

What You Make Possible



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, enterprise 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



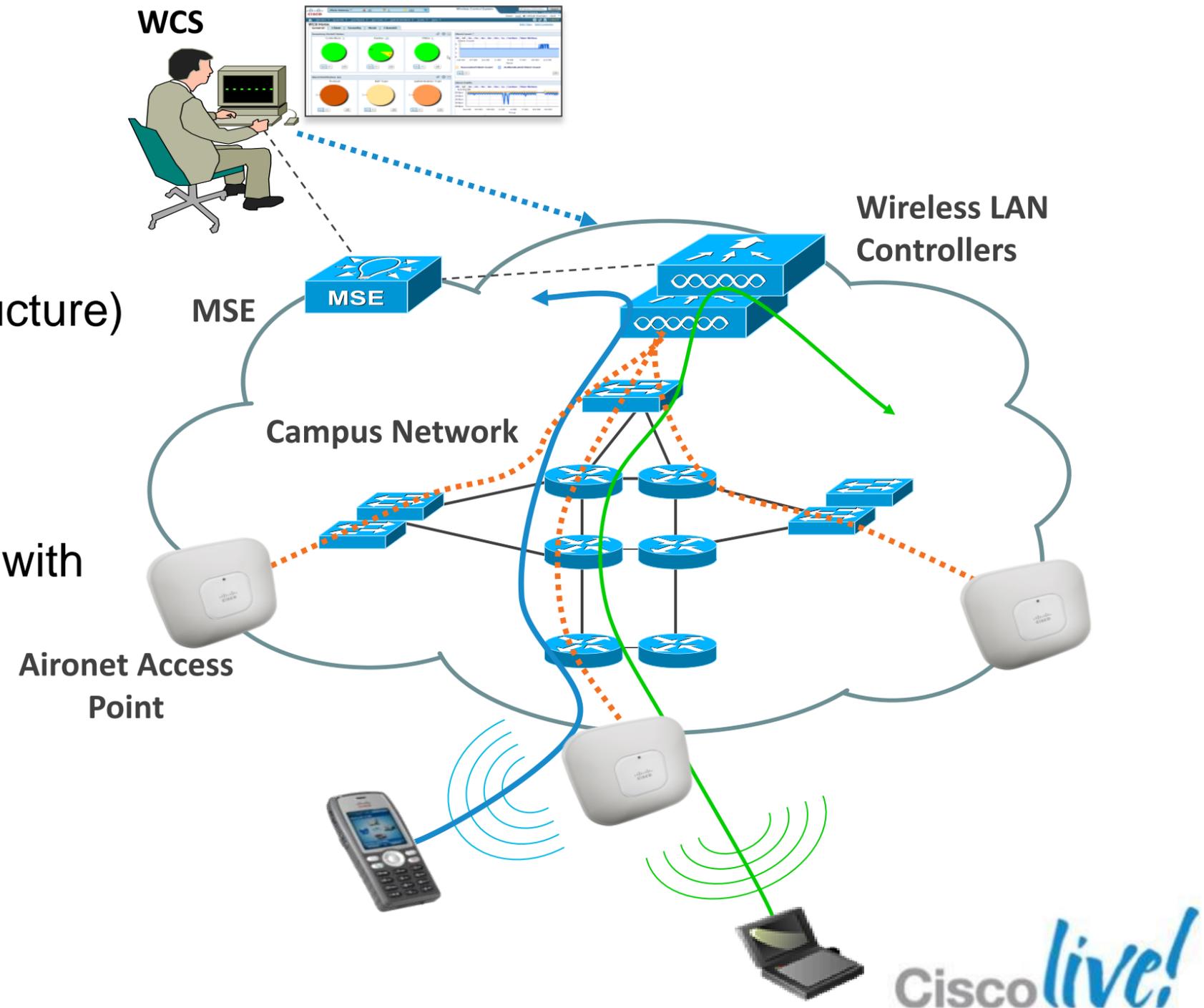
Cisco Unified Wireless Principles

■ Components

- Wireless LAN controllers
- Aironet access points
- Management System (Prime Infrastructure)
- Mobility Service Engine (MSE)

■ Principles

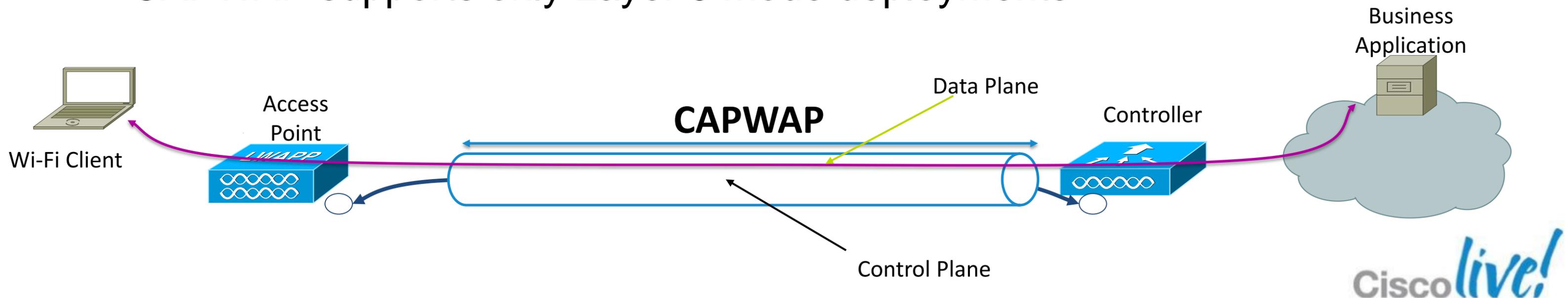
- AP must have CAPWAP connectivity with WLC
- Configuration downloaded to AP by WLC
- All Wi-Fi traffic is forwarded to the WLC



CAPWAP Overview

Control and Provisioning of Wireless Access Point

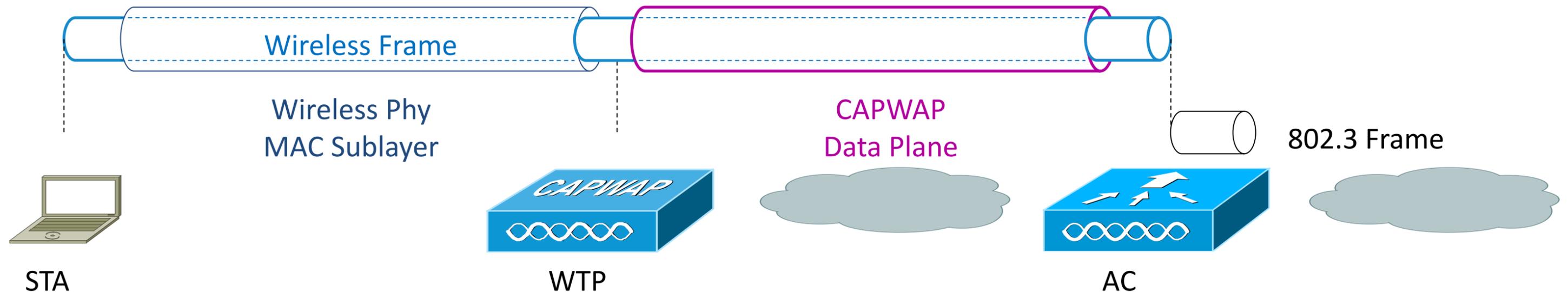
- CAPWAP is a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs)
- CAPWAP carries control and data traffic between the two
 - Control plane is DTLS encrypted
 - Data plane is DTLS encrypted (optional)
- CAPWAP supports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



CAPWAP Modes

Split MAC

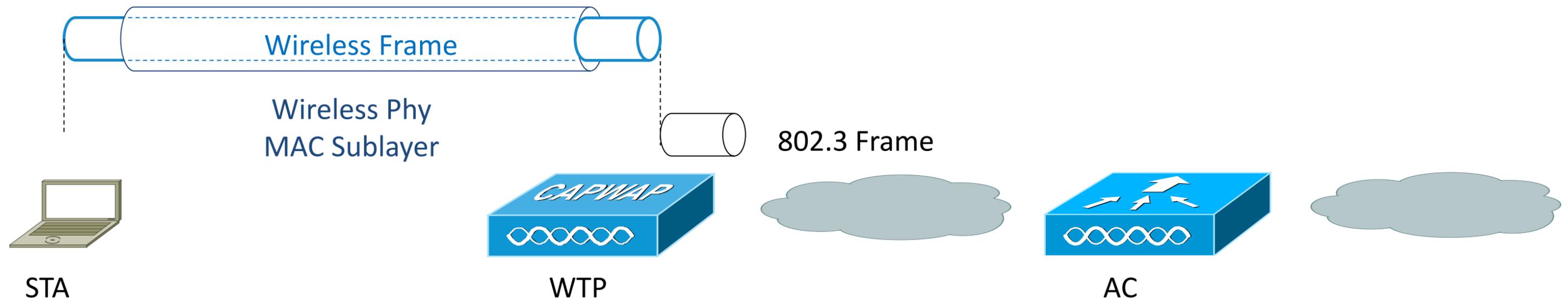
- The CAPWAP protocol supports two modes of operation
 - Split MAC (Centralised Mode)
 - Local MAC (H-REAP/FlexConnect)
- Split MAC



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

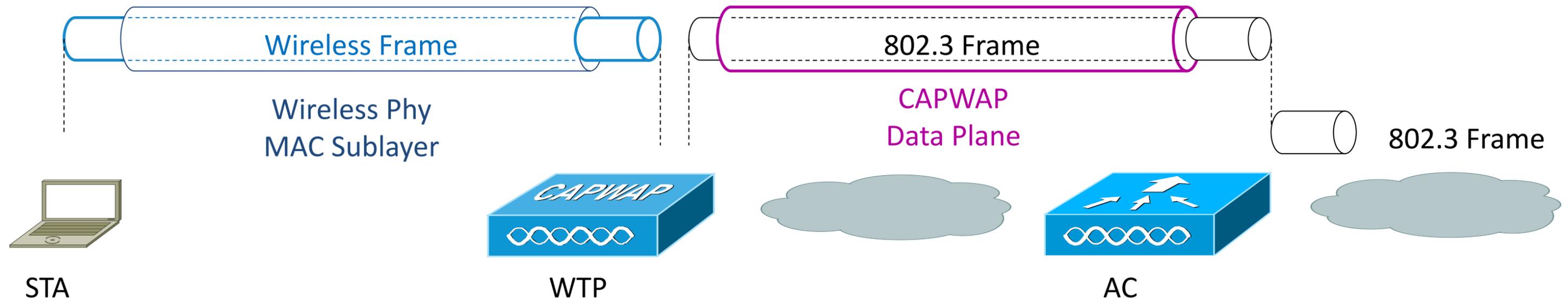


- FlexConnect supports locally bridged MAC and split MAC per SSID**

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

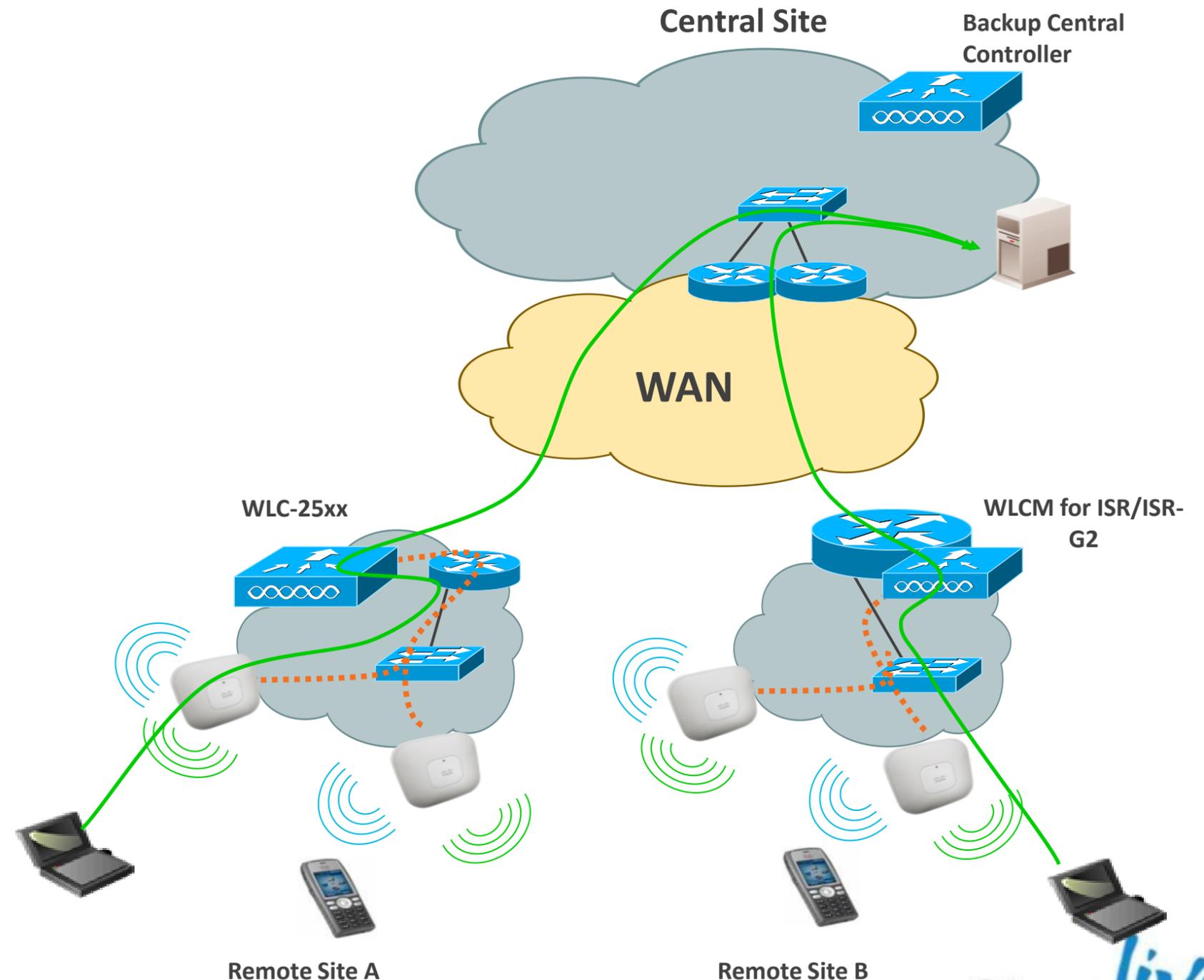
Wireless Branch Deployment Options



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

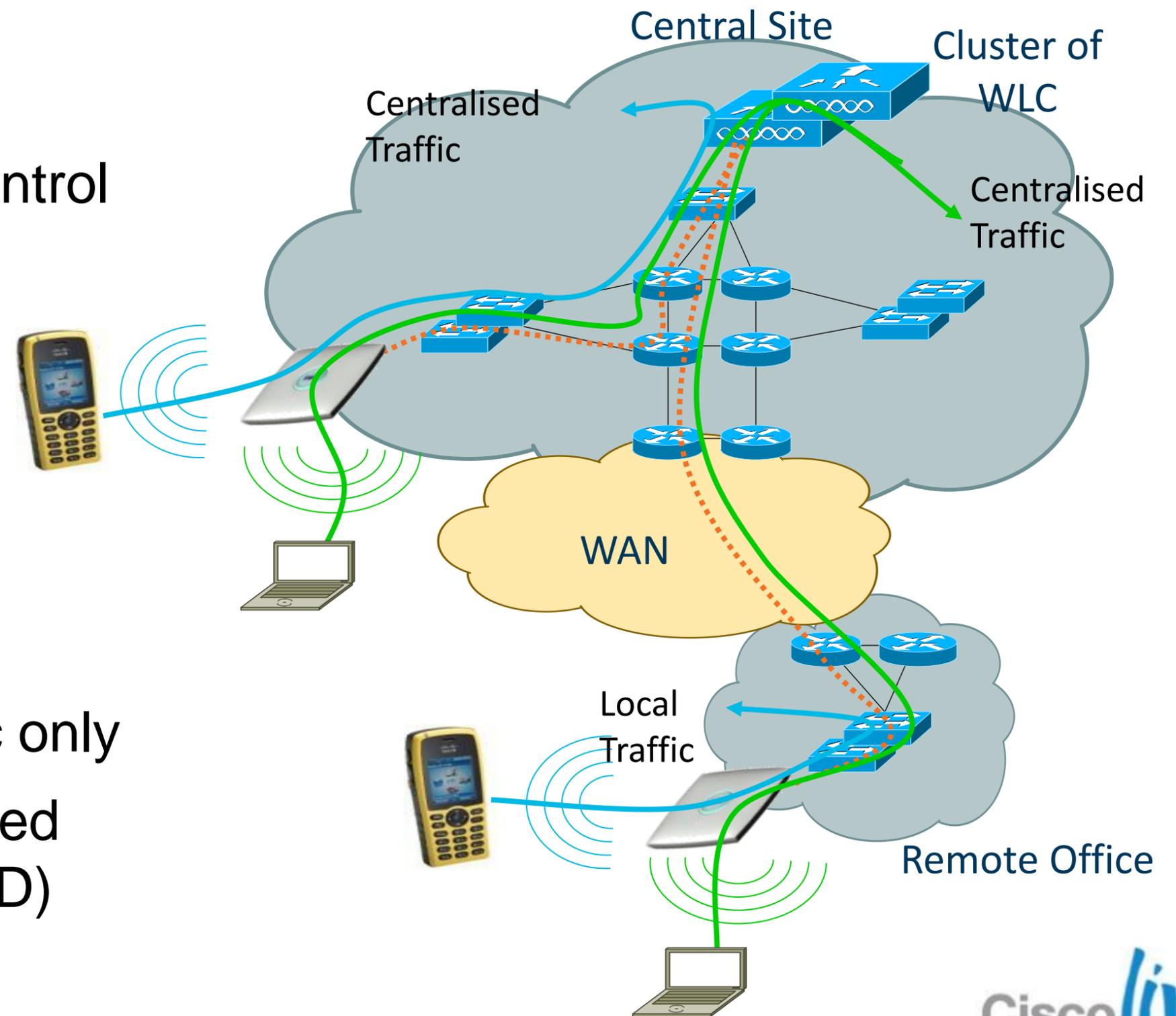
- Cookie cutter configuration for every branch site
- Layer-3 roaming within the branch
- Reliable Multicast (filtering)
- IPv6 L3 Mobility
- AAA-ACL & QoS Override

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

All APs > Details for AP_1142

General Credentials Interfaces High Availability

General

| | |
|--------------------|-------------------|
| AP Name | AP_1142 |
| Location | default location |
| AP MAC Address | 00:22:90:90:90:90 |
| Base Radio MAC | 00:22:90:92:ba:d0 |
| Admin Status | Enable |
| AP Mode | FlexConnect |
| AP Sub Mode | local |
| Operational Status | FlexConnect |
| Port Number | monitor |
| Venue Group | Rogue Detector |
| | Sniffer |
| | Bridge |

IP

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

WLANs > Edit 'FlexConnect'

General **Security** **QoS** **Advanced**

Client Exclusion ³ Enabled
Timeout Value (secs)

Maximum Allowed Clients ⁸

Static IP Tunneling ¹¹ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching ² Enabled

FlexConnect Local Auth ¹² Enabled

Learn Client IP Address ⁵ Enabled

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing

Client Band Select ^Z

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

Re-anchor Roamed Voice Clients Enabled

KTS based CAC Policy Enabled

Client Profiling

Client Profiling Enabled

Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

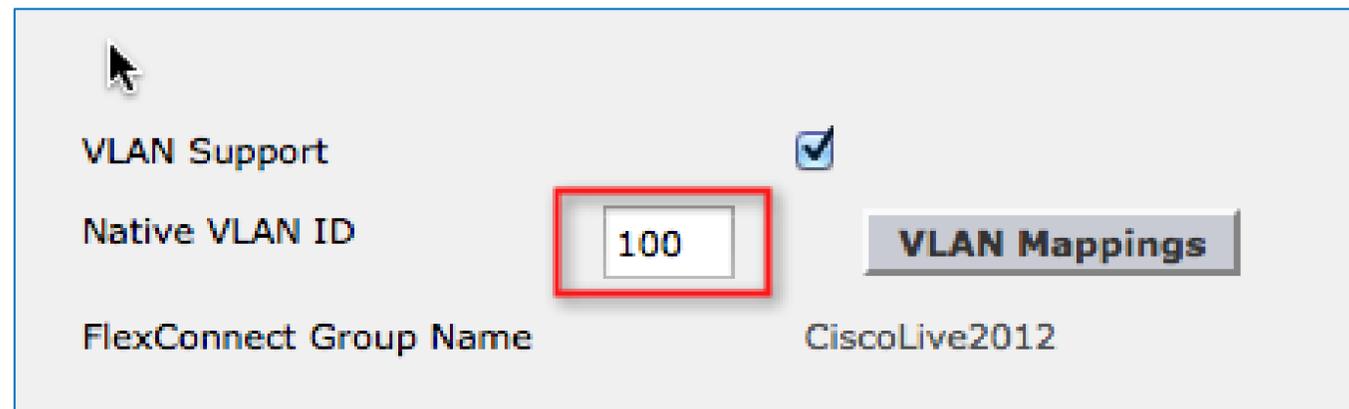
- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN Support provides the ability to configure remote VLAN to WLAN mappings. VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using Prime Infrastructure templates

The screenshot shows the configuration page for AP_1142 in Cisco Prime Infrastructure. The 'FlexConnect' tab is selected and highlighted with a red box. Under the 'FlexConnect' section, the 'VLAN Support' checkbox is checked and highlighted with a red box. The 'Native VLAN ID' is set to 100. Below this, there is a 'VLAN Mappings' button. The 'FlexConnect Group Name' is set to 'CiscoLive2012'. There are also sections for 'PreAuthentication Access Control Lists' with a link to 'External WebAuthentication ACLs', and 'OfficeExtend AP' options which are currently unchecked. A 'Reset Personal SSID' button is located at the bottom of the configuration area.

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.



VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name CiscoLive2012

```
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

The image shows two screenshots of the Cisco FlexConnect configuration interface. The first screenshot, labeled '1', shows the 'FlexConnect' tab with the 'VLAN Mappings' button highlighted. The second screenshot, labeled '2', shows the 'VLAN Mappings' configuration page for AP_1142, with a table of WLAN Id, SSID, and VLAN ID mappings. The row for WLAN Id 20 (FlexConnect) with VLAN ID 502 is highlighted.

1

General | Credentials | Interfaces | High Availability | Inventory | FlexConnect

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name CiscoLive2012

PreAuthentication Access Control Lists

2

All APs > AP_1142 > VLAN Mappings

AP Name AP_1142

Base Radio MAC 00:22:90:92:ba:d0

| WLAN Id | SSID | VLAN ID |
|---------|-------------|----------------------------------|
| 21 | WebAuth | <input type="text" value="503"/> |
| 20 | FlexConnect | <input type="text" value="502"/> |

Centrally switched Wlans

| WLAN Id | SSID | VLAN ID |
|---------|------|---------|
|---------|------|---------|

- 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

The screenshot shows the Cisco Prime Network Control System interface. The top navigation bar includes Home, Monitor, Configure, Services, Reports, and Administration. The main content area is titled "Lightweight AP Template Detail : 'CiscoLive2012_Flex'". Below the title is a breadcrumb trail: "Configure > AP Configuration Templates > Lightweight AP > Lightweight AP Template Detail". A red box highlights the configuration options for the FlexConnect tab. On the left, there are checkboxes for "FlexConnect Configuration" (checked), "OfficeExtend" (unchecked), "Least Latency Controller Join" (unchecked), and "VLAN Support" (checked). A text field for "Native VLAN ID" contains the value "100". On the right, under "Profile Name-VLAN Mappings", there is a list of mappings: "FlexConnect" (checked) with a value of "502", "Michaels_Secure" (unchecked) with a value of "1", and "Michaels_Voice" (unchecked) with a value of "1".

Evaluate FlexConnect Architectural Requirements





FlexConnect Design Considerations

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
 - 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?

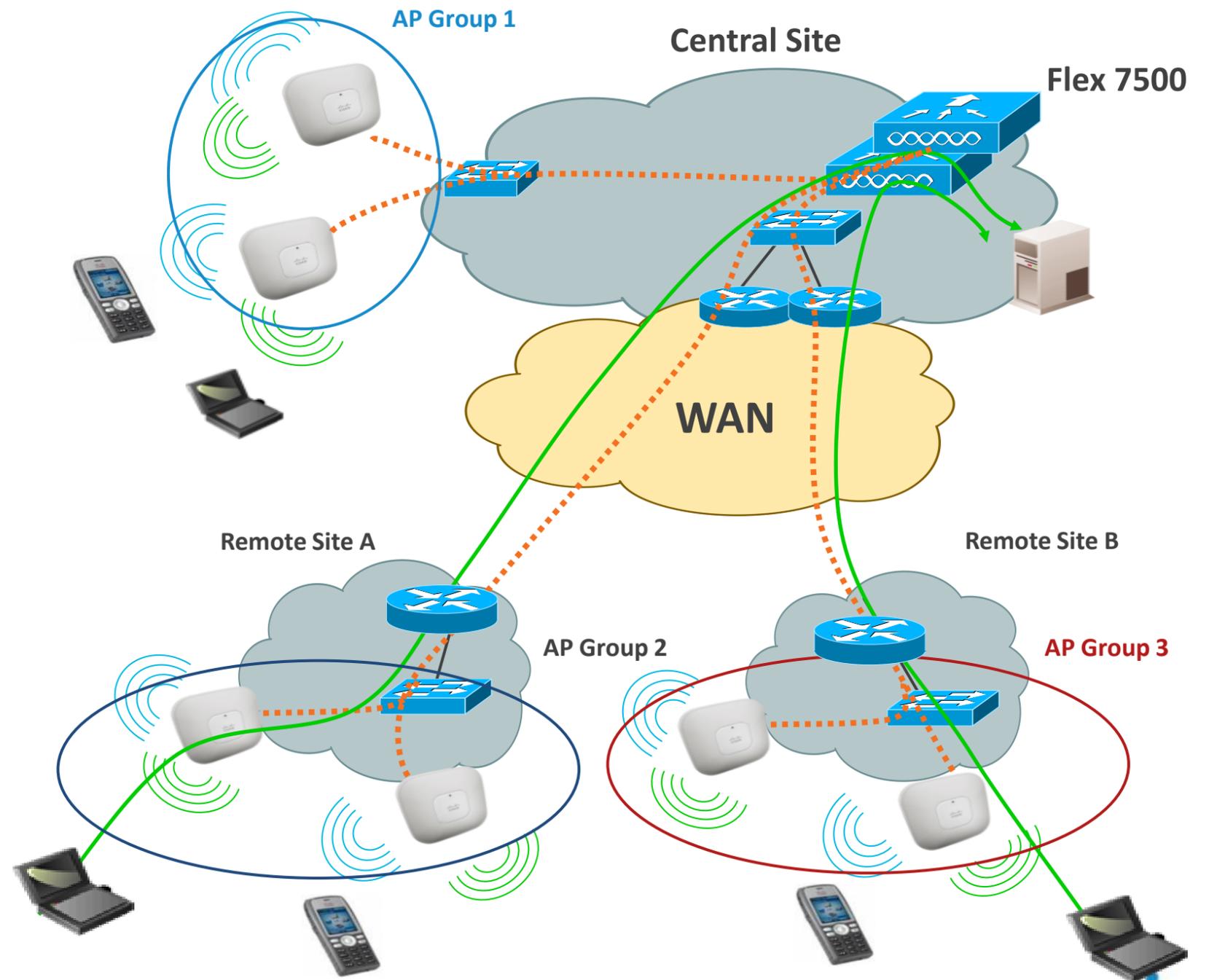


Understanding AP Groups

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

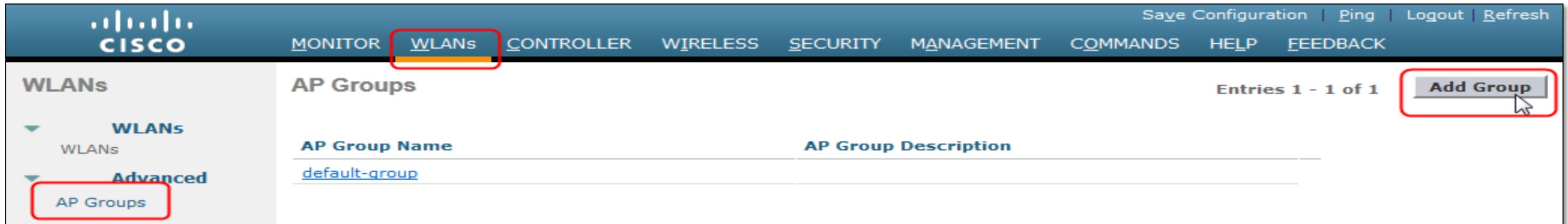
- An AP can be in only one AP Group
- One WLAN (SSID) can be in several AP Groups
- WLAN with ID 1-16 can not be removed from the ‘default-group’
- WLAN with ID greater than 16 will never be part of the ‘default-group’
- All AP with no AP Group name or an unknown AP Group name will be part of the ‘default-group’

■ 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



The screenshot shows the Cisco configuration interface for AP Groups. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu is expanded, and 'AP Groups' is selected. The main content area displays 'AP Groups' with a table containing one entry: 'default-group'. An 'Add Group' button is highlighted with a red box in the top right corner. The left sidebar shows 'WLANs' and 'Advanced' menus, with 'AP Groups' also highlighted.



The screenshot shows the 'Add New AP Group' dialog box. The dialog has two input fields: 'AP Group Name' with the value 'AP-Group-1' and 'Description' with the value 'AP Group for Site 1'. Below the fields are 'Add' and 'Cancel' buttons. The dialog is highlighted with a red box. The background shows the same configuration page as the first screenshot, but the 'Add Group' button is no longer highlighted.

AP Groups

Configuration: Add AP or APs to Group

Ap Groups > Edit 'AP-Group-1' < Back

General | **WLANs** | **RF Profile** | **APs** | **802.11u**

APs currently in the Group Remove APs

| <input type="checkbox"/> AP Name | Ethernet MAC |
|----------------------------------|--------------|
| | |

Add APs to the Group Add APs

| <input type="checkbox"/> AP Name | Group Name |
|---|---------------|
| <input checked="" type="checkbox"/> AP-1140-B | default-group |
| <input type="checkbox"/> AP-CleanAir-Sur-RackMobi | default-group |
| <input type="checkbox"/> AP-CleanAir-Sur-RackSecu | default-group |
| <input type="checkbox"/> AP-CleanAir-Mur | default-group |
| <input checked="" type="checkbox"/> AP-1140-A | default-group |



Ap Groups > Edit 'AP-Group-1' < Back

General | **WLANs** | **RF Profile** | **APs** | **802.11u**

APs currently in the Group Remove APs

| <input type="checkbox"/> AP Name | Ethernet MAC |
|------------------------------------|-------------------|
| <input type="checkbox"/> AP-1140-A | 00:22:90:90:9a:4a |
| <input type="checkbox"/> AP-1140-B | 00:22:90:e3:37:be |

Add APs to the Group Add APs

| <input type="checkbox"/> AP Name | Group Name |
|---|---------------|
| <input type="checkbox"/> AP-CleanAir-Sur-RackMobi | default-group |
| <input type="checkbox"/> AP-CleanAir-Sur-RackSecu | default-group |
| <input type="checkbox"/> AP-CleanAir-Mur | default-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**

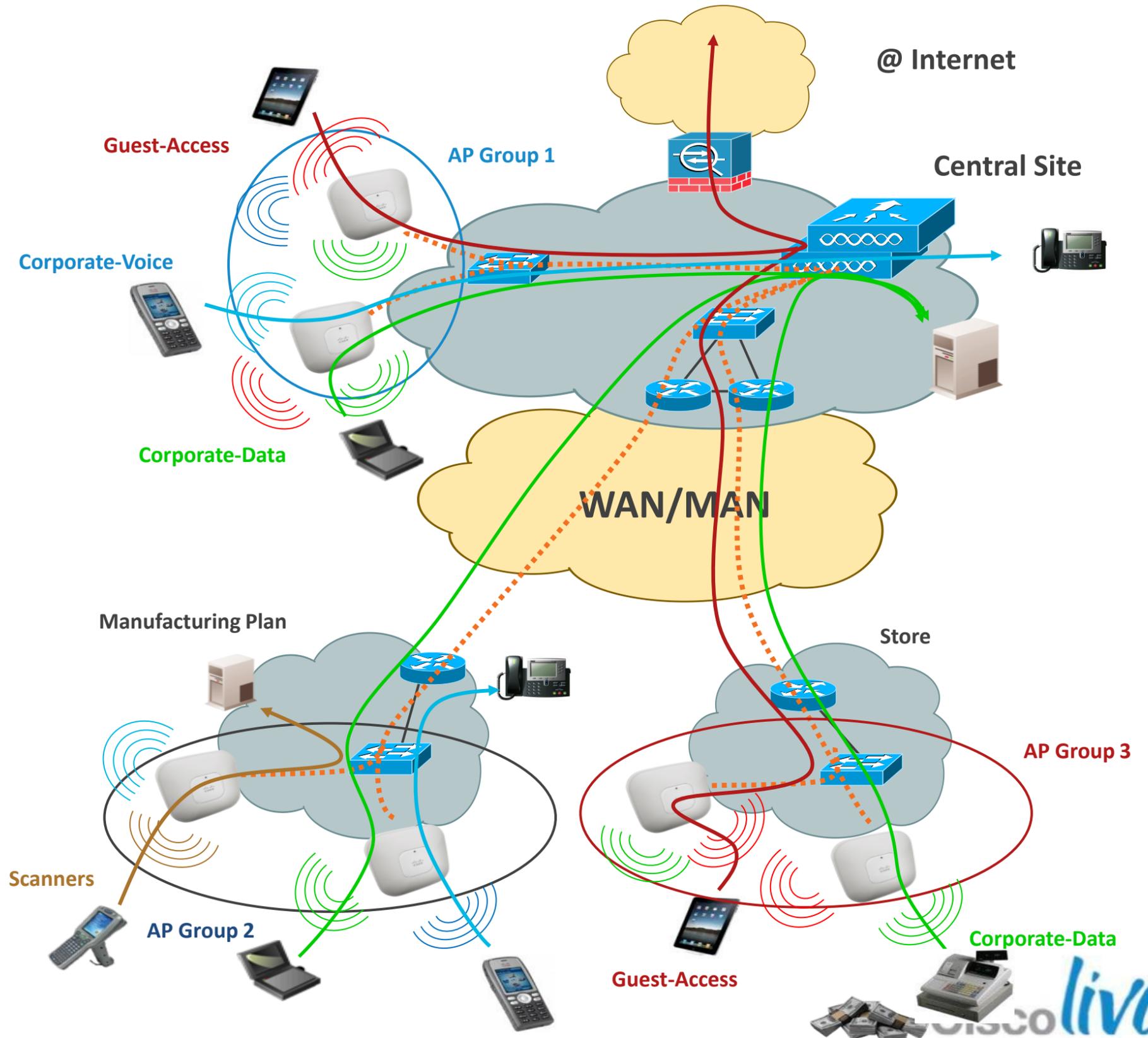
Corporate-Voice,
Corporate-Data,
Guest-Access

- **Manufacturing Plant**

Corporate-Voice,
Corporate-Data,
Scanners

- **Store**

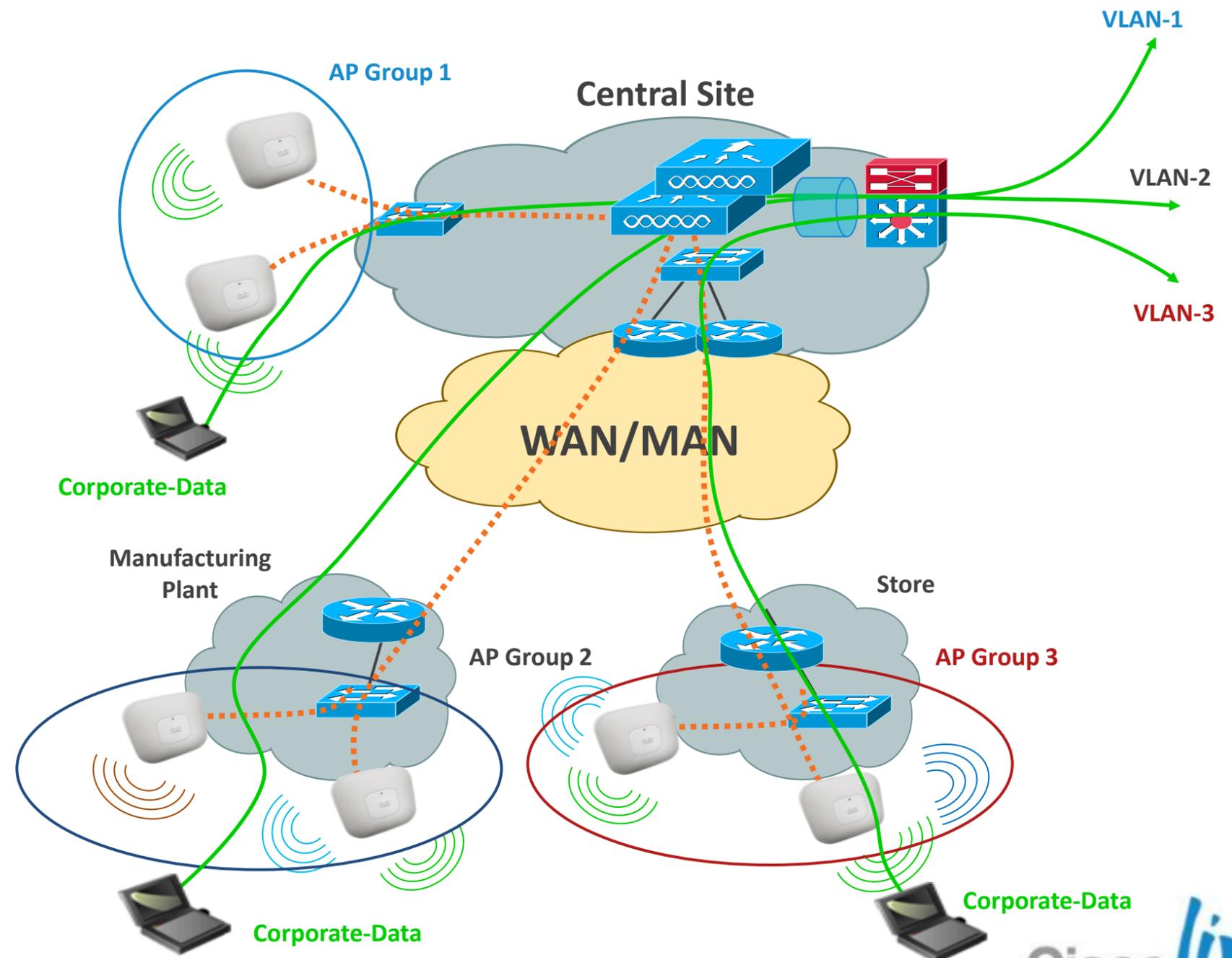
Corporate-Data,
Guest-Access



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

Ap Groups > Edit 'AP-Group-1'

General **WLANs** RF Profile APs 802.11u

Add New

WLAN SSID: RackMobility(1)

Interface /Interface Group(G): partenaires [1](#)

SNMP NAC State: Enabled

Add Cancel

Add New

Ap Groups > Edit 'AP-Group-1' [< Back](#)

General **WLANs** RF Profile APs 802.11u

Add New

| WLAN ID | WLAN SSID | Interface/Interface Group(G) | SNMP NA |
|---------|--------------|------------------------------|----------|
| 1 | RackMobility | partenaires | Disabled |

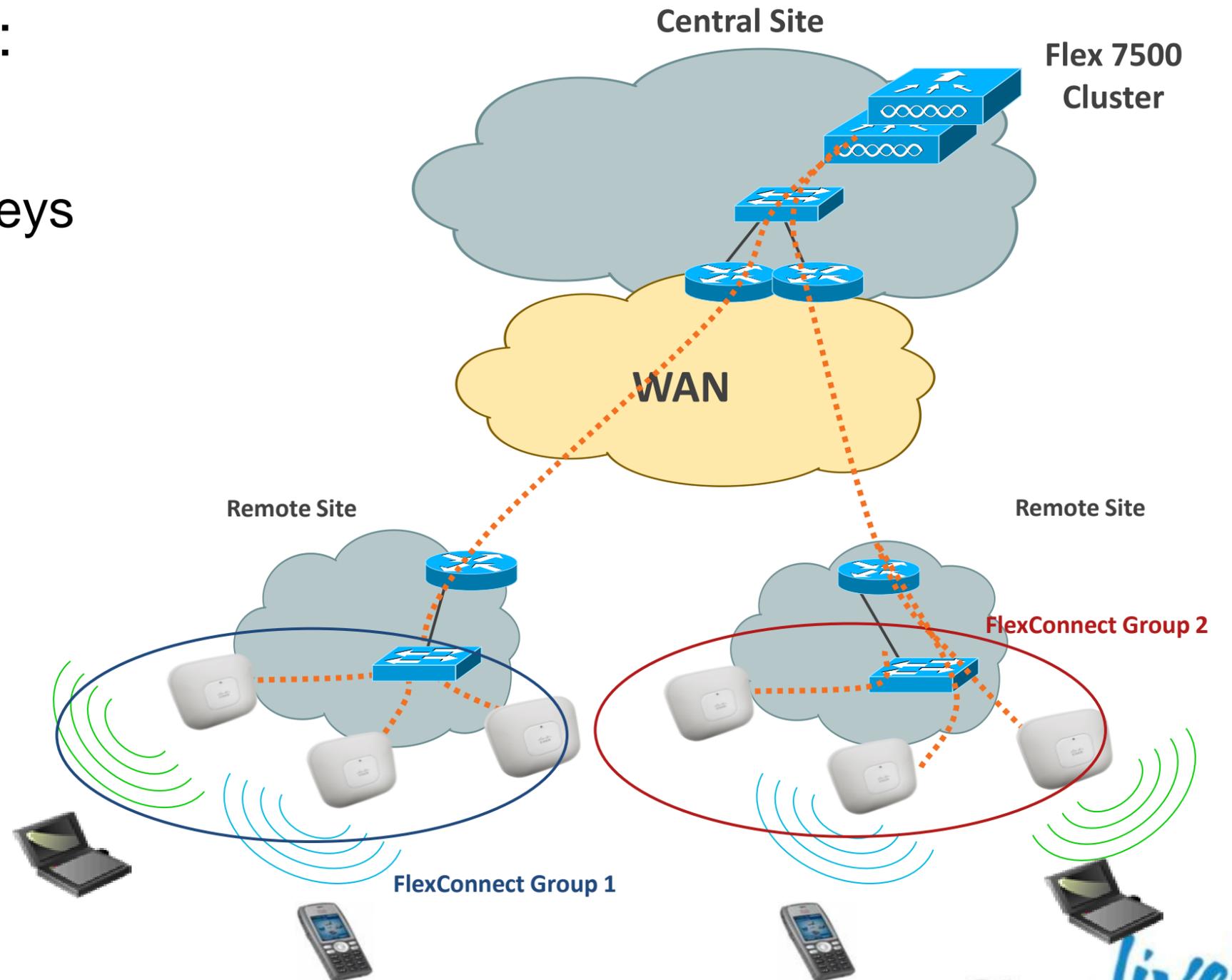
Understanding FlexConnect Groups

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

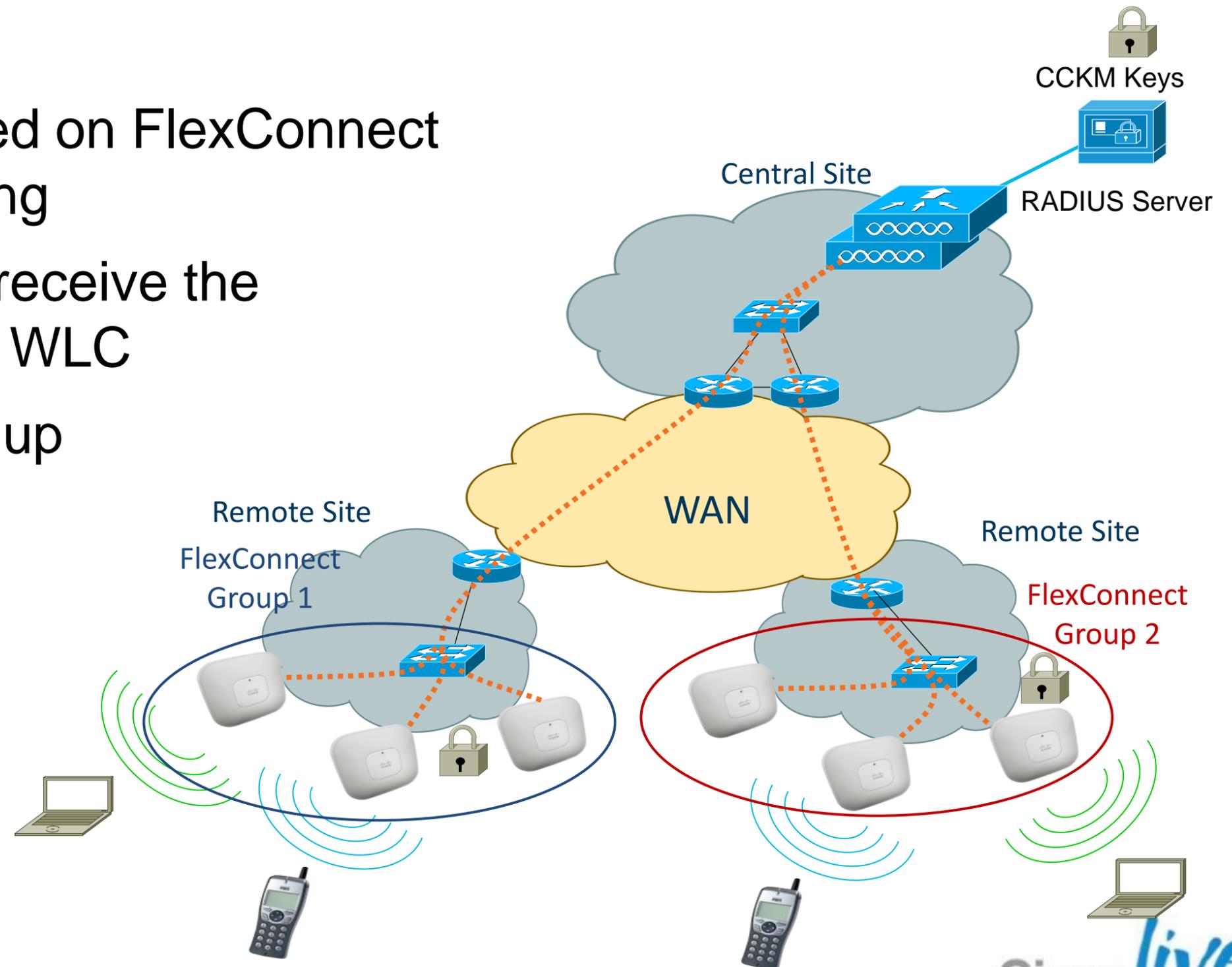
Scaling information

| 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

The screenshot displays the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The 'WIRELESS' tab is highlighted with a red box and a circled '1'. The left sidebar shows the 'FlexConnect Groups' menu item highlighted with a red box. The main content area shows the 'FlexConnect Groups > New' configuration page. The 'Group Name' field is populated with 'FlexConnect-Site-1'. A blue arrow points from this field to the 'FlexConnect Groups > Edit 'FlexConnect-Site-1'' configuration page, which is also circled with a '2'. This edit page has tabs for 'General', 'Local Authentication', 'Image Upgrade', and 'VLAN-ACL mapping'. The 'Local Authentication' tab is active. It shows the 'Group Name' as 'FlexConnect-Site-1' and a section for 'FlexConnect APs'. Under 'Add AP', there is a checkbox for 'Select APs from current controller' (unchecked), an 'Ethernet MAC' input field, and 'Add' and 'Cancel' buttons. Below this is a table with columns for 'AP MAC Address', 'AP Name', and 'Status'. One entry is shown: '00:22:90:90:9a:4a', 'AP-1140-A', and 'Associated'.

Step 2: Add APs to the FlexConnect Group

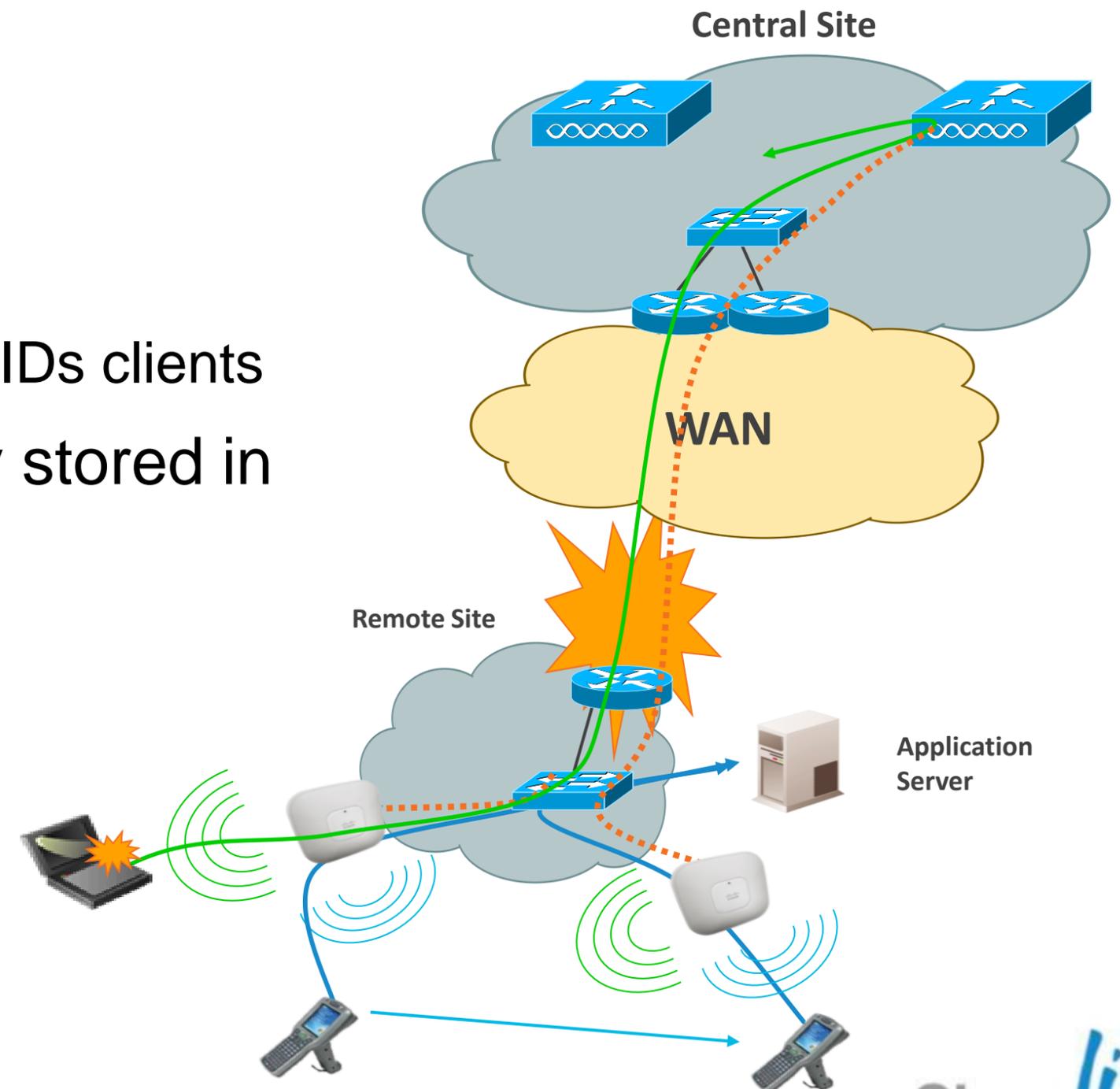
Design Wireless Branch Designing a Resilient Network



FlexConnect Backup Scenario

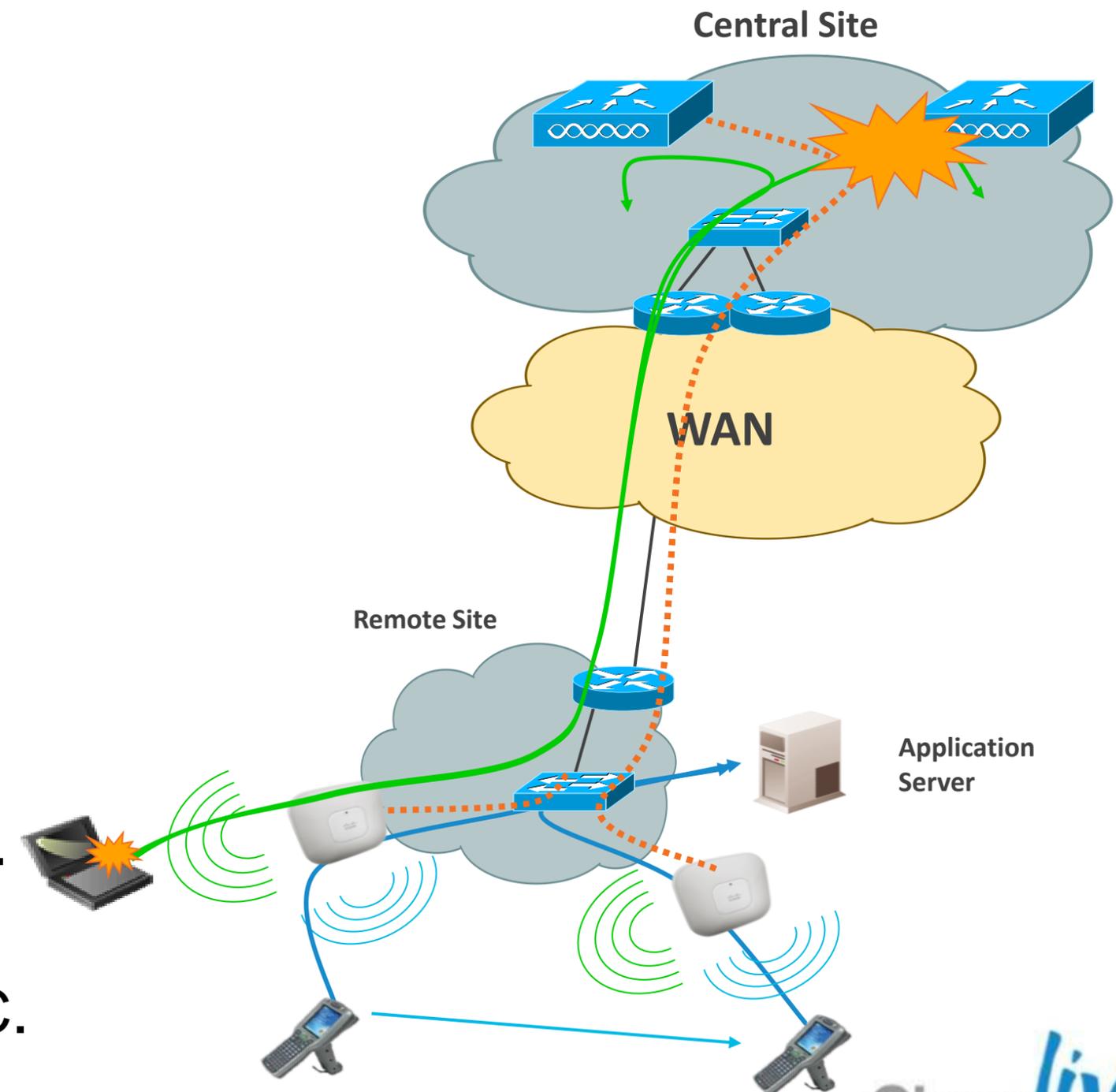
WAN Failure

- 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

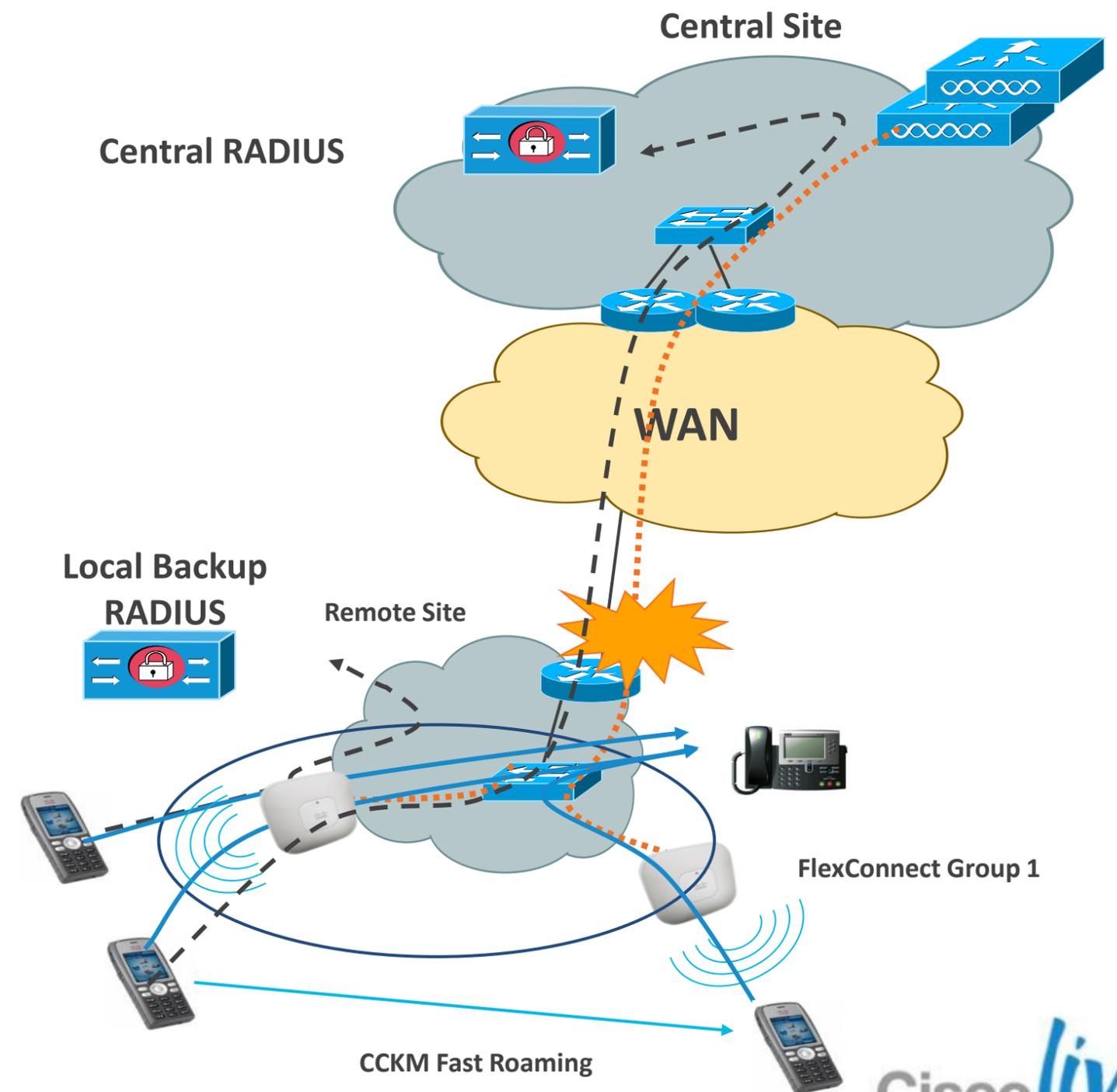
- FlexConnect will first backup on local switched mode
 - No impact for locally switched SSIDs
 - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with WLC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

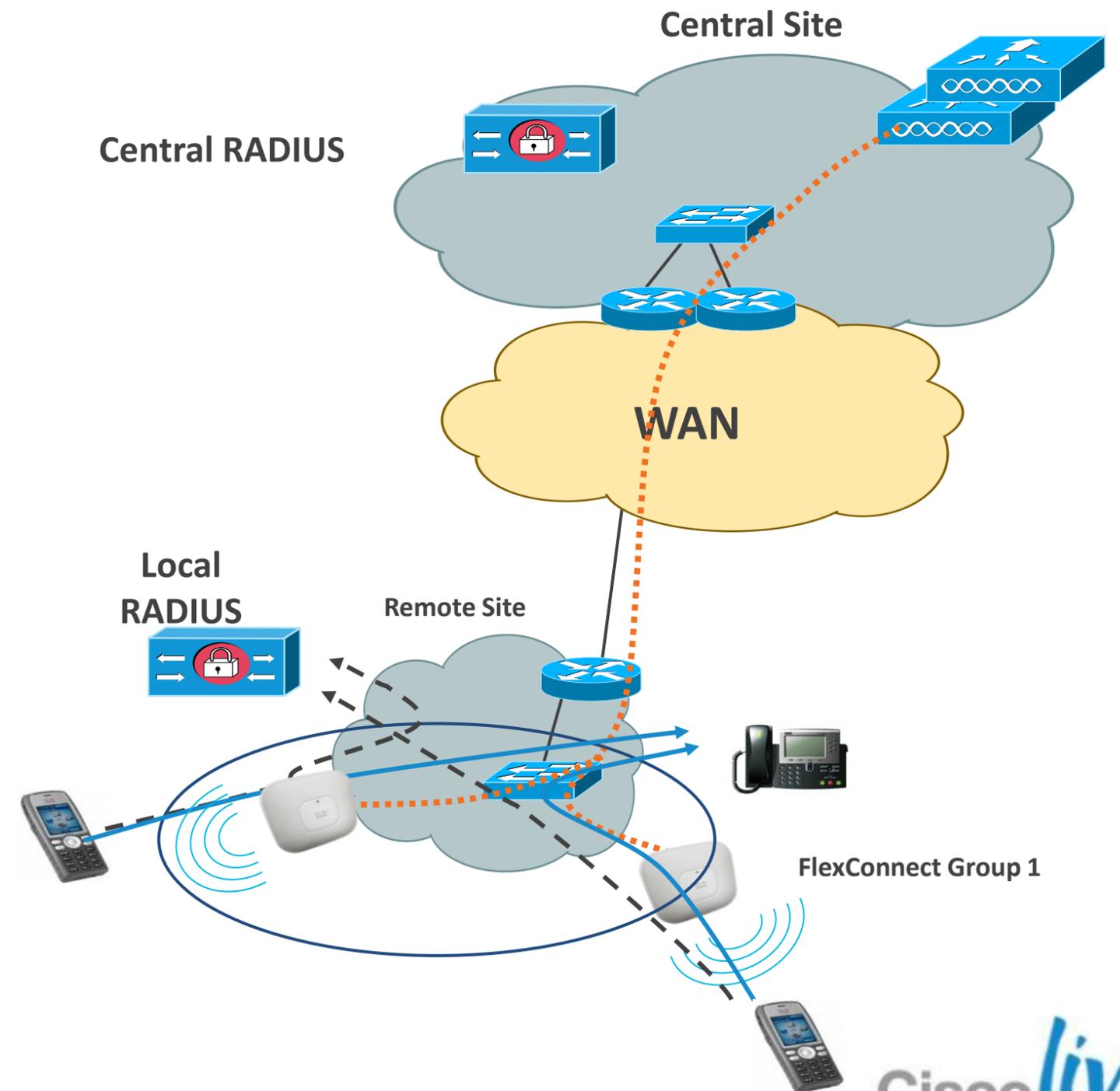
The screenshot shows the configuration page for the 'SanJose' FlexConnect Group. The 'Local Authentication' tab is active. The 'Group Name' is 'SanJose'. Under 'FlexConnect APs', there is a table with two entries:

| AP MAC Address | AP Name | Status | |
|-------------------|-----------------|------------|-------------------------------------|
| 1c:df:0f:94:bb:e9 | Branch-AP2-1040 | Associated | <input checked="" type="checkbox"/> |
| c4:71:fe:49:f6:59 | Branch-AP1 | Associated | <input checked="" type="checkbox"/> |

Under the 'AAA' section, the 'Primary Radius Server' is set to 'IP:11.11.11.15, Port:1812'. The 'Secondary Radius Server' is set to 'None'. The 'Enable AP Local Authentication' checkbox is checked.

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

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'RackMobility' < Back Apply

General Security QoS **Advanced**

Maximum Allowed Clients 802.11b/g/n (1 - 255) 1

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching Enabled

FlexConnect Local Auth Enabled

Learn Client IP Address Enabled

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Passive Client

Passive Client

Voice

Media Session Snooping Enabled

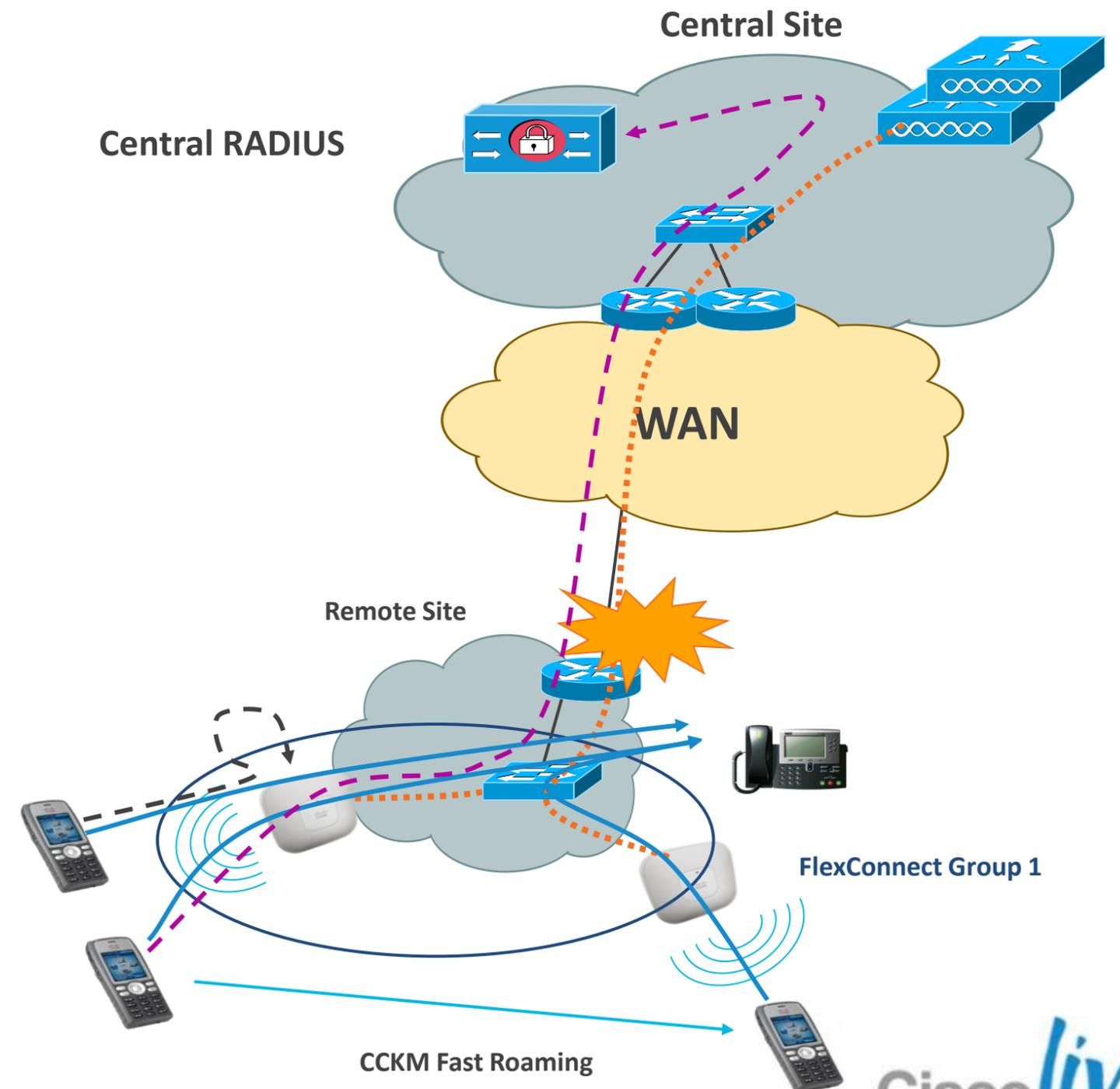
Re-anchor Roamed Voice Clients Enabled

KTS based CAC Policy Enabled

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 Groups > Edit 'CiscoLive2012' **1**

General **Local Authentication** **Image Upgrade**

Local Users **Protocols**

No of Users 2

User Name

| | |
|----------------|---|
| CiscoLiveUser1 | ▼ |
| CiscoLiveUser2 | ▼ |

Local Users **Protocols** **2**

LEAP

Enable LEAP Authentication

EAP Fast

Enable EAP Fast Authentication

Server Key (in hex) Enable Auto key generation

Authority ID (in hex)

Authority Info

PAC Timeout (2 to 4095 days)

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

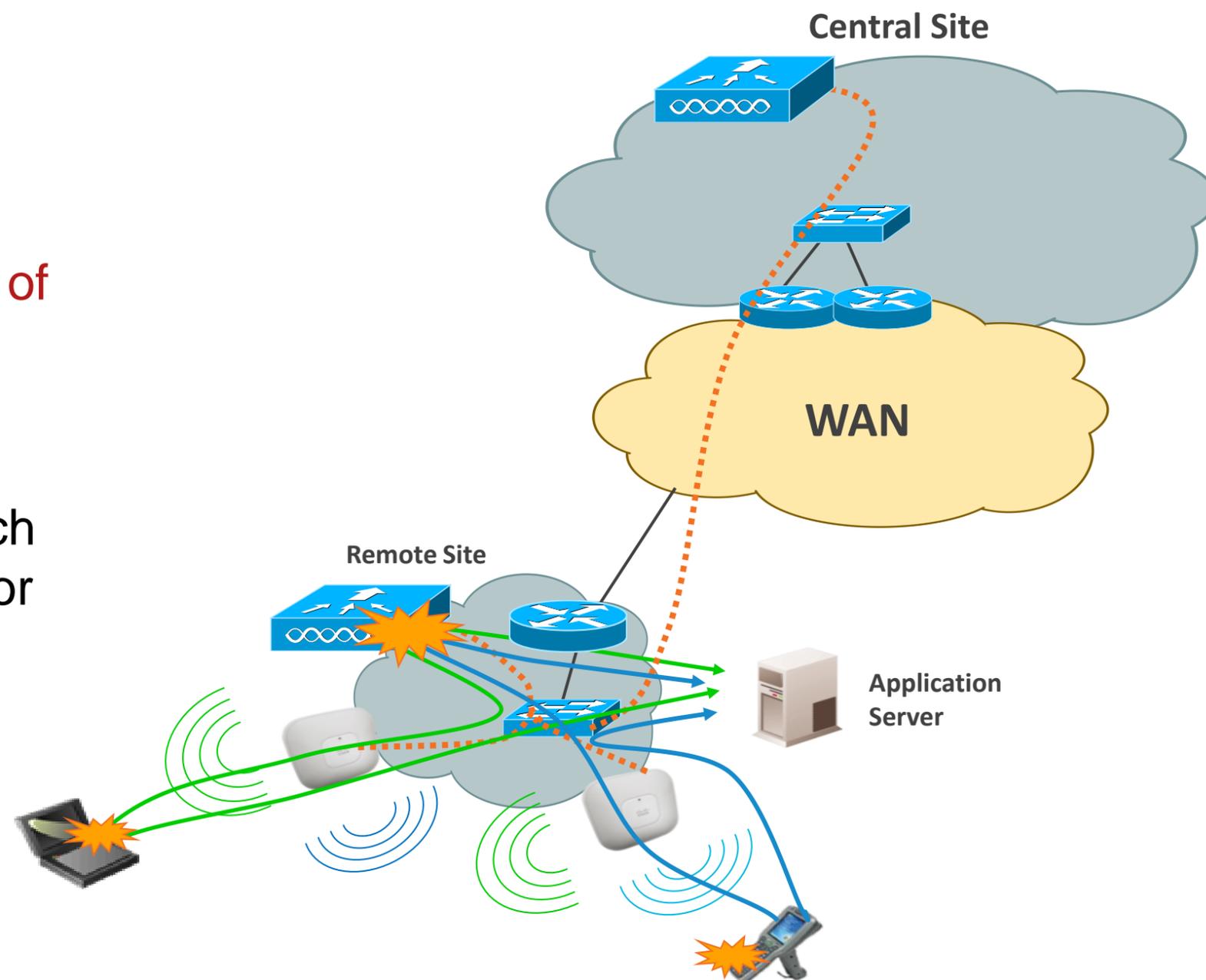
Changing mode is a configuration task of the AP

- 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

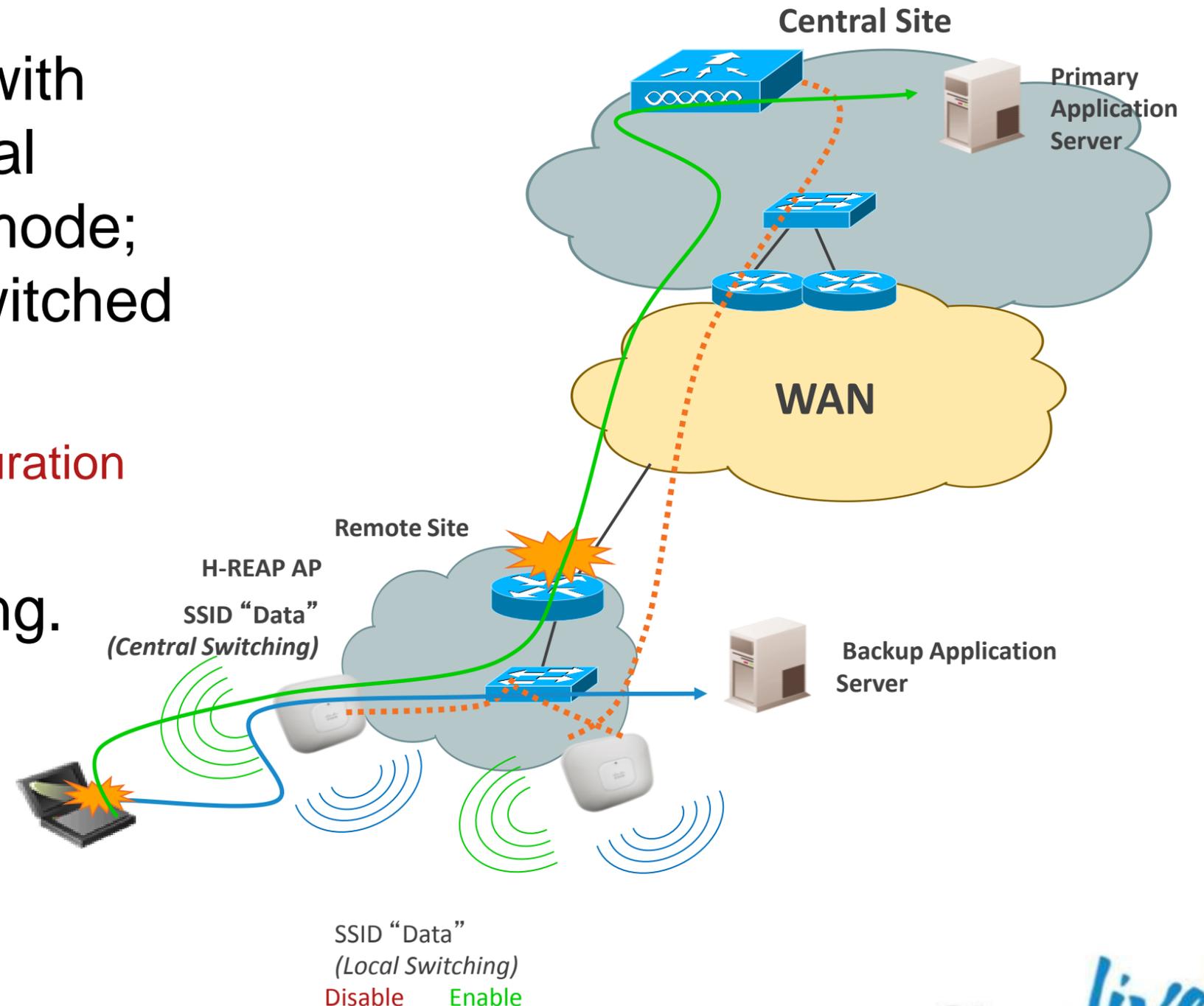
Changing enable status of an SSID is a configuration task of the WLC level

- Cisco recommends using Local Switching. Why?

Fault Tolerance will always keep client connection UP.



Not Supported Backup Scenario



Failover Matrix



| 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 |

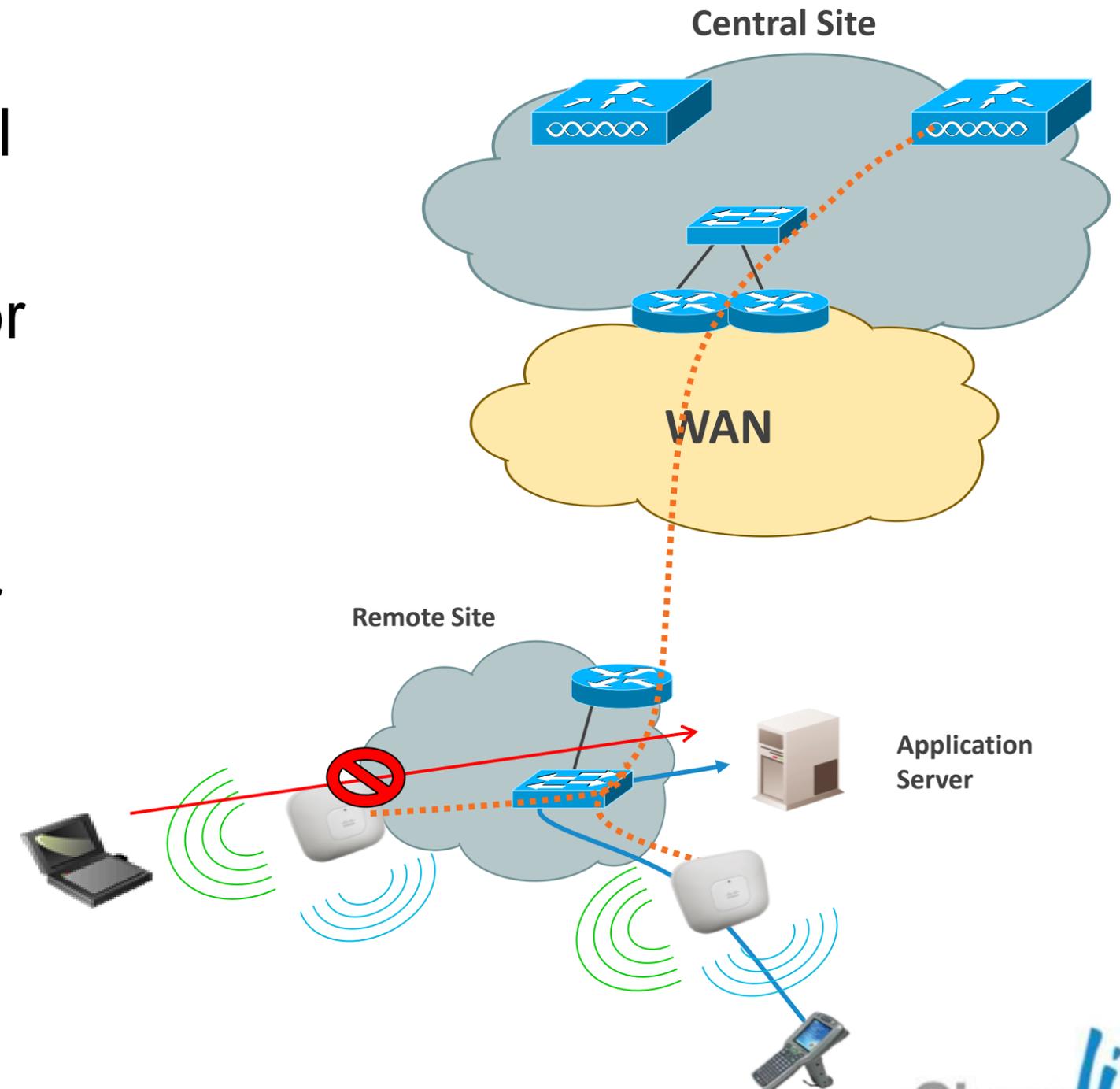
Designing Secure & BYOD Enabled Branch Network



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

Click to add ACL rules

Step 2

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest |
|-------------------|--------|-----------------------------|--------------------------------------|----------|-------------|------|
| 1 | Permit | 192.168.3.0 / 255.255.255.0 | 192.168.3.1 / 255.255.255.255 | Any | Any | Any |
| 2 | Deny | 192.168.3.0 / 255.255.255.0 | 192.168.3.0 / 255.255.255.0 | Any | Any | Any |

Step 3

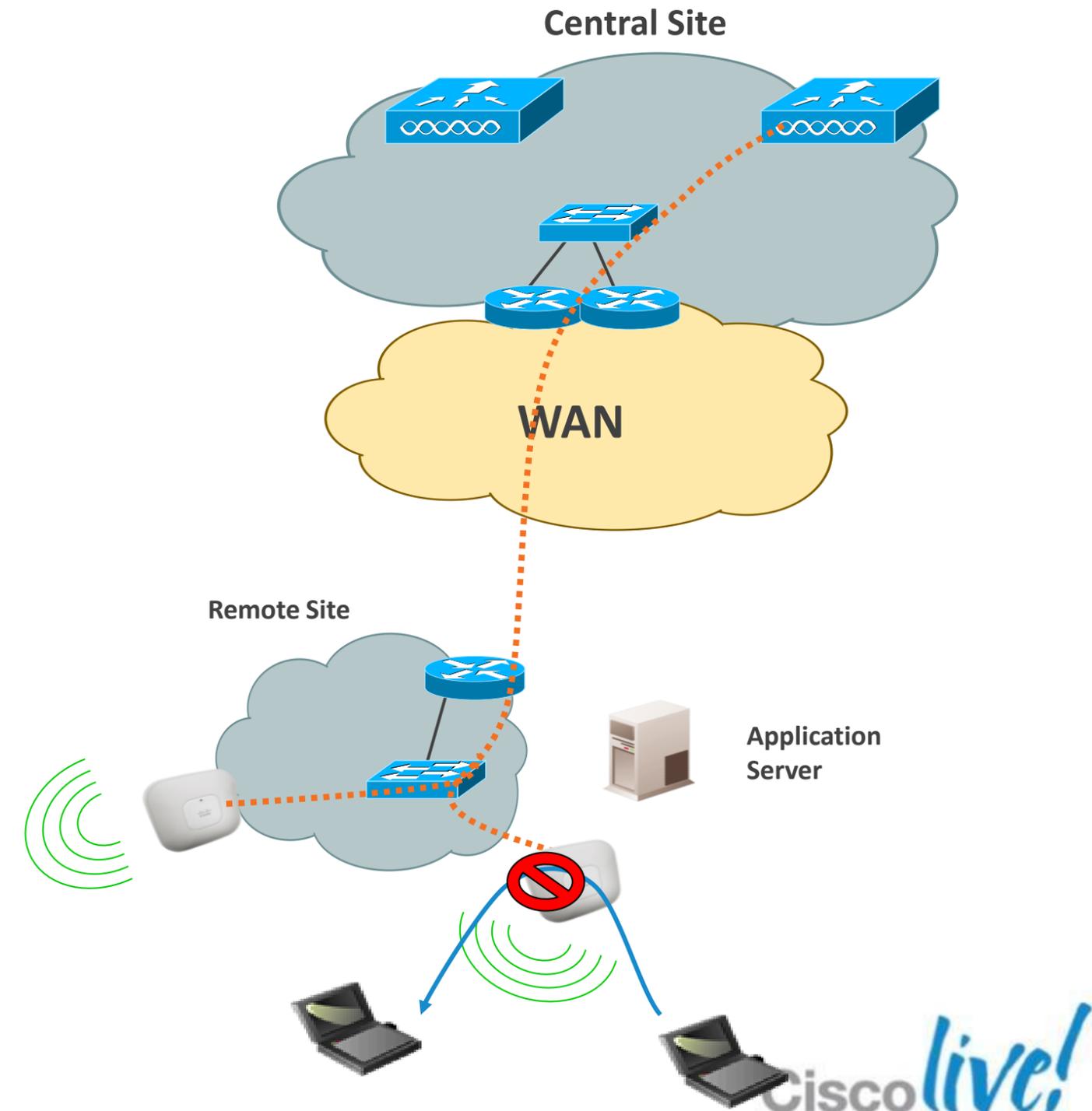
Provision to assign separate Inbound & Outbound ACLs

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

WLANs > Edit 'FlexDemo'

General Security QoS Advanced

P2P Blocking Action Disabled

Client Exclusion [3](#)

Maximum Allowed Clients [0](#)

Disabled

Drop

Forward-UpStream (secs)

=

WLANs > Edit 'FlexDemo'

General Security QoS Advanced

P2P Blocking Action

Client Exclusion [3](#)

Maximum Allowed Clients [0](#)

Disabled

Drop

Forward-UpStream (secs)

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

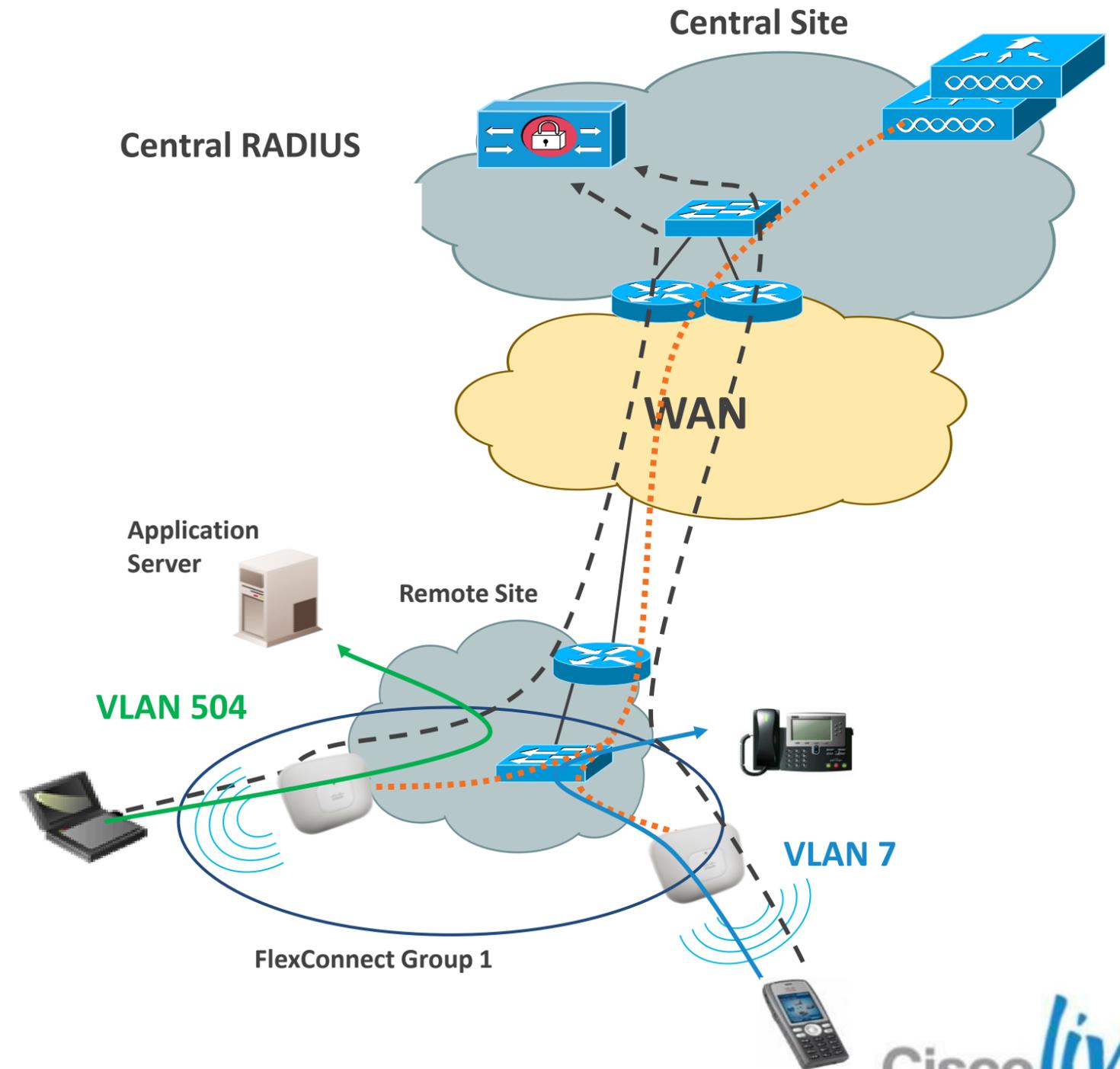
* Central Switching WLAN will support "Forward - UpStream" and will send the packet to the next upstream node connected to WLC

FlexConnect AAA VLAN Override

New in 7.2

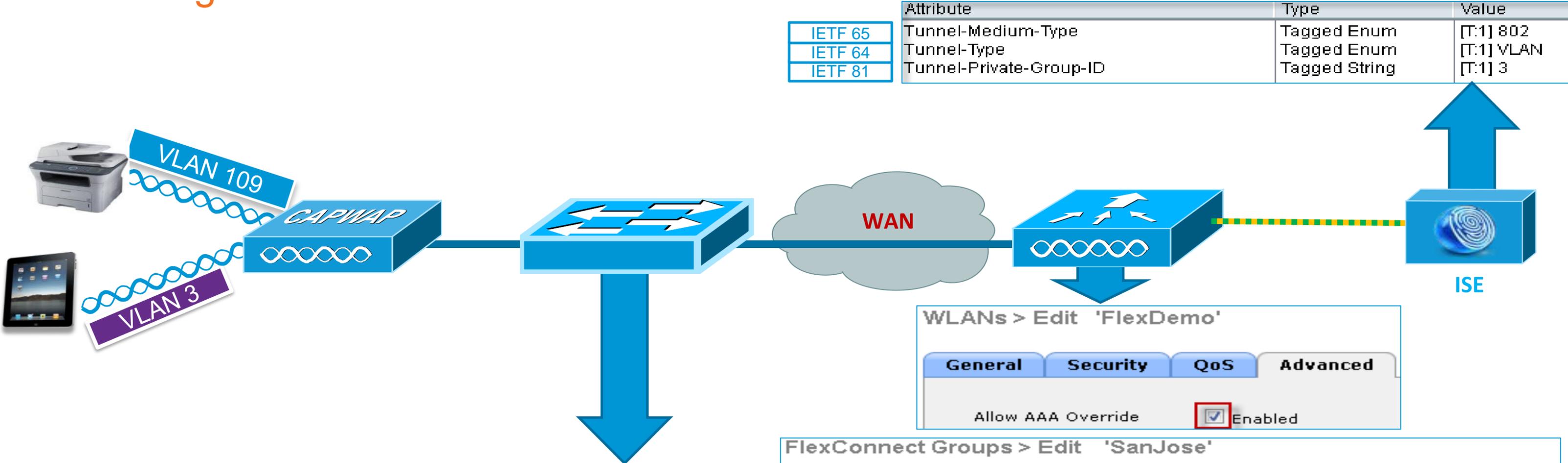
Description

- 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



```
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

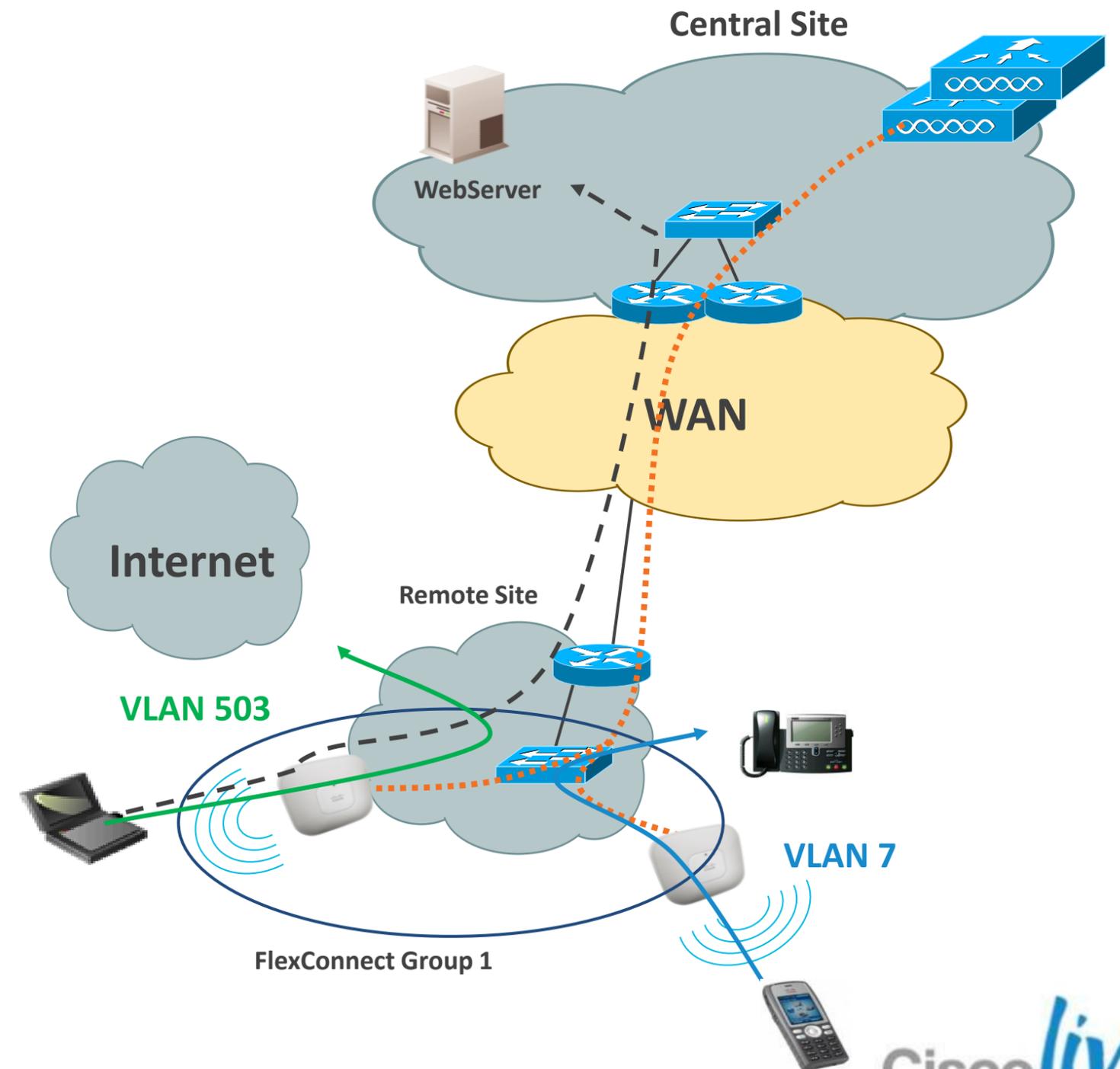
Add

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

FlexConnect Access Control Lists

Acl Name

- FlexConnect
- Flex AAA Override ACL
- Pre-WebAuthPolicy-ACL**
- WebAuth ACL

Access Control Lists > Edit

General

Access List Name: Pre-WebAuthPolicy-ACL

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP |
|----------|--------|-------------------|--------------------------------|----------|-------------|-----------|------|
| <u>1</u> | Permit | 0.0.0.0 / 0.0.0.0 | 192.168.1.11 / 255.255.255.255 | Any | Any | Any | Any |

External Web-Server IP

External WebAuth with Local Switching

Configuration

Step 2: Apply Pre-Auth ACL to WLAN

WLANs > Edit 'WebAuth'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security

Web Policy [1](#)

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure [10](#)

Preauthentication ACL IPv4 IPv6 WebAuth FlexAcl

Over-ride Global Config Enable

Apply Pre-Auth ACL to WLAN

External WebAuth with Local Switching

Configuration

Step 3: Apply Pre-Auth ACL to FlexConnect Group

FlexConnect Groups > Edit 'CiscoLive2012'

General Local Authentication Image Upgrade VLAN-ACL mapping **WLAN-ACL mapping**

WLAN ACL Mapping

WLAN Id

WebAuth ACL

| WLAN Id | WLAN Profile Name | WebAuth ACL |
|---------|-------------------|--|
| 21 | WebAuth | <input type="text" value="Pre-WebAuthPolicy-ACL"/> |

Map WLAN-Id to Pre-Auth ACL

External WebAuth with Local Switching

Configuration

Step 4: Configure External Web Server

The screenshot shows the Cisco configuration interface for the 'Web Login Page'. The 'Web Authentication Type' is set to 'External (Redirect to external server)'. The 'Redirect URL after login' is 'http://www.cisco.com'. The 'External Webauth URL' is 'http://192.168.1.11/login.html', which is highlighted with a red box. A blue callout box with a white border points to this field, containing the text 'External Web-Server IP'.

| | |
|--------------------------|--|
| Web Authentication Type | External (Redirect to external server) |
| Redirect URL after login | http://www.cisco.com |
| External Webauth URL | http://192.168.1.11/login.html |

External WebAuth with Local Switching

Configuration Verification

Finally ensure ACL assignment is correct at AP

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name CiscoLive2012

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)



All APs > AP_1142 > ACL Mappings

AP Name AP_1142

Base Radio MAC 00:22:90:92:ba:d0

WLAN ACL Mapping

WLAN Id

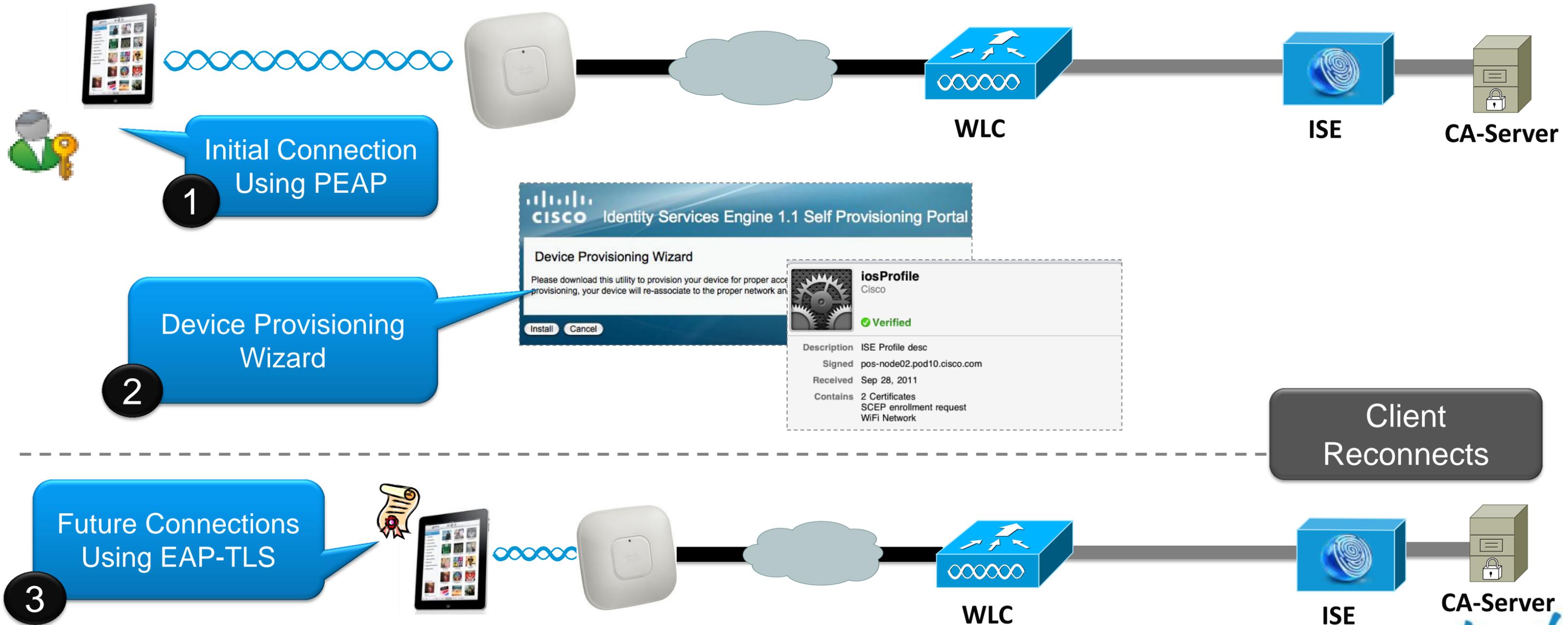
WebAuth ACL **Add**

| WLAN Id | WLAN Profile Name | WebAuth ACL |
|---------|-------------------|--|
| 21 | WebAuth | Pre-WebAuthPolicy-ACL <input type="text" value="Pre-WebAuthPolicy-ACL"/> |

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

The screenshot displays the Cisco ISE configuration interface. On the left, a navigation tree shows 'Security' > 'AAA' > 'RADIUS' > 'Authentication'. The main area is titled 'RADIUS Authentication Servers > New'. It contains several configuration fields: 'Server Index (Priority)' set to 3, 'Server IP Address' set to 10.10.10.10, 'Shared Secret Format' set to ASCII, and two masked 'Shared Secret' fields. A checkbox for '(Designed for FIPS customers and requires a key wrap compliant RADIUS server)' is unchecked. Below this, 'Server Status' is set to 'Enabled', and 'Support for RFC 3576' is also set to 'Enabled'. A blue callout bubble with the number '1' points to the 'Support for RFC 3576' field, containing the text 'Enable "RFC 3576" for Support Change of Authorisation'. Below the authentication configuration is the 'RADIUS Accounting Servers' section. It includes a 'MAC Delimiter' dropdown set to 'Hyphen'. Below this is a table with columns: 'Network User', 'Server Index', 'Server Address', 'Port', 'IPSec', 'Admin Status', and a dropdown arrow. The table contains one entry: a checked checkbox, '1', '10.10.10.10', '1813', 'Disabled', 'Enabled', and a dropdown arrow. A blue callout bubble with the number '2' points to this table, containing the text 'Add to Accounting Servers to Receive Session Statistics'.

1 Enable "RFC 3576" for Support Change of Authorisation

2 Add to Accounting Servers to Receive Session Statistics

| Network User | Server Index | Server Address | Port | IPSec | Admin Status |
|-------------------------------------|-------------------|----------------|------|----------|--------------|
| <input checked="" type="checkbox"/> | 1 | 10.10.10.10 | 1813 | Disabled | Enabled |

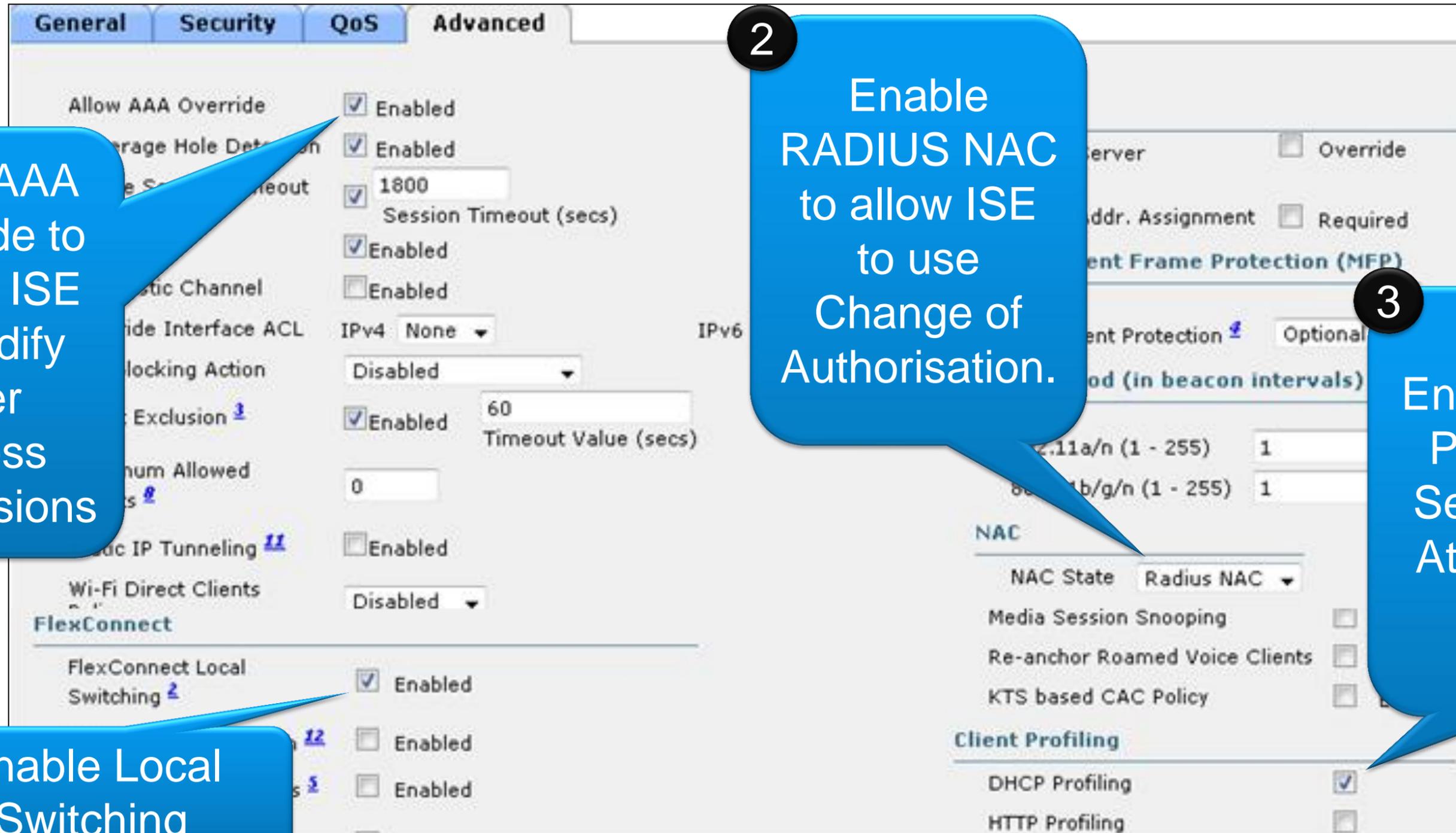
Configuring the WLAN for Secure Connectivity

Enabling Secure Authentication and Encryption with WPA2-Enterprise

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'CorporateX'. The navigation menu at the top includes MONITOR, WLANs (selected), CONTROLLER, WIRELESS, and SECURITY. The left sidebar shows the configuration tree with 'WLANs' expanded to 'Advanced'. The main content area has tabs for General, Security (selected), QoS, and Advanced. Under the Security tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The Layer 2 Security is set to 'WPA+WPA2'. Below this, there is a checkbox for 'MAC Filtering' which is unchecked. The 'WPA+WPA2 Parameters' section includes: 'WPA Policy' (unchecked), 'WPA2 Policy' (checked), 'WPA2 Encryption' with 'AES' checked and 'TKIP' unchecked, 'Auth Key Mgmt' set to '802.1X', and 'WPA gtk-randomize State' set to 'Enable'.

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

The screenshot shows the configuration page for ISE Profiling Sensors. It is organized into several sections, each with a checkbox and a title:

- NETFLOW**: A section with a checked checkbox and a right-pointing arrow.
- DHCP**: A section with a checked checkbox and a downward-pointing arrow. It contains three input fields: "Interface" (GigabitEthernet 0), "Port" (67), and "Description" (DHCP).
- DHCPSPAN**: A section with a checked checkbox and a right-pointing arrow.
- HTTP**: A section with a checked checkbox and a downward-pointing arrow. It contains two input fields: "Interface" (GigabitEthernet 0) and "Description" (HTTP).
- RADIUS**: A section with a checked checkbox and a right-pointing arrow.
- Network Scan (NMAP)**: A section with a checked checkbox and a downward-pointing arrow. It contains two input fields: "Description" (NMAP) and "Manual Scan Subnet" (empty). Below these are "Run Scan" and "Cancel Scan" buttons, and a link "Click to see latest scan results".
- DNS**: A section with a checked checkbox and a downward-pointing arrow.

- 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.

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
 - Access Control Lists
 - CPU Access Control Lists
 - FlexConnect ACLs

Access Control Lists > Edit

< Back Add New Rule

General

Access List Name ACL-Web-Redirect

Deny Counters 0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|----------|--------|----------------|---------------------|----------|-------------|-----------|------|-----------|----------------|
| <u>1</u> | Permit | 0.0.0.0 / | 10.10.10.10 / | Any | Any | Any | Any | Inbound | 0 |
| <u>2</u> | Permit | 0.0.0.0 / | 255.255.255.255 / | Any | Any | Any | Any | Outbound | 0 |

1 This ACL will be referenced by name by the ISE to restrict the user.

2 Use the ISE server's IP address to allow only traffic to that site.

Create WebPolicies for FlexConnect Group

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

FlexConnect Groups > Edit 'CiscoLive 2012'

General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping WebPolicies

WebPolicies

WebPolicy ACL

WebPolicy Access Control Lists

ACL-Web-Redirect

This will force all the APs in this FlexConnect Group to support Device On-Boarding

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

The screenshot shows the configuration page for AP-1140-1, with the 'Advanced' tab selected. The 'Link Latency' section is highlighted with a red box. It shows the 'Enable Link Latency' checkbox checked. Below it is a table with latency data.

| | Current (mSec) | Minimum (mSec) | Maximum (mSec) |
|--------------|----------------|----------------|----------------|
| Link Latency | <1 | <1 | <1 |
| Data Latency | <1 | <1 | <1 |

Other settings visible include: Regulatory Domains (FR (France)), AP Group Name (AP-Group-1), Statistics Timer (180), and various protocol checkboxes (Rogue Detection, Telnet, SSH, TCP Adjust MSS). The 'Power Over Ethernet Settings' and 'AP Core Dump' sections are also visible on the right.

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”

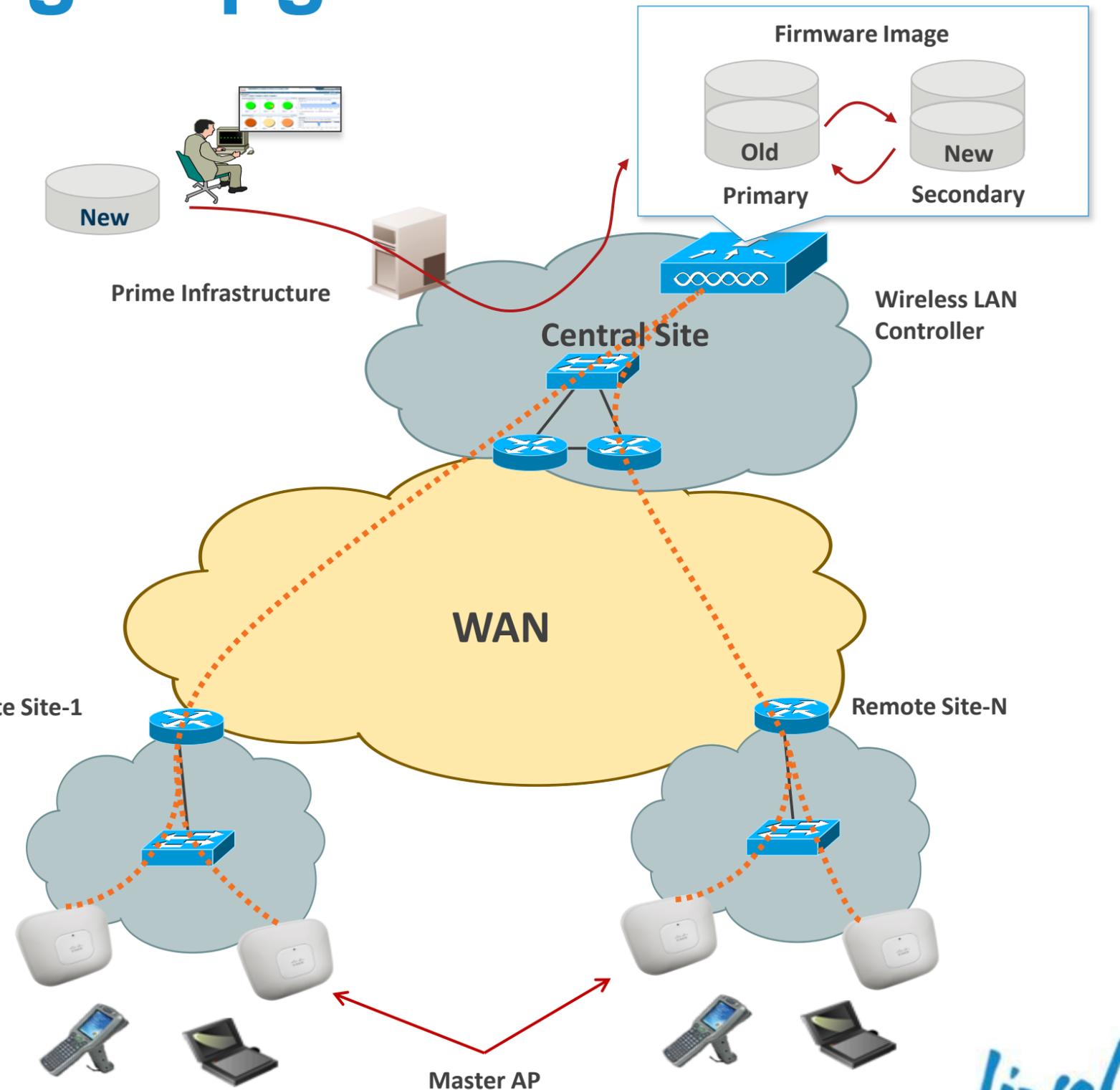
FlexConnect Smart AP Image Upgrade

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

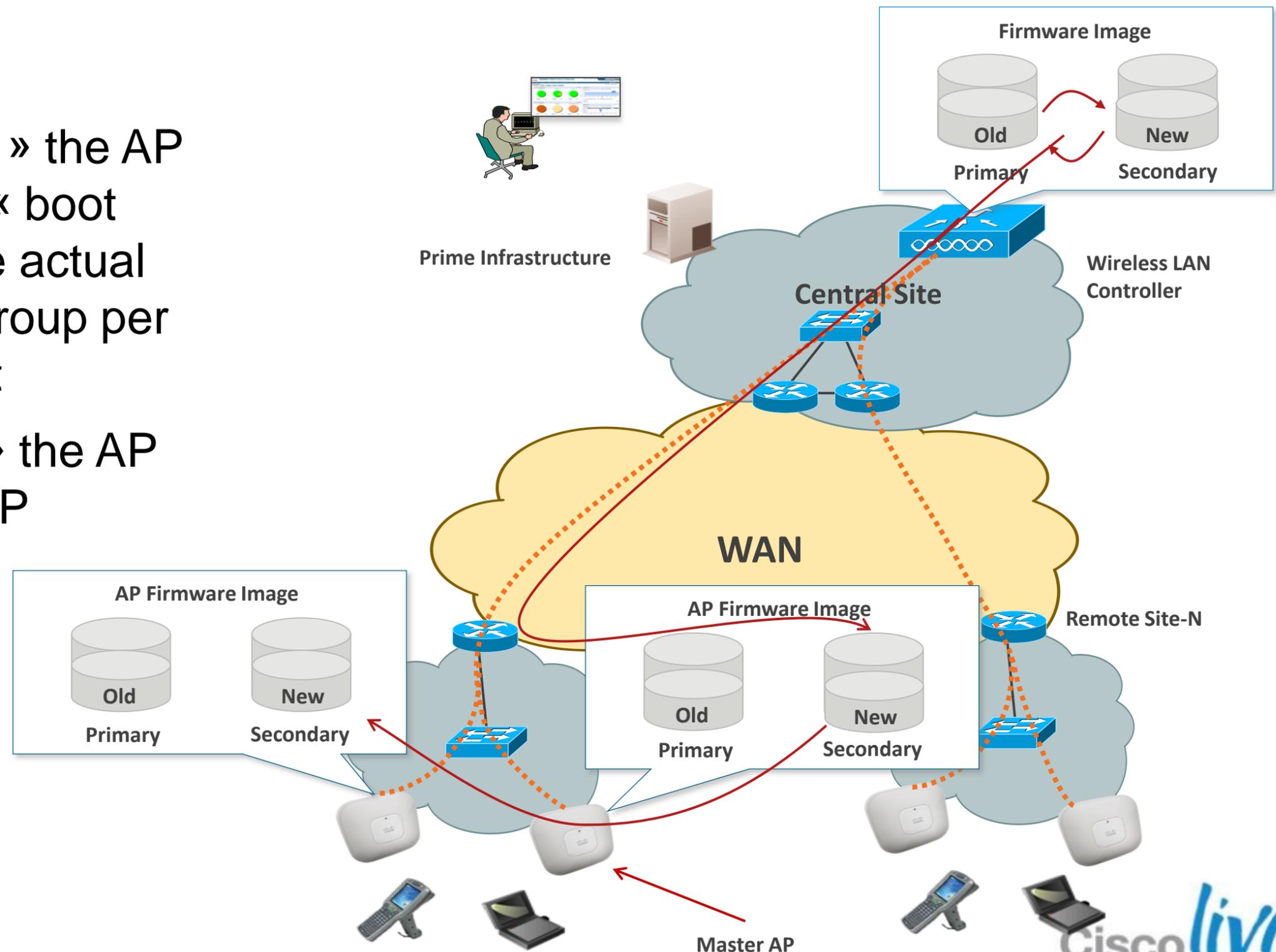
1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)



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 Groups > Edit 'SanJose'

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

FlexConnect AP Upgrade

Slave Maximum Retry Count 44 ← Valid Range is 1-63

Upgrade Image Primary FlexConnect Upgrade

FlexConnect Master APs

AP Name 1140-1

Add Master

| Master AP Name | AP Model | Manual |
|----------------|----------|--------|
| 1140-1 | c1140 | yes |

“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)

FlexConnect Groups > Edit 'SanJose'

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

FlexConnect AP Upgrade

Slave Maximum Retry Count: 44

Upgrade Image: Primary

FlexConnect Upgrade

FlexConnect Master APs

AP Name: 1140-1

Add Master

Per Branch or FlexConnect Group Upgrade

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

CISCO

MONITOR | **WLANS** | CONTROLLER | WIRELESS | SECURITY

Wireless

Access Points

All APs

Radios

802.11a/n

802.11b/g/n

Global Configuration

AP Image Pre-download

Download Primary | Download Backup

Interchange Image | Abort Predownload

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.wv

Cisco *live!*

