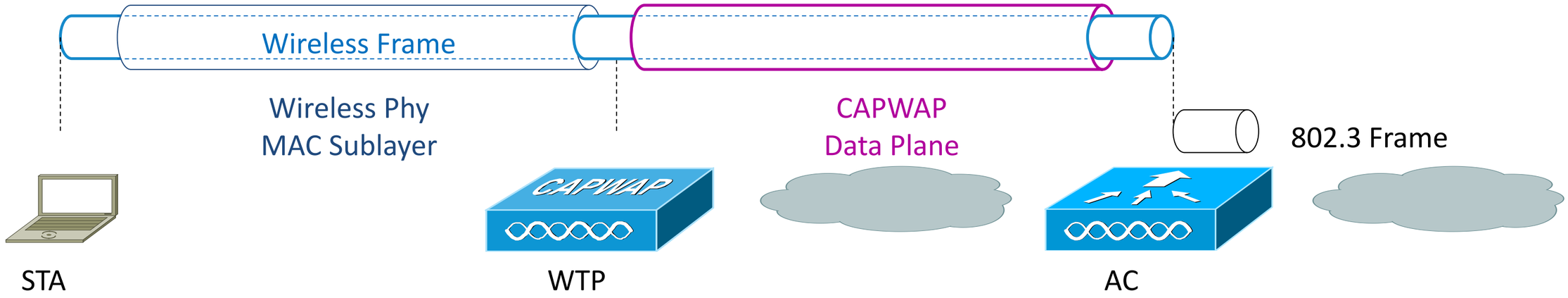
- CAPWAP is a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs)
- CAPWAP carries control and data traffic between the two
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (optional)
- CAPWAP supports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



CAPWAP Modes

Split MAC

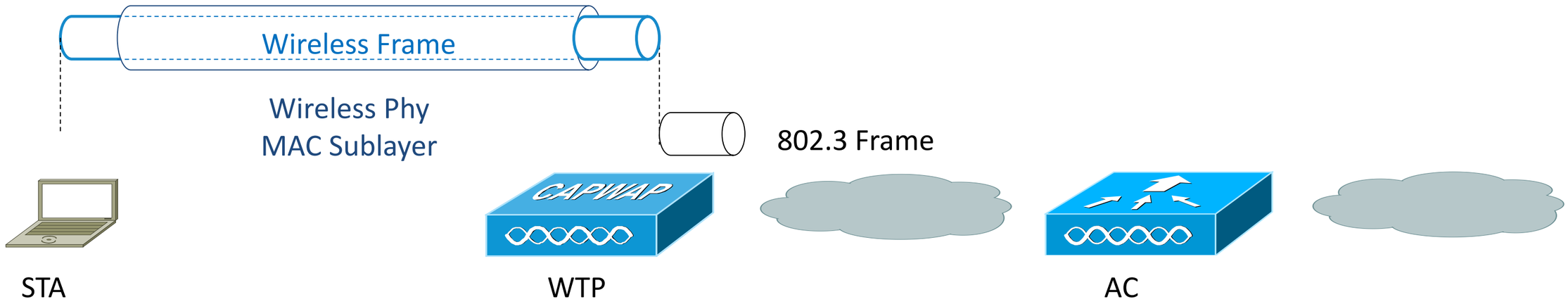
- The CAPWAP protocol supports two modes of operation
  - Split MAC (Centralised Mode)
  - Local MAC (H-REAP/FlexConnect)
- Split MAC



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

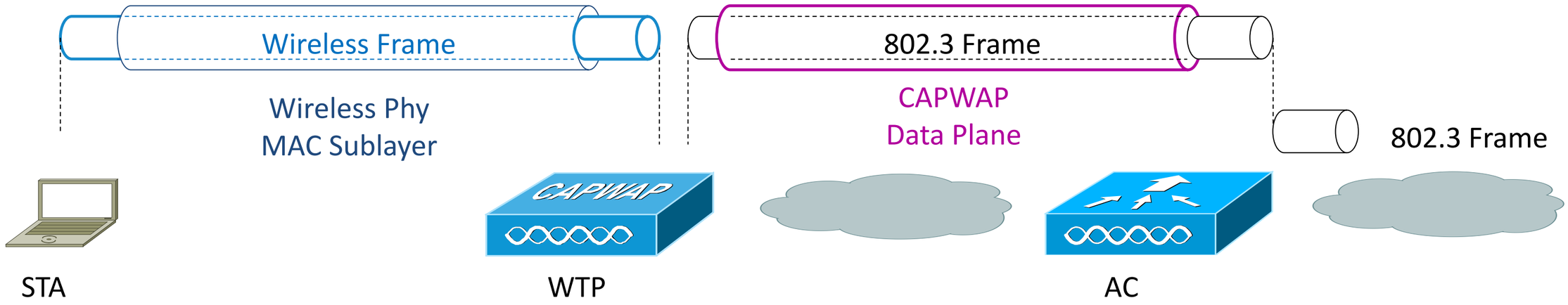


- **FlexConnect supports locally bridged MAC and split MAC per SSID**

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



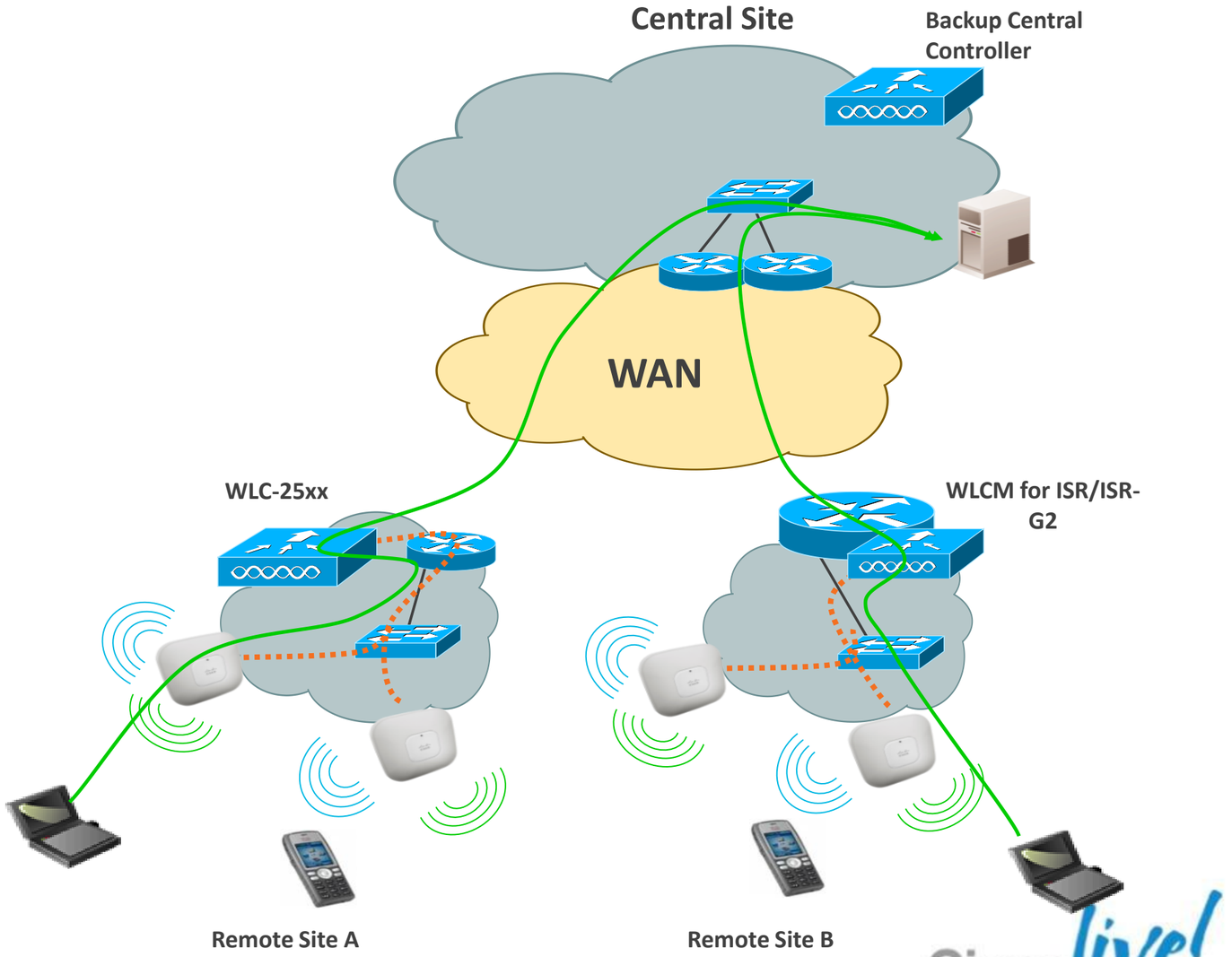
- Tunneled local MAC is not supported by Cisco

Wireless Branch Deployment Options

Branch Office with Local WLAN Controller

Overview

- Branches can also have local remote controllers
- Small form factor WLC are available to for small campus: WLC-25xx, integrated controller modules in ISR/ISR-G2, or Catalyst 3850 Switch
- 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
- AAA-ACL & QoS Override

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

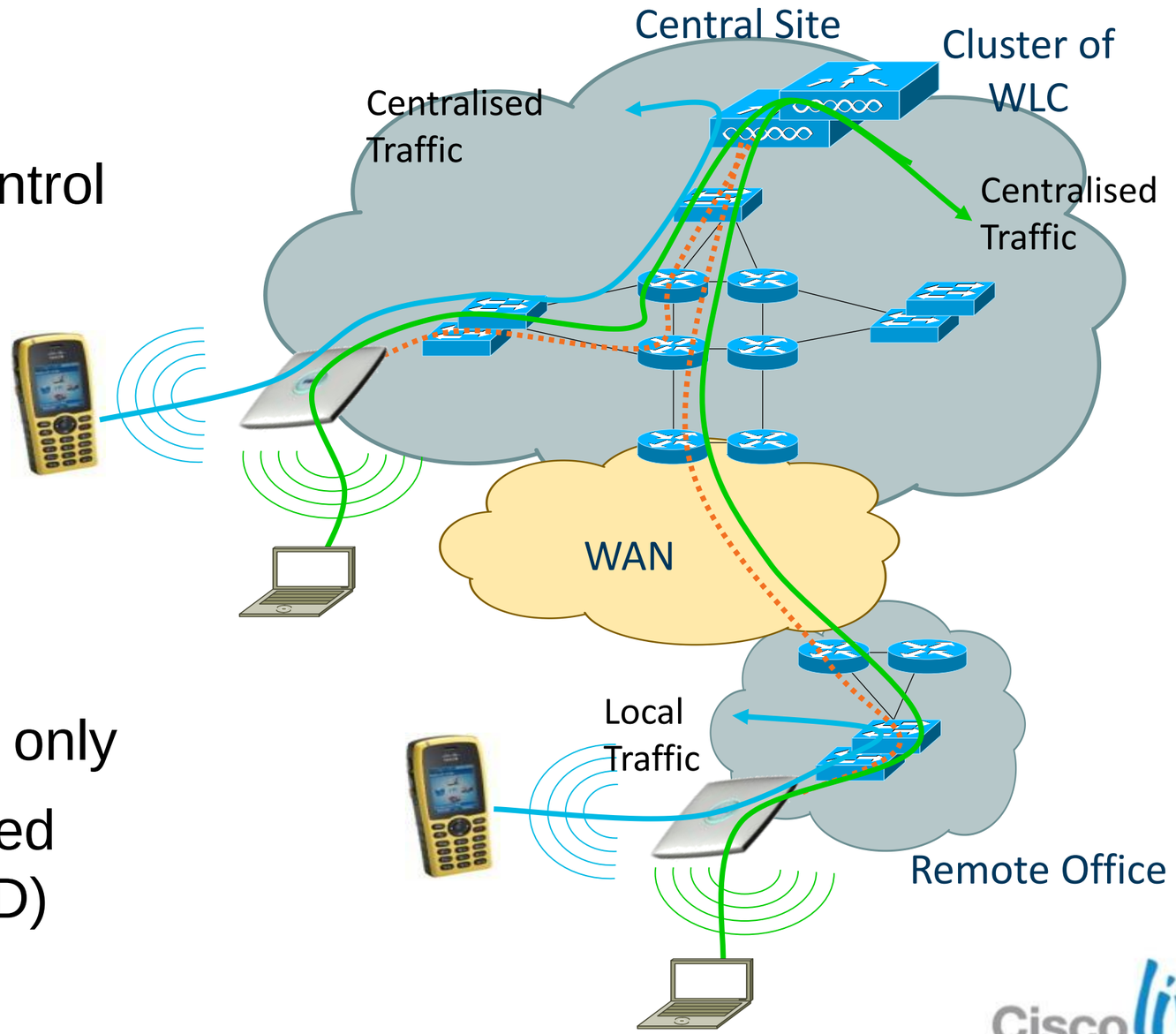
FlexConnect (HREAP)

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

  Centralised 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

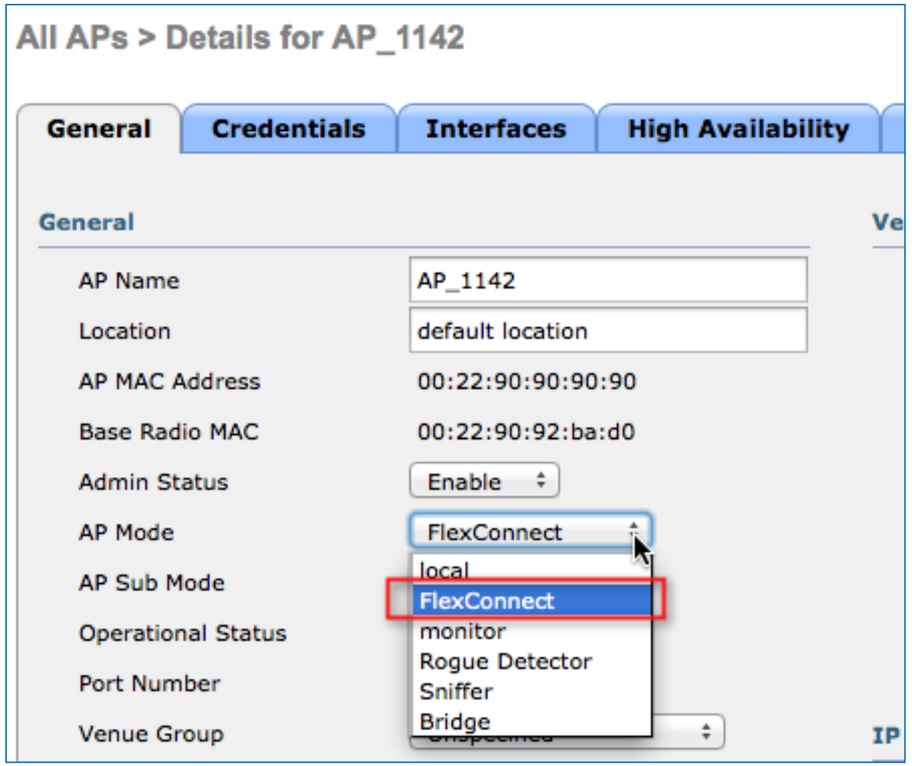
- **Connected Mode** – When FlexConnect can reach Controller (connected state), it gets help from controller to complete client authentication.
- **Standalone mode** – When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.

- **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

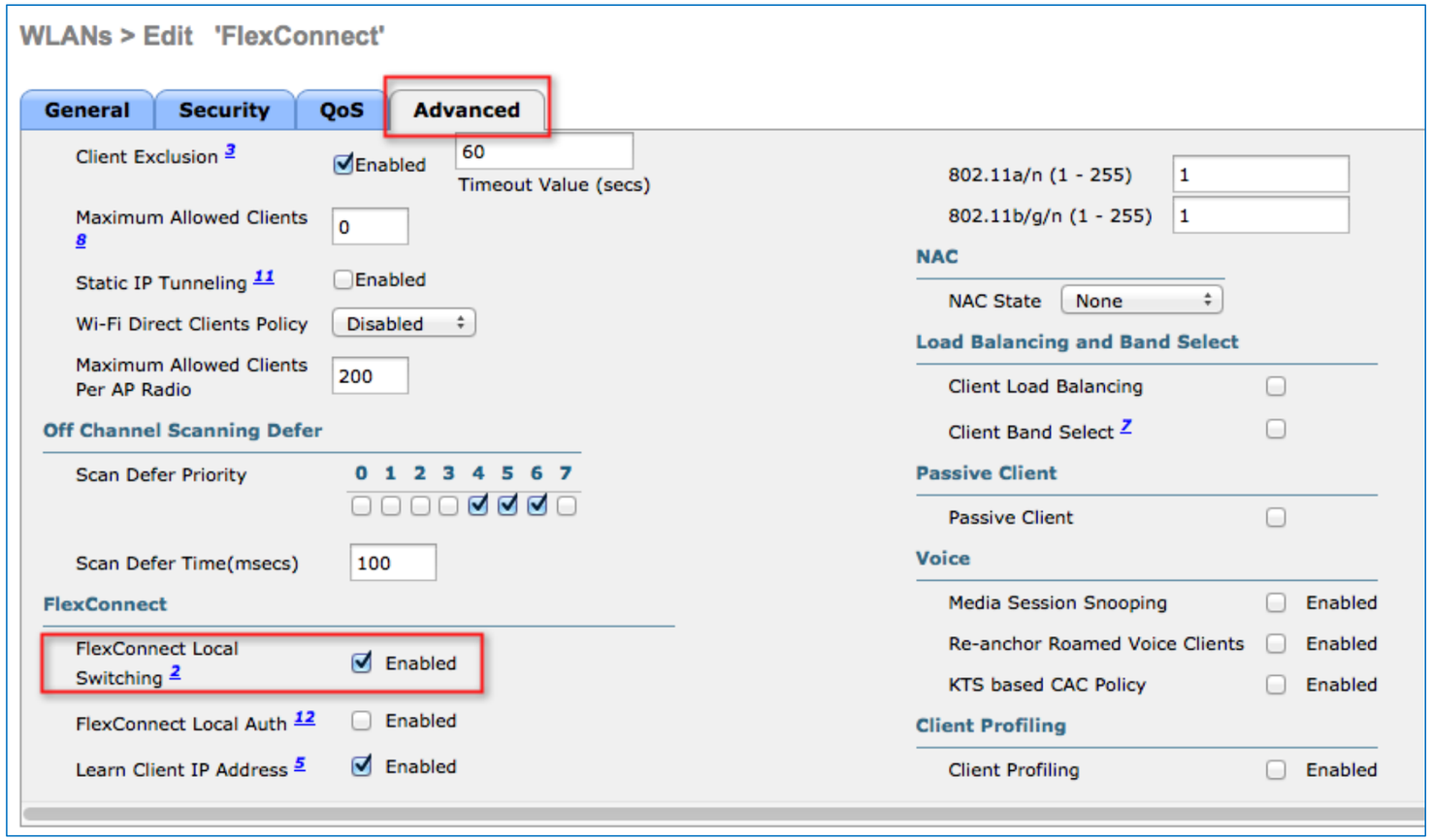
- Enable FlexConnect mode per AP
- Supported AP: AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600, AP-2600, AP-3600



Configure FlexConnect Local Switching

Step 2: Enable Local Switching per WLAN

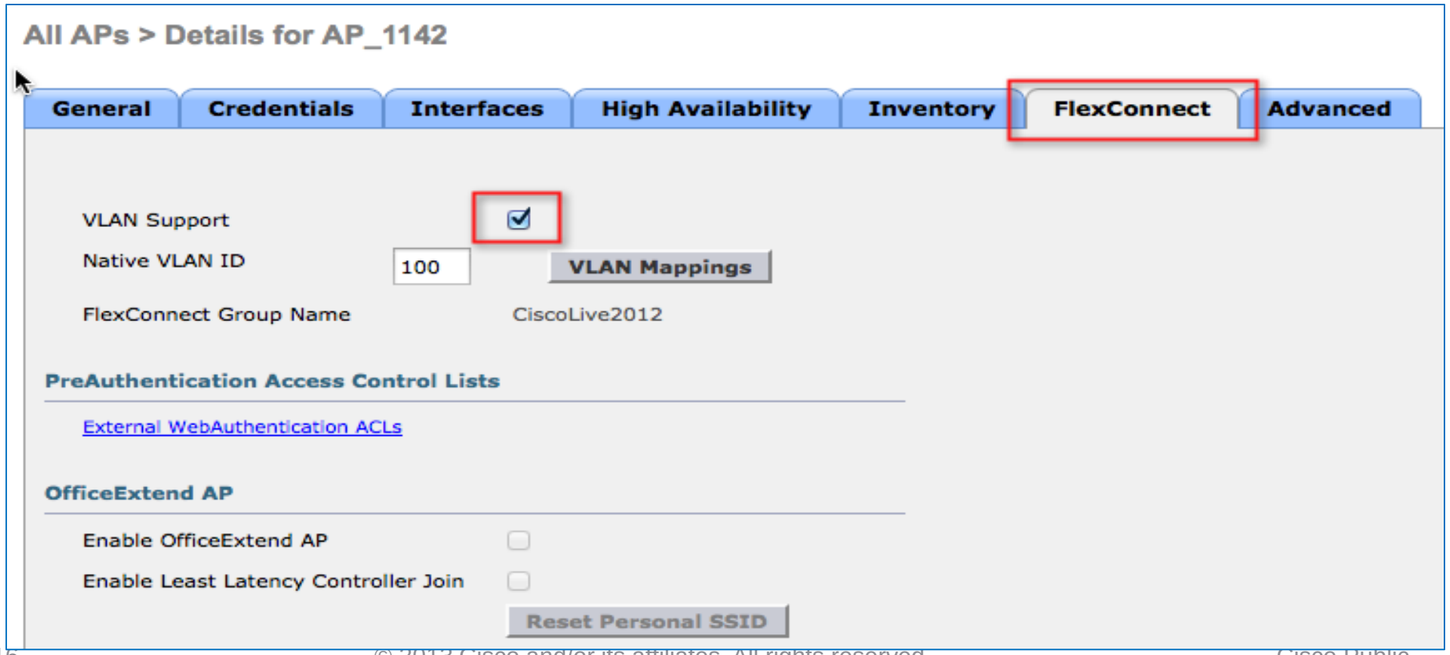
- Only WLAN with “FlexConnect Local Switching” enabled will allow local switching on the FlexConnect AP



Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

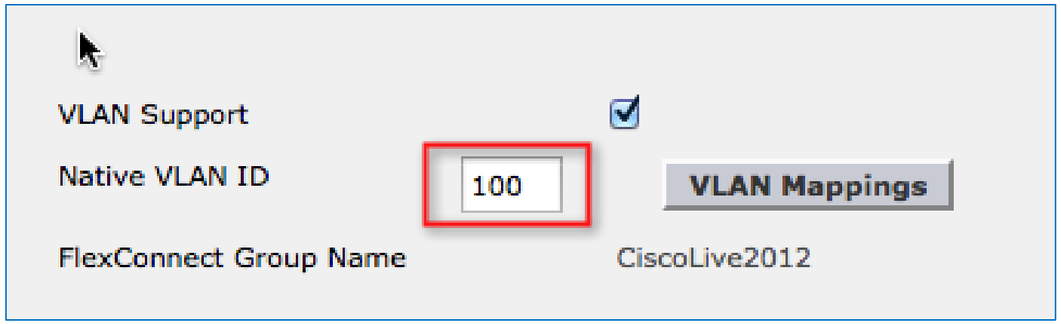
- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN Support provides the ability to configure remote VLAN to WLAN mappings. VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using Prime Infrastructure templates



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.

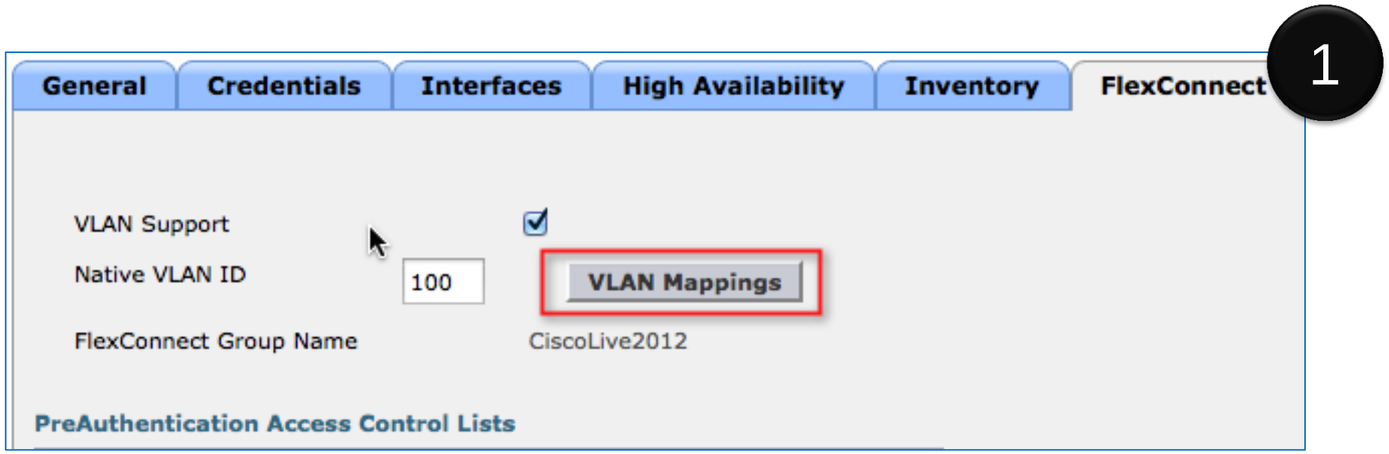


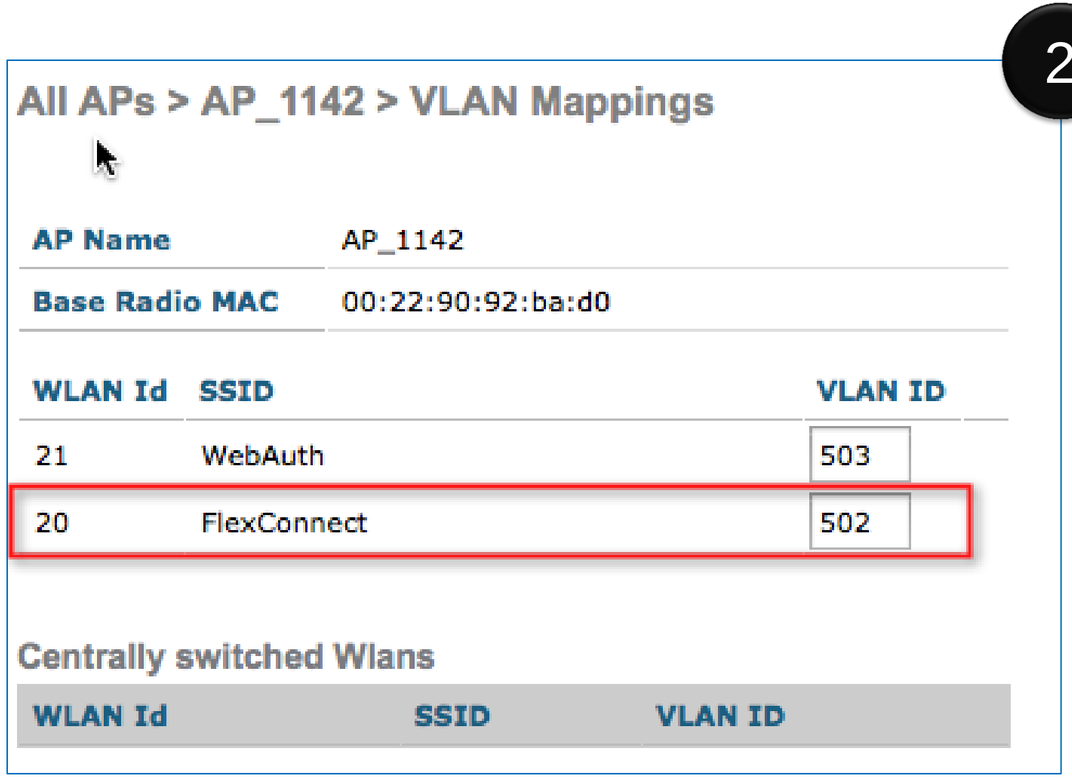

```
Current configuration : 227 bytes
!
interface GigabitEthernet0/37
 switchport access vlan 100
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,502-504
 switchport mode trunk
 spanning-tree portfast
end
```

Configure FlexConnect VLAN Mapping

Step 5: Per AP SSID to VLAN Mapping

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



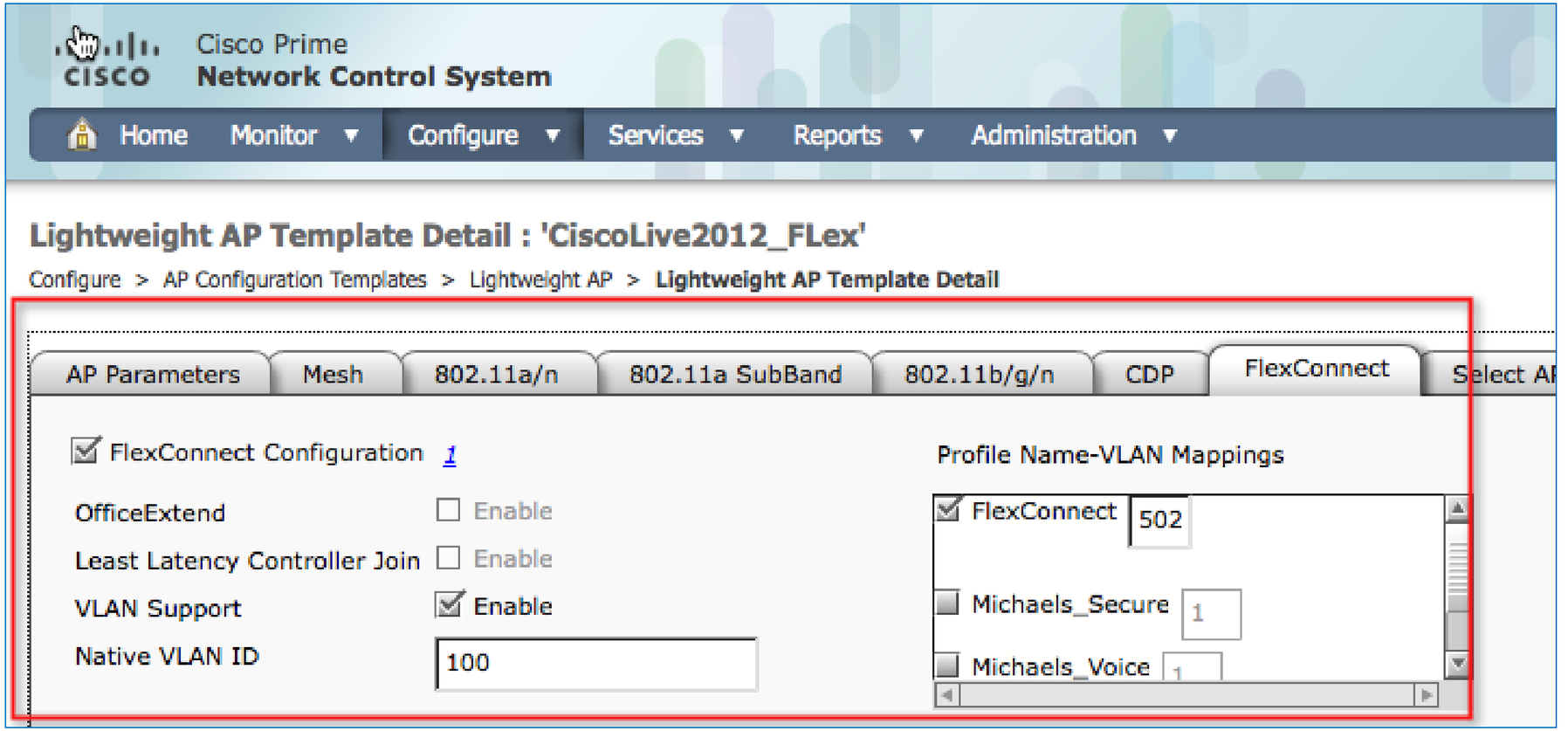


- Or the use of NCS via configuration templates

Configure FlexConnect VLAN Mapping

Step 6: Using NCS

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



Evaluate FlexConnect Architectural Requirements

FlexConnect Design Considerations

WAN Limitations Apply

For Your Reference

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
  - Mesh AP
  - VideoStream
  - IPv6 L3 Mobility
  - SXP TrustSec
  - AAA ACL & QoS override
  - 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	6000
Access Points / Branch	100
Deployment Model	FlexConnect
Form Factor	1 RU
IO Interface	2 x 10GE
Upgrade Licenses	100, 200, 500, 1K

Key Differentiation

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

Flex 7500 Scale & Feature Update - 7.0.116.0 to 7.4

Scalability	7.0.116.0	7.2	7.4
Total APs	2000	3000	6000
Total Clients	20,000	30,000	64,000
Total FlexConnect Group	500	1000	2000
Support for OEAPs	No	Yes	Yes
Central Switching BW Limit	~250 Mb	~1 Gb	~1 Gb
Data DTLS Support	No	Yes	Yes
Central Switching 802.1x	No	Yes	Yes

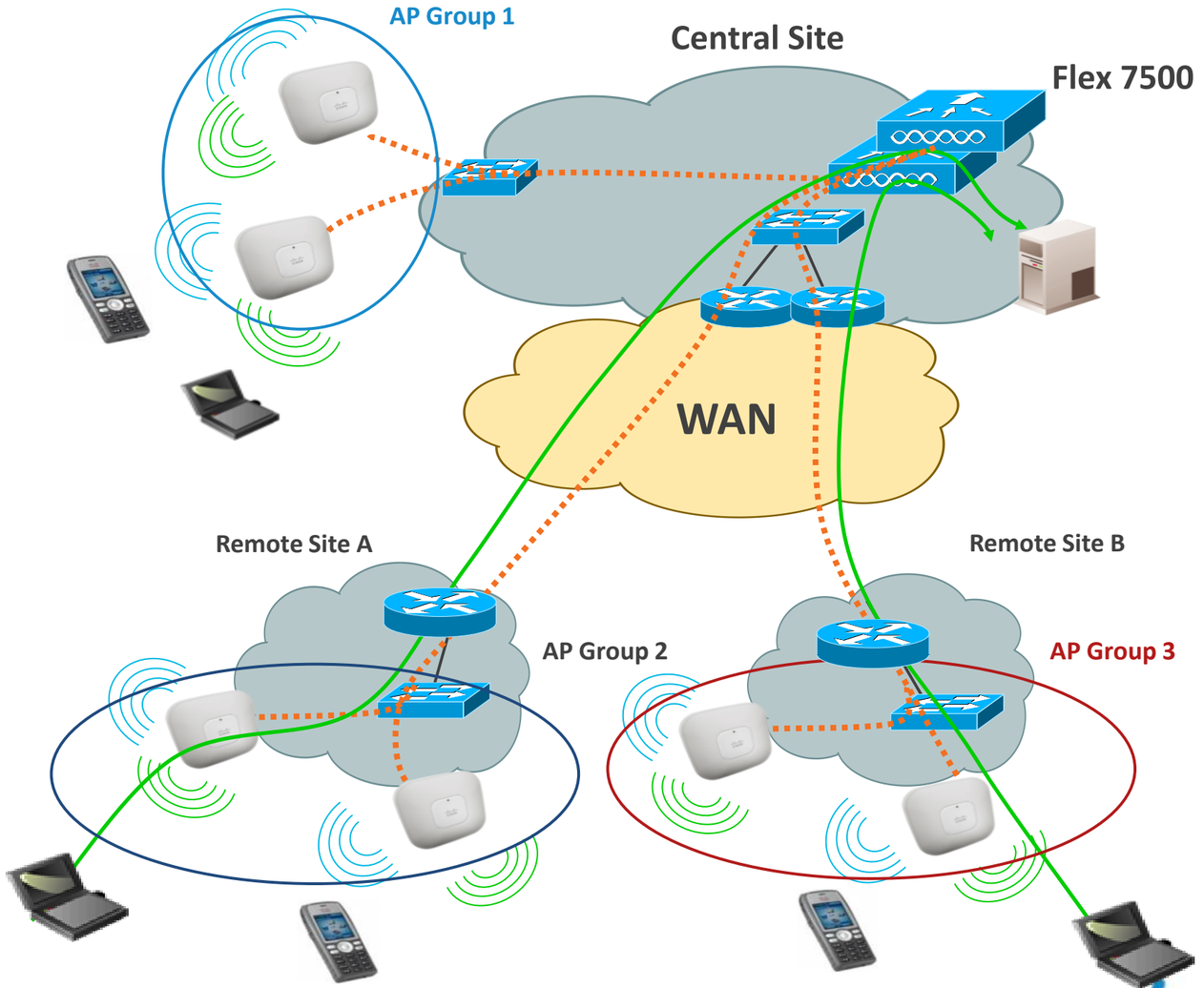
FlexConnect Improvements in Release 7.3 & 7.4

- AAA-VLAN over ride in Local Switching
- ACL support in Local Switching
- P2P Blocking support in Local Switching
- Smart AP Image Upgrade
- External Web-Auth support for Guest Deployments in Local Switching
- Mobile Device On-boarding support in Local Switching
- WGB/uWGB Support for Local Switching WLANs
- VLAN Based Central Switching
- Split Tunnelling

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 group



Scaling	Flex 7500	CT-5508	WiSM-2	CT-2504
# AP Groups	2000	512	512	30
# WLAN (SSID)	512	512	512	16
# VLAN (Interfaces)	512	512	512	16

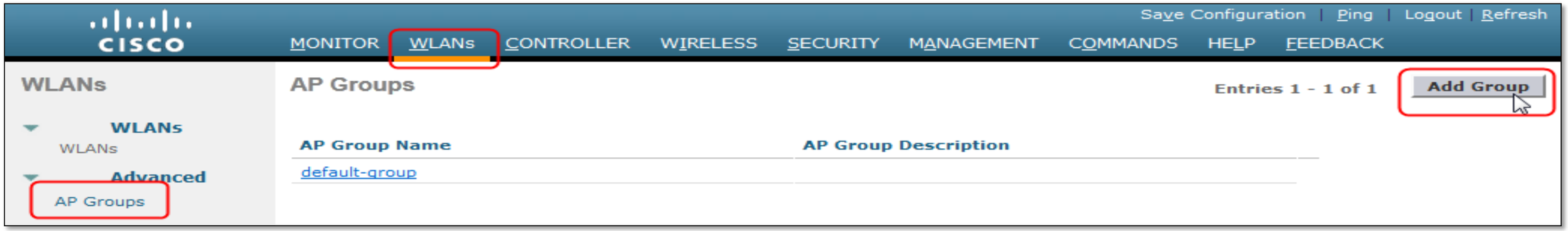
Understanding AP Groups

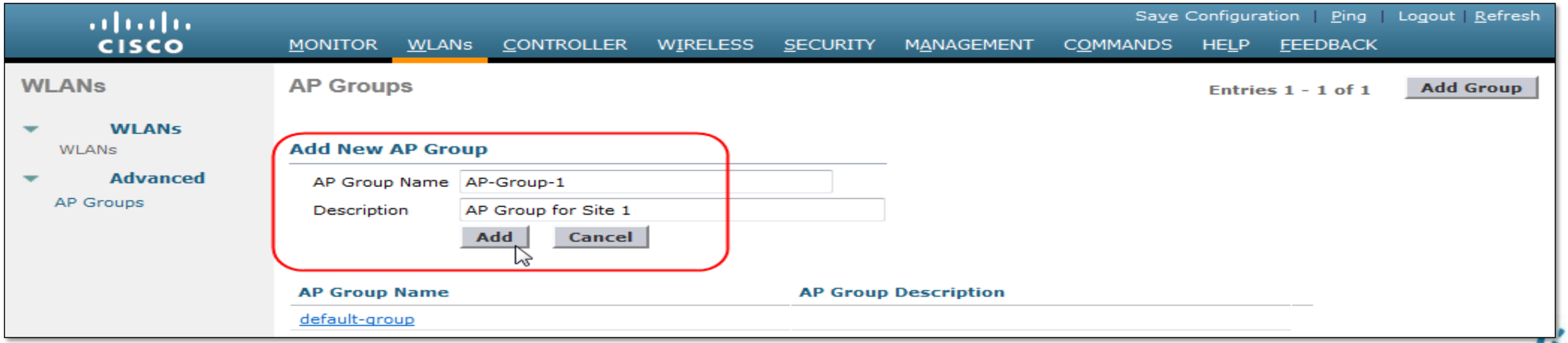
Rules to Know

- **Rules**
  - An 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

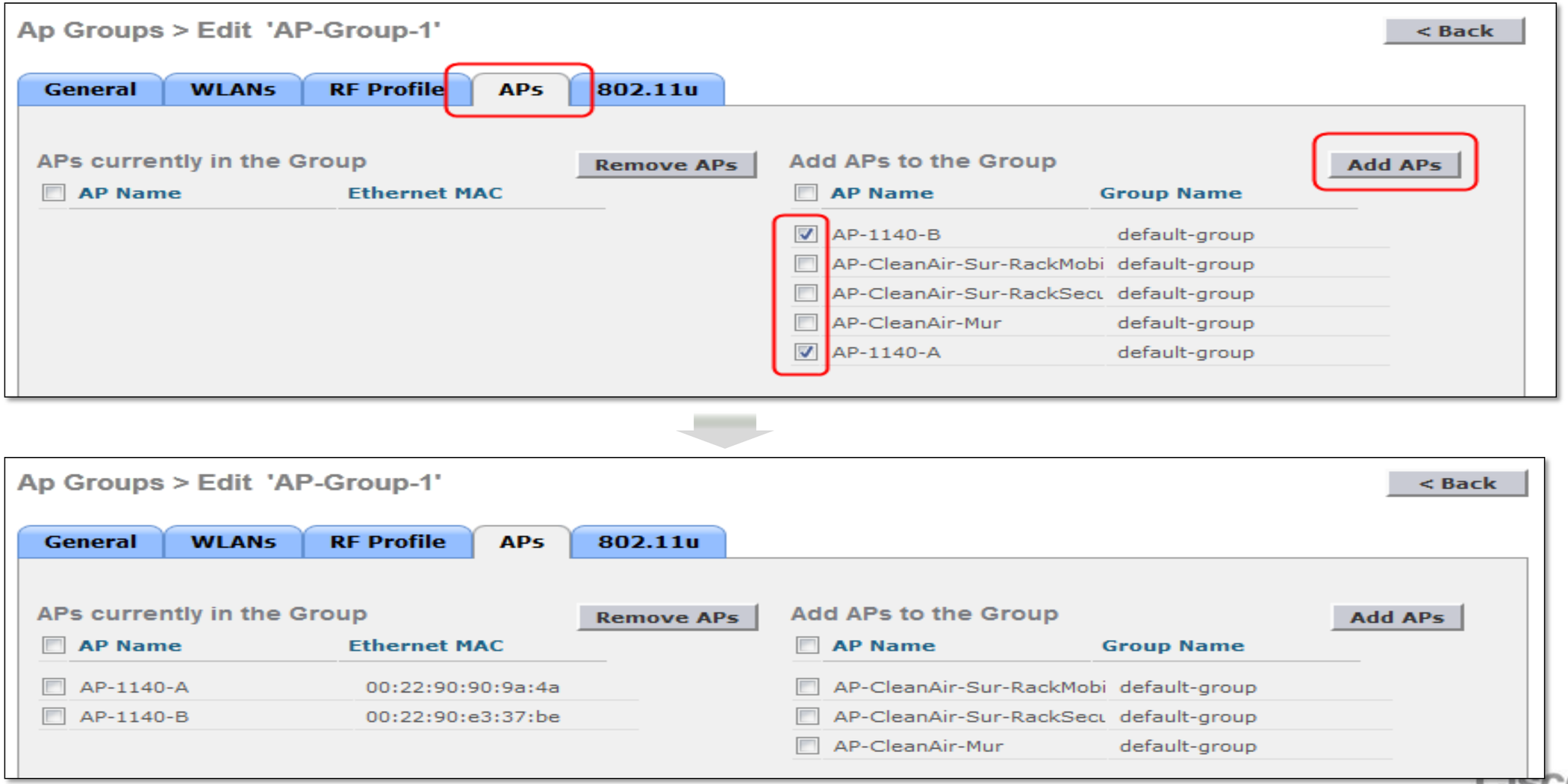
Configuration: Create a New Group





AP Groups

Configuration: Add AP or APs to Group



AP Groups Usage

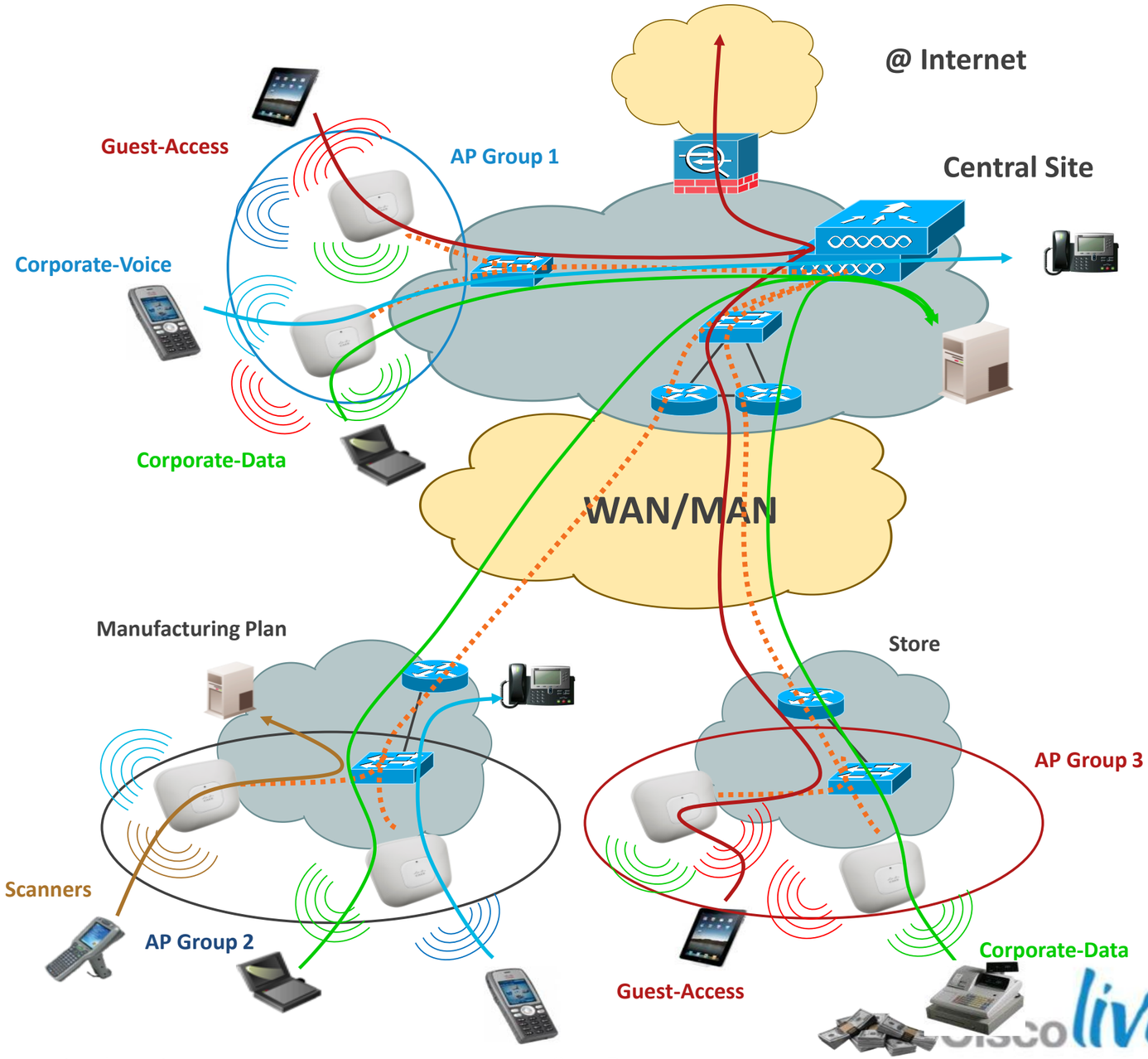
Per Location SSID

- 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 Plant**

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

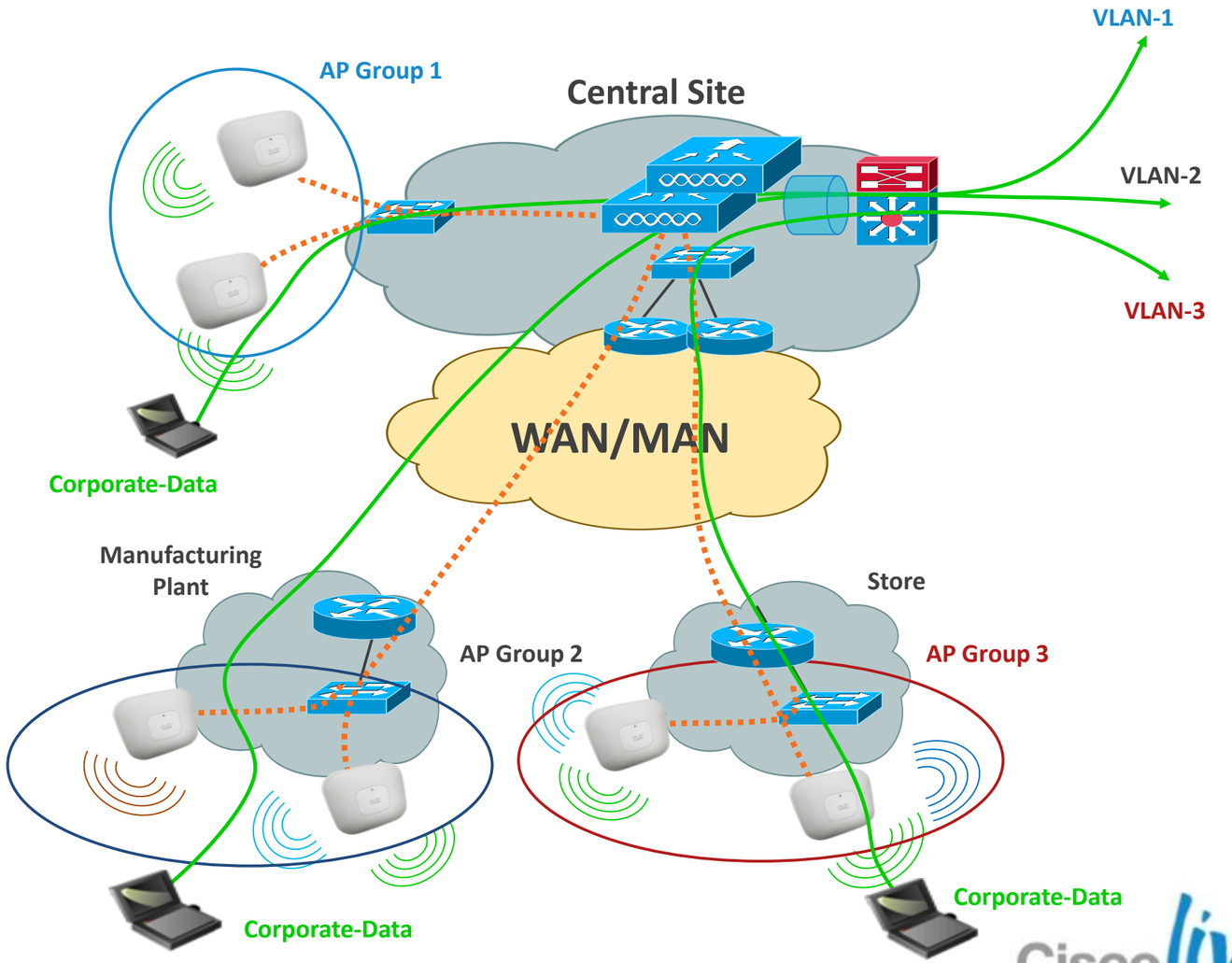
    Corporate-Data,
    Guest-Access



AP Groups Usage

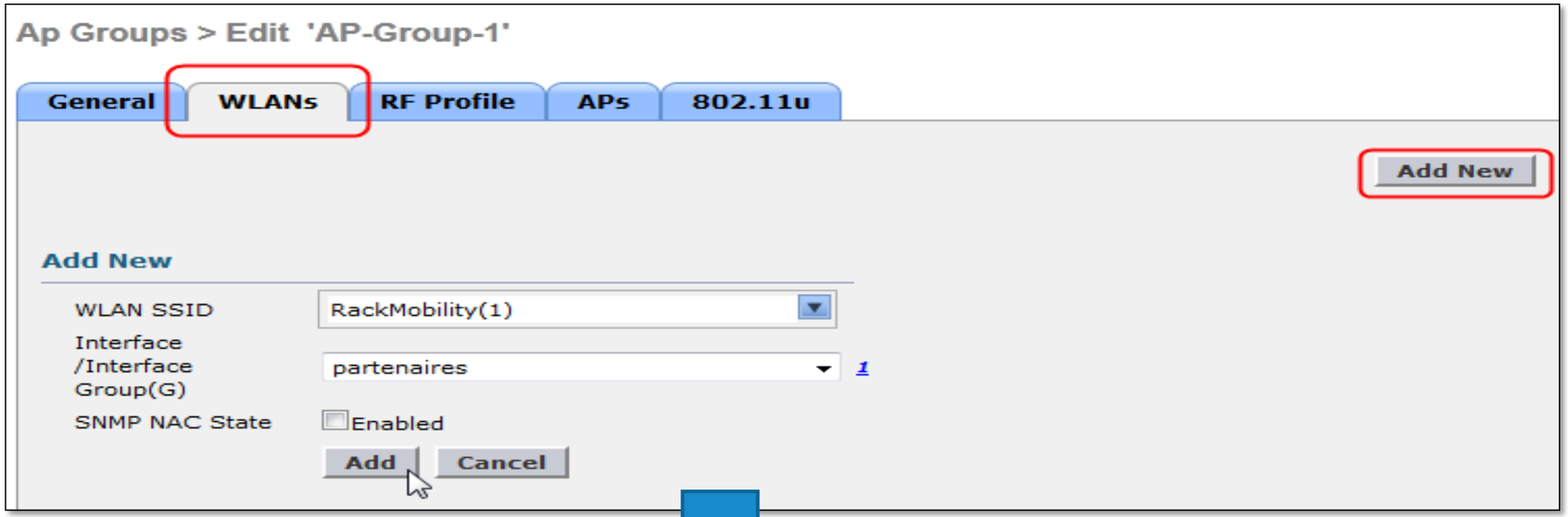
Per AP Group SSID to VLAN Mapping

- 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 and 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

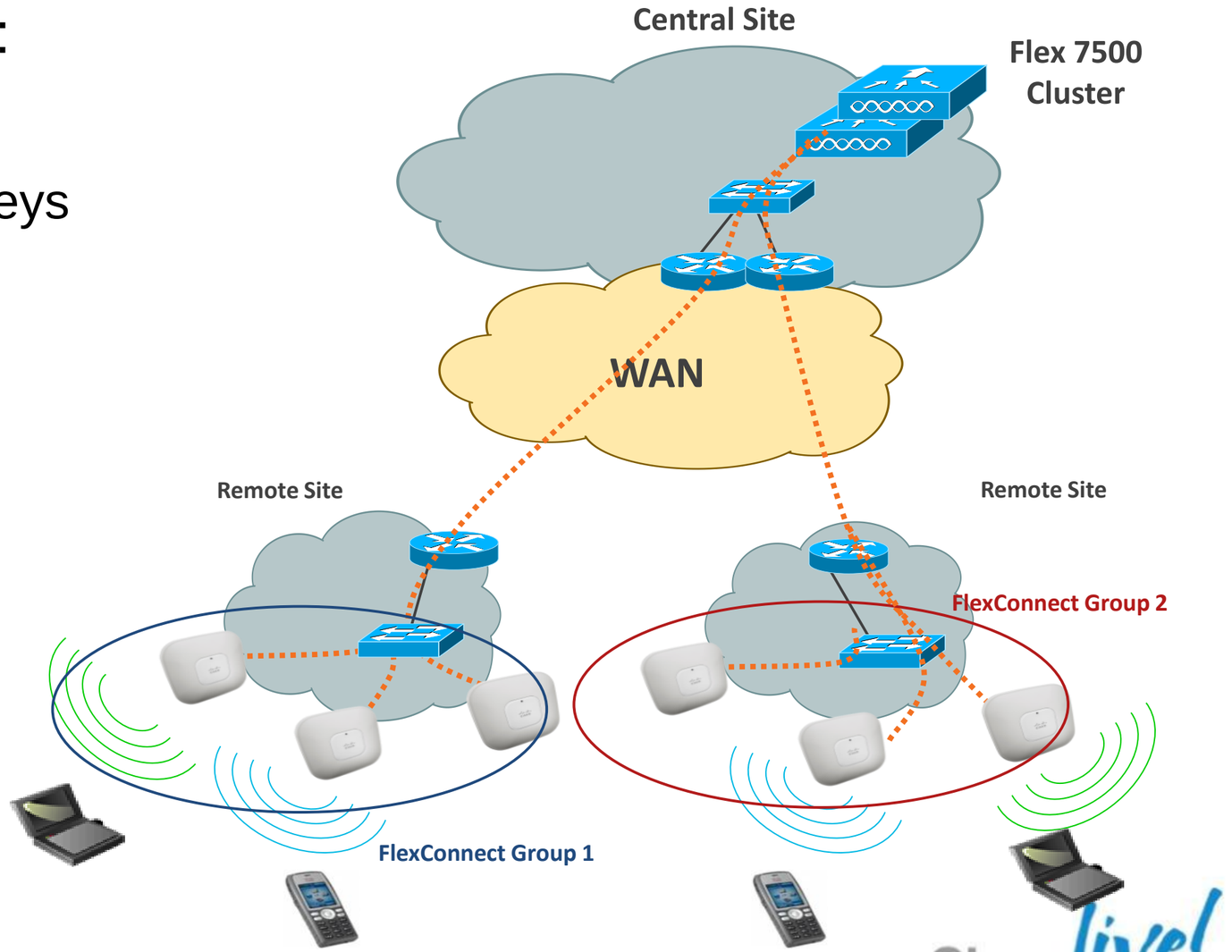


Understanding FlexConnect Groups

Overview

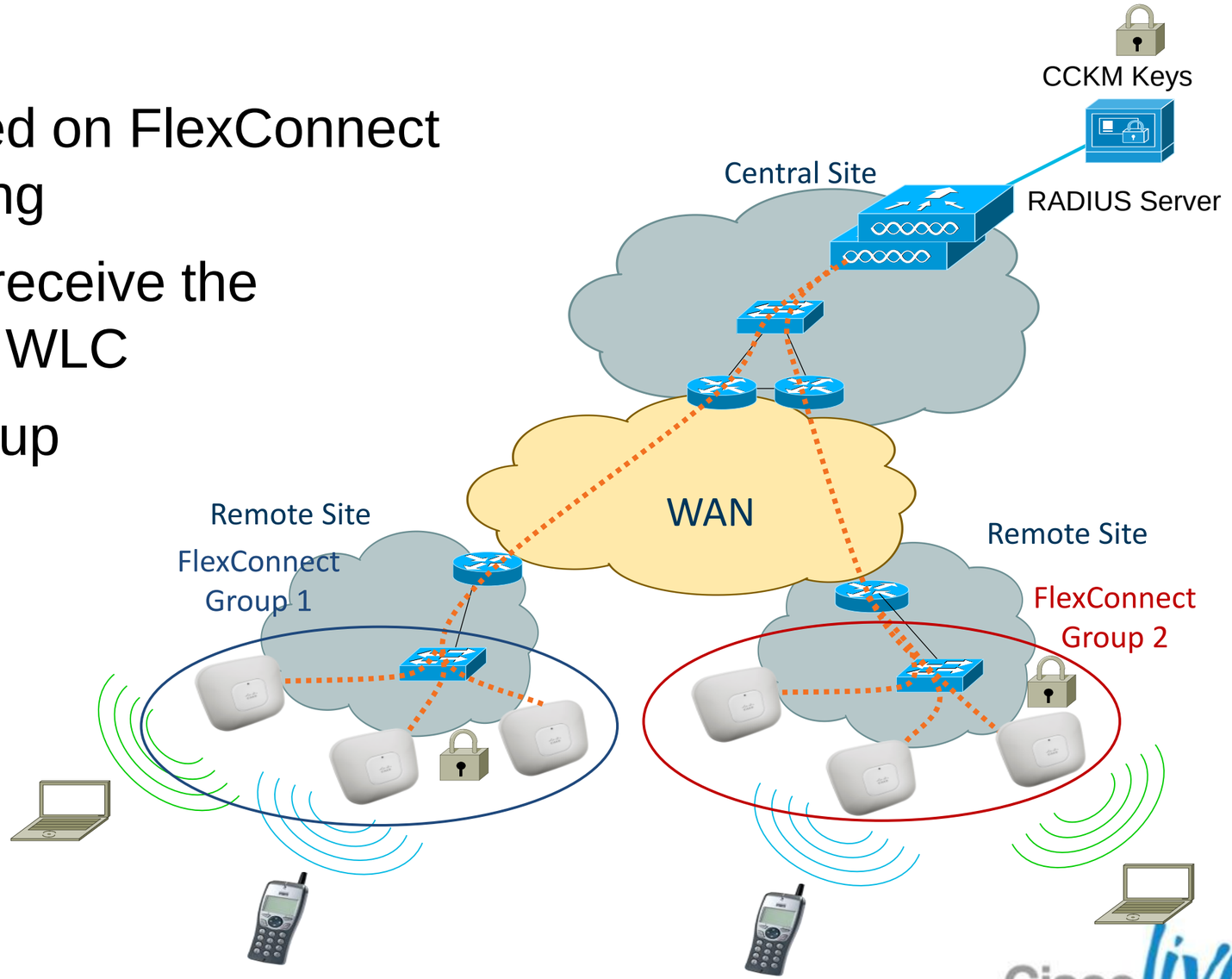
- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade
- Scaling information

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504
FlexConnect Groups	2000	100	100	20
AP per Group	100	25	25	25



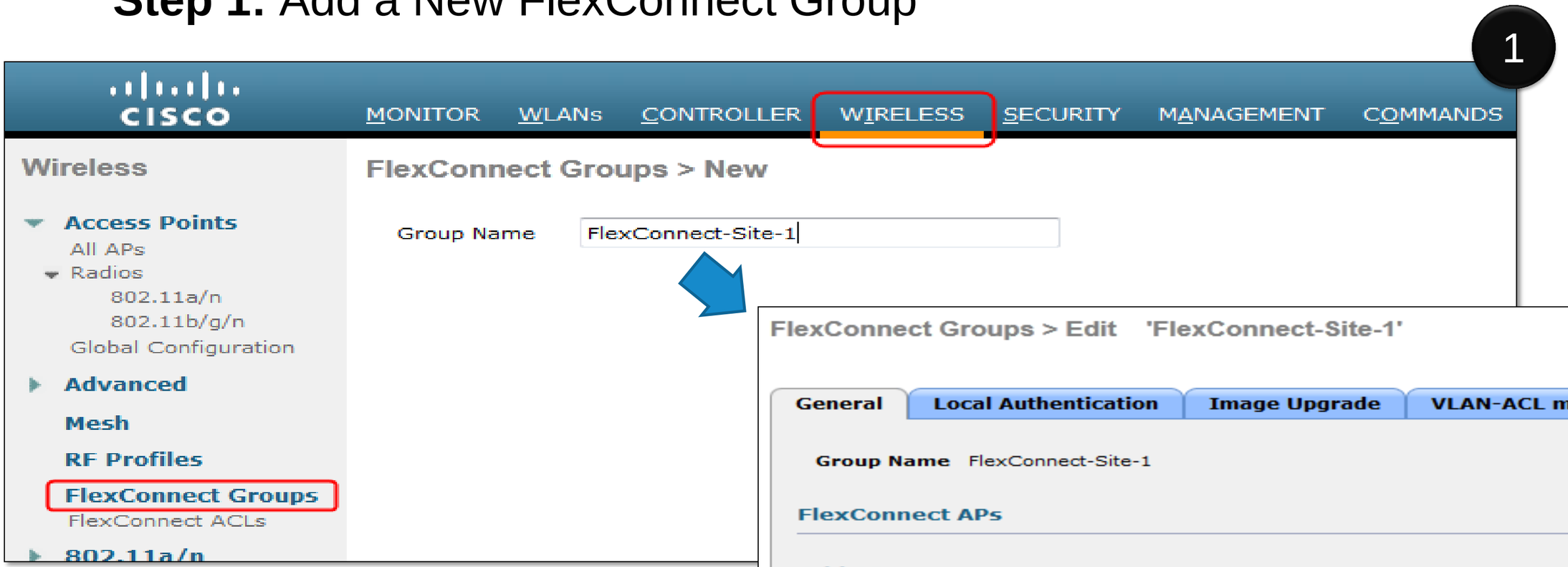
FlexConnect Groups and CCKM/OKC Keys

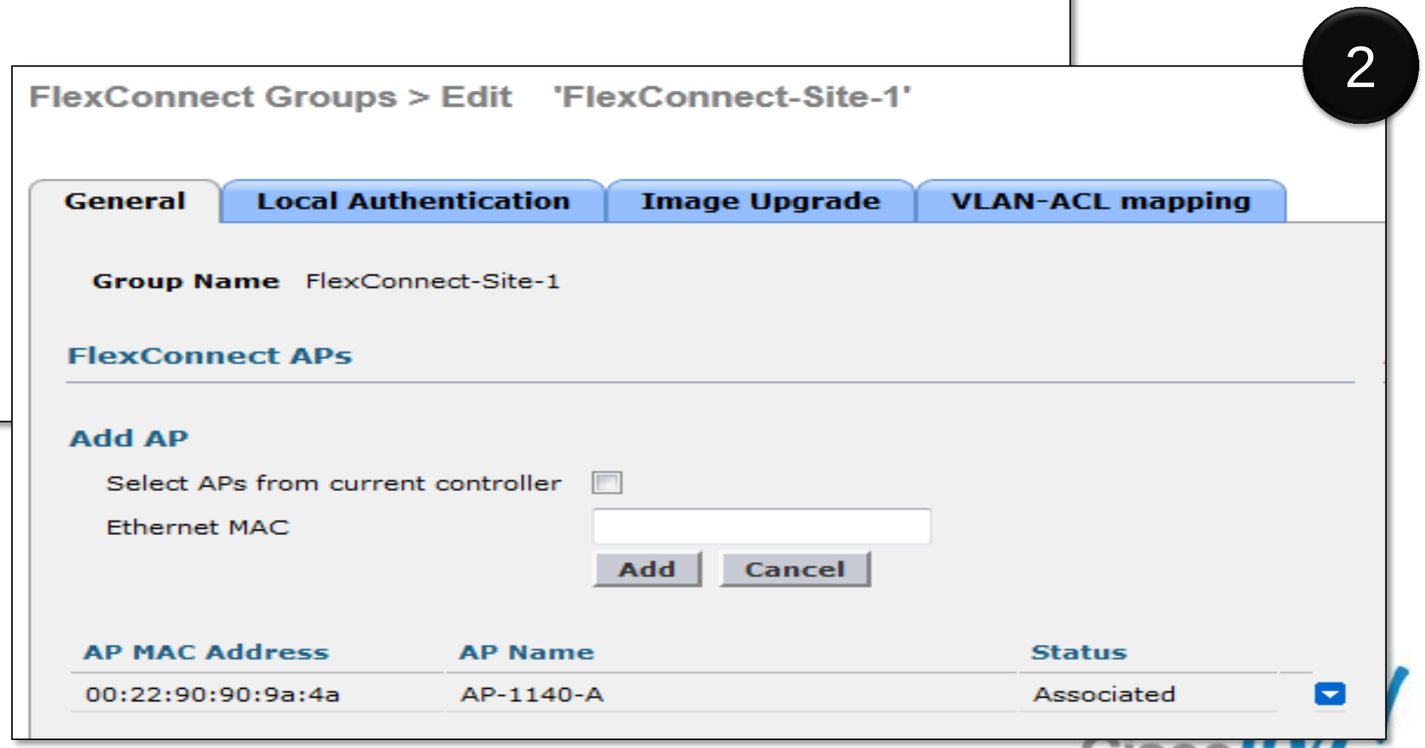
- CCKM/OKC keys are stored on FlexConnect APs for Layer 2 fast roaming
- The FlexConnect APs will receive the CCKM/OKC keys from the WLC
- If a FlexConnect AP boots up in standalone mode, it will not get the OKC/CCKM keys from the WLC so fast roaming will not be supported



FlexConnect Groups Creation

Step 1: Add a New FlexConnect Group





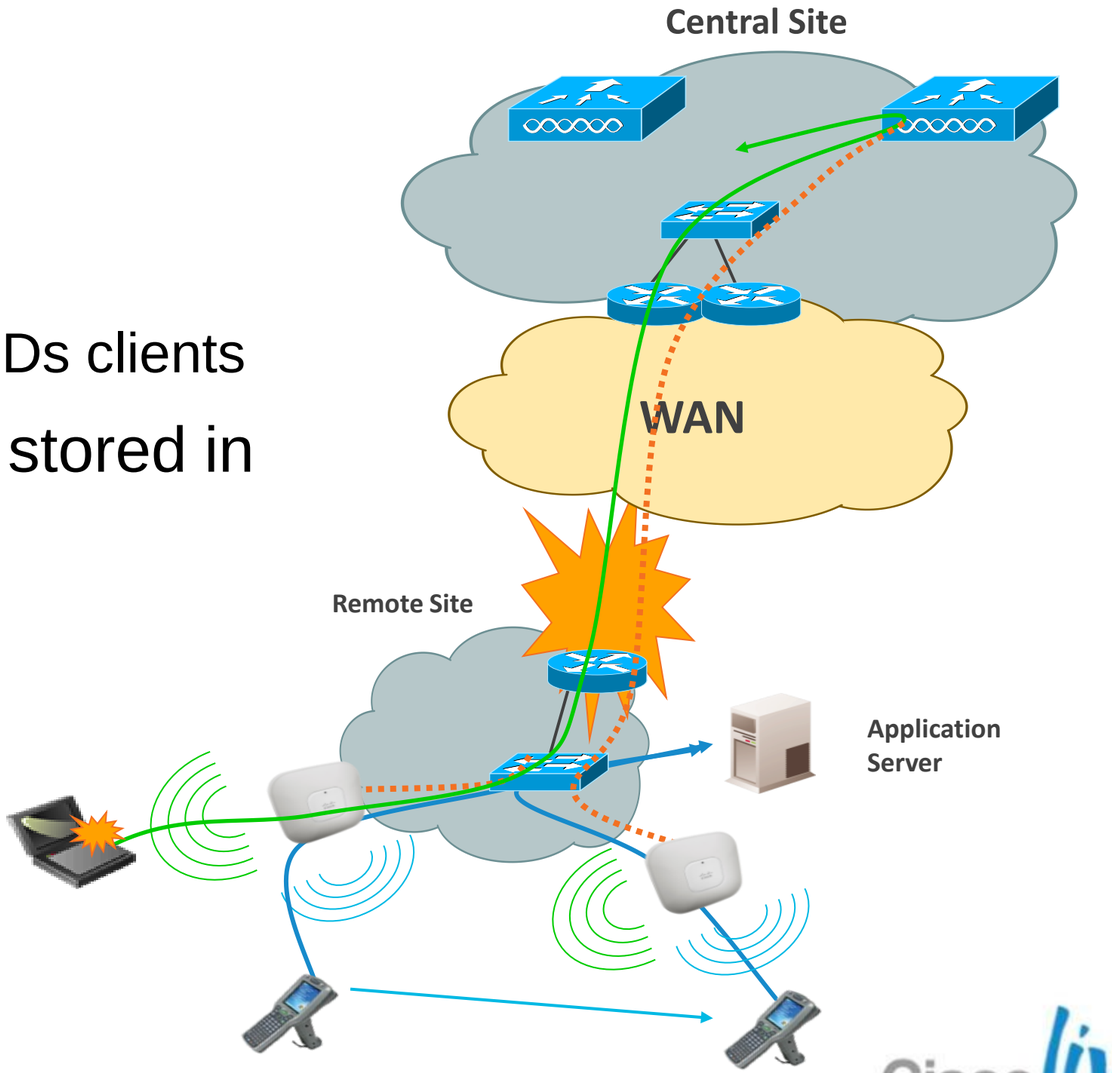
Step 2: Add APs to the FlexConnect Group

Design Wireless Branch
Designing a Resilient Network

FlexConnect Backup Scenario

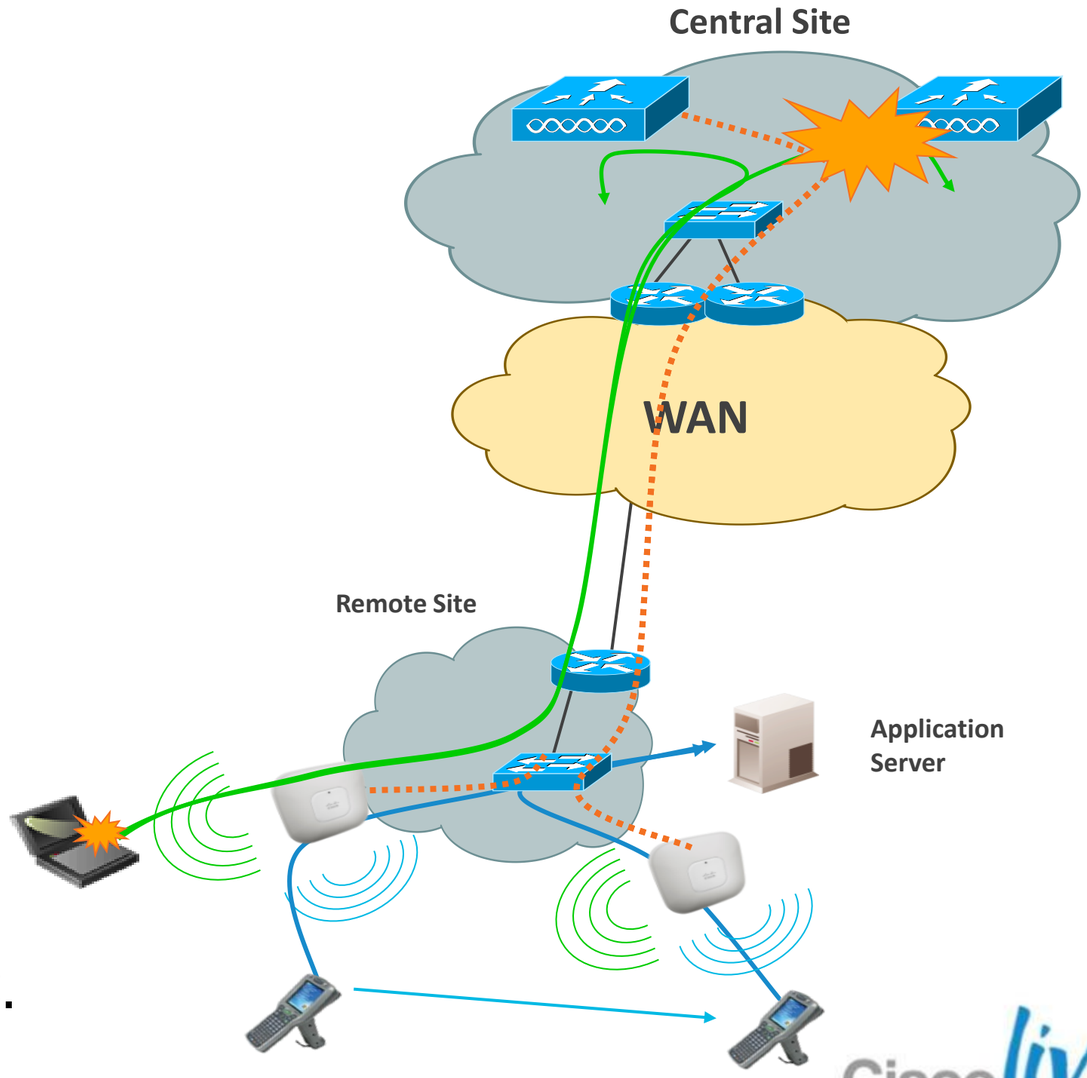
WAN Failure

- 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*

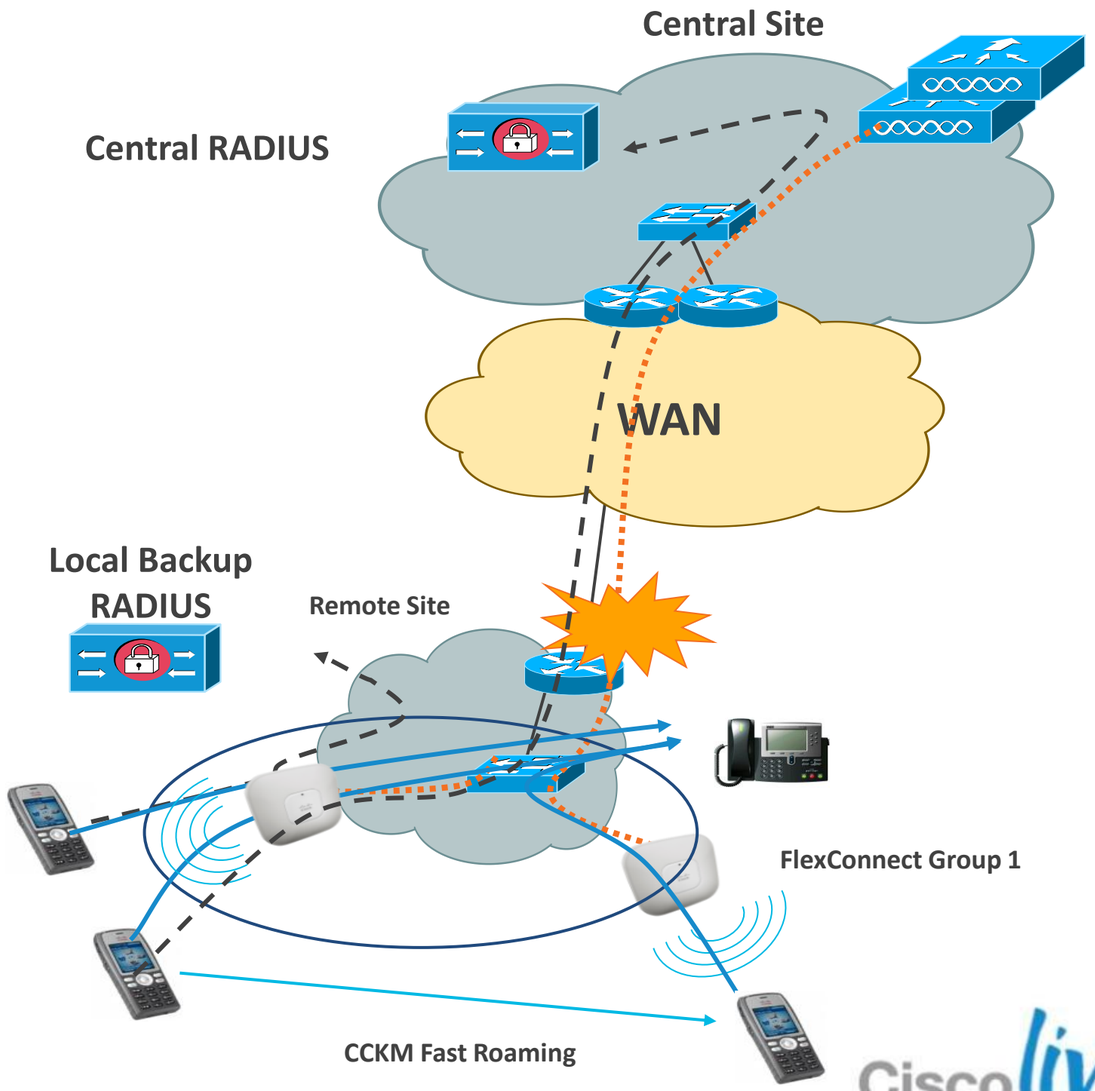
- FlexConnect will first backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with 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

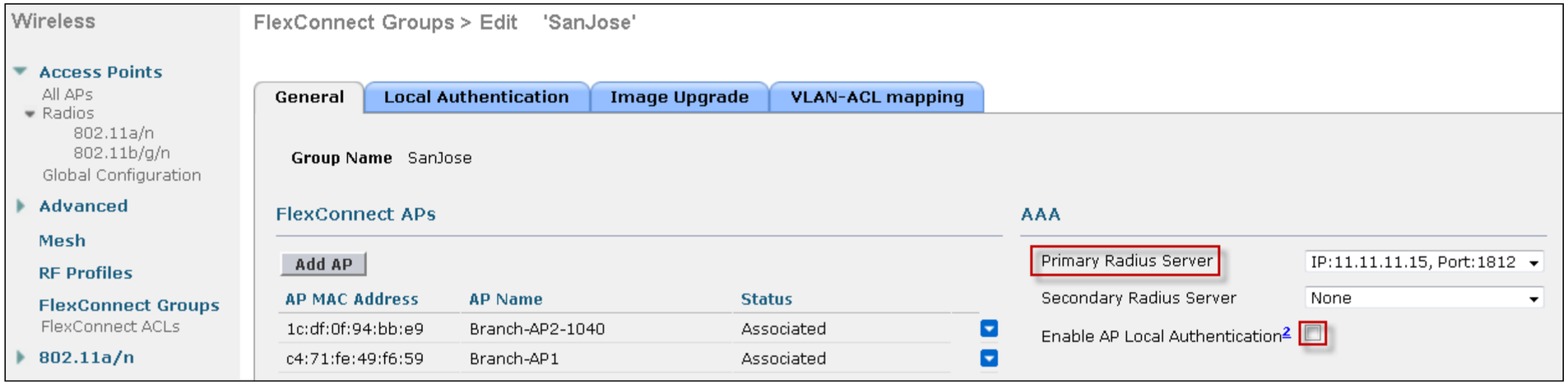
Backup Scenario

- 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



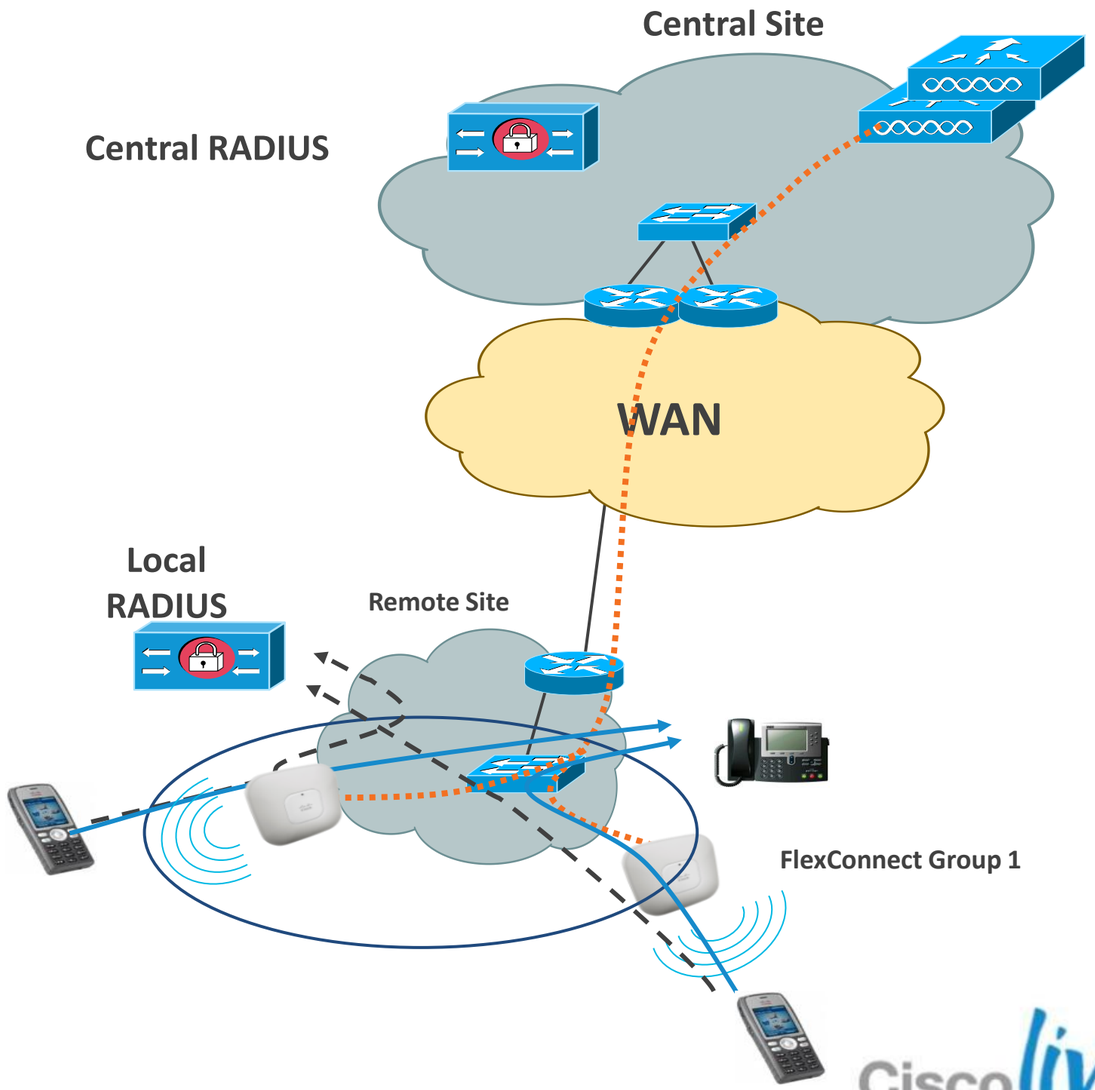
H-REAP Group: Local Backup RADIUS
Configuration

- Define primary and secondary local backup RADIUS server per H-REAP group



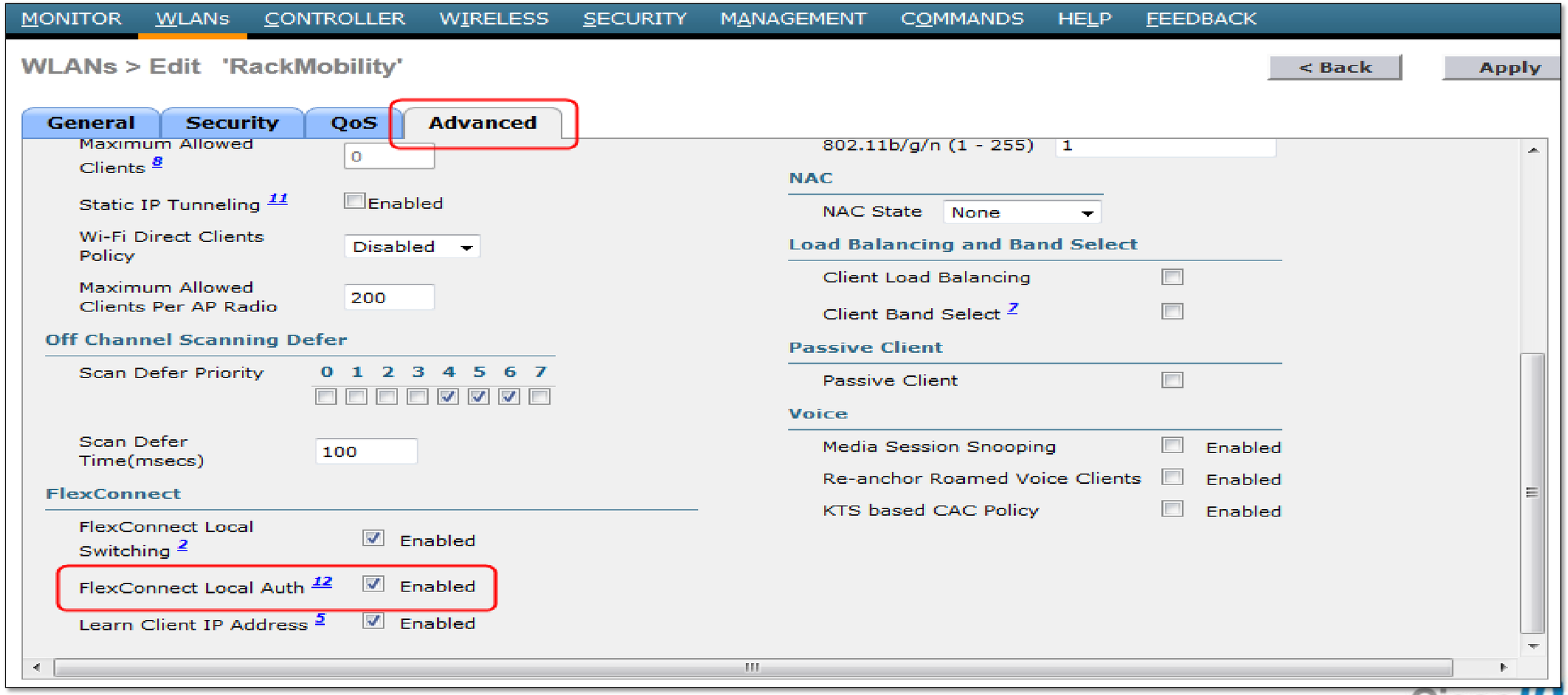
Local Authentication

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



Local Authentication

Configuration



FlexConnect Group: Local Backup Authentication

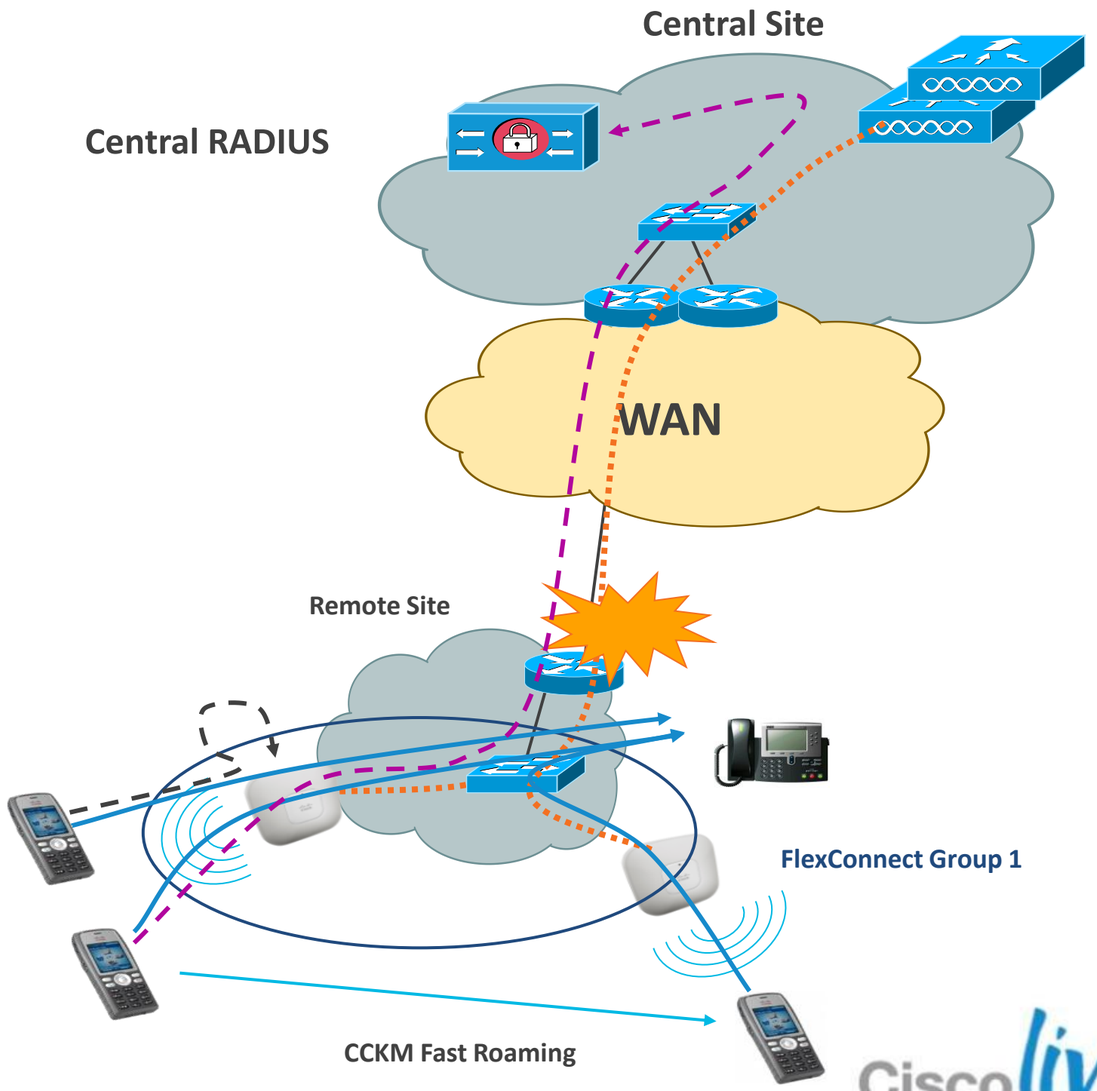
Backup Scenario

- 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

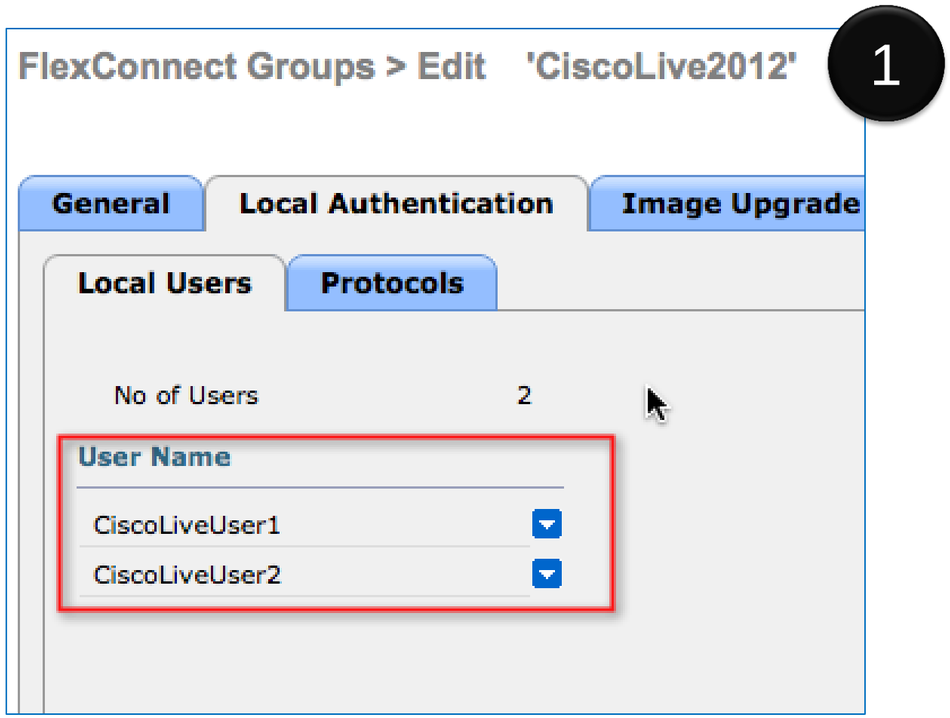
⚠ Only LEAP and EAP-FAST Supported

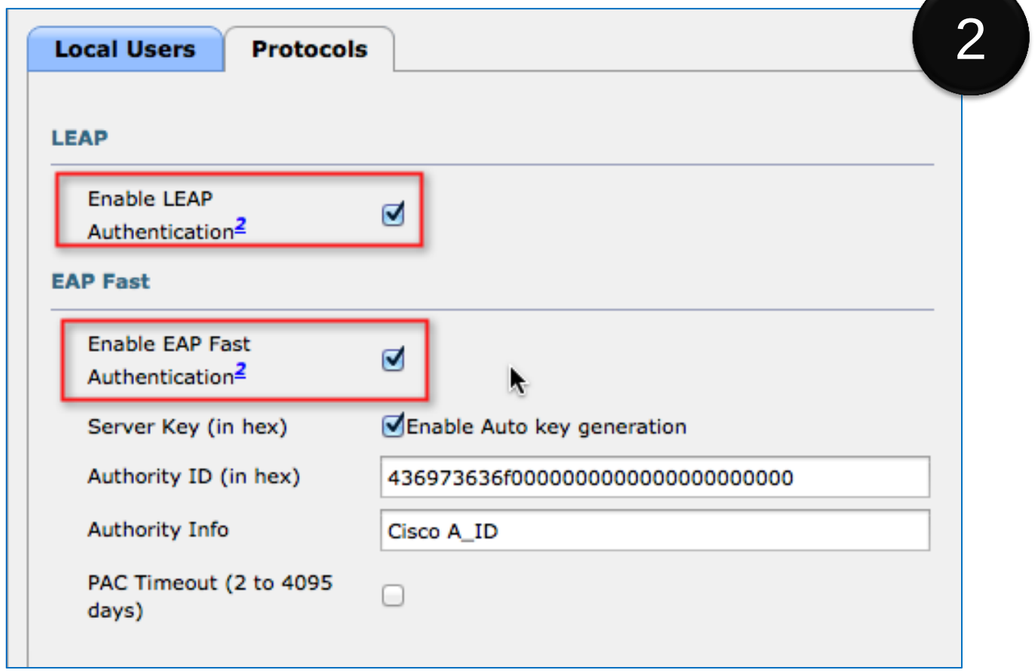


FlexConnect Group: Local Backup Authentication

Configuration

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





FlexConnect Backup Scenario

WAN Down Behaviour (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.

Not Supported Backup Scenario

AP Changing Mode on Failure

- AP can not automatically change from local mode to FlexConnect mode on local WLC failure

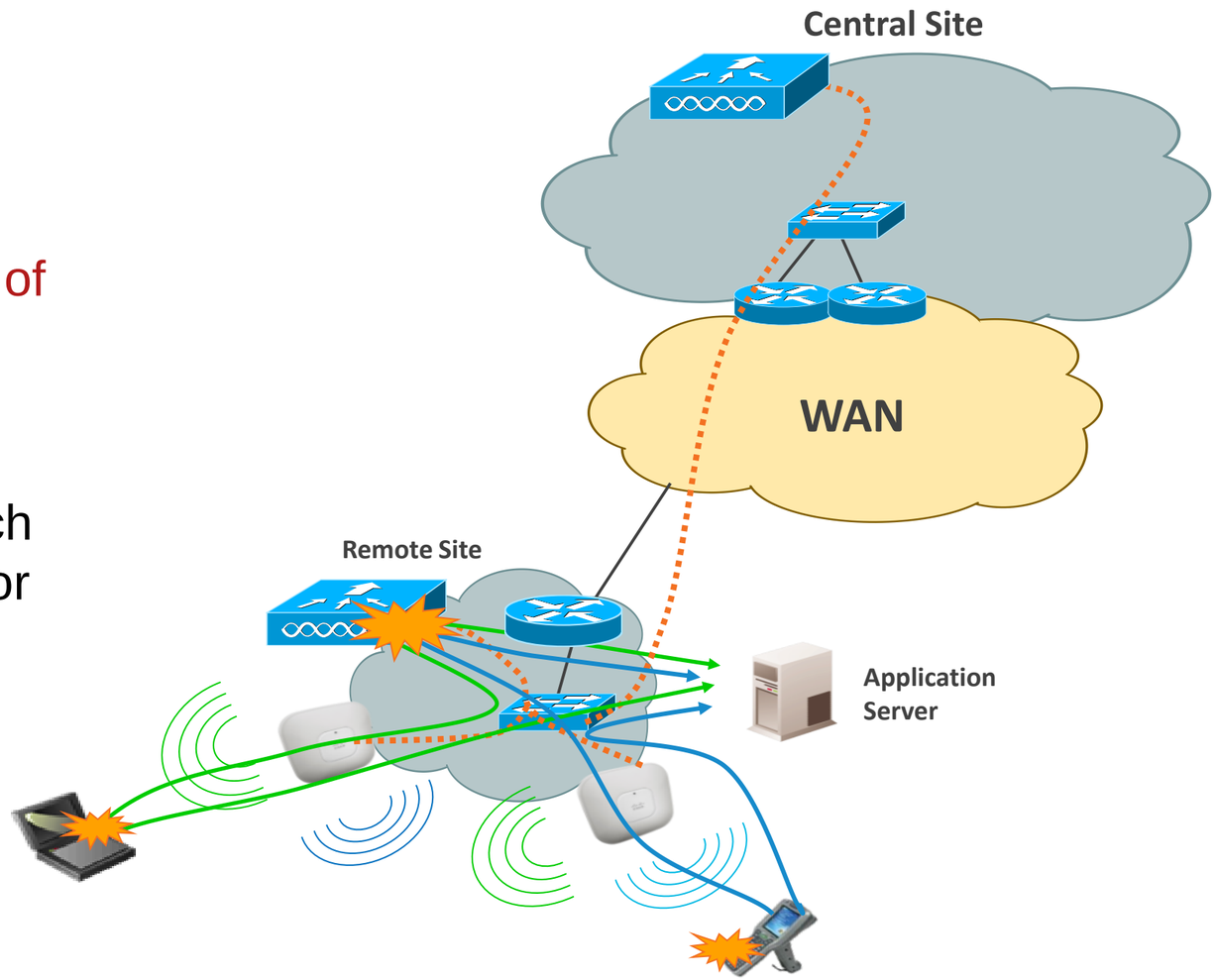
  Changing mode is a configuration task of the AP

- Why it does not make sense

  Need for dual configuration at the switch level (access port for central, 802.1Q for FlexConnect)

  Lost controller features when going to FlexConnect

  If you accept FlexConnect locally, then don't implement local WLC



Not Supported Backup Scenario

Not Supported Backup Scenario

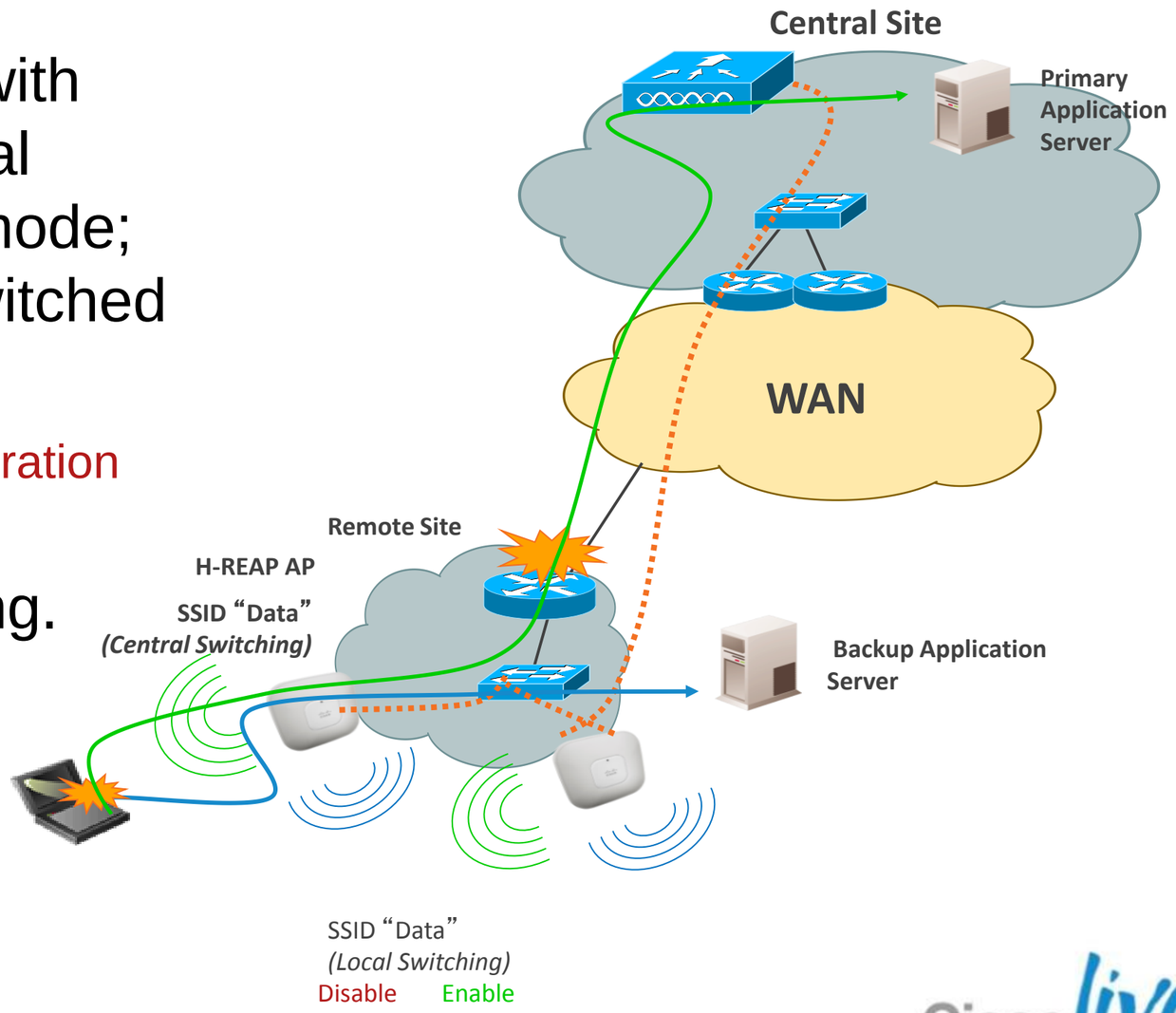
Auto-Enabling Backup Local Switching

- FlexConnect AP can not be configured with two SSID with same name; one in central switching mode, one in local switching mode; when central switching is down, local switched SSID becomes active

  Changing enable status of an SSID is a configuration task of the WLC level

- Cisco recommends using Local Switching. Why?

  Fault Tolerance will always keep client connection UP.



Not Supported Backup Scenario

Failover Matrix

For Your Reference

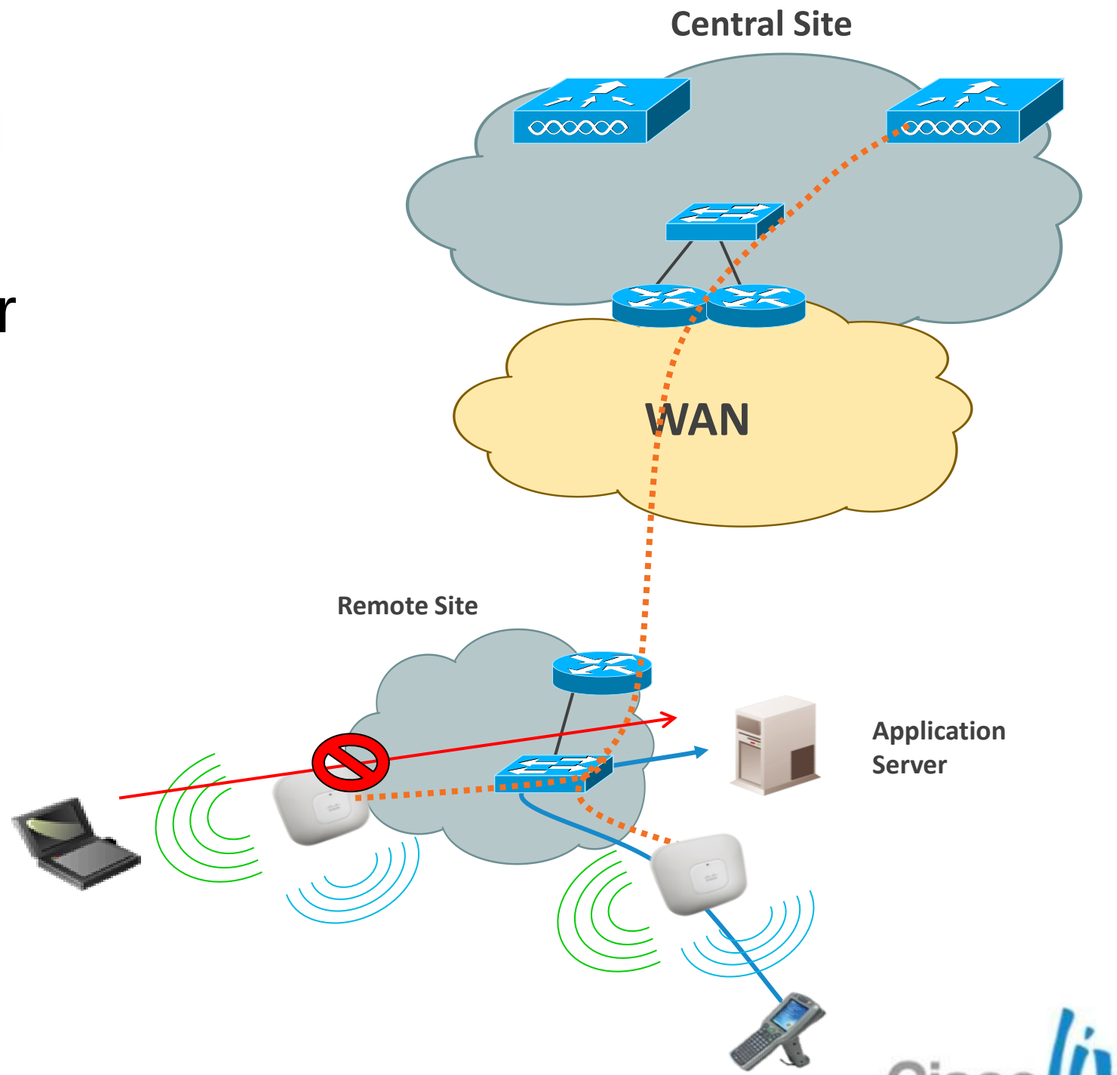
Feature	WAN Up (Connected)	WAN Down (Standalone)
Static Security Keys (WEP, WPA2/PSK)	Yes	Yes
802.1x/EAP	Yes	Yes
RADIUS	Yes	Yes (local RADIUS Backup)
Local Authentication	Yes	Yes
OKC Fast Roaming	Yes	Yes (not new clients)
WebAuth & MAC Auth	Yes	No

Designing Secure & BYOD Enabled Branch Network

Understanding Local Switched Access Lists

Description

- Support for ACL in FlexConnect local switching mode
- ACL mapped to local VLAN per AP or FlexConnect Group
- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 rules per ACL
- No IPv6 ACL

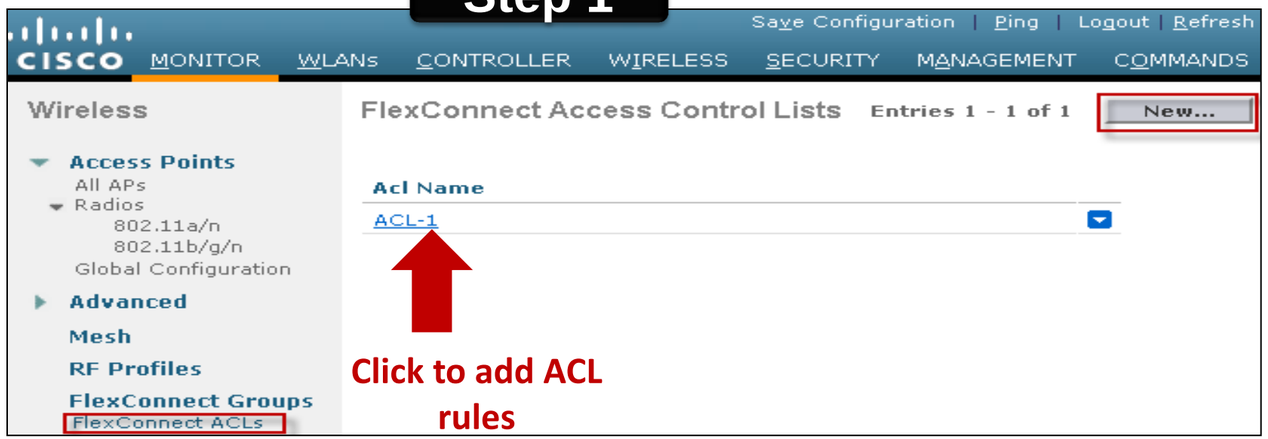


Local Switching Access Lists

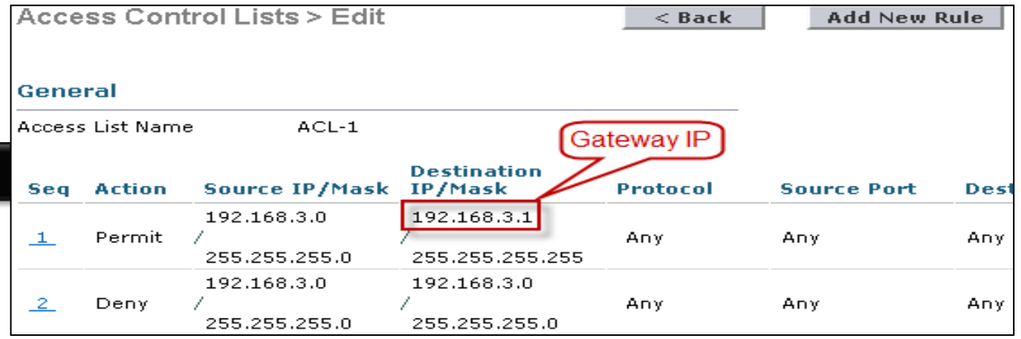
Configuration

- ACL rule creation and application for FlexConnect is identical to WLC rule creation for Local Mode
- **Example**: **P2P Blocking for 192.168.3.0 network.**

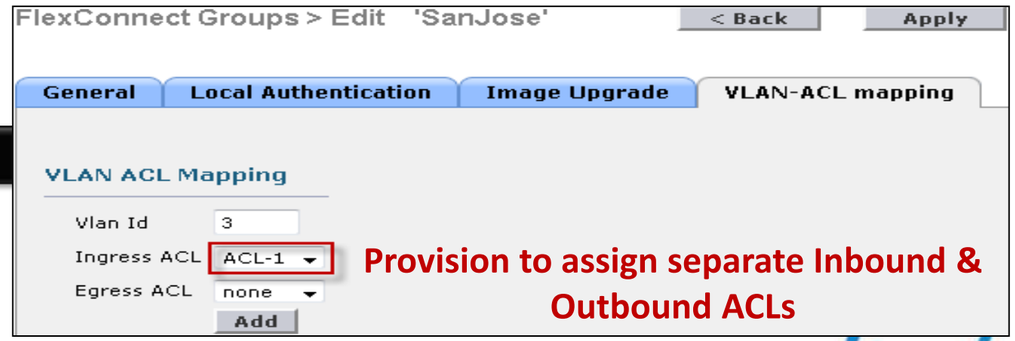
Step 1



Step 2



Step 3

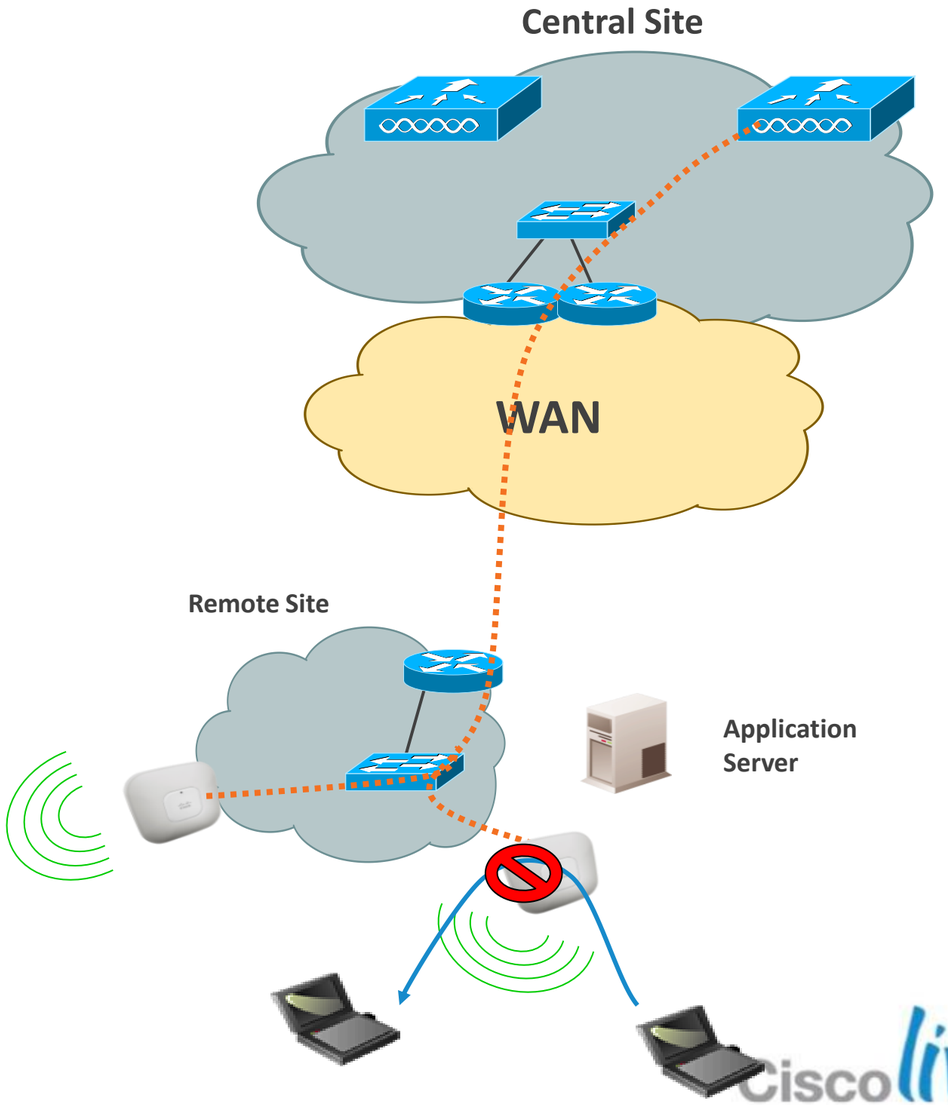


Local Switching Peer-to-peer Blocking

New in 7.2

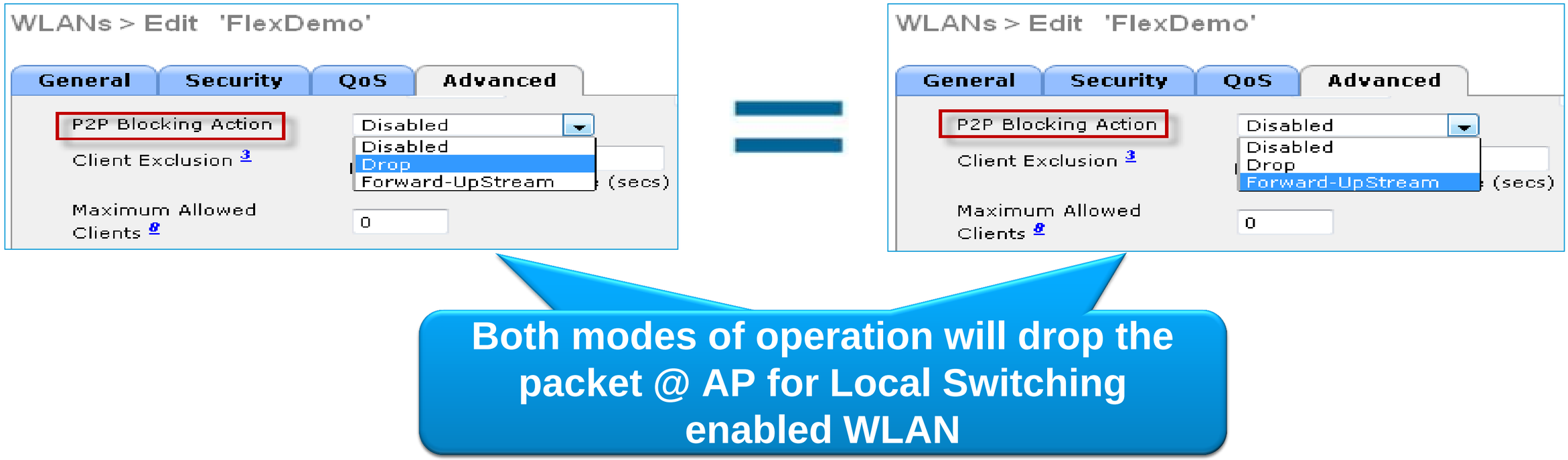
Description

- 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



Both modes of operation will drop the packet @ AP for Local Switching enabled WLAN

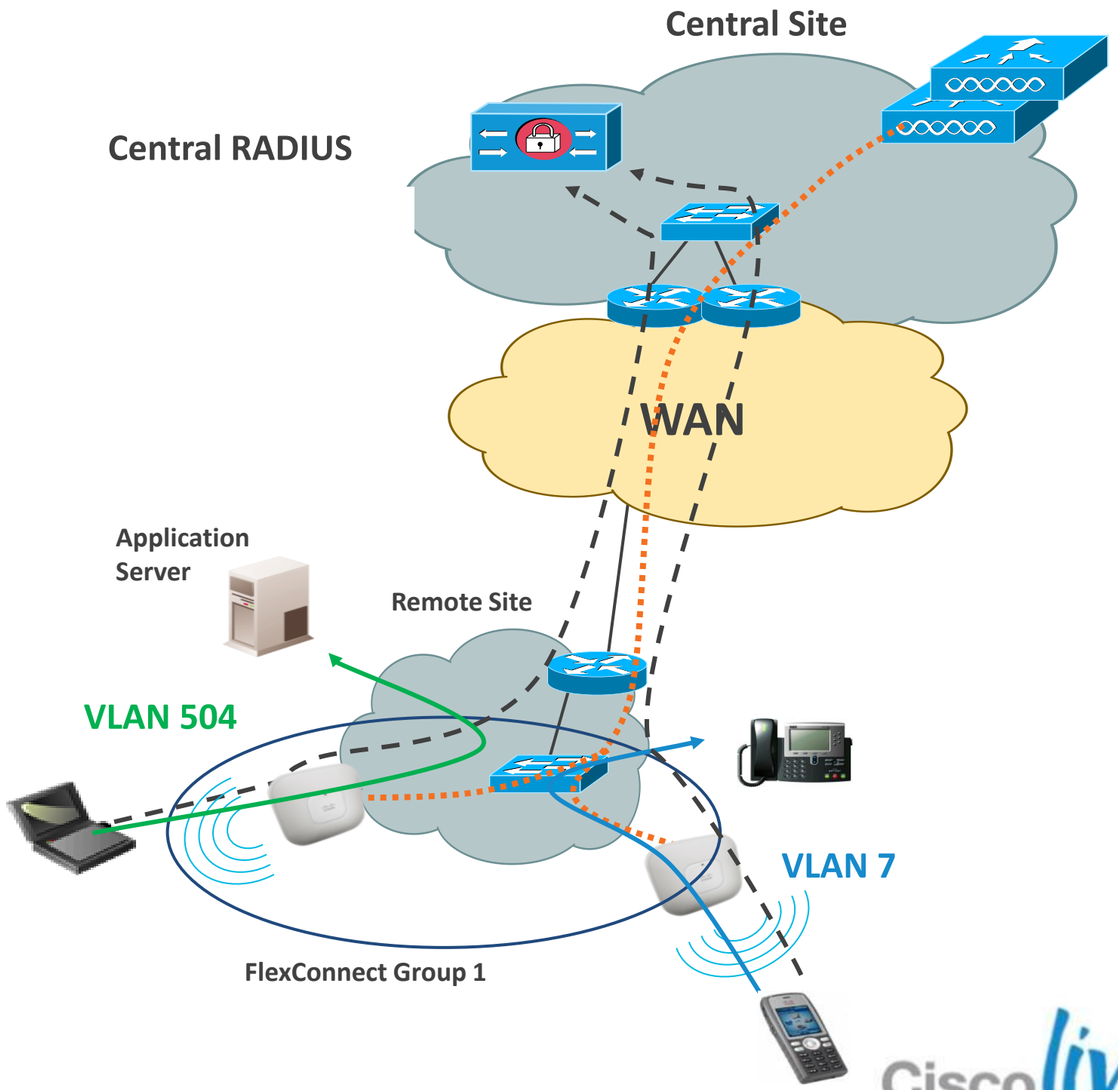
* Central Switching WLAN will support “Forward - UpStream” and will send the packet to the next upstream node connected to WLC

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
- QoS and ACL Override is not supported.



FlexConnect AAA VLAN Override

Configuration

	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

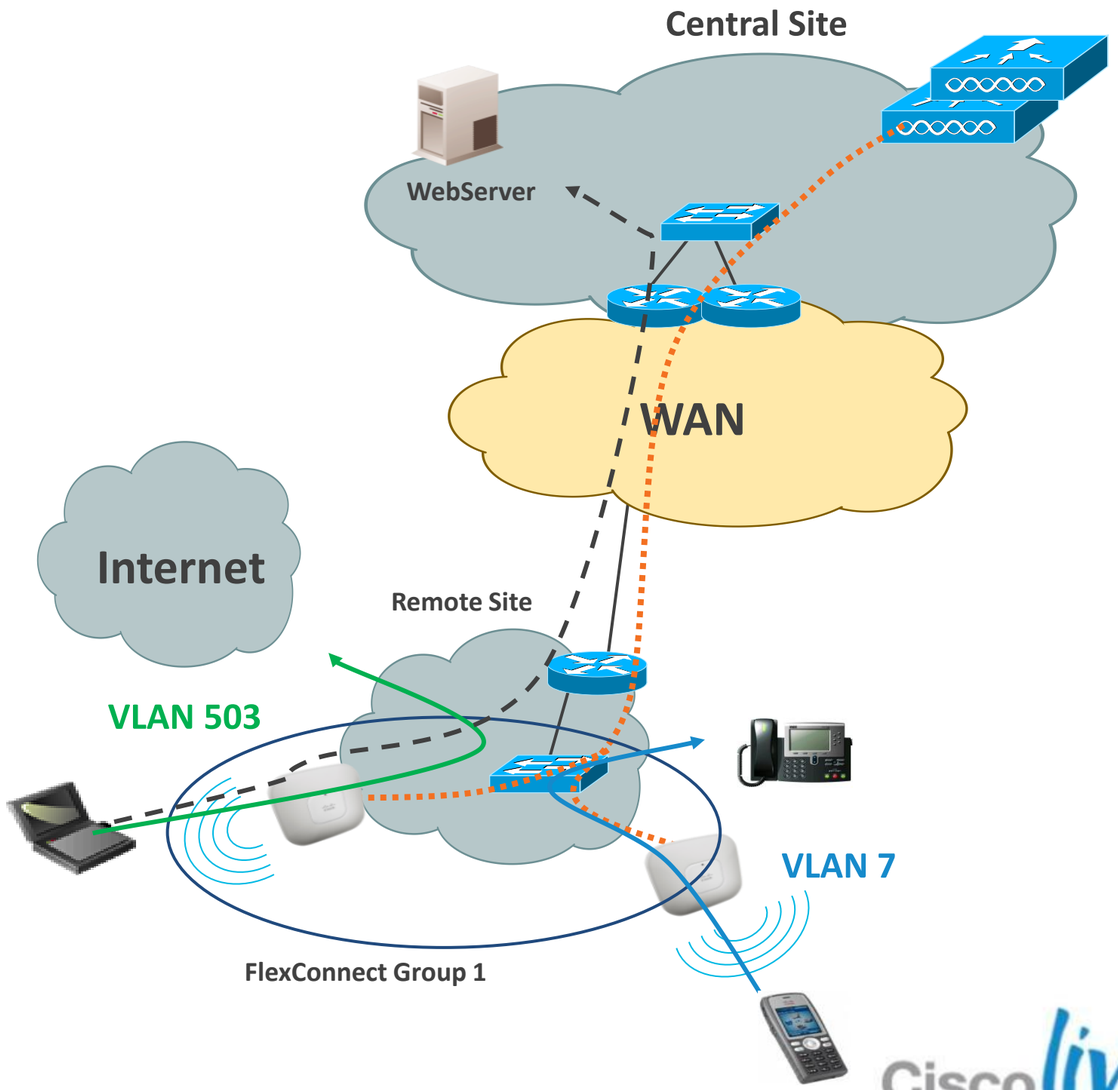
Add

Create Sub-Interface on FlexConnect AP

External WebAuth with Local Switching

Description

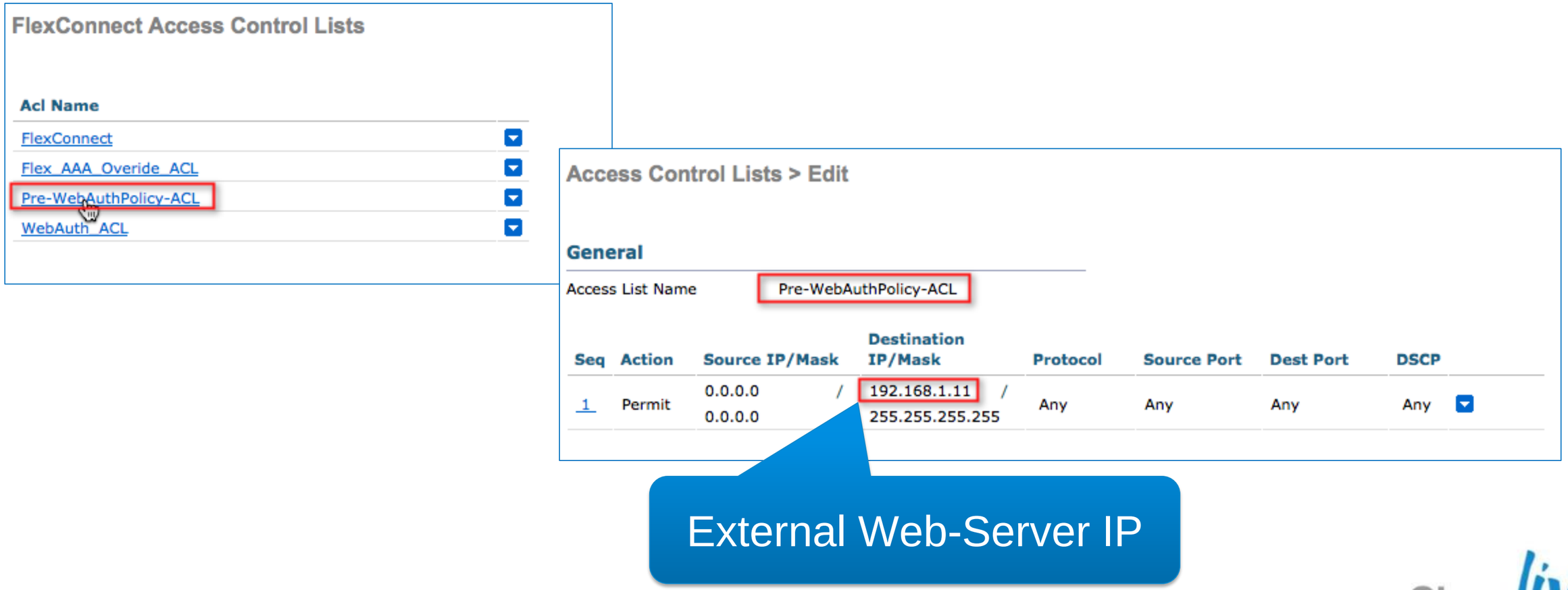
- Provides L3 Web Redirect from locally switched vlan
- Reduces WAN traffic by locally switching guest traffic
- Flexible and centralised web portal creation for multiple sites
- Provides flexible use of Conditional and Splash Page Web Redirect
- FlexConnect AP must be in Connected state with Centralised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



External WebAuth with Local Switching

Configuration

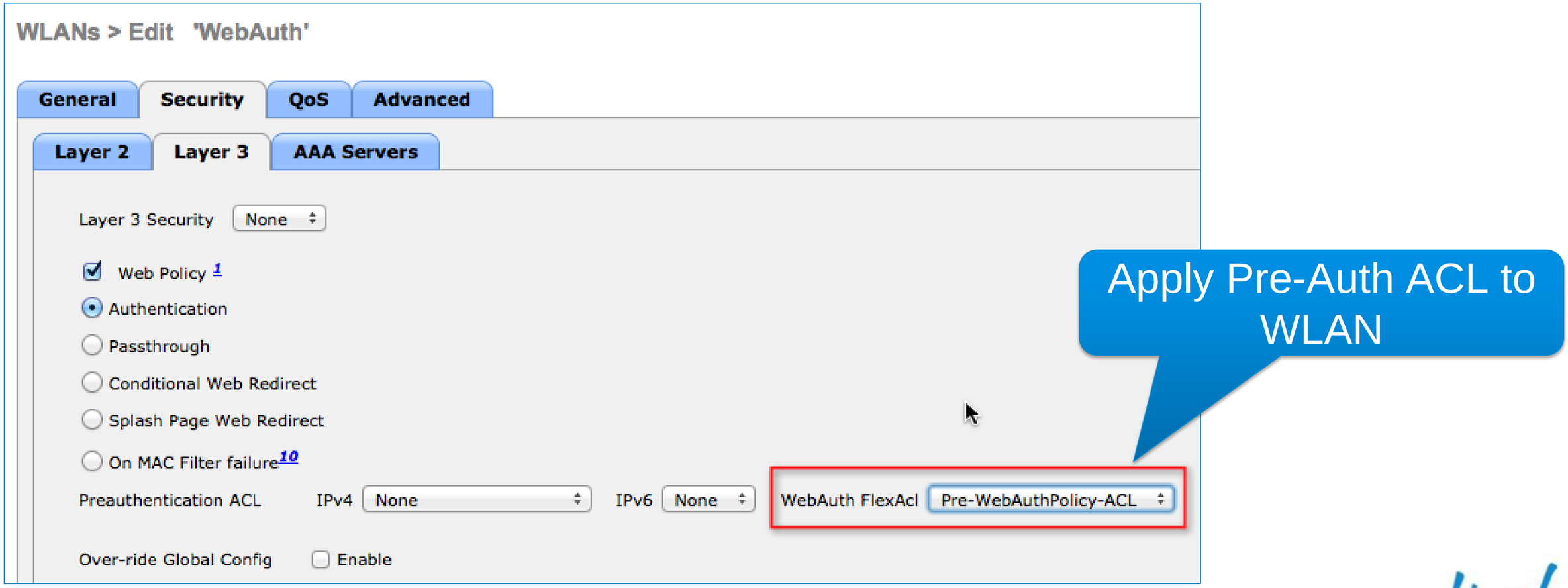
Step 1: Configure Pre-Auth ACL that will be applied to FlexConnect Group, AP or WLAN



External WebAuth with Local Switching

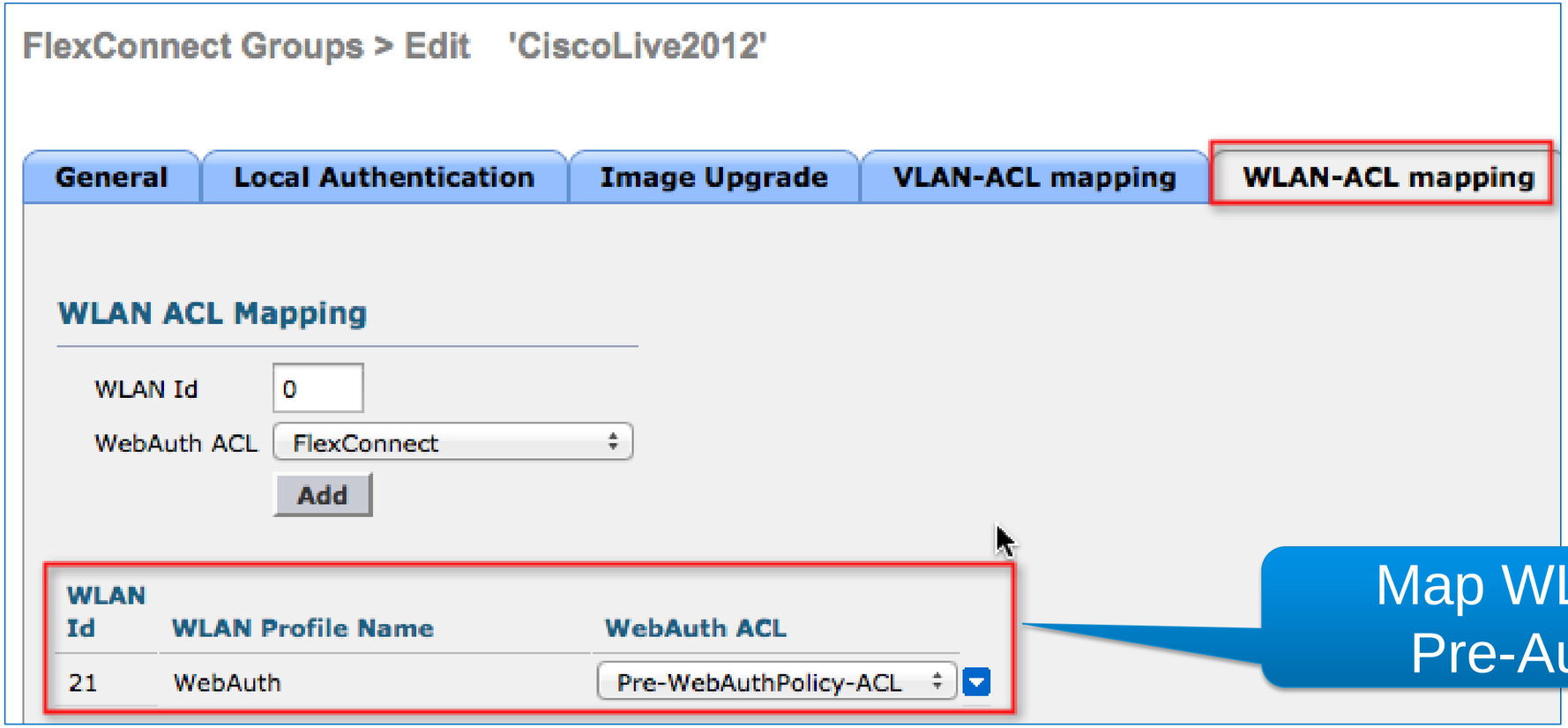
Configuration

Step 2: Apply Pre-Auth ACL to WLAN



External WebAuth with Local Switching
Configuration

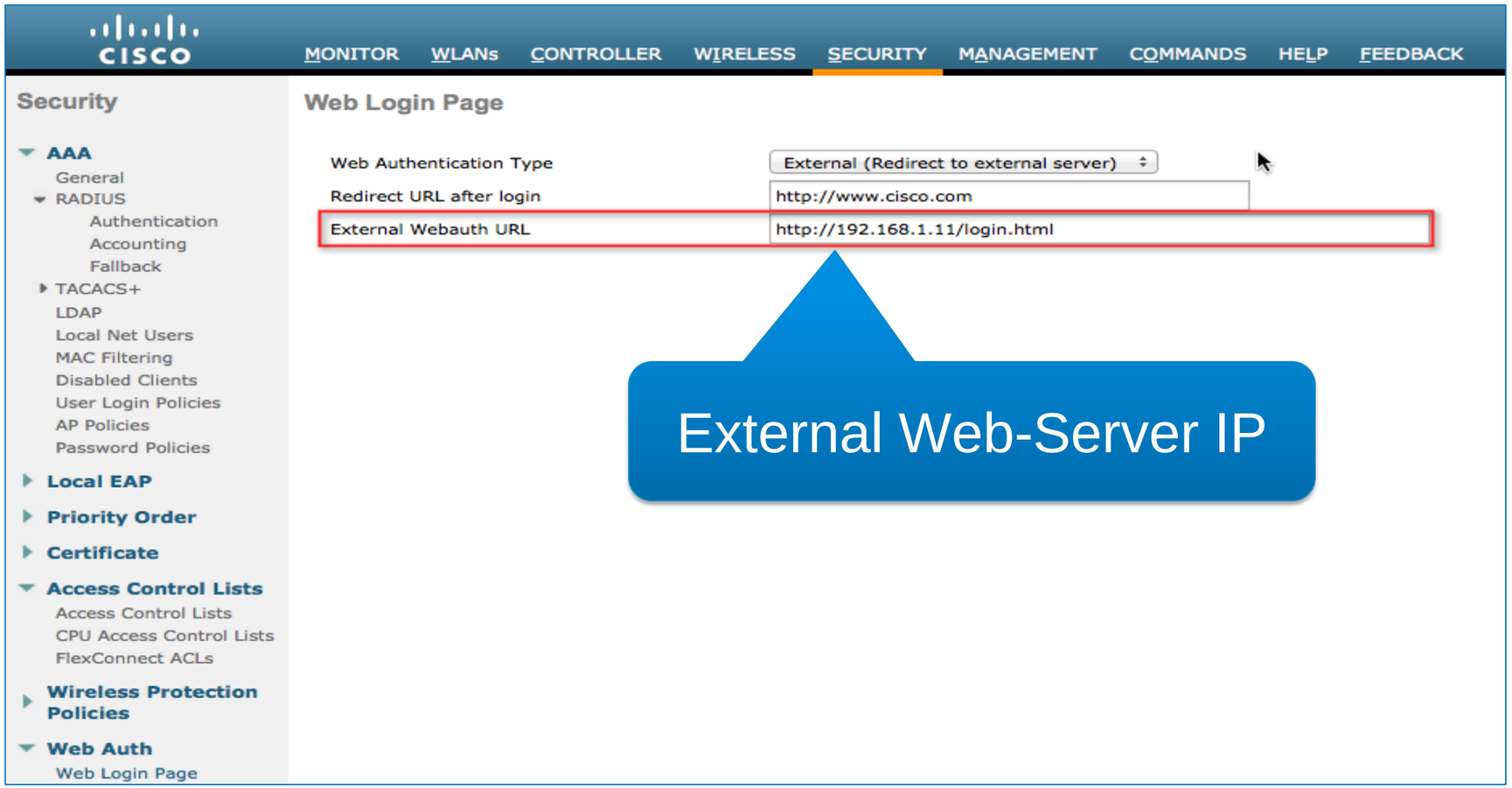
Step 3: Apply Pre-Auth ACL to FlexConnect Group



External WebAuth with Local Switching

Configuration

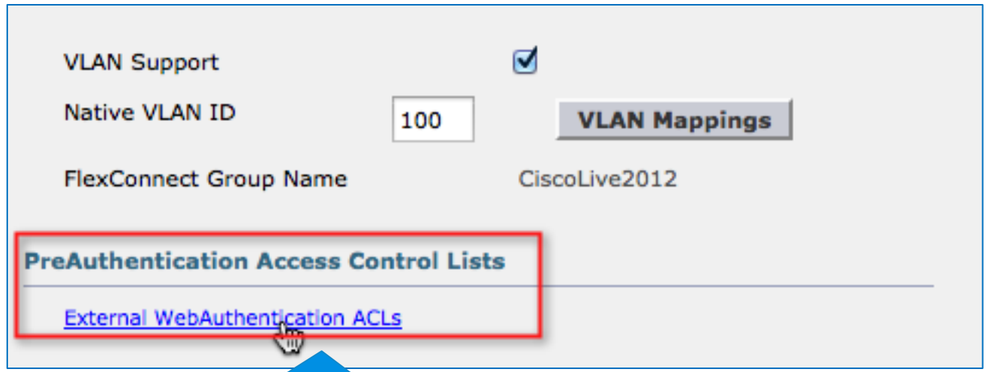
Step 4: Configure External Web Server

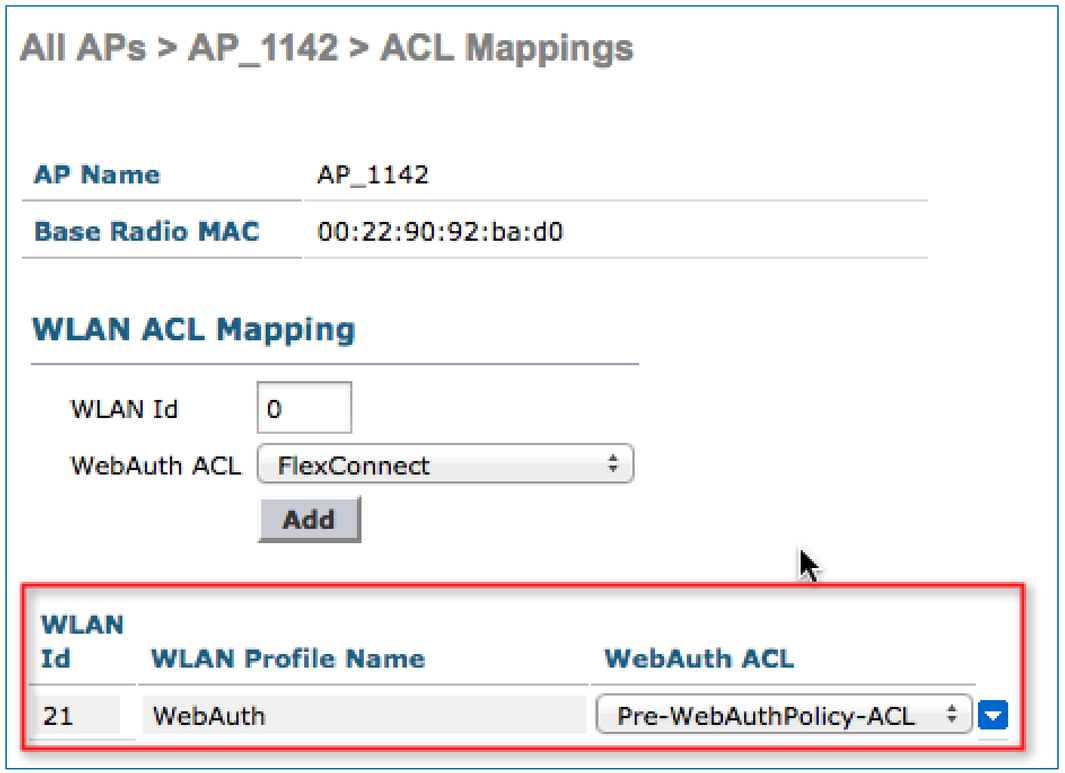


External WebAuth with Local Switching

Configuration Verification

Finally ensure ACL assignment is correct at AP

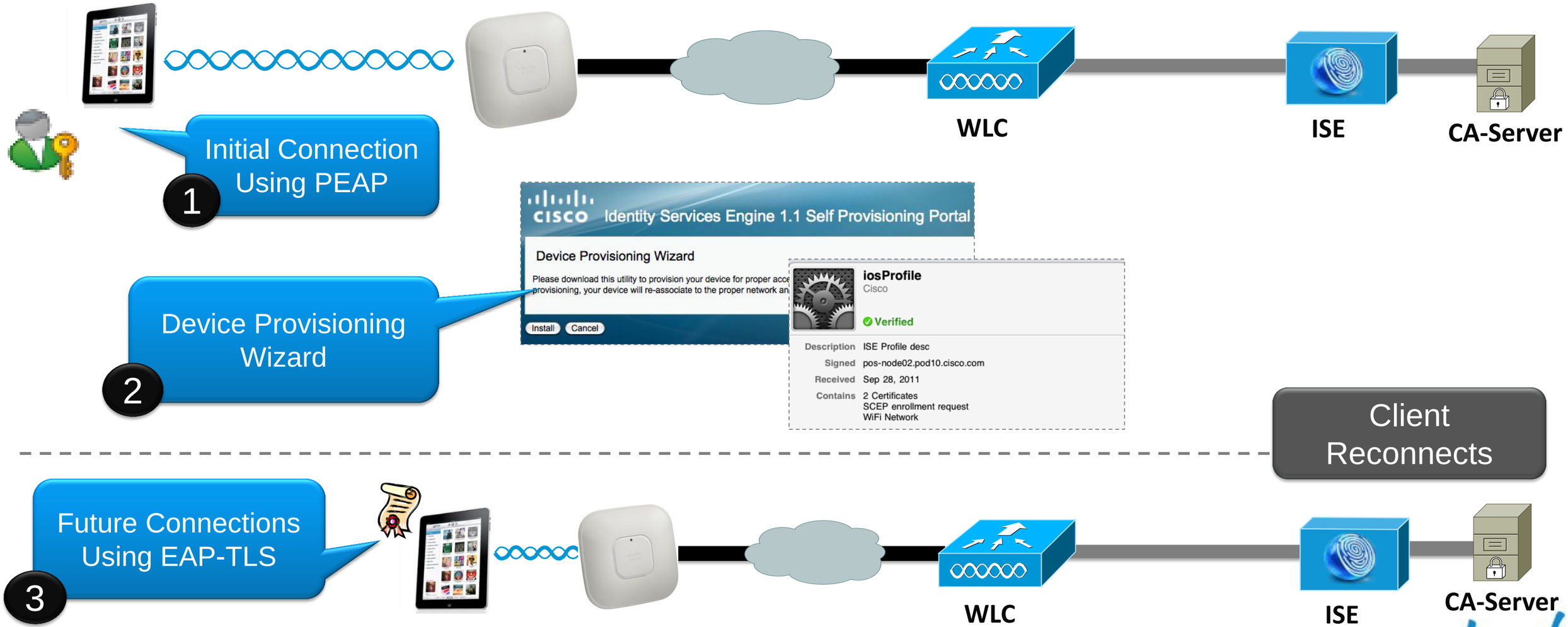




Navigate to "**Wireless > All APs > <Flex AP> > FlexConnect**"
Click External WebAuth ACLs

BYOD Device On-Boarding in Local Switching

Example: Apple iOS Device Provisioning



Steps for Integrating the Controller and ISE

1. Configure WLAN for 802.1x Authentication

- Configure RADIUS Server on Controller
- Setup WLAN for AAA Override, Profiling and RADIUS NAC

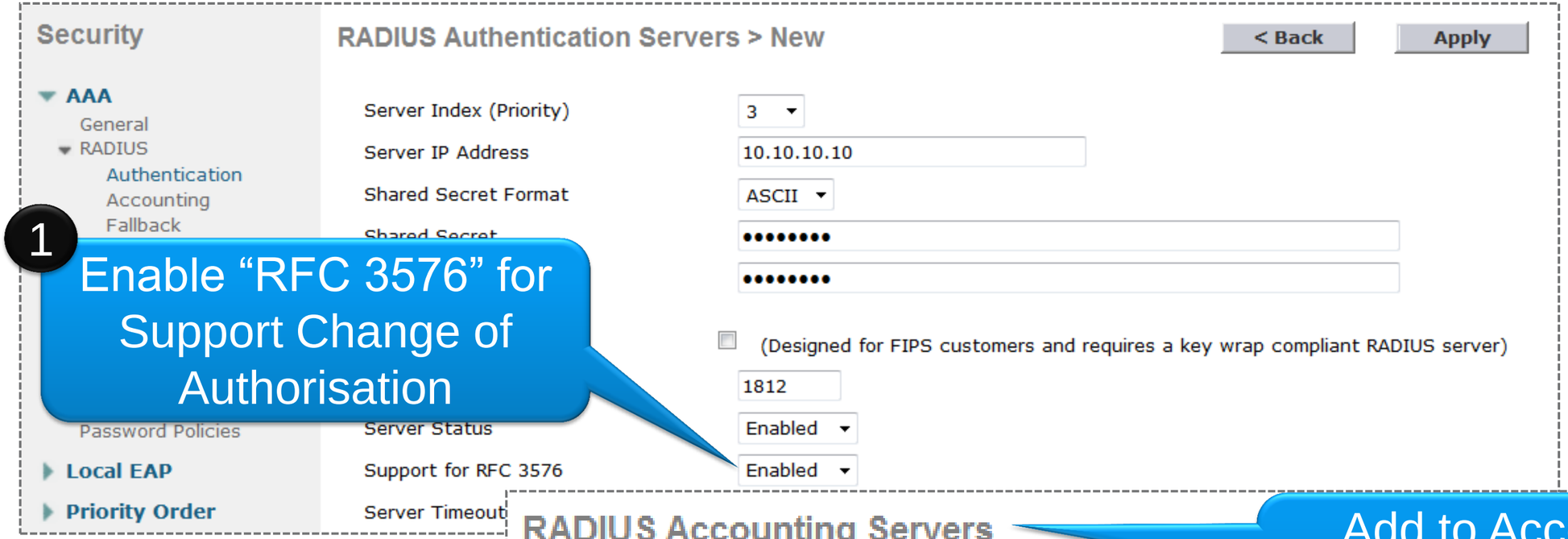
2. Configure ISE Profiling

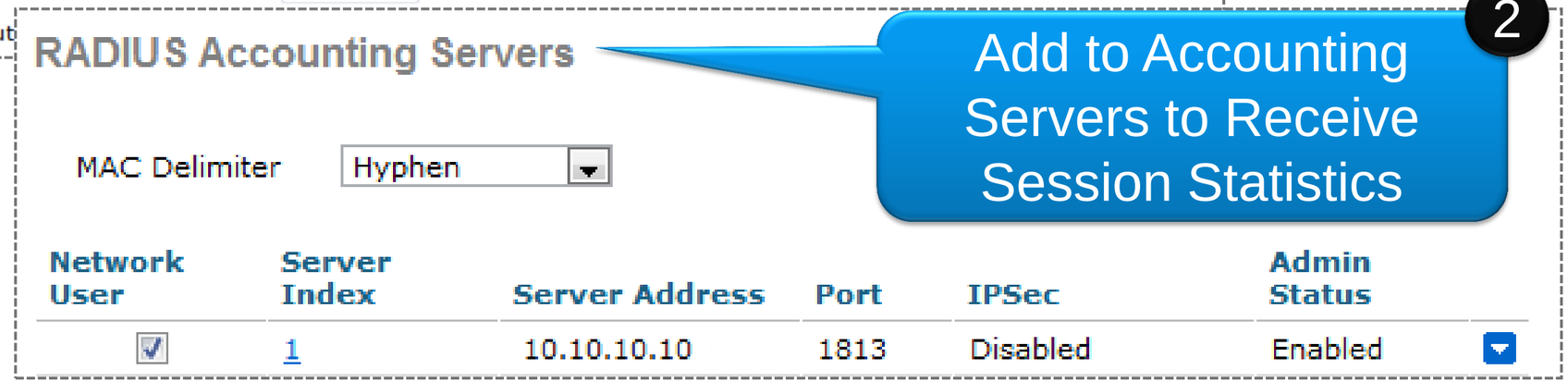
- Enable profiling sensors

3. Setup Access Restrictions

- Configure ACLs to filter and control network access.

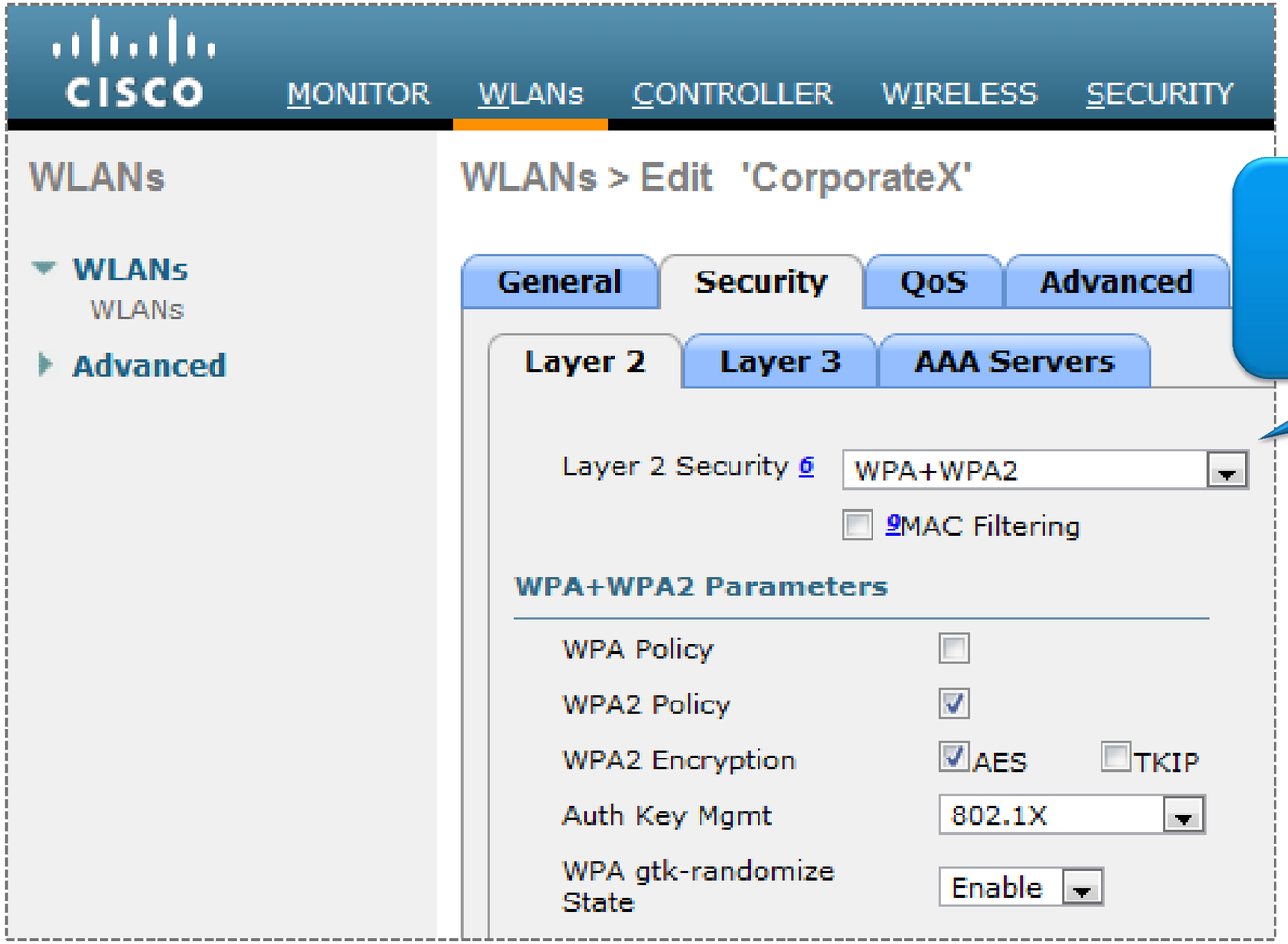
Configuring ISE as the Authentication Server and Accounting Server





Configuring the WLAN for Secure Connectivity

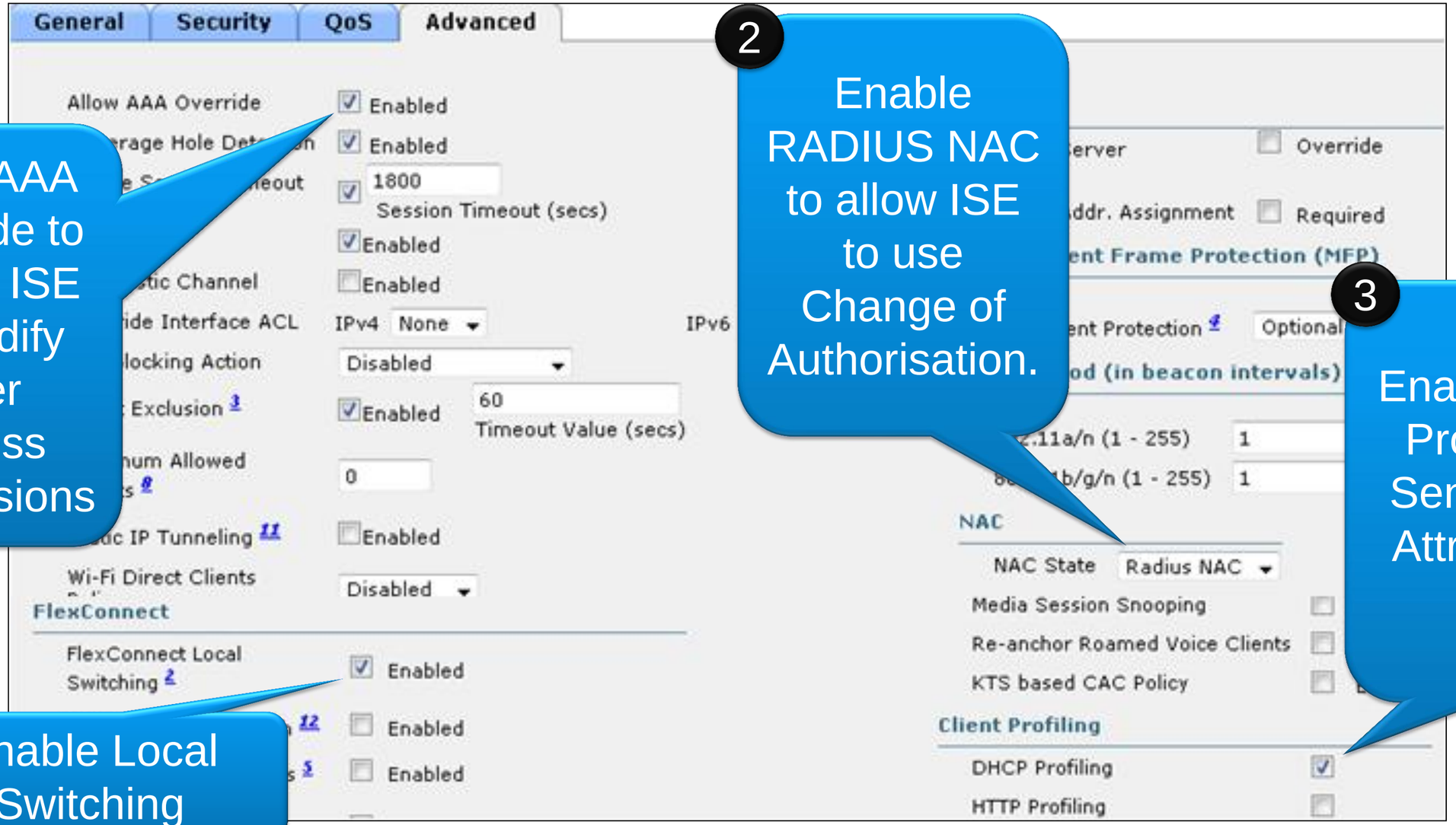
Enabling Secure Authentication and Encryption with WPA2-Enterprise



1

WPA2 Security with AES Encryption

Configuring the WLAN for ISE Identity-based Networking Cont'd



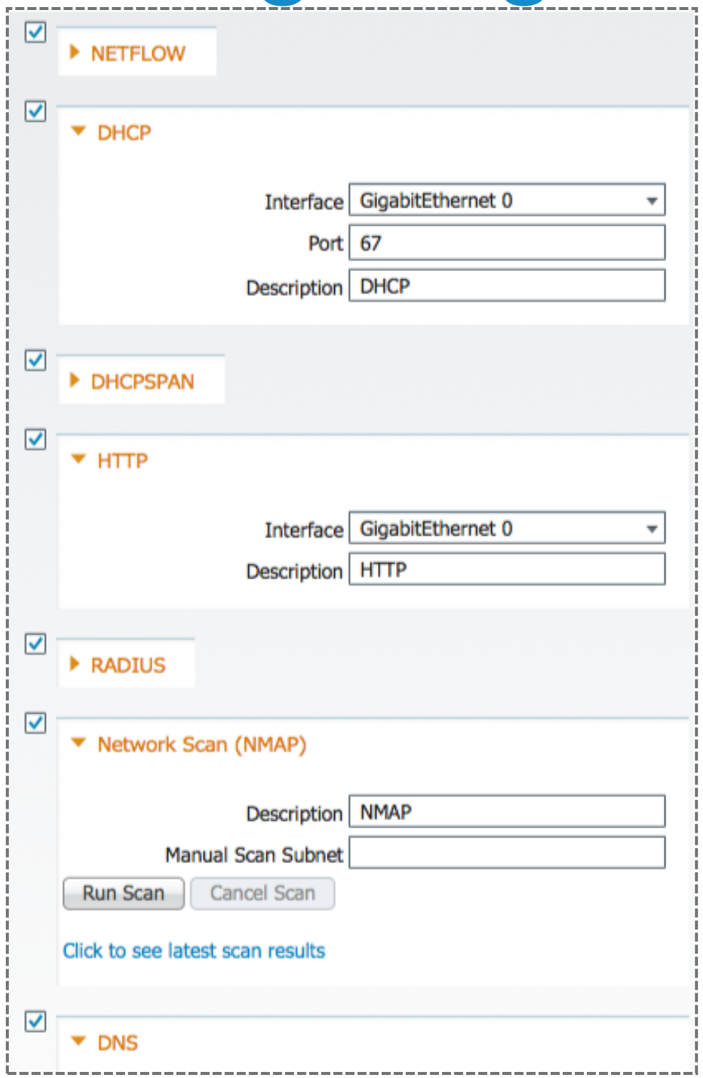
1 Allow AAA Override to Permit ISE to Modify User Access Permissions

2 Enable RADIUS NAC to allow ISE to use Change of Authorisation.

3 Enable Client Profiling to Send DHCP Attributes to ISE.

4 Enable Local Switching

Configuring ISE Profiling Sensors

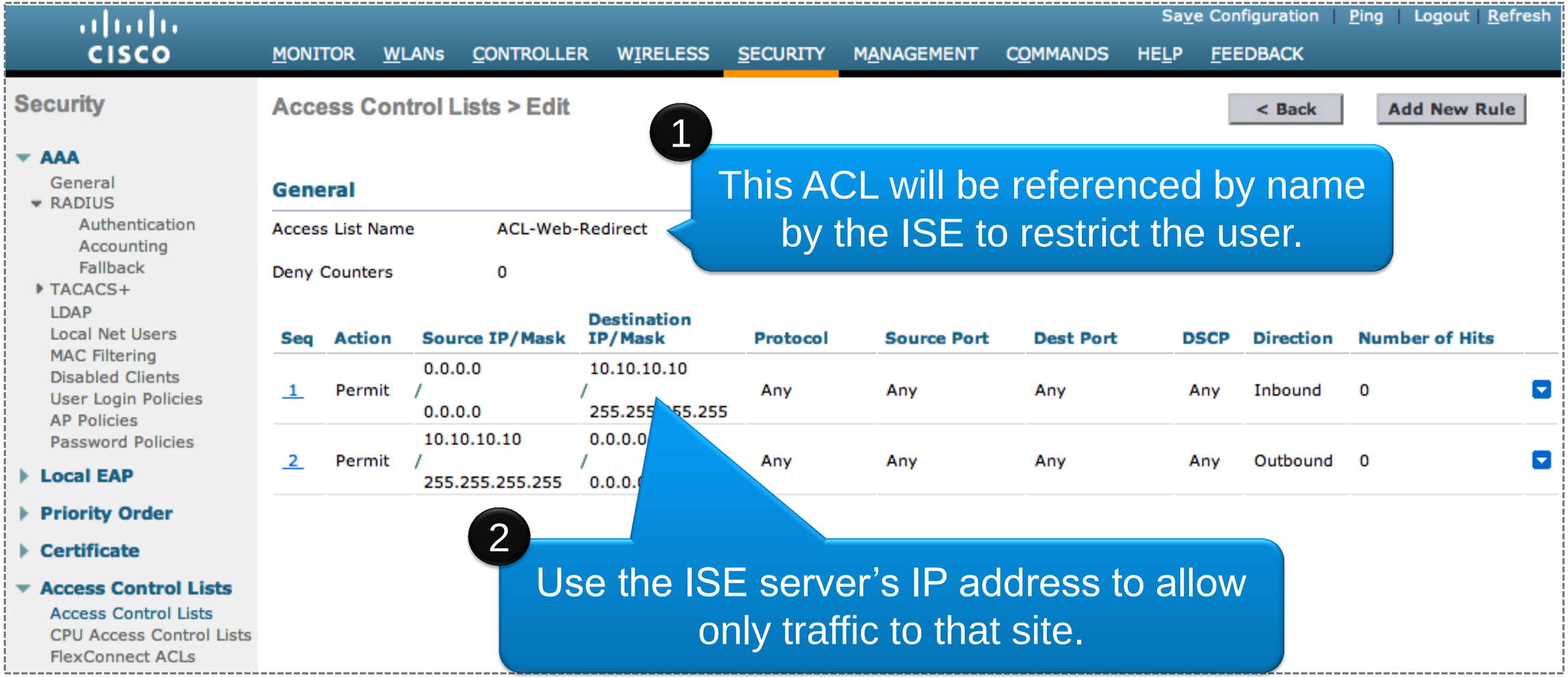


- Profiling relies on a multitude of “sensors” to assess the client’s device type.
- Profiling can always be achieved through a span port, more efficient profiling is achieved through sensors which selectively forward attributes.
- For DHCP Profiling:
  - Option A: Use v7.2 MR1 code to send DHCP attributes in RADIUS accounting messages.
  - Option B: Use Cisco IOS “ip helper” addressed to ISE on switches adjacent to the WLC.
- For HTTP Profiling:
  - Use the Web-Authentication redirect to get the HTTP user agent.

ISE Deployment Guide: http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080ba6514.shtml

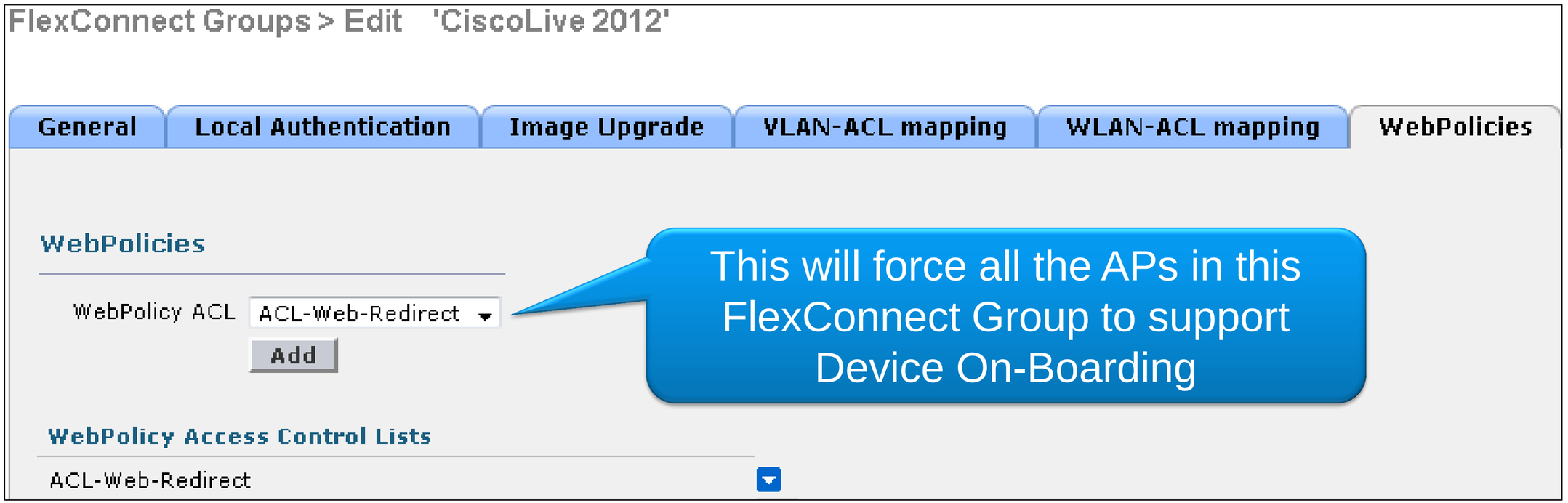
Configuring the Web-Authentication Redirect ACL

The ACL is used in HTTP profiling as well as posture and client provisioning.



Create WebPolicies for FlexConnect Group

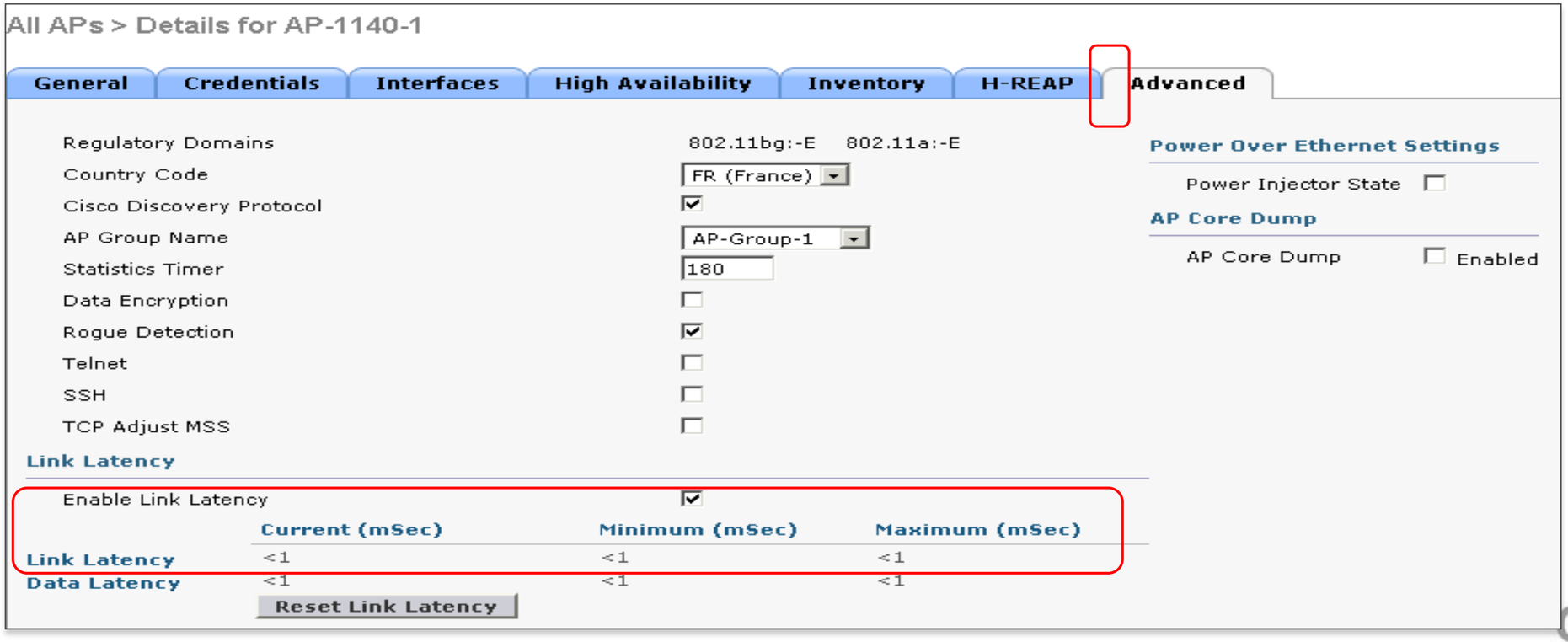
The ACL is used in HTTP profiling as well as posture and client provisioning.



Operating Wireless Branch Smart Upgrade over WAN

Monitor FlexConnect Latency

- RTT for FlexConnect AP :
  - Is recommended to be max 300ms for data
  - Must be max 100ms for voice roaming
- Latency tool will help monitor WAN latency



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
  - Exhaustion of the WAN link
  - Risk of failures during the download
- Release 7.2 introduced “Smart AP Image Upgrade”

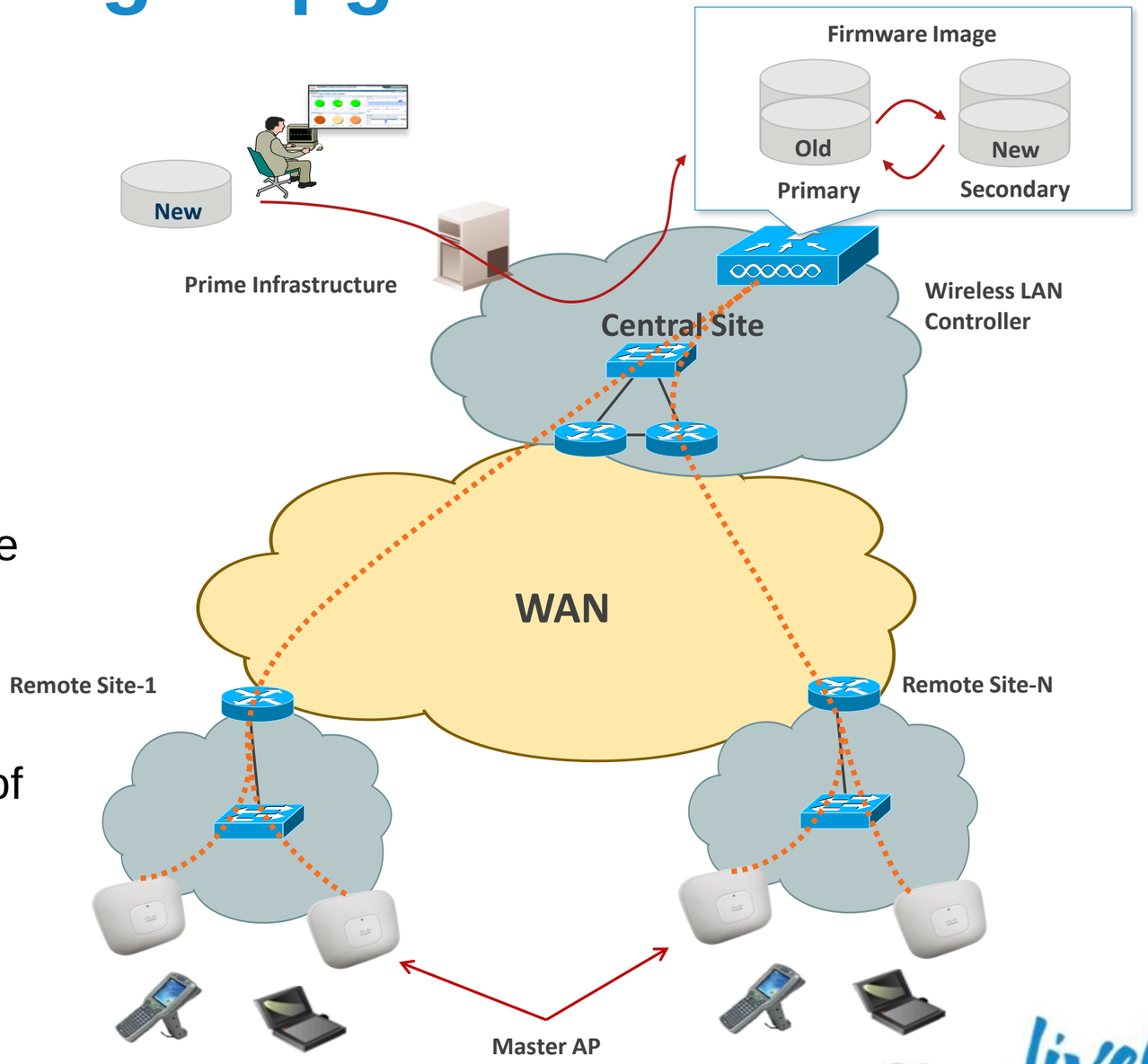
FlexConnect Smart AP Image Upgrade

Description

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

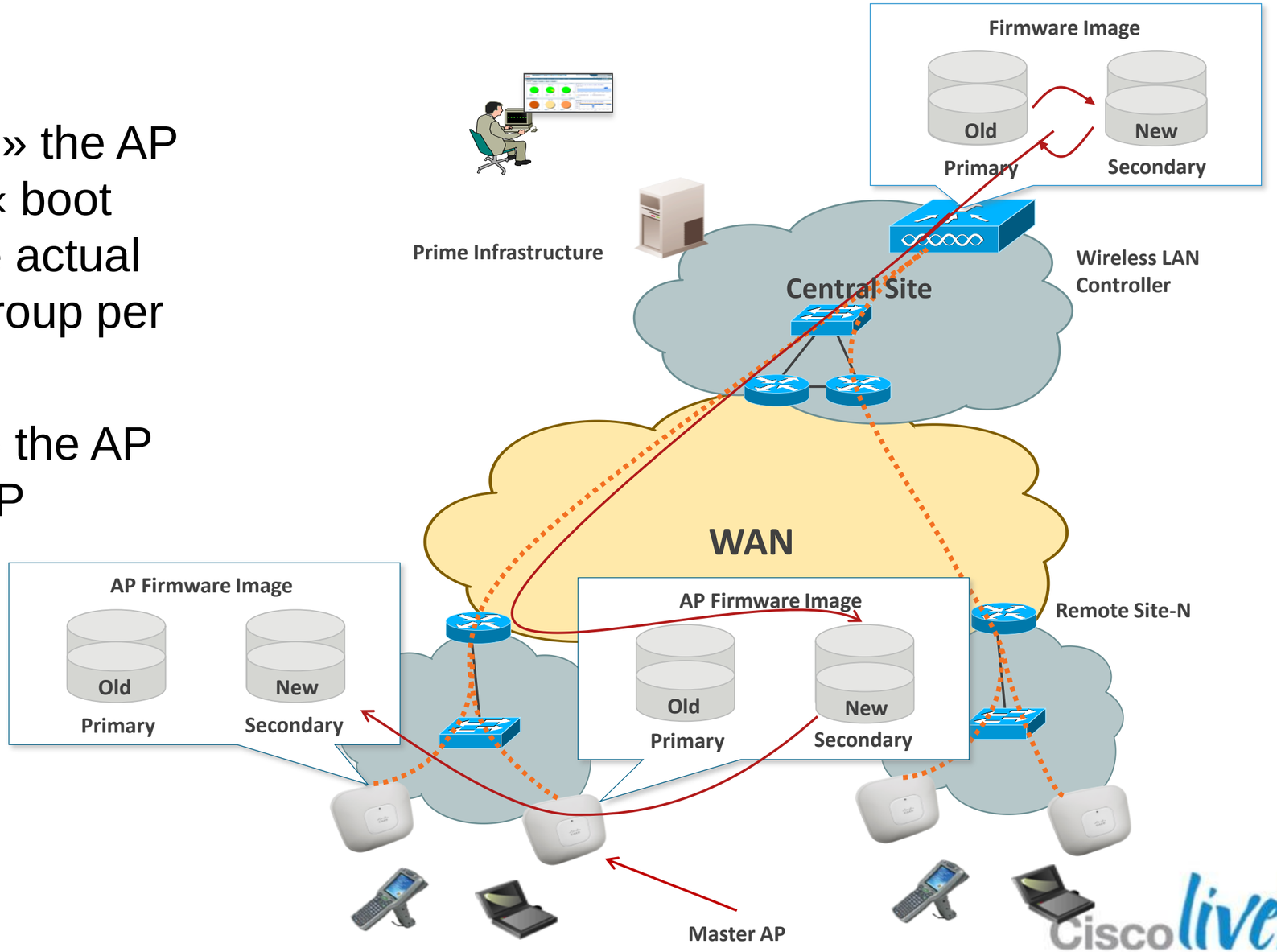
1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)



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



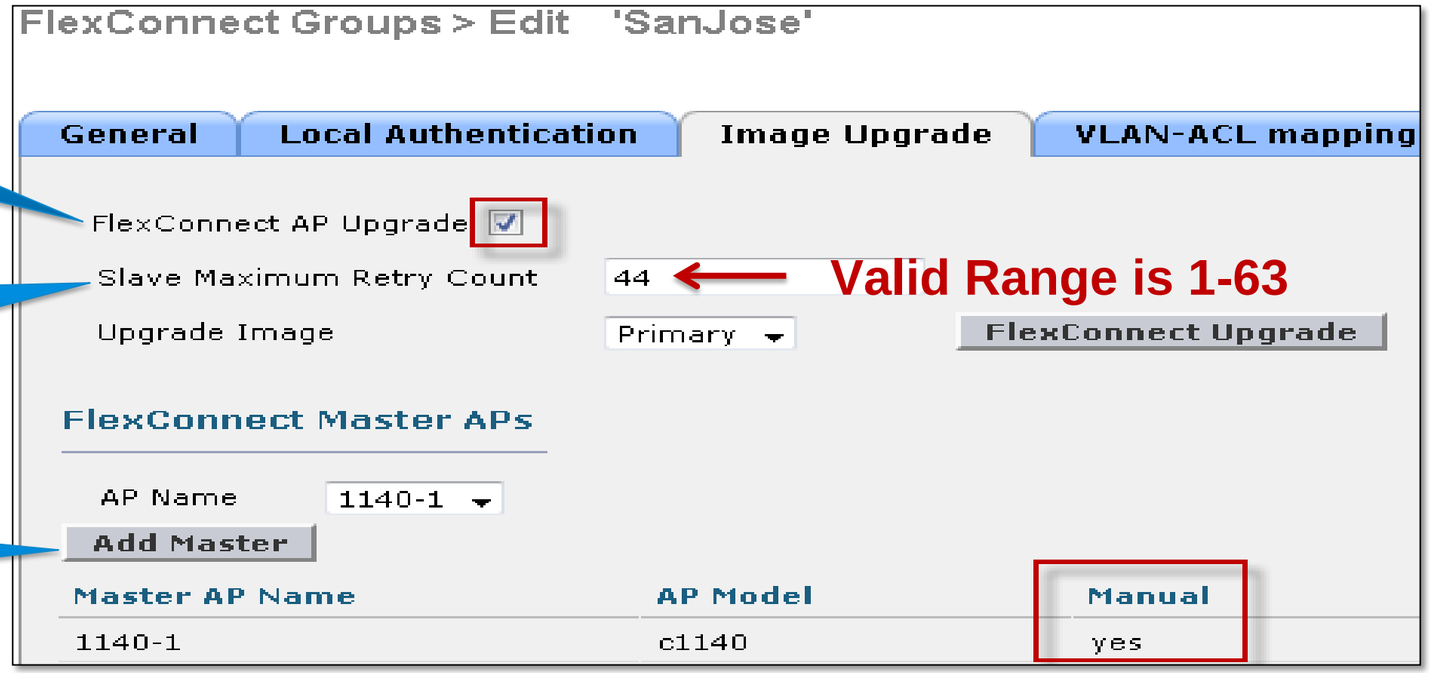
FlexConnect Smart AP Image Upgrade

Configuration

Enable Efficient AP Image Upgrade

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

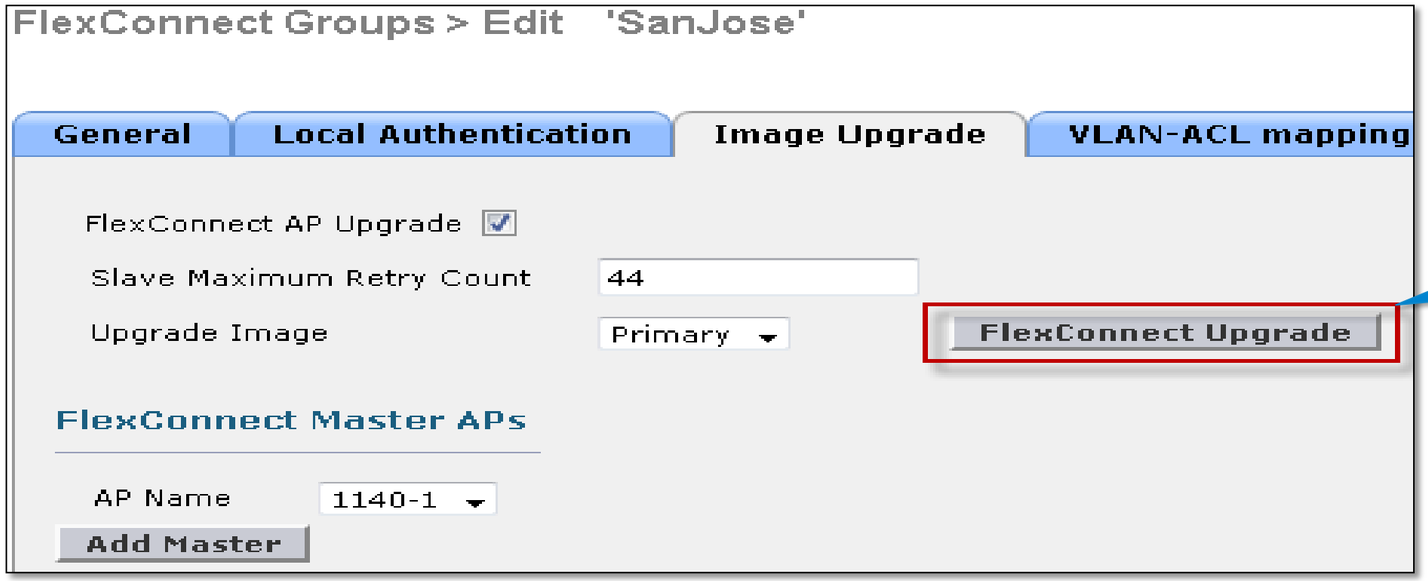
Master AP Selection is Optional



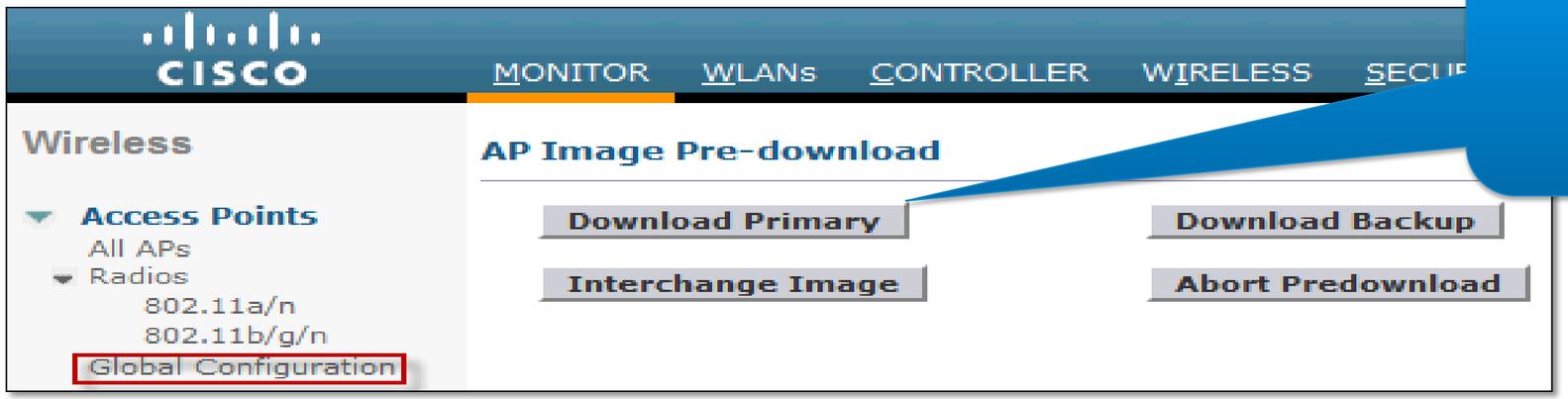
"FlexConnect AP Upgrade" checkbox has to be enabled for each FlexConnect Group.
By default, Master AP for each FlexConnect Group is selected using Lower-MAC algorithm.
One Master select per AP type.

FlexConnect Smart AP Image Upgrade

Configuration (Cont)



Per Branch or FlexConnect Group Upgrade



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

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 Deployment Guide: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

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.ww

Cisco live!