



Architecting Network 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

One Policy, One Management, One Network

Unified Access Wireless

Autonomous

FlexConnect

Centralized

Converged Access

New

Unparalleled Deployment Flexibility

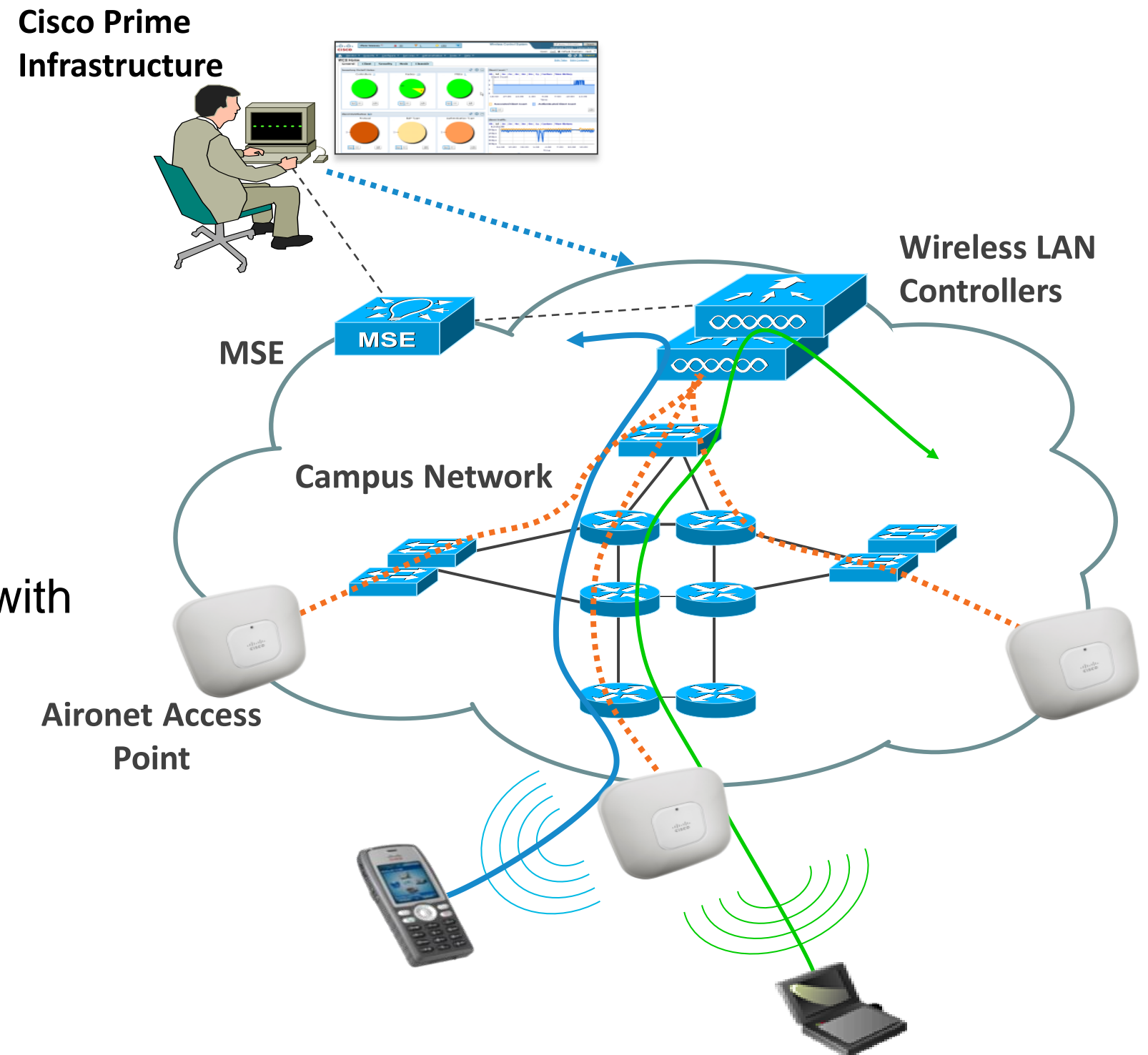
Cisco Unified Wireless Principles

- Components

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

- Principles

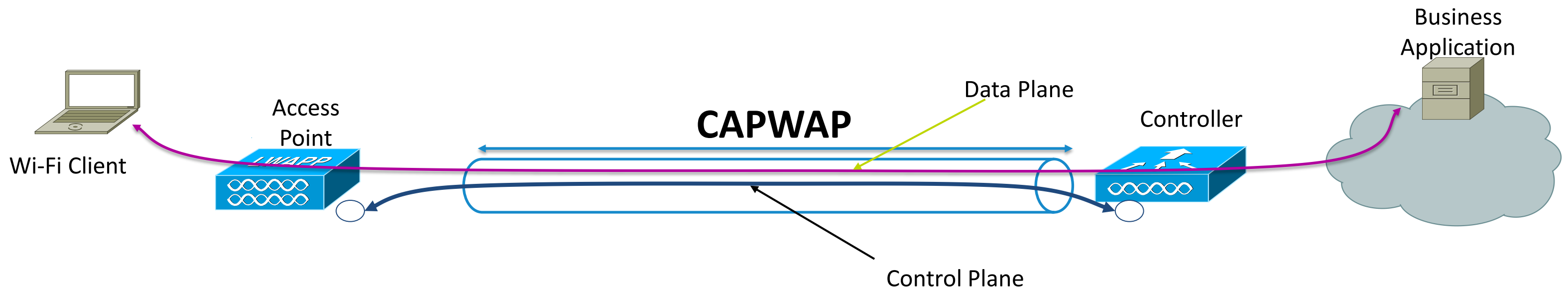
- AP must have CAPWAP connectivity with WLC
- Configuration downloaded to AP by WLC
- All Wi-Fi traffic is forwarded to the WLC



CAPWAP Overview

Control and Provisioning of Wireless Access Point

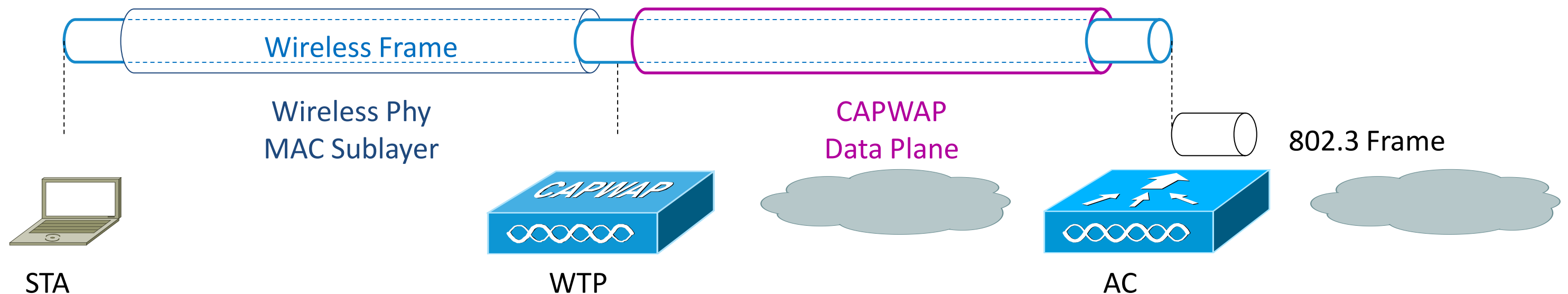
- CAPWAP is a standard, interoperable protocol that enables an Access Controller (AC) to manage a collection of Wireless Termination Points (WTPs)
- CAPWAP carries control and data traffic between the two
 - Control plane is DTLS encrypted
 - Data plane is DTLS encrypted (optional)
- CAPWAP supports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



CAPWAP Modes

Split MAC

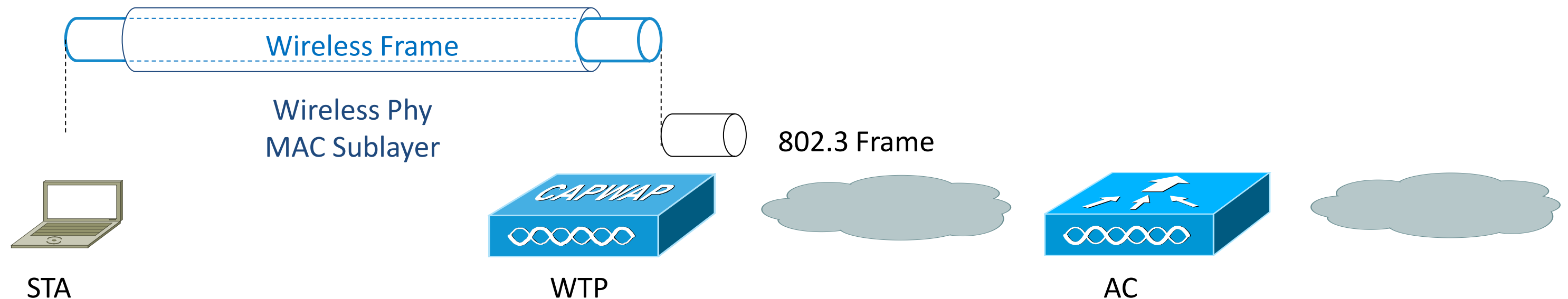
- The CAPWAP protocol supports two modes of operation
 - Split MAC (Centralized Mode)
 - Local MAC (H-REAP/FlexConnect)
- Split MAC



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

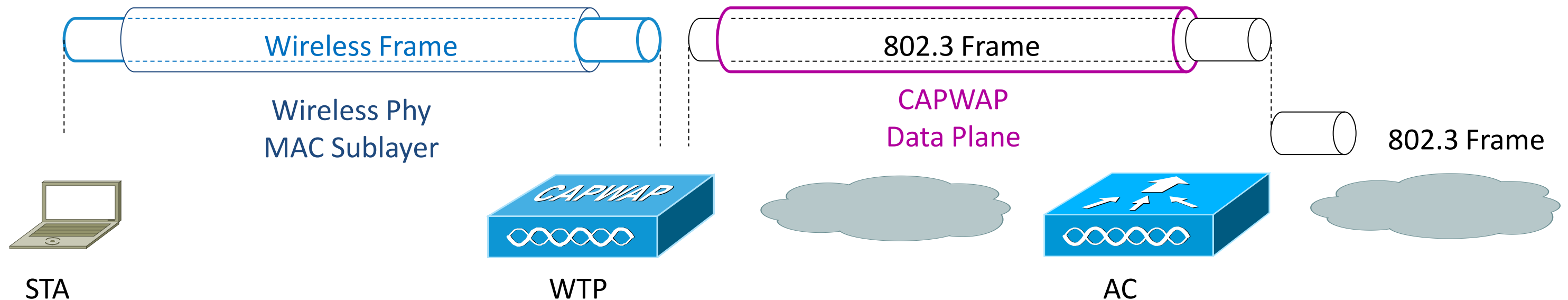


- **FlexConnect support locally bridged MAC and split MAC per SSID**

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

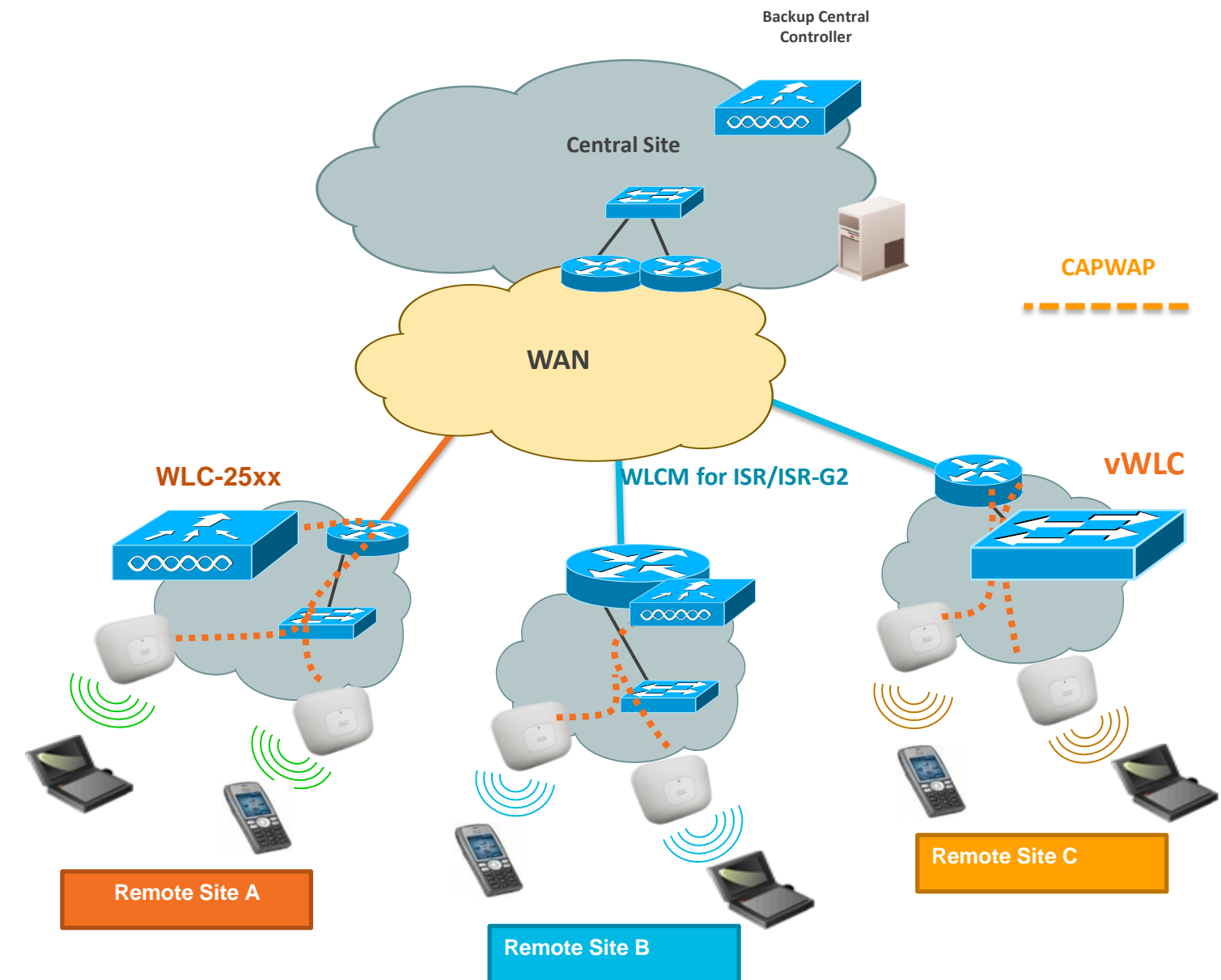


Wireless Branch Deployment Options

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

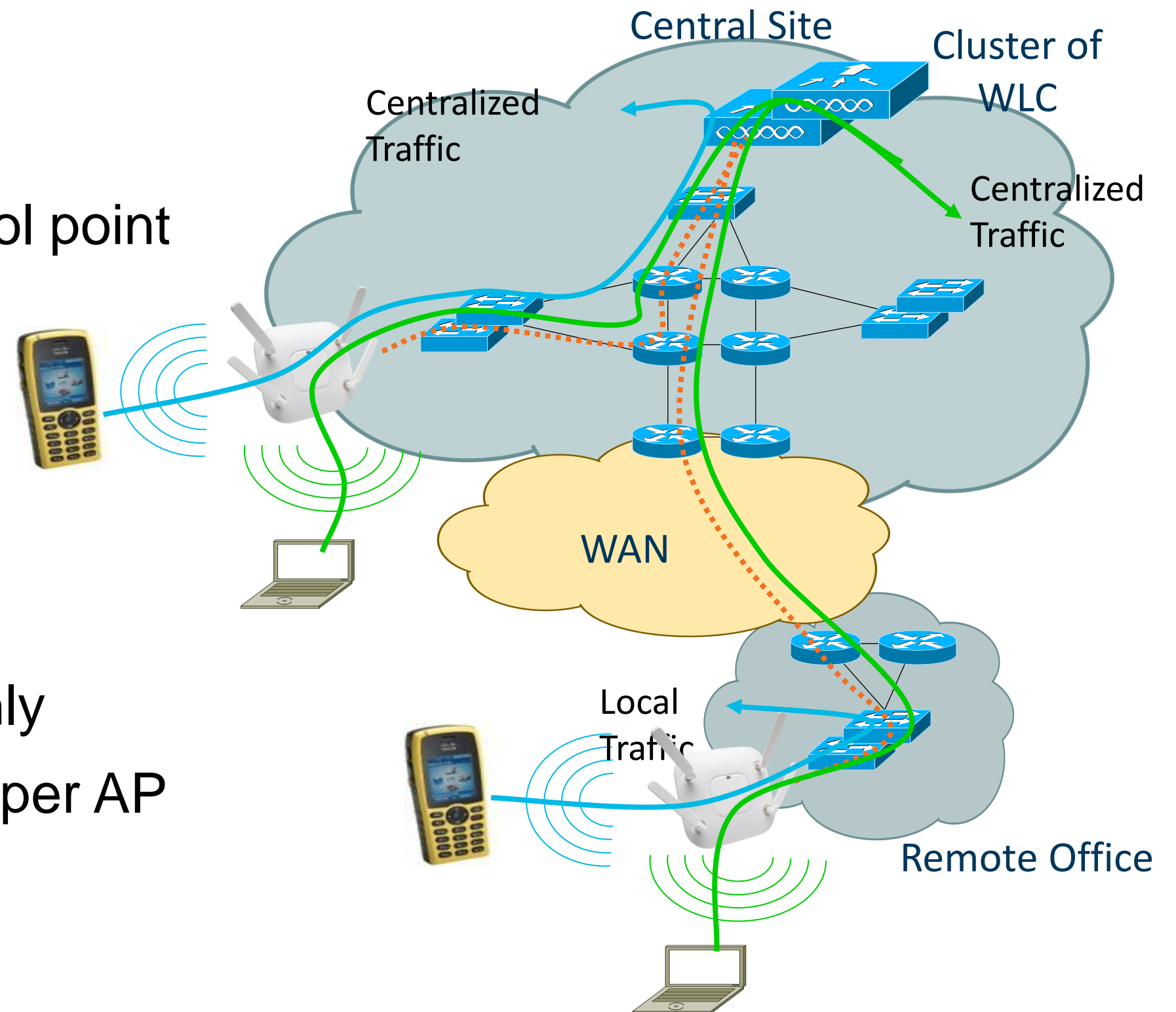
- Cookie cutter configuration for every branch site
- Layer-3 roaming within the branch
- Reliable Multicast (filtering)
 - IPv6 L3 Mobility
 - IPv6 ACL

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

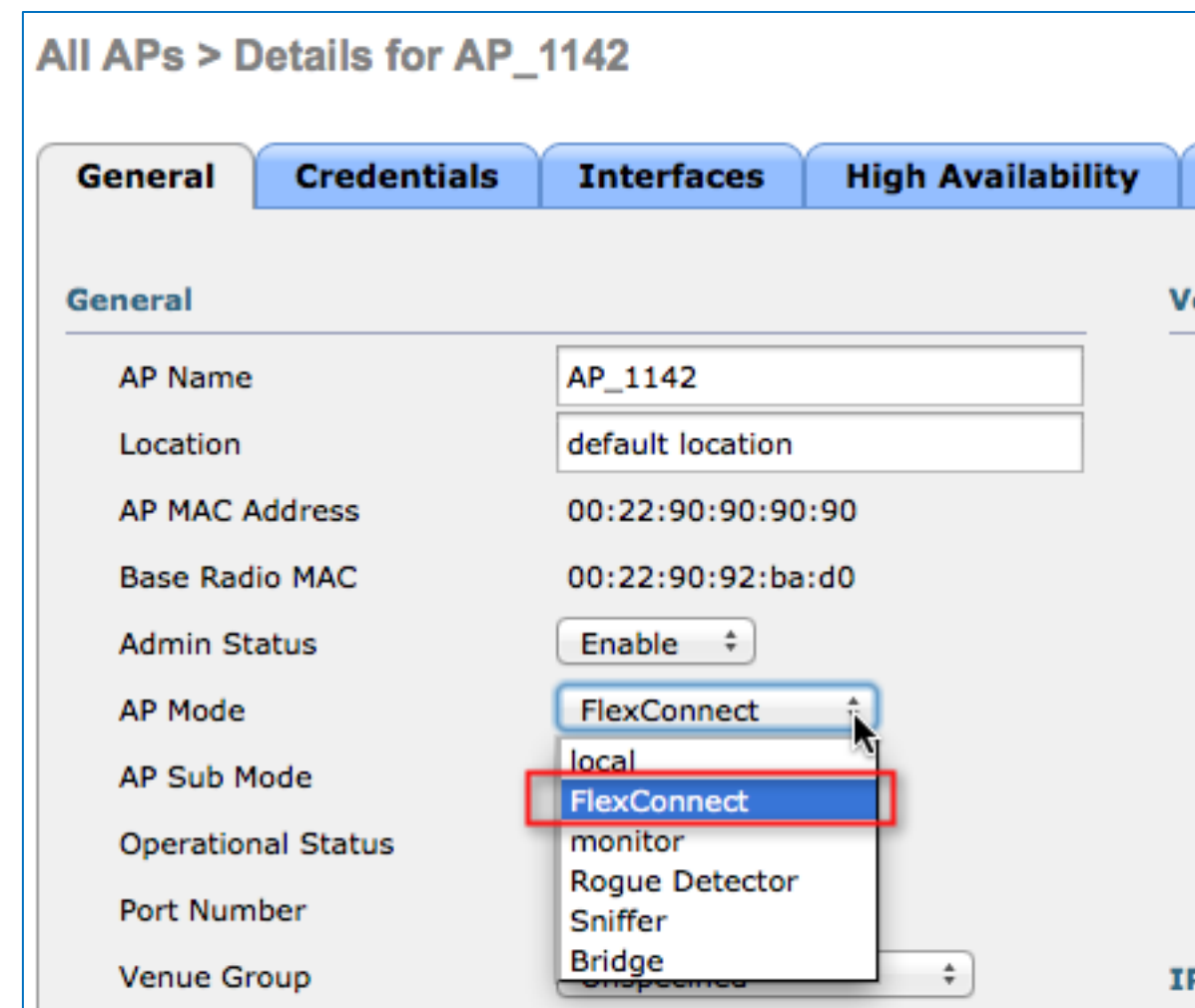
- **Connected Mode** – When FlexConnect can reach Controller (connected state), it gets help from controller to complete client authentication.
 - **Standalone mode** – When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.
-

- **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

The screenshot shows the configuration page for a WLAN named 'FlexConnect'. The 'Advanced' tab is selected and highlighted with a red box. In the 'FlexConnect' section, 'FlexConnect Local Switching' is checked and enabled, also highlighted with a red box. Other settings include 'Client Exclusion' (Enabled, 60s timeout), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (Disabled), 'Wi-Fi Direct Clients Policy' (Disabled), 'Maximum Allowed Clients Per AP Radio' (200), 'Off Channel Scanning Defer' (Scan Defer Priority 4, 5, 6 checked; Scan Defer Time 100msecs), 'FlexConnect Local Auth' (Disabled), and 'Learn Client IP Address' (Enabled). On the right, 'NAC State' is set to 'None', and 'Client Load Balancing', 'Client Band Select', and 'Passive Client' are all disabled. Under 'Voice', 'Media Session Snooping', 'Re-anchor Roamed Voice Clients', and 'KTS based CAC Policy' are all enabled. 'Client Profiling' is also disabled.

Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

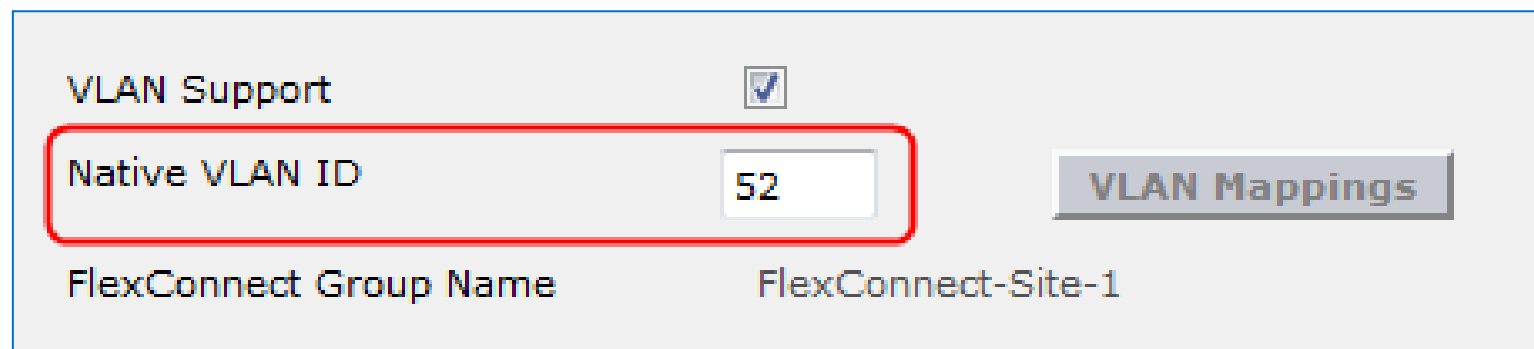
- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN Support provides the ability to configure remote VLAN to WLAN mappings. VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using NCS templates

The screenshot shows the configuration page for AP-3600-A, specifically the FlexConnect tab. The page has a breadcrumb trail 'All APs > Details for AP-3600-A' and a navigation bar with tabs: General, Credentials, Interfaces, High Availability, Inventory, FlexConnect, and Advanced. The FlexConnect tab is active. In the configuration area, 'VLAN Support' is checked with a red box around it. Below it, 'Native VLAN ID' is set to 52, and there is a 'VLAN Mappings' button. The 'FlexConnect Group Name' is set to 'FlexConnect-Site-1'. At the bottom, there are links for 'PreAuthentication Access Control Lists', including 'External WebAuthentication ACLs', 'Local Split ACLs', and 'Central DHCP Processing'.

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.



The screenshot shows a configuration panel for FlexConnect. At the top, 'VLAN Support' is checked with a blue checkmark. Below it, 'Native VLAN ID' is set to '52' in a text box, which is highlighted with a red border. To the right of this text box is a button labeled 'VLAN Mappings'. At the bottom, 'FlexConnect Group Name' is set to 'FlexConnect-Site-1'.

```
!  
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

1

All APs > Details for AP-3600-A

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

VLAN Support

Native VLAN ID

FlexConnect Group Name FlexConnect-Site-1

VLAN Mappings

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

[Central DHCP Processing](#)

2

All APs > AP-3600-A > VLAN Mappings

AP Name AP-3600-A

Base Radio MAC 64:d9:89:43:4f:50

WLAN Id	SSID	VLAN ID	NAT-PAT
3	RackMobilityFlex	154	no

Centrally switched Wlans

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

- 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

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes the Cisco logo, the text "Cisco Prime Infrastructure", and menu items for "Home", "Monitor", "Configure", and "Services". The main heading is "Lightweight AP Template Detail : 'FlexConnect-VLAN-Mapping'". Below this, there are several tabs: "AP Parameters", "Mesh", "802.11a/n", "802.11a SubBand", "802.11b/g/n", "CDP", "FlexConnect", and "S". The "FlexConnect" tab is active. On the left side, under "FlexConnect Configuration", the "VLAN Support" checkbox is checked and labeled "Enable". Below it, the "Native VLAN ID" is set to "52". On the right side, under "Profile Name-VLAN Mappings", the "RackMobilityFlex" checkbox is checked and labeled "154".



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
 - 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



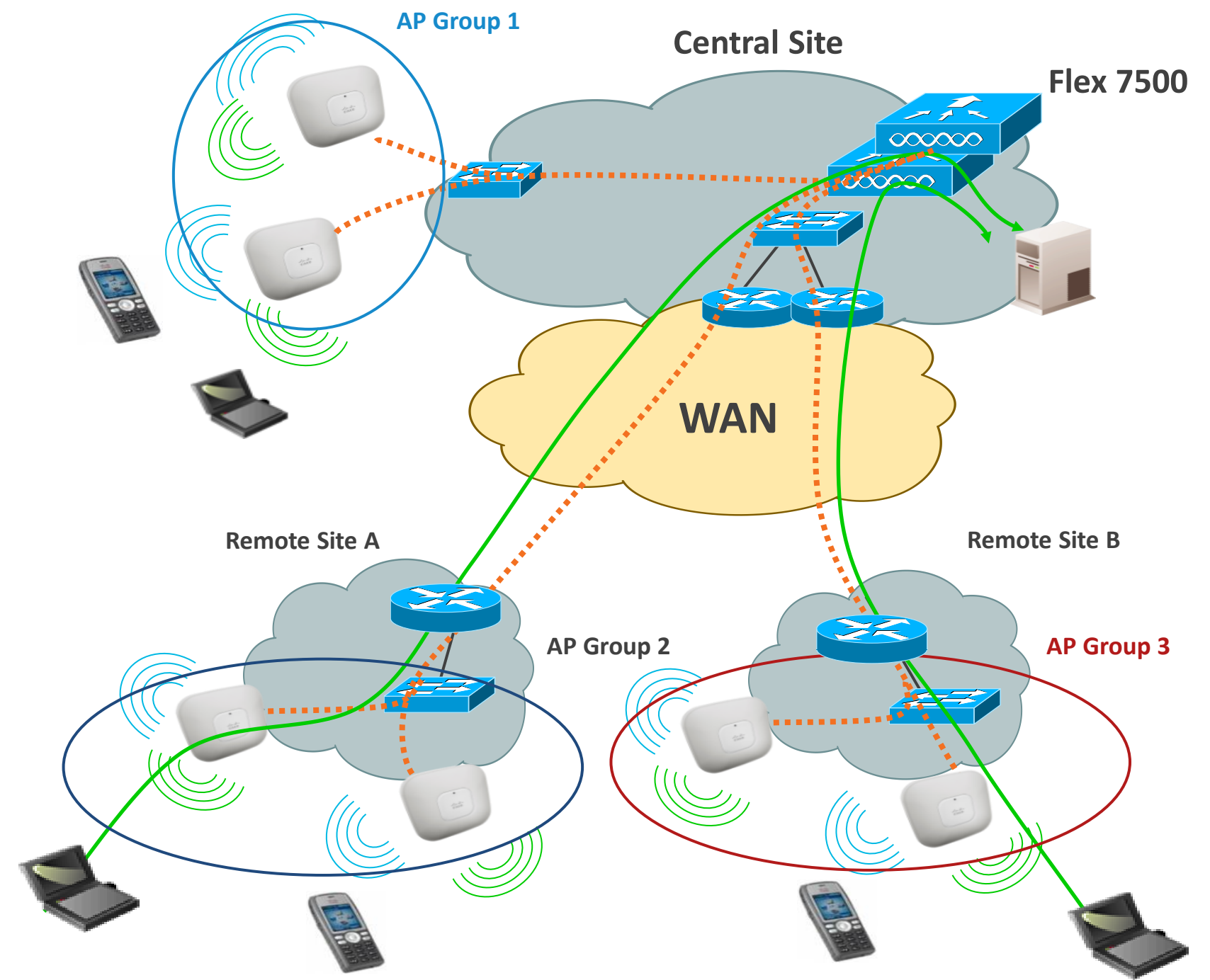
Why do we need FlexConnect & AP
Groups?

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**

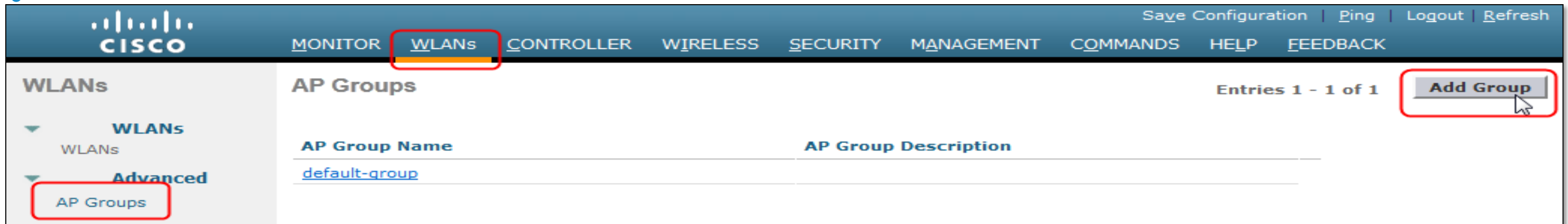
- One AP can be in only one AP Group
- One WLAN(SSID) can be in several AP Groups
- WLAN with ID 1-16 can not be removed from the ‘default-group’
- WLAN with ID greater than 16 will never be part of the ‘default-group’
- All AP with no AP Group name or an unknown AP Group name will be part of the ‘default-group’

- **Well known mistakes**

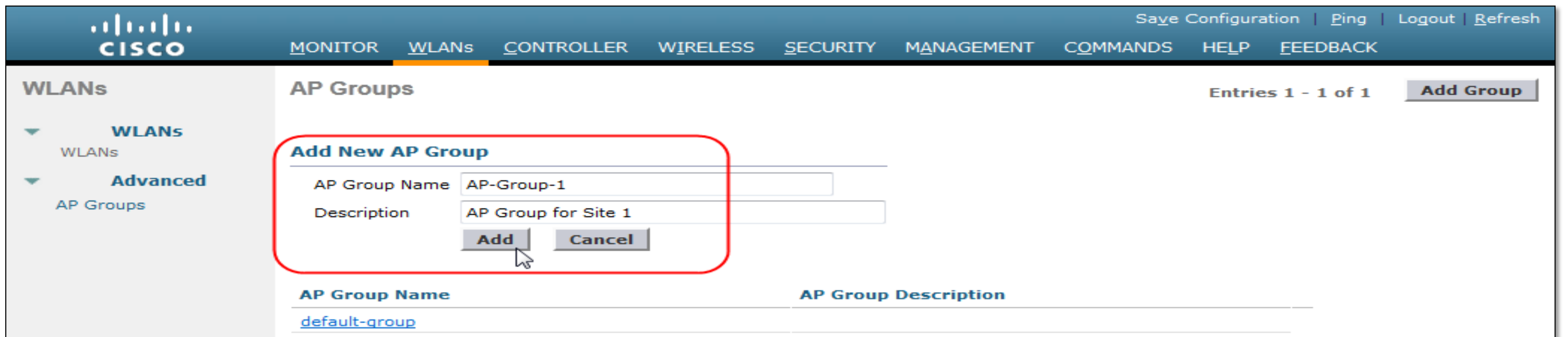
- Create no AP group, but create a WLAN with ID 17+.
- Having AP groups defined, Create WLAN with ID 17+ but never map the WLAN to any AP Group.

AP Groups

Configuration: Create a New Group



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, showing 'WLANs' and 'Advanced' sub-menus, with 'AP Groups' selected. The main content area displays 'AP Groups' with a table containing one entry: 'default-group'. An 'Add Group' button is highlighted in the top right corner.



The screenshot shows the 'Add New AP Group' form. The form fields are: 'AP Group Name' with the value 'AP-Group-1', and 'Description' with the value 'AP Group for Site 1'. There are 'Add' and 'Cancel' buttons below the form. The 'Add' button is highlighted. The background shows the same navigation and table as the previous screenshot.

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

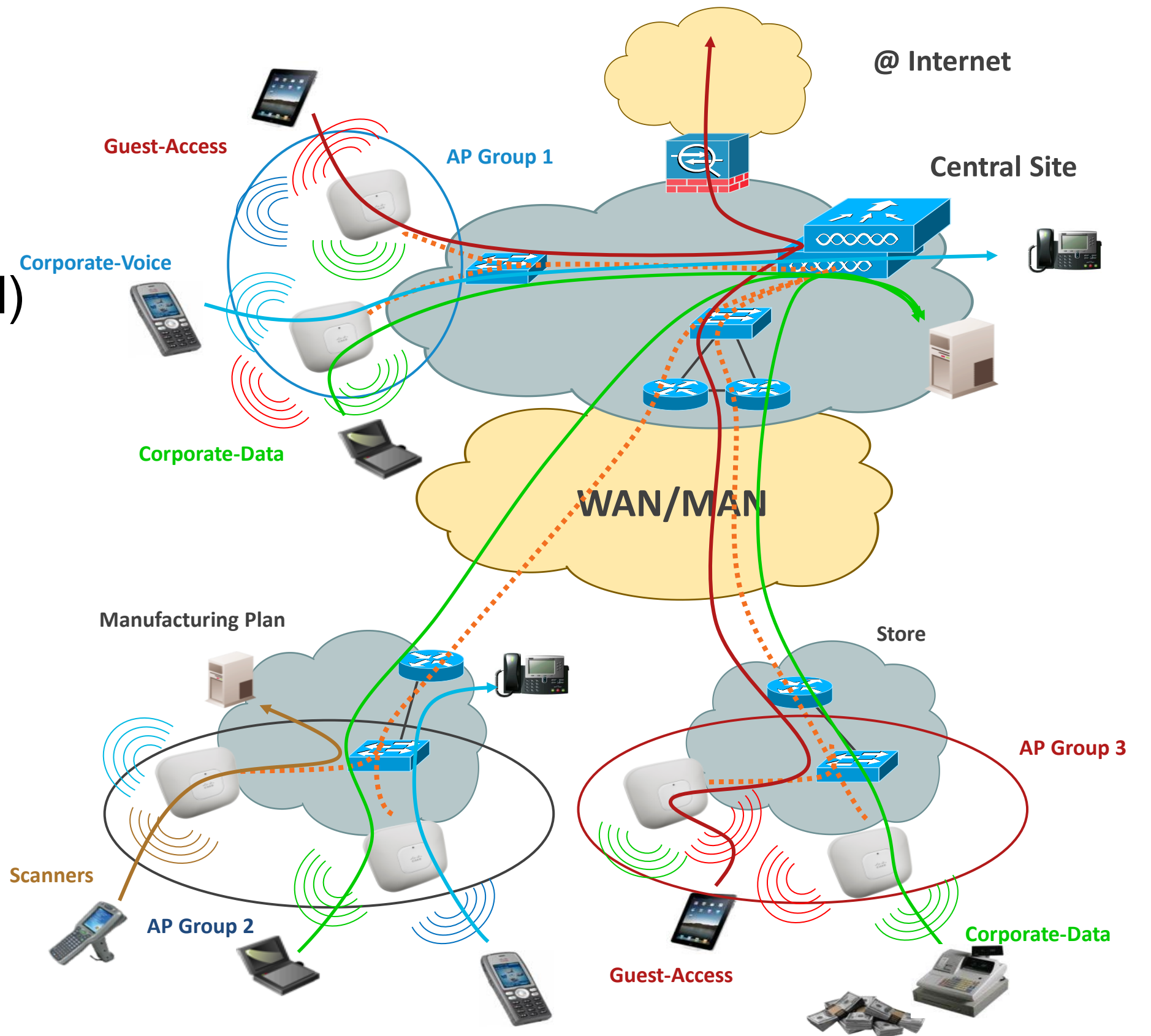
Add APs to the Group [Add APs](#)

<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

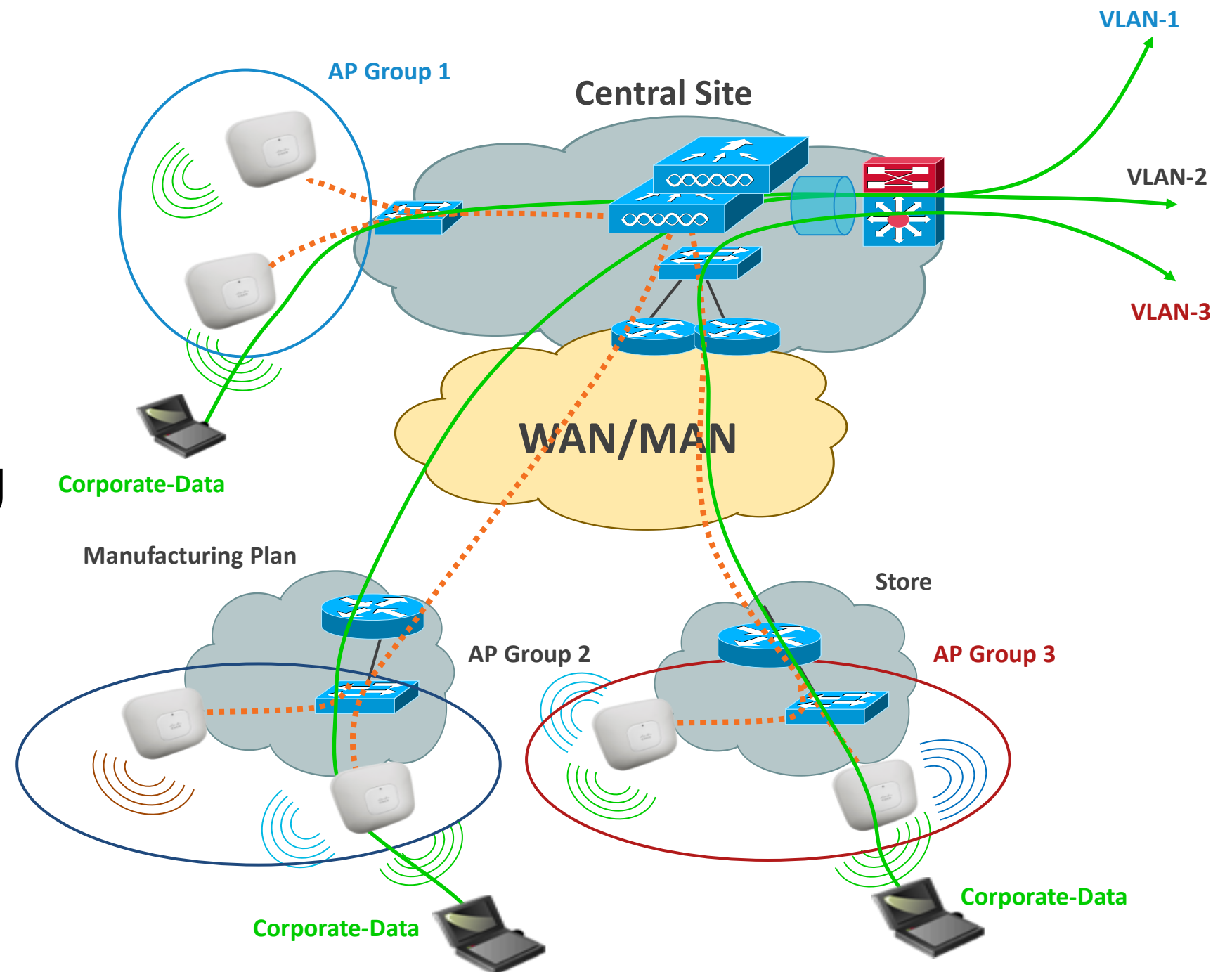
- AP groups give the ability to enable Wi-Fi Services (WLAN) based on physical location
- Example
 - **Central Site**
Corporate-Voice, Corporate-Data, Guest-Access
 - **Manufacturing Plant**
Corporate-Voice, Corporate-Data, Scanners
 - **Store**
Corporate-Data, Guest-Access



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 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

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

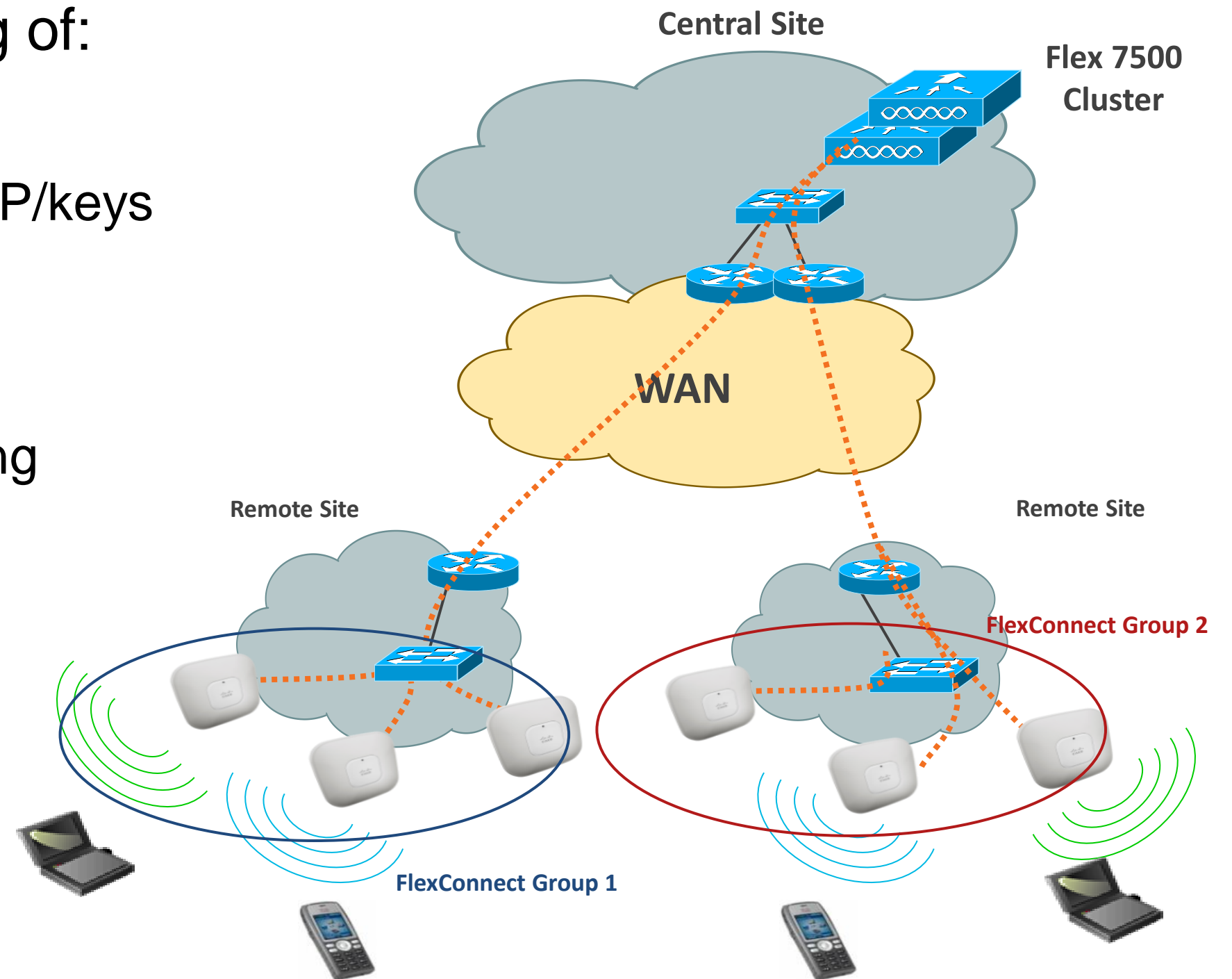
Understanding FlexConnect Groups

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

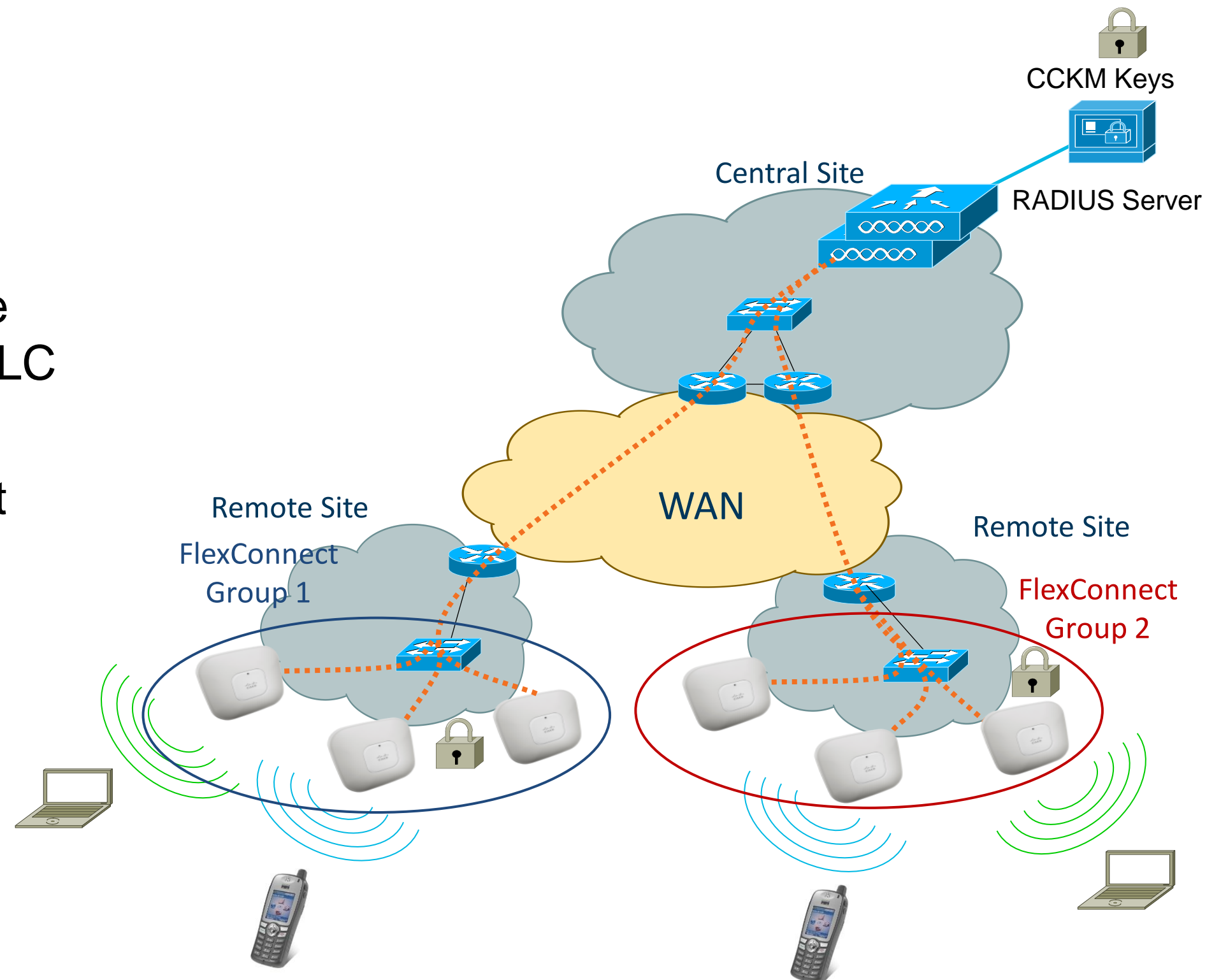
Scaling information

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504	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

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted with a red box and a blue circle labeled '1'), SECURITY, MANAGEMENT, and COMMANDS. The left sidebar shows the 'FlexConnect Groups' menu item highlighted with a red box. The main content area is titled 'FlexConnect Groups > New' and contains a text input field for 'Group Name' with the value 'FlexConnect-Site-1'. A blue arrow points from this field to a second screenshot. The second screenshot is titled 'FlexConnect Groups > Edit 'FlexConnect-Site-1'' and shows the 'Local Authentication' tab selected. It displays 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'. The table contains one entry: '00:22:90:90:9a:4a', 'AP-1140-A', and 'Associated'.

Step 2: Add APs to the FlexConnect Group

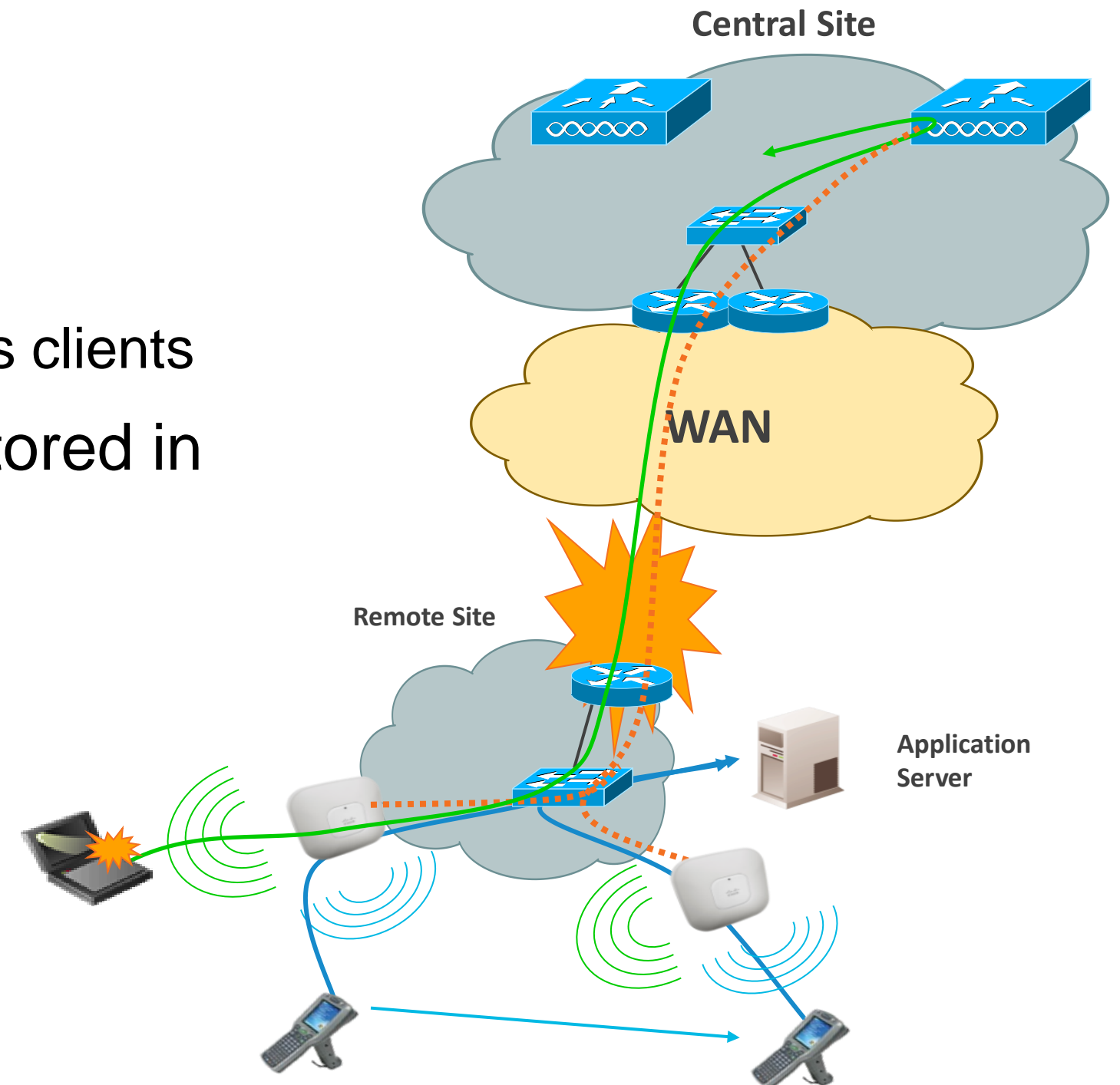


Design Wireless Branch
Designing a Resilient Network

FlexConnect Backup Scenario

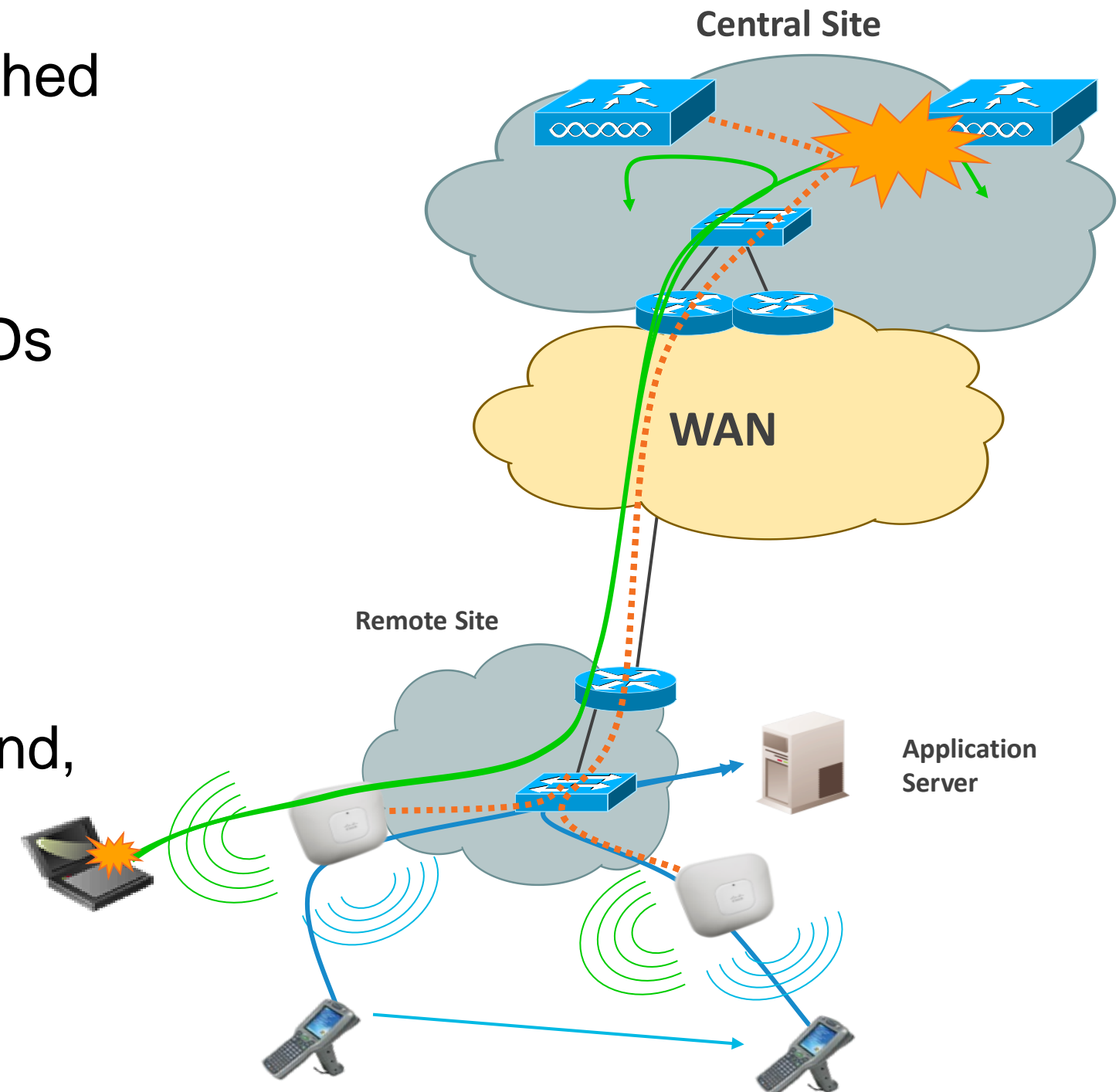
WAN Failure

- 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

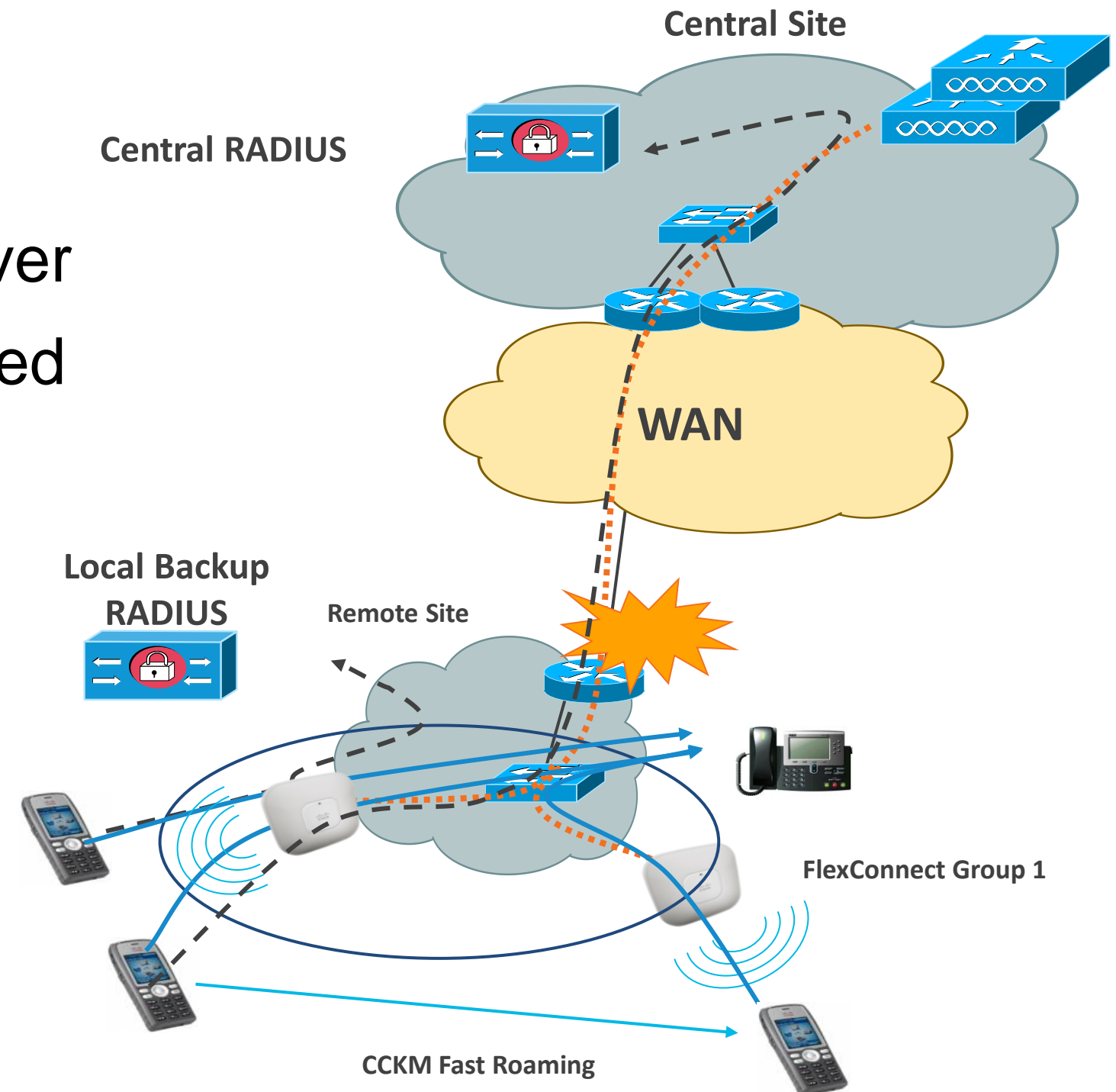
- FlexConnect will first backup on local switched mode
 - No impact for locally switched SSIDs
 - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with WLC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



FlexConnect Group: Local Backup RADIUS

Configuration

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

The screenshot shows the configuration page for a FlexConnect Group named 'SanJose'. The page is divided into several sections:

- General:** Shows the Group Name as 'SanJose'.
- FlexConnect APs:** A table listing associated APs with their MAC addresses and names.
- AAA:** Configuration for RADIUS servers and local authentication.

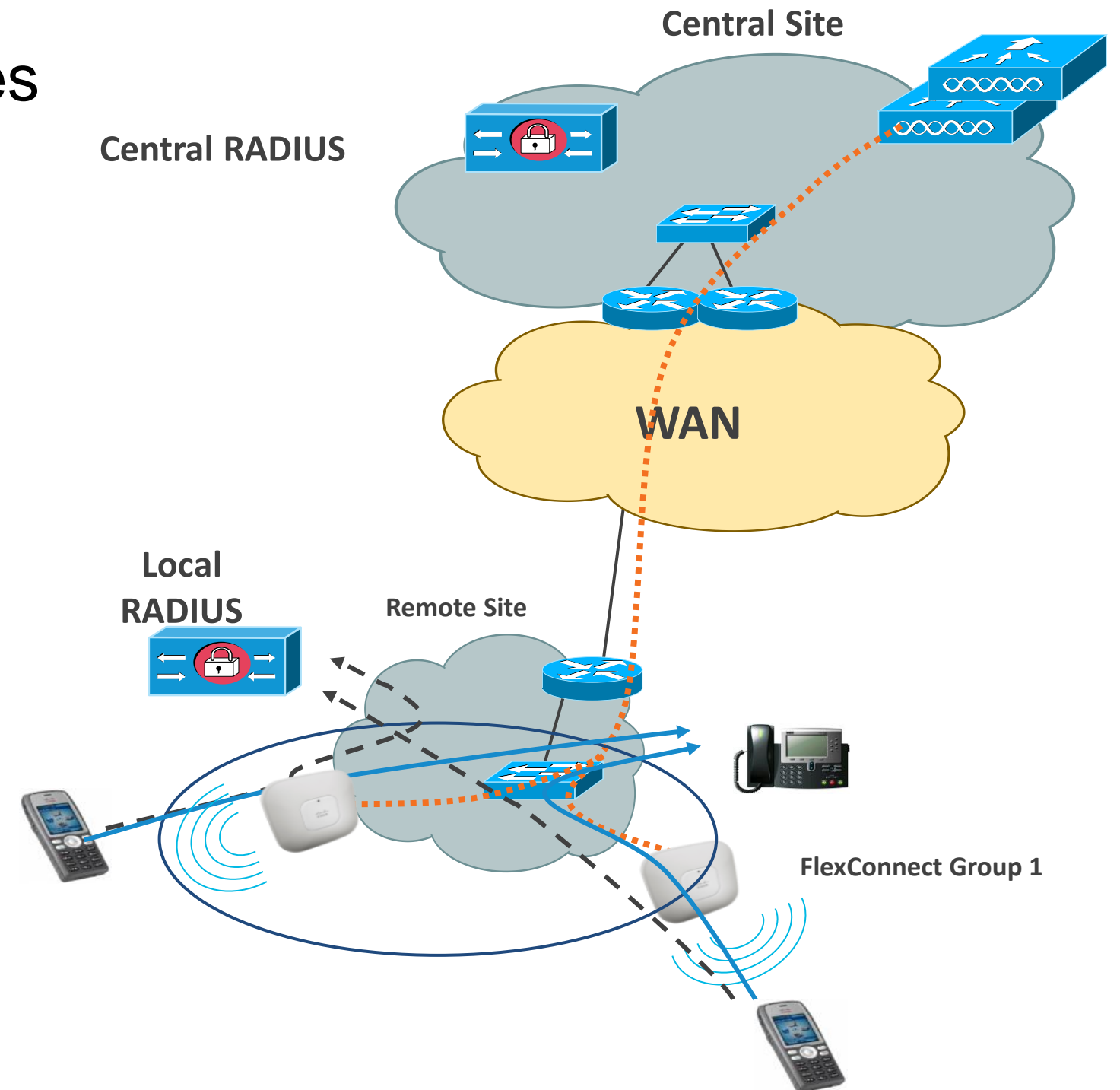
AP MAC Address	AP Name	Status
1c:df:0f:94:bb:e9	Branch-AP2-1040	Associated
c4:71:fe:49:f6:59	Branch-AP1	Associated

AAA Configuration:

- Primary Radius Server: IP:11.11.11.15, Port:1812
- Secondary Radius Server: None
- Enable AP Local Authentication:

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

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'RackMobility'. The 'Advanced' tab is selected and highlighted with a red box. The configuration is divided into several sections:

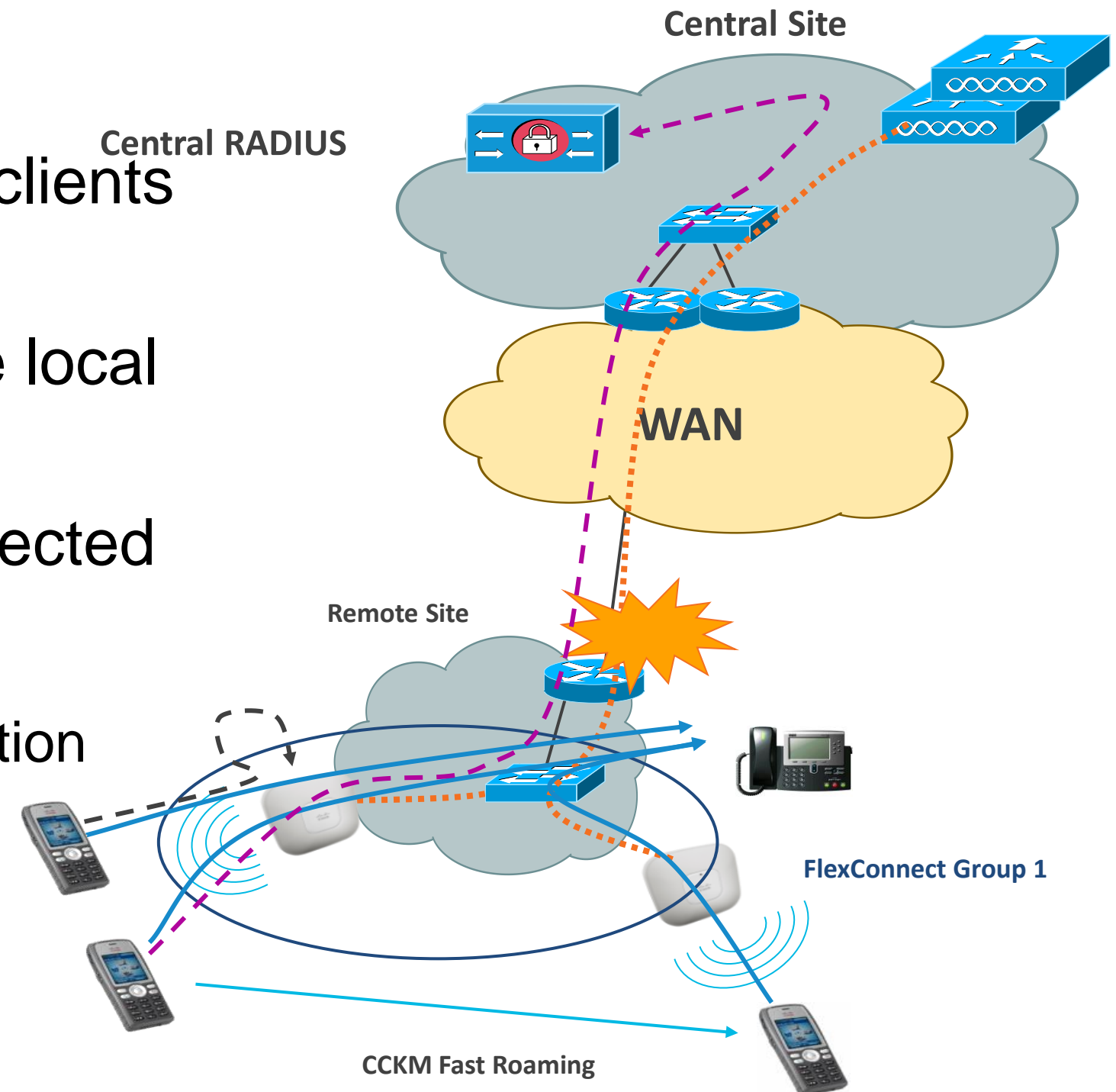
- General:** Maximum Allowed Clients (0), Static IP Tunneling (Disabled), Wi-Fi Direct Clients Policy (Disabled), Maximum Allowed Clients Per AP Radio (200).
- Off Channel Scanning Defer:** Scan Defer Priority (checkboxes for 0-7, with 4, 5, and 6 checked), Scan Defer Time(msecs) (100).
- FlexConnect:** FlexConnect Local Switching (Enabled), FlexConnect Local Auth (Enabled, highlighted with a red box), Learn Client IP Address (Enabled).
- Advanced (Right Side):** 802.11b/g/n (1 - 255) 1, NAC State (None), Client Load Balancing (Disabled), Client Band Select (Disabled), Passive Client (Disabled), 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

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 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) 436973636f000000000000000000000000

Authority Info Cisco A_ID

PAC Timeout (2 to 4095 days)

PEAP

Enable PEAP Authentication **New**

EAP TLS

Enable EAP TLS Authentication

EAP TLS Certificate download

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

The screenshot shows the Cisco configuration interface for creating and editing FlexConnect ACLs. It is divided into two main sections: 'New' and 'Edit'.

1. New: The 'Access Control Lists > New' page shows the 'Access Control List Name' field set to 'FlexConnect-Acl-1'. Below this, the 'FlexConnect Access Control Lists' section has a dropdown menu for 'Acl Name' with 'FlexConnect-Acl-1' selected. A red box highlights the dropdown, and a blue circle with the number '1' is in the top right corner.

2. Edit: The 'Access Control Lists > Edit' page shows the 'Access List Name' as 'FlexConnect-Acl-1'. An 'Add New Rule' button is highlighted with a red box. Below the 'General' section is a table of rules:

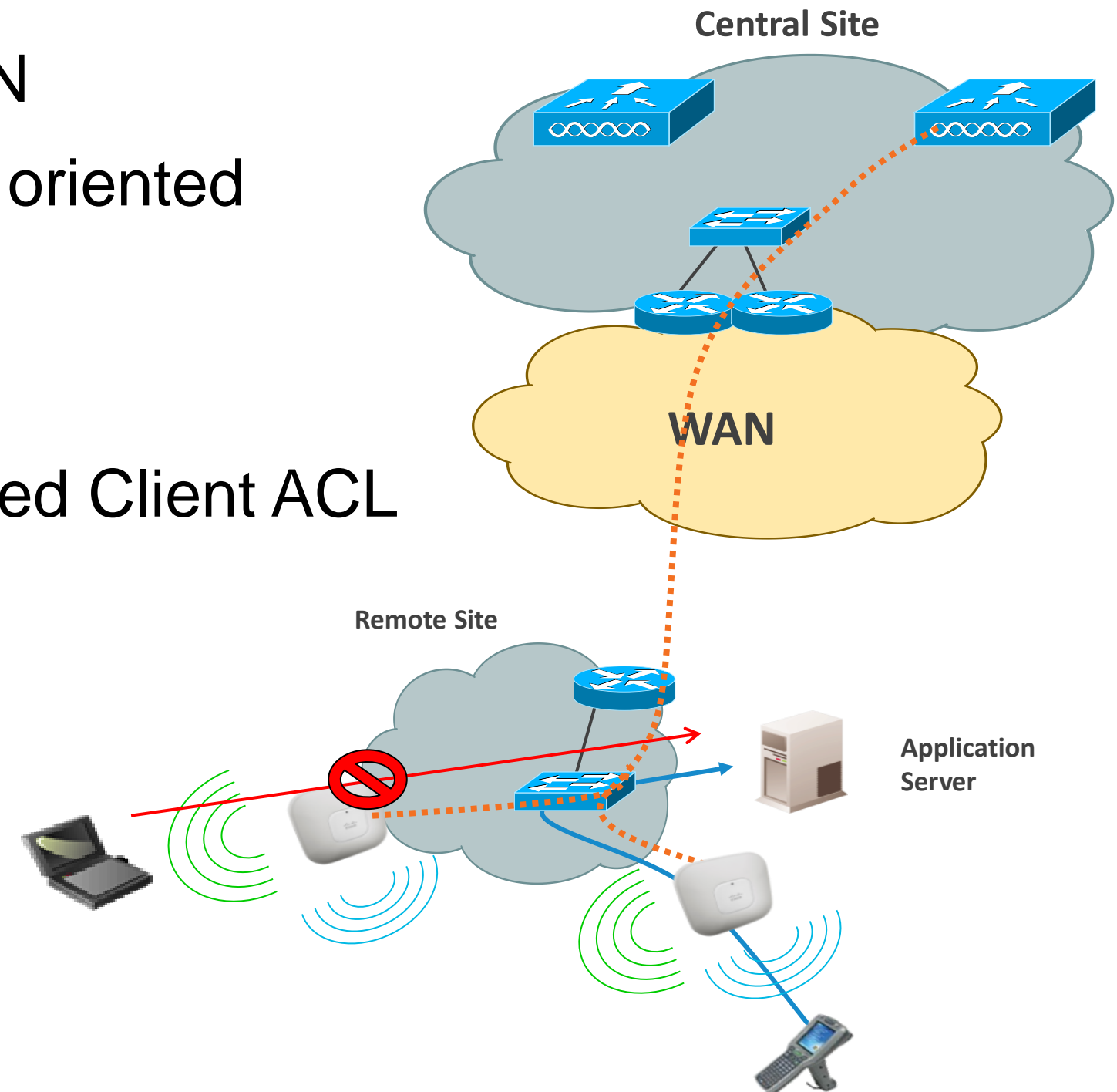
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Deny	0.0.0.0 /	10.150.5.0 /	Any	Any	Any	Any <input checked="" type="checkbox"/>
		0.0.0.0 /	255.255.255.0 /				
2	Deny	10.150.5.0 /	0.0.0.0 /	Any	Any	Any	Any <input checked="" type="checkbox"/>
		255.255.255.0 /	0.0.0.0 /				
3	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any <input checked="" type="checkbox"/>
		0.0.0.0 /	0.0.0.0 /				

A blue circle with the number '2' is in the middle right, and a blue circle with the number '3' is in the top right corner.

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

All APs > Details for AP-3600-A

General Credentials Interfaces High Availability Inventory FlexConnect Advanced

VLAN Support

Native VLAN ID 52

FlexConnect Group Name FlexConnect-Site-1

VLAN Mappings

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

[Central DHCP Processing](#)

1

All APs > AP-3600-A > VLAN Mappings

AP Name AP-3600-A

Base Radio MAC 64:d9:89:43:4f:50

WLAN Id	SSID	VLAN ID	NAT-PAT
3	RackMobilityFlex	154	no

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
1	RackMobility	N/A
2	RackMobilityPSK	N/A
5	RackMobilityGuest	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
154	FlexConnect-Acl-1	FlexConnect-Acl-1

2

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.

1

FlexConnect Groups > Edit 'FlexConnect-Site-1'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP

AAA VLAN-ACL mapping WLAN-ACL mapping WebPolicies

AAA VLAN ACL Mapping

Vlan Id

Ingress ACL

Egress ACL

Add

Vlan Id	Ingress ACL	Egress ACL
154	<input type="text" value="FlexConnect-Acl-1"/>	<input type="text" value="FlexConnect-Acl-1"/>

2

General Local Authentication Image Upgrade **ACL Mapping**

AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

AAA VLAN ACL Mapping

Vlan Id

Ingress ACL

Egress ACL

Add

Vlan Id	Ingress ACL	Egress ACL
154	<input type="text" value="FlexConnect-Acl-1"/>	<input type="text" value="FlexConnect-Acl-1"/>



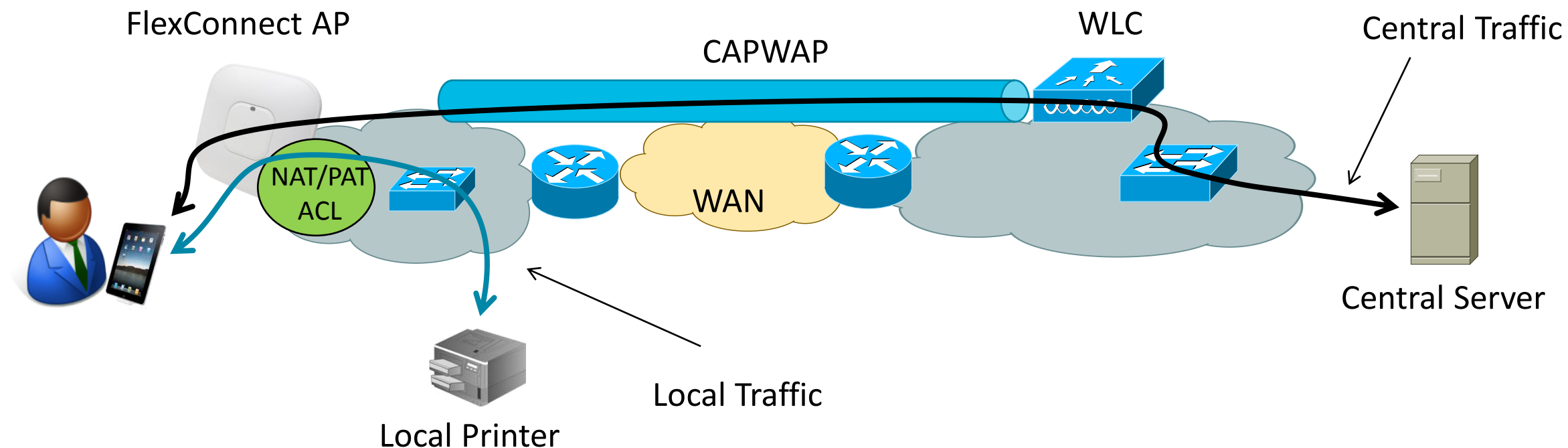
FlexConnect Split Tunneling

(Using FlexConnect Split ACL)

FlexConnect ACL – Split Tunneling

Overview

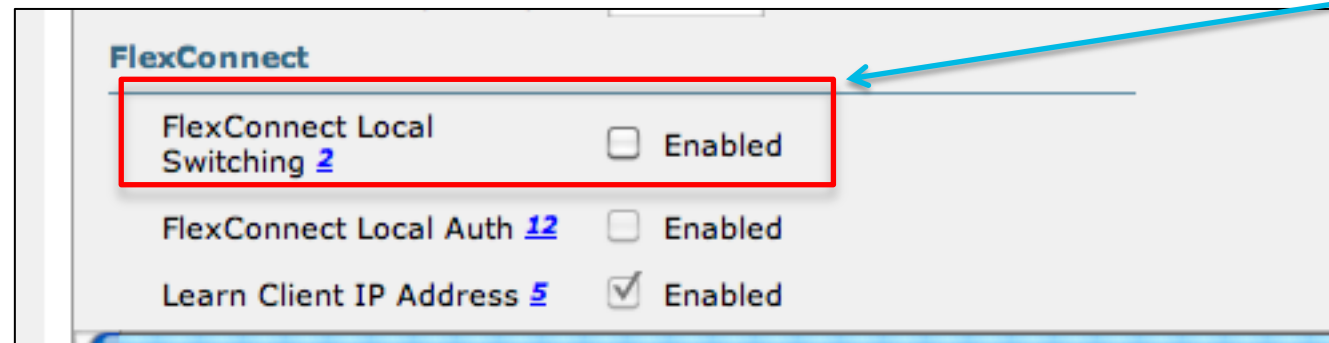
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP@ for the NAT/PAT feature



FlexConnect ACL – Split Tunneling

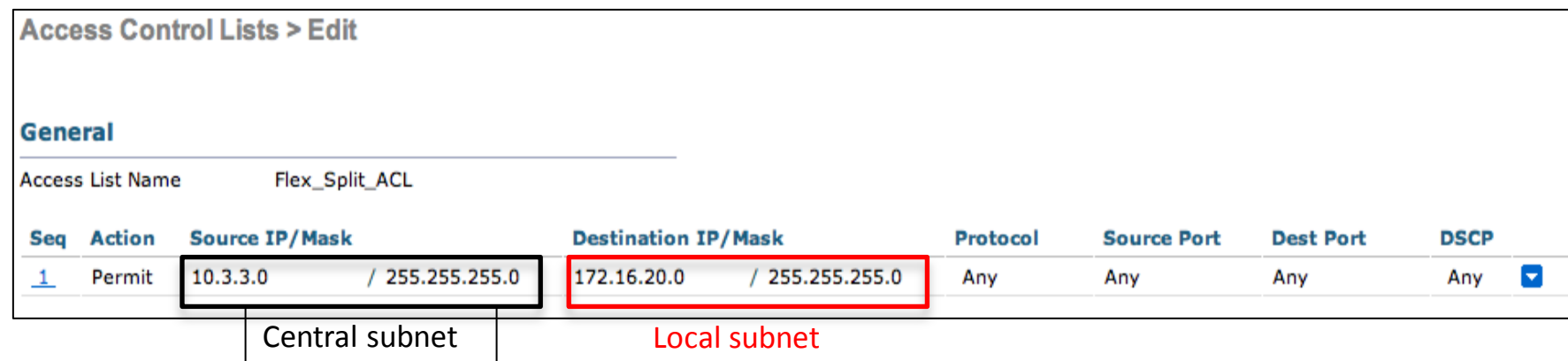
Configuration

- Create a centrally switched WLAN



Flex Local switching should not be checked

- Define Flex ACL to match traffic to be locally switched



FlexConnect ACL – Split Tunneling

Configuration – Access Point

All APs > Details for AP-3600-A

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name FlexConnect-Site-1

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

[Central DHCP Processing](#)

All APs > AP-3600-A > ACL Mappings

AP Name AP-3600-A

Base Radio MAC 64:d9:89:43:4f:50

WLAN ACL Mapping

WLAN Id

Local-Split ACL

Add

WLAN Id	WLAN Profile Name	Local-Split ACL
1	RackMobility	Flex_Split_ACL

FlexConnect ACL – Split Tunneling

Configuration – FlexConnect Group

FlexConnect Groups > Edit 'FlexConnect-Site-1'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP

AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies


Web Auth ACL Mapping

WLAN Id
WebAuth ACL

Local Split ACL Mapping

WLAN Id
Local Split ACL

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL
			1	RackMobility	<input type="text" value="Flex_Split_ACL"/>



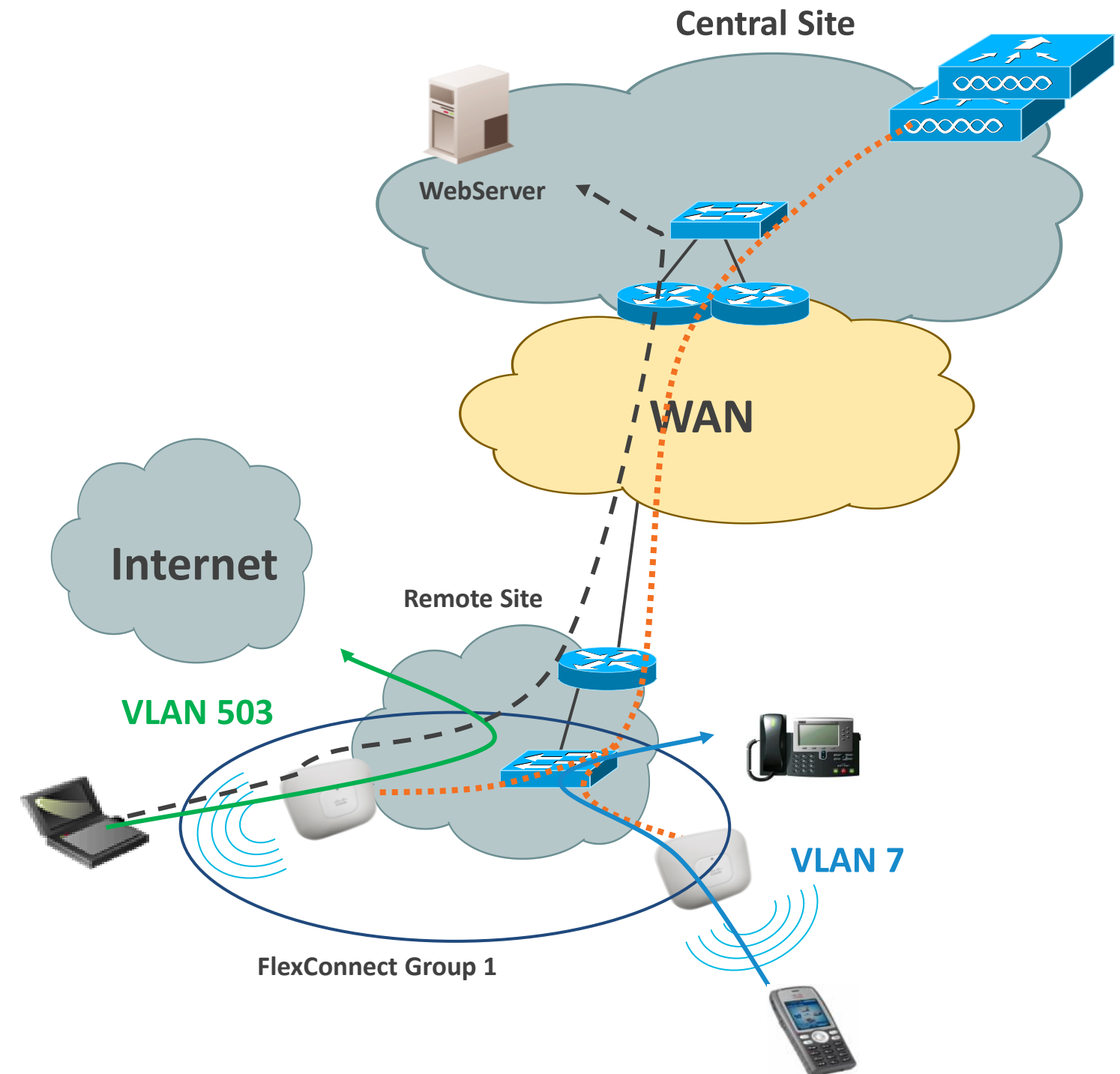
Deploying External WebAuth with FlexConnect and Local Switching *(Using FlexConnect WebAuth ACL)*

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

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 AP

The image shows two overlapping screenshots from the Cisco configuration interface. The left screenshot shows the 'FlexConnect' tab for AP-3600-A, with the 'External WebAuthentication ACLs' link highlighted. The right screenshot shows the 'ACL Mappings' page, where a WLAN ACL mapping is being added for WLAN Id 4, mapping it to the 'Pre-WebAuthPolicy-ACL'.

All APs > Details for AP-3600-A

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

VLAN Support
Native VLAN ID: 52 **VLAN Mappings**
FlexConnect Group Name: FlexConnect-Site-1

PreAuthentication Access Control Lists

- External WebAuthentication ACLs**
- Local Split ACLs
- Central DHCP Processing

All APs > AP-3600-A > ACL Mappings

AP Name: AP-3600-A
Base Radio MAC: 64:d9:89:43:4f:50

WLAN ACL Mapping

WLAN Id: 4
WebAuth ACL: Pre-WebAuthPolicy-ACL **Add**

WLAN Id	WLAN Profile Name	WebAuth ACL
4	WebAuth	Pre-WebAuthPolicy-ACL

WebPolicies

WebPolicy ACL: FlexConnect-Acl-1 **Add**

WebPolicy Access Control Lists

Map WLAN-Id to Pre-Auth ACL

External WebAuth with Local Switching

Configuration

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

FlexConnect Groups > Edit 'FlexConnect-Site-1'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP

AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id
WebAuth ACL

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

Local Split ACL Mapping

WLAN Id
Local Split ACL

WLAN Id	WLAN Profile Name	LocalSplit 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 bubble points to this field with the text 'External Web-Server IP'.

Field	Value
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

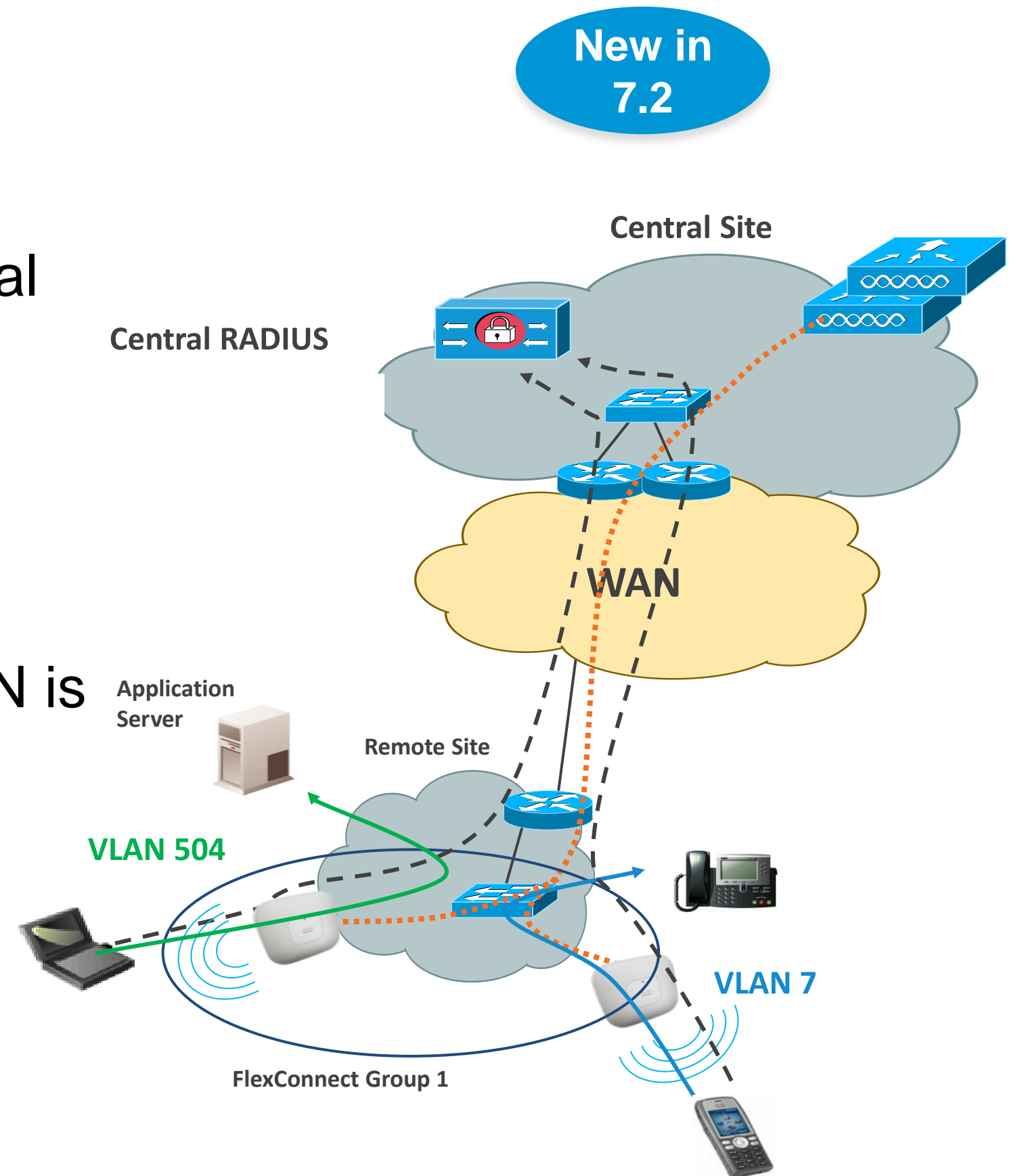


FlexConnect AAA VLAN Override

FlexConnect AAA VLAN Override

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.



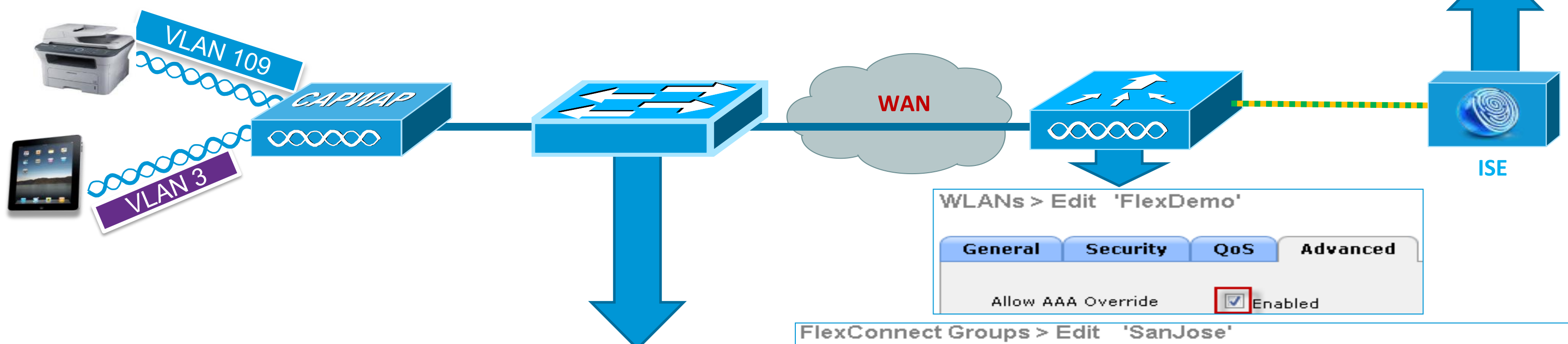
FlexConnect AAA VLAN Override

Configuration



For Your Reference

	Attribute	Type	Value
IETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802
IETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN
IETF 81	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

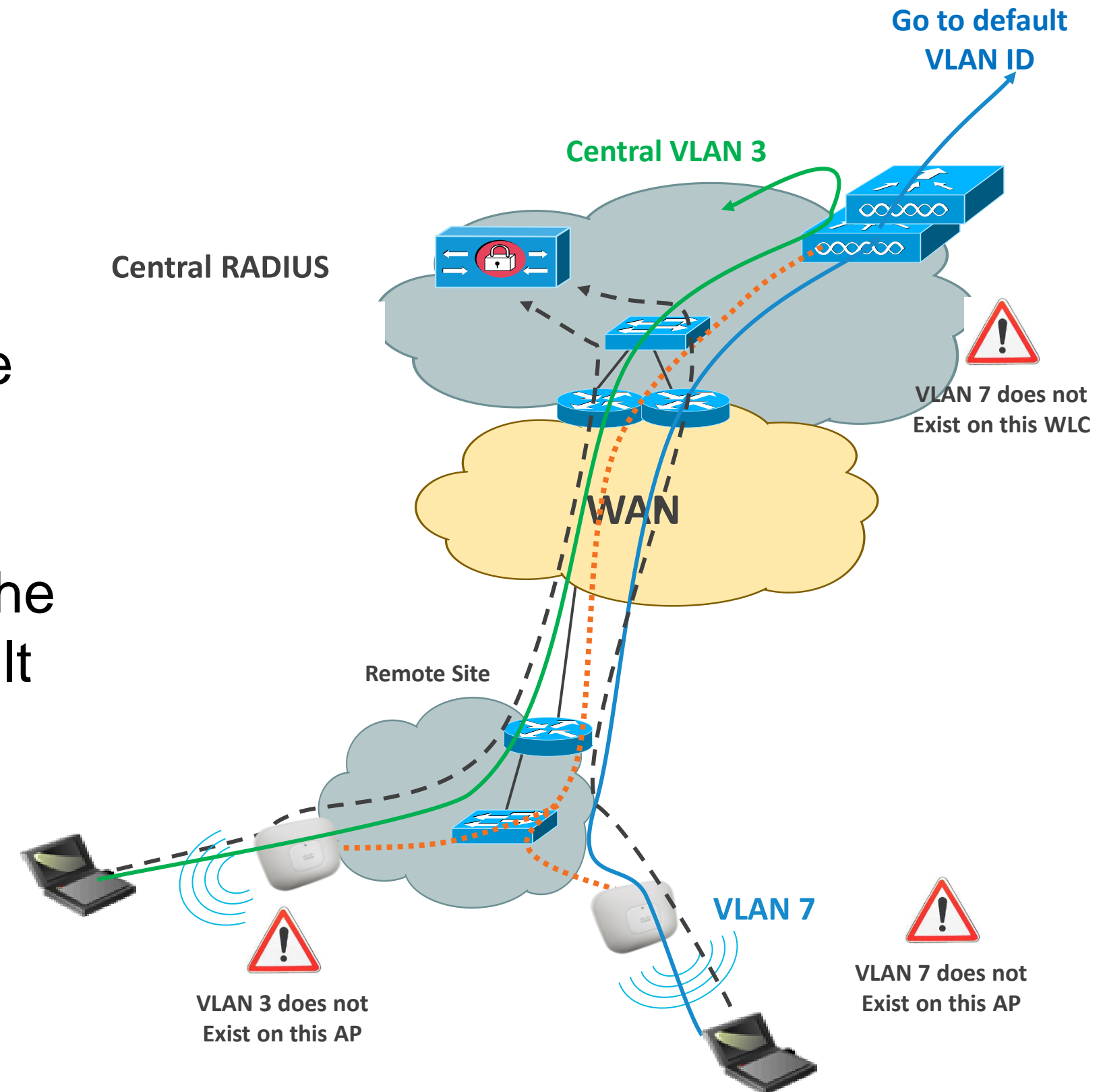
Add

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





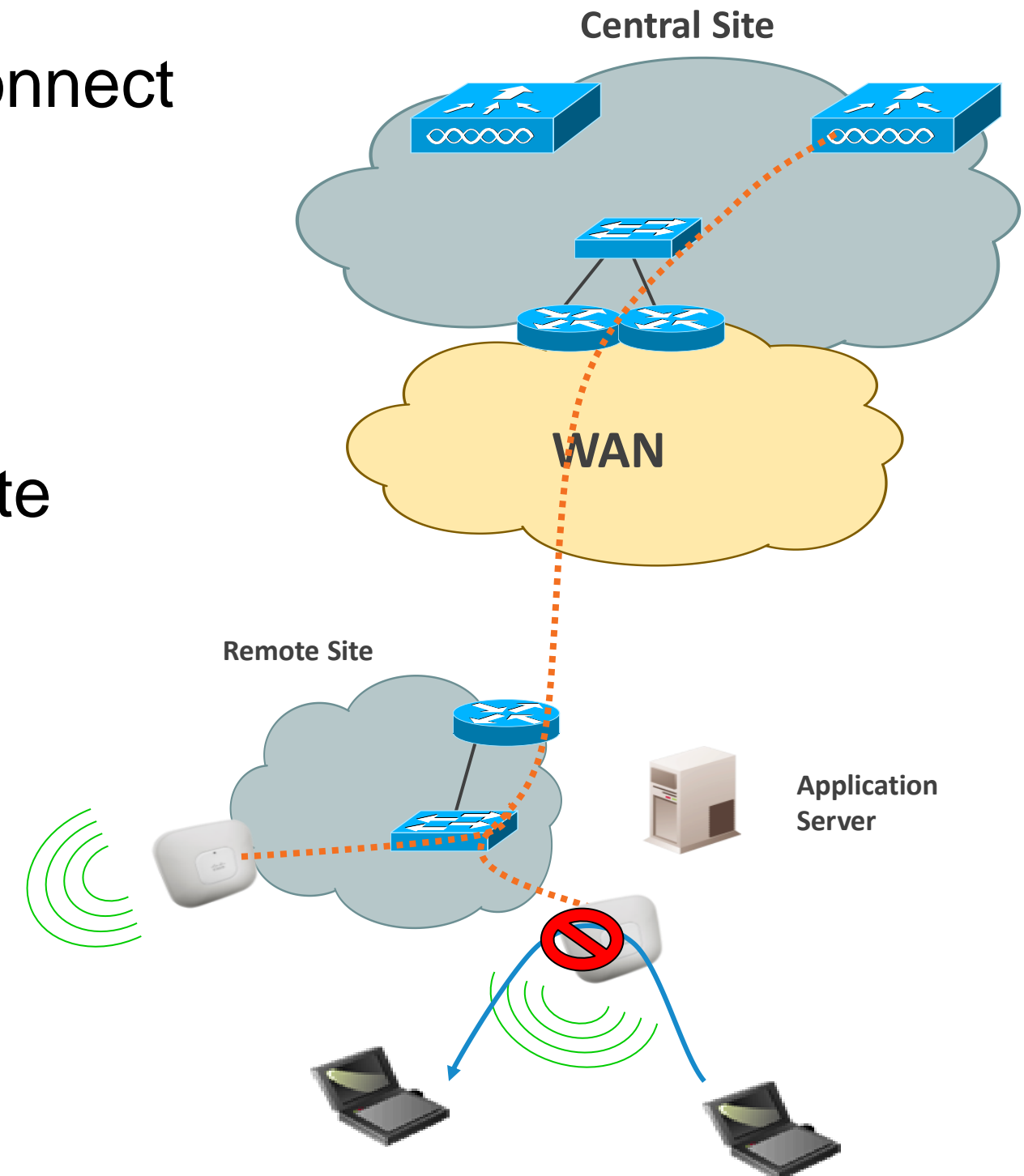
FlexConnect Peer-to-peer Blocking

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

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 Disabled

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



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”

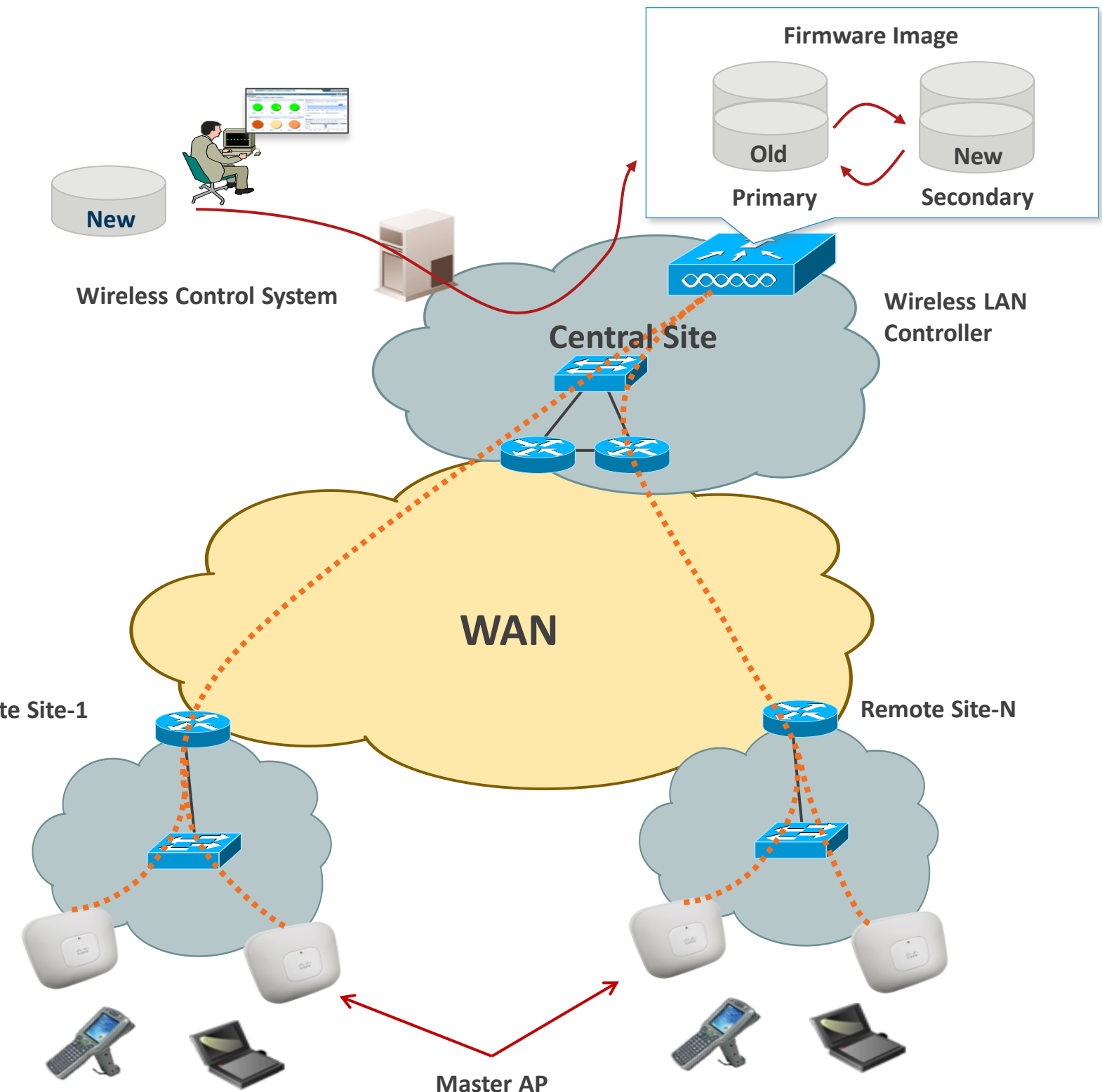
FlexConnect Smart AP Image Upgrade

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

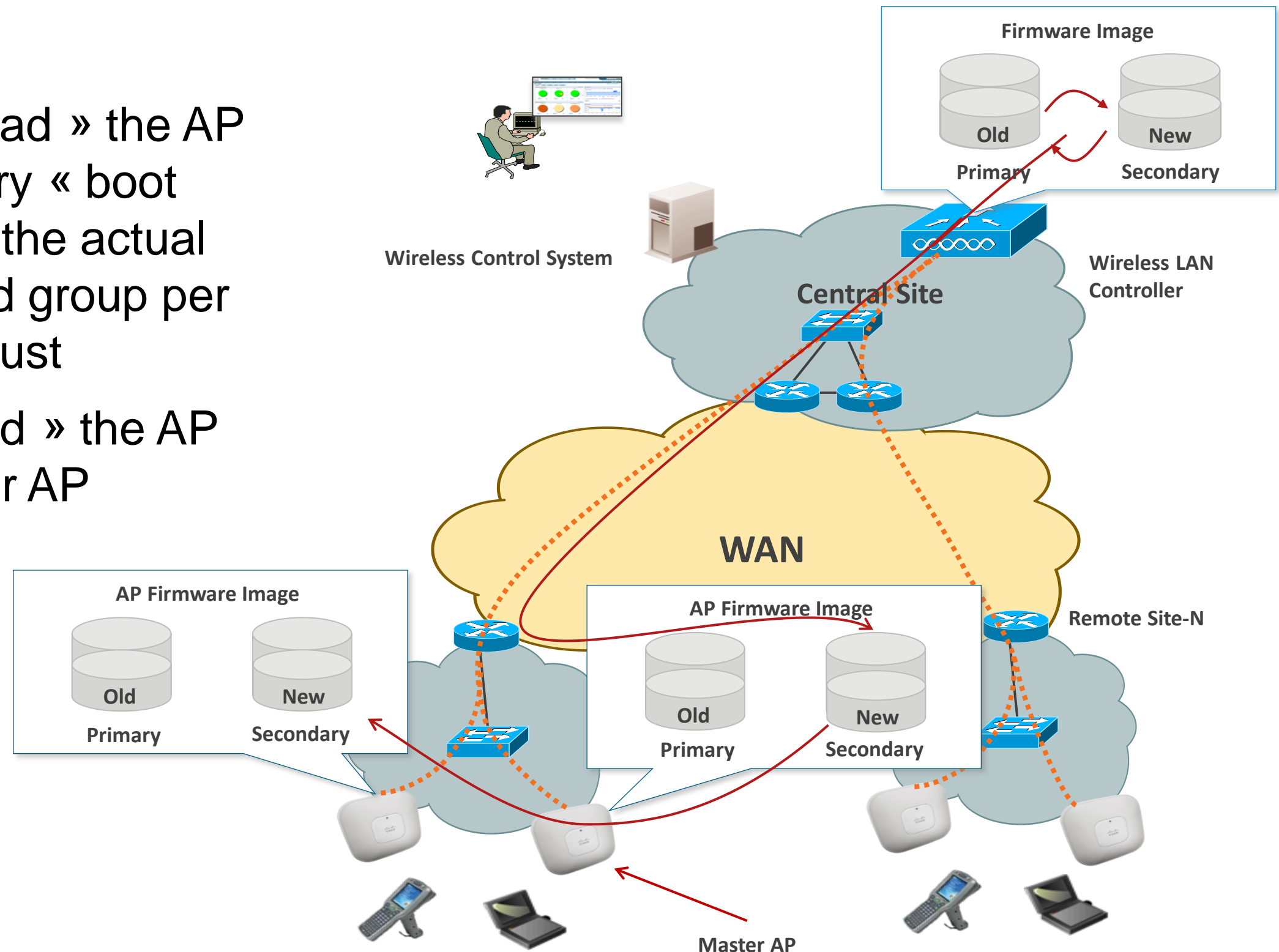
1. Download WLC upgraded firmware (will become primary)
2. Force the « boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)



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 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)



For Your Reference

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

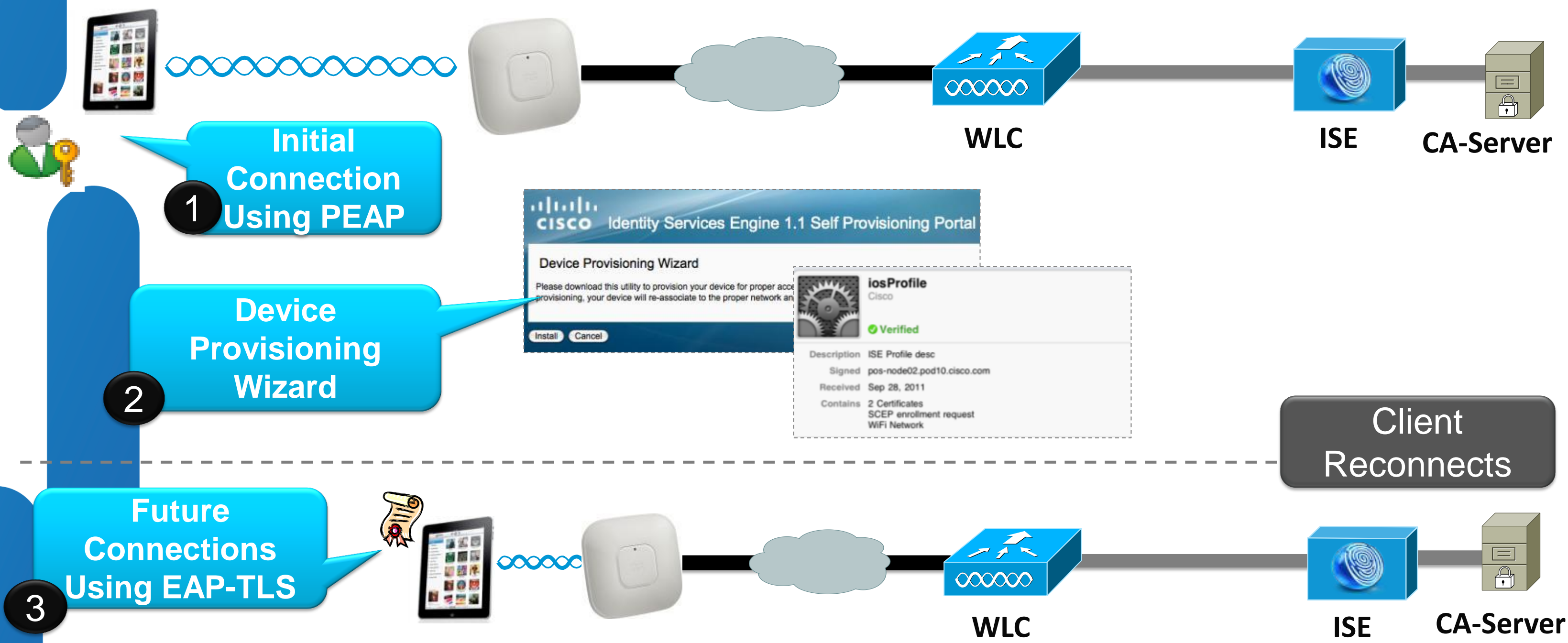


Deploying BYOD with
FlexConnect and Local Switching
(Using FlexConnect WebPolicies ACL)

BYOD Device On-Boarding in FlexConnect

Example: Apple iOS Device Provisioning

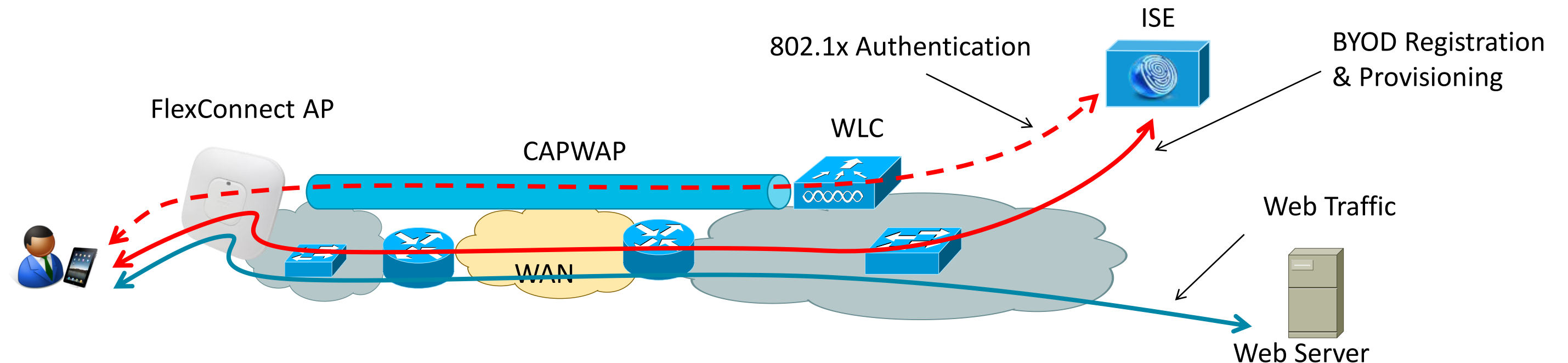
Starting from 7.4



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

The image shows two overlapping screenshots from the Cisco FlexConnect configuration interface. The left screenshot shows the 'FlexConnect' tab for AP-3600-A, with the 'External WebAuthentication ACLs' link highlighted in a red box. A red arrow points from this link to the right screenshot. The right screenshot shows the 'ACL Mappings' page for AP-3600-A, where the 'WebPolicies' section is highlighted in a red box. This section shows 'WebPolicy ACL' set to 'FlexConnect-Acl-1' with an 'Add' button. Below it, the 'WebPolicy Access Control Lists' section shows 'FlexConnect-Acl-1' with a checkmark.

Left Screenshot: Details for AP-3600-A

- General
- Credentials
- Interfaces
- High Availability
- Inventory
- FlexConnect**

VLAN Support

Native VLAN ID: 52 **VLAN Mappings**

FlexConnect Group Name: FlexConnect-Site-1

PreAuthentication Access Control Lists

- External WebAuthentication ACLs**
- Local Split ACLs
- Central DHCP Processing

Right Screenshot: AP-3600-A > ACL Mappings

AP Name: AP-3600-A

Base Radio MAC: 64:d9:89:43:4f:50

WLAN ACL Mapping

WLAN Id: 0

WebAuth ACL: FlexConnect-Acl-1 **Add**

WLAN Id	WLAN Profile Name	WebAuth ACL
---------	-------------------	-------------

WebPolicies

WebPolicy ACL: FlexConnect-Acl-1 **Add**

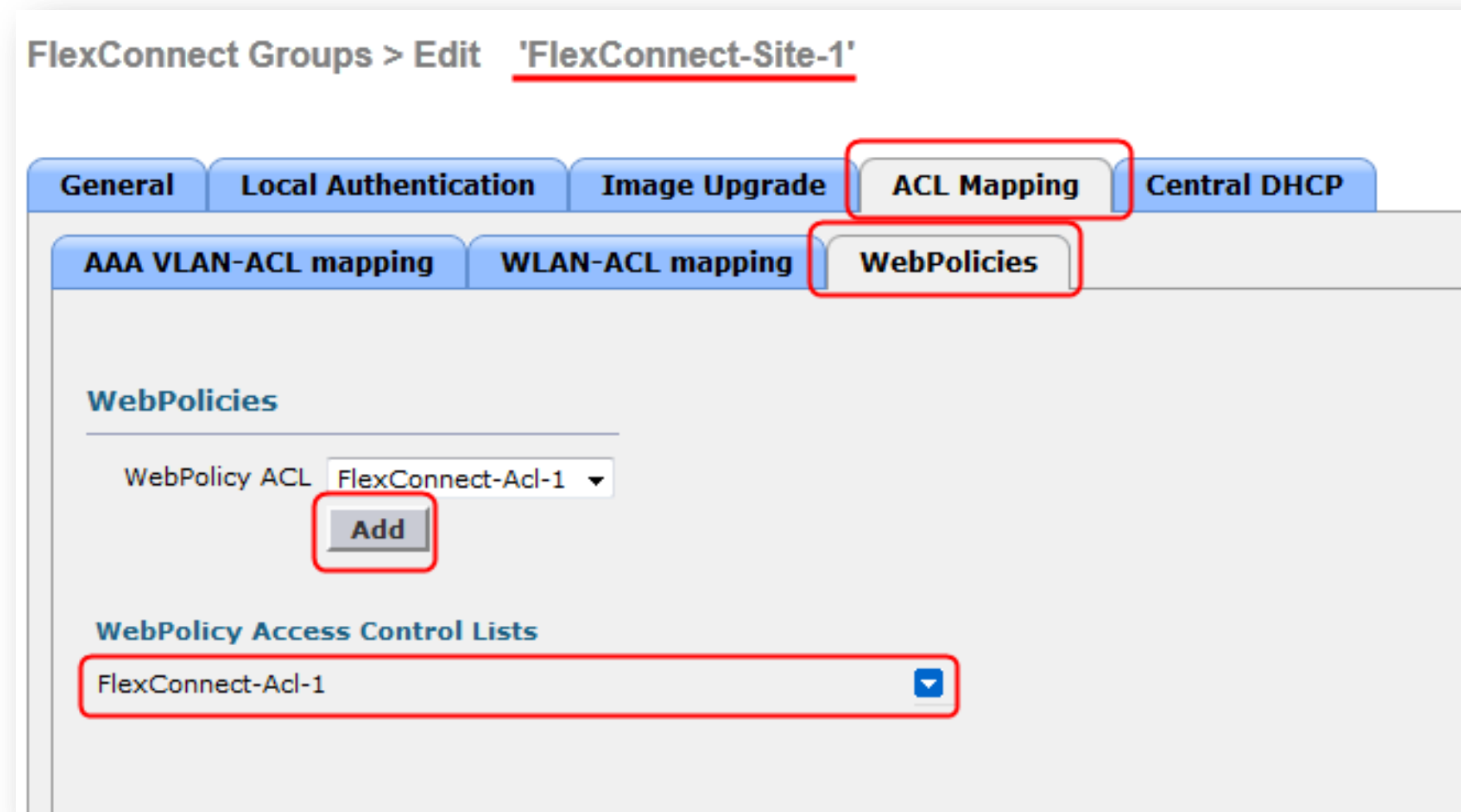
WebPolicy Access Control Lists

FlexConnect-Acl-1

FlexConnect Web Policy ACL

Configure Web Policy ACL per FlexConnect Group

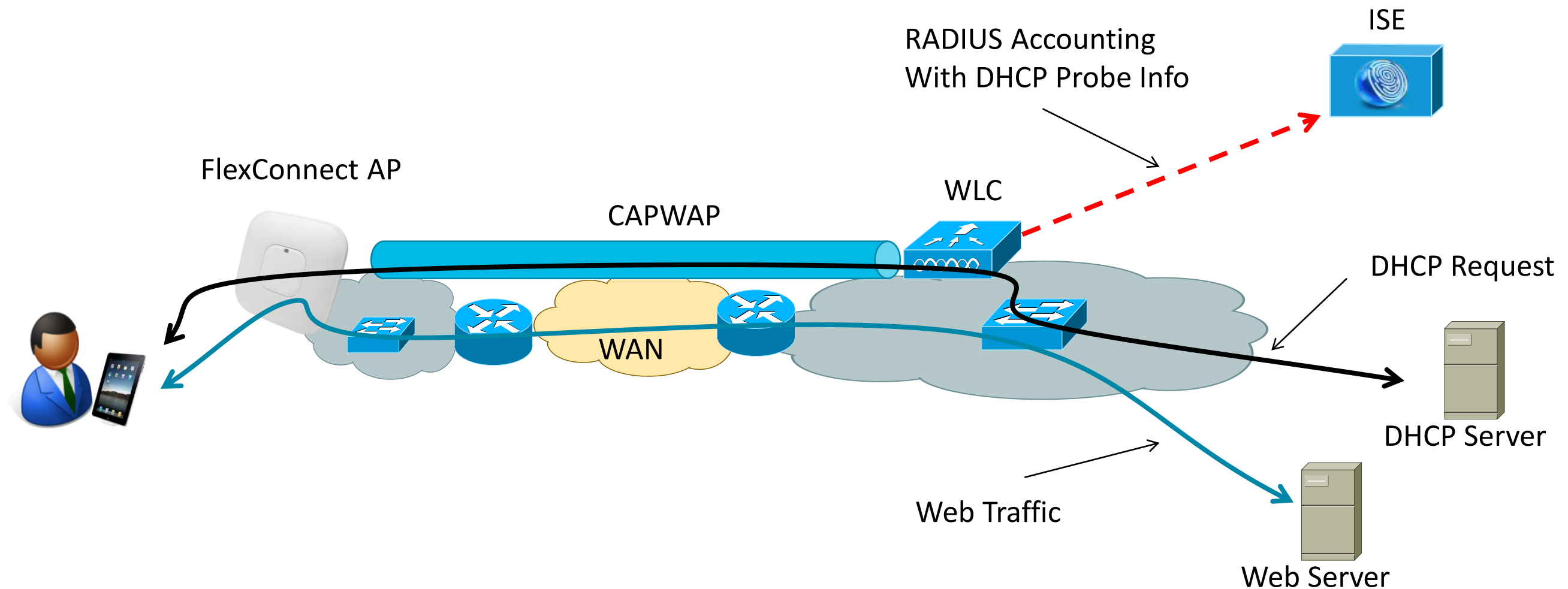
- Use ACL Mapping tab in FlexConnect Group configuration
- WebPolicies ACL are not the same as VLAN ACL or WebAuthentication ACL.



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.

All APs > Details for AP-3600-A

General Credentials Interfaces High Availability Inventory **FlexConnect**

VLAN Support

Native VLAN ID [VLAN Mappings](#)

FlexConnect Group Name

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

[Central DHCP Processing](#)

All APs > AP-3600-A > Central DHCP Processing

AP Name

Base Radio MAC

WLAN DHCP Mapping

WLAN Id

Central DHCP

Override DNS

NAT-PAT

[Add](#)

WLAN Id	WLAN Profile Name	Central DHCP	Override DNS	NAT-PAT	Inheritance level
3	RackMobilityFlex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Wlan

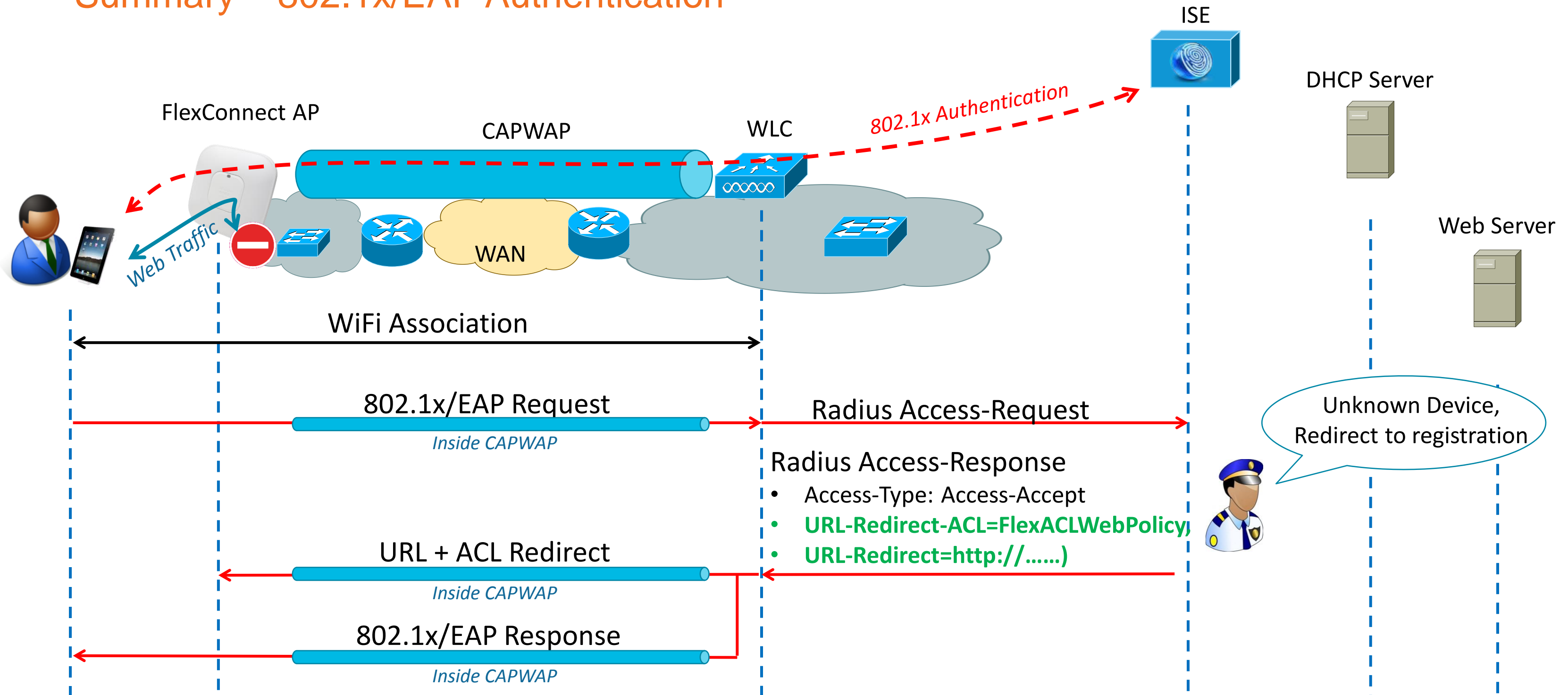
Deploying BYOD with FlexConnect Wireless

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

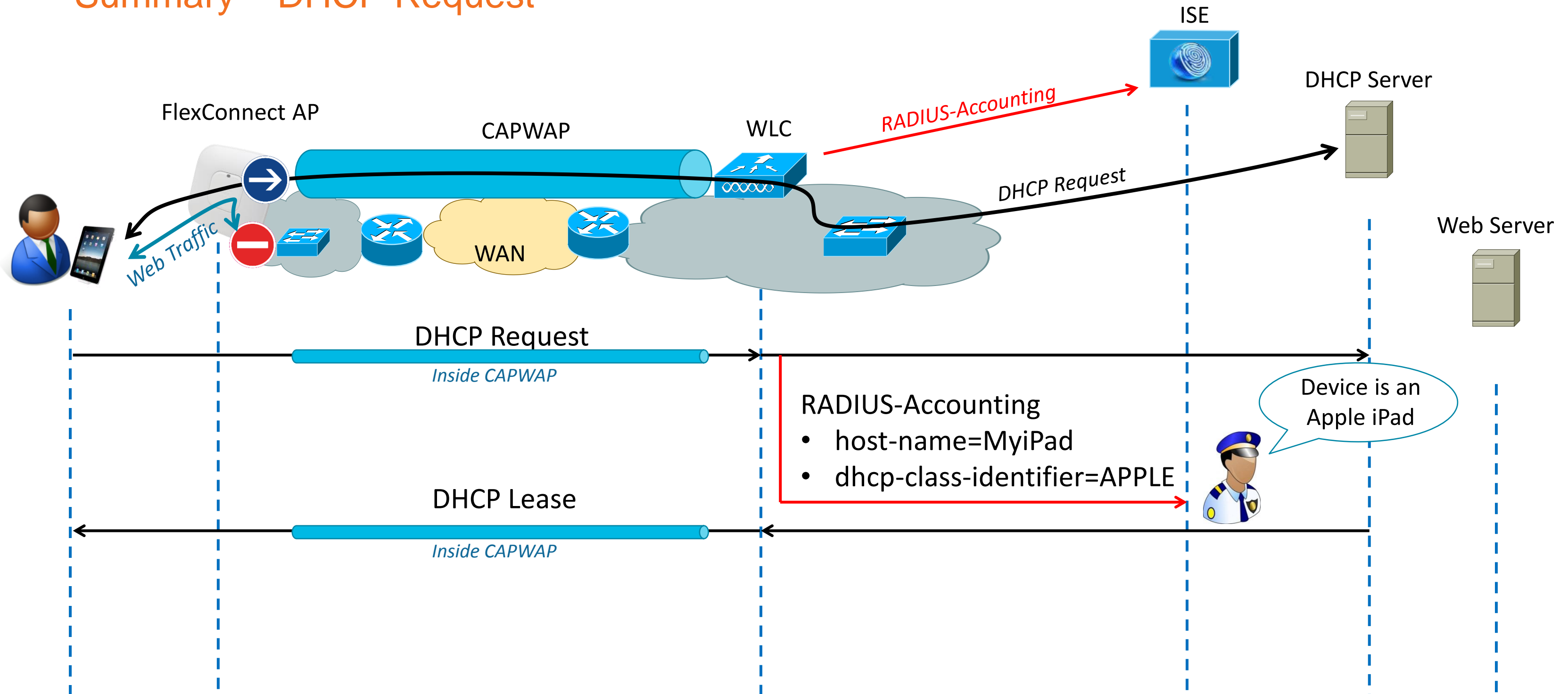
Deploying BYOD with FlexConnect Wireless

Summary – 802.1x/EAP Authentication



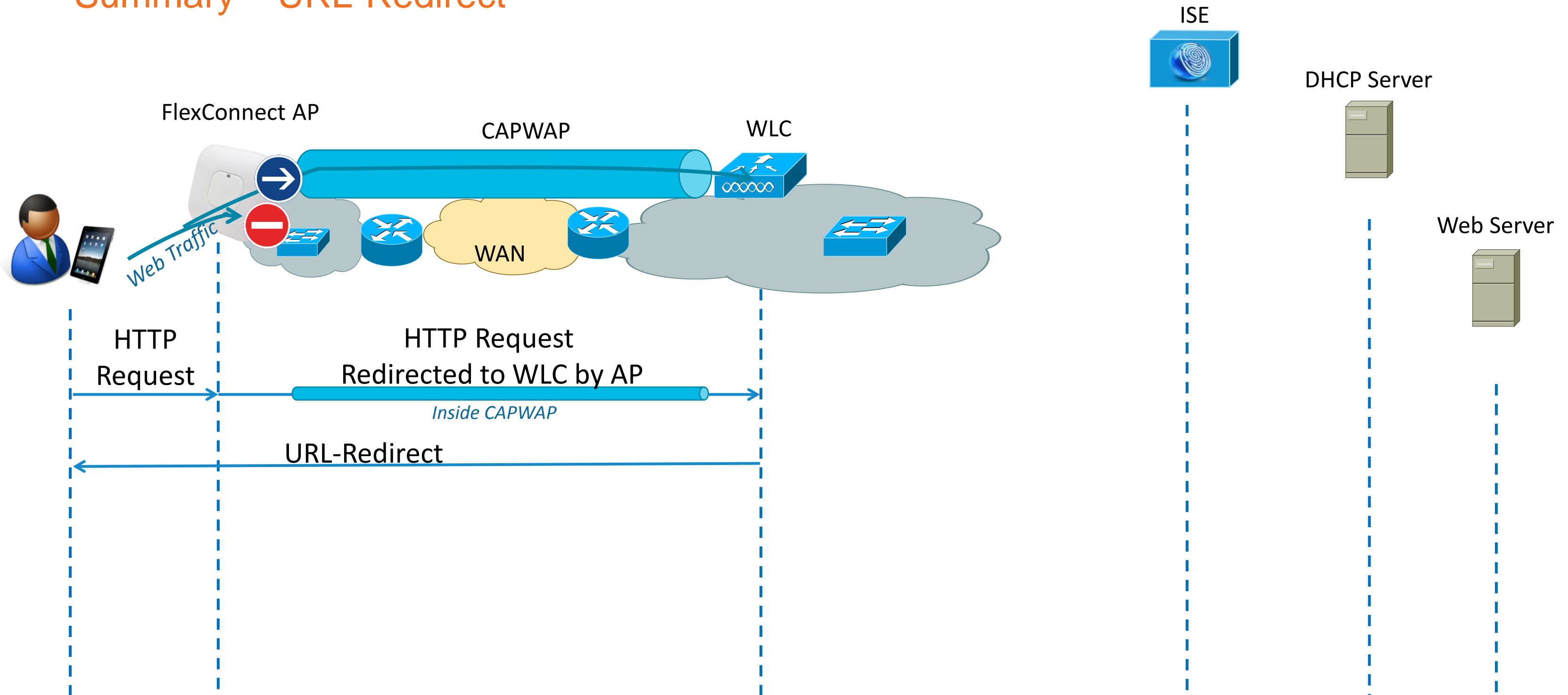
Deploying BYOD with FlexConnect Wireless

Summary – DHCP Request



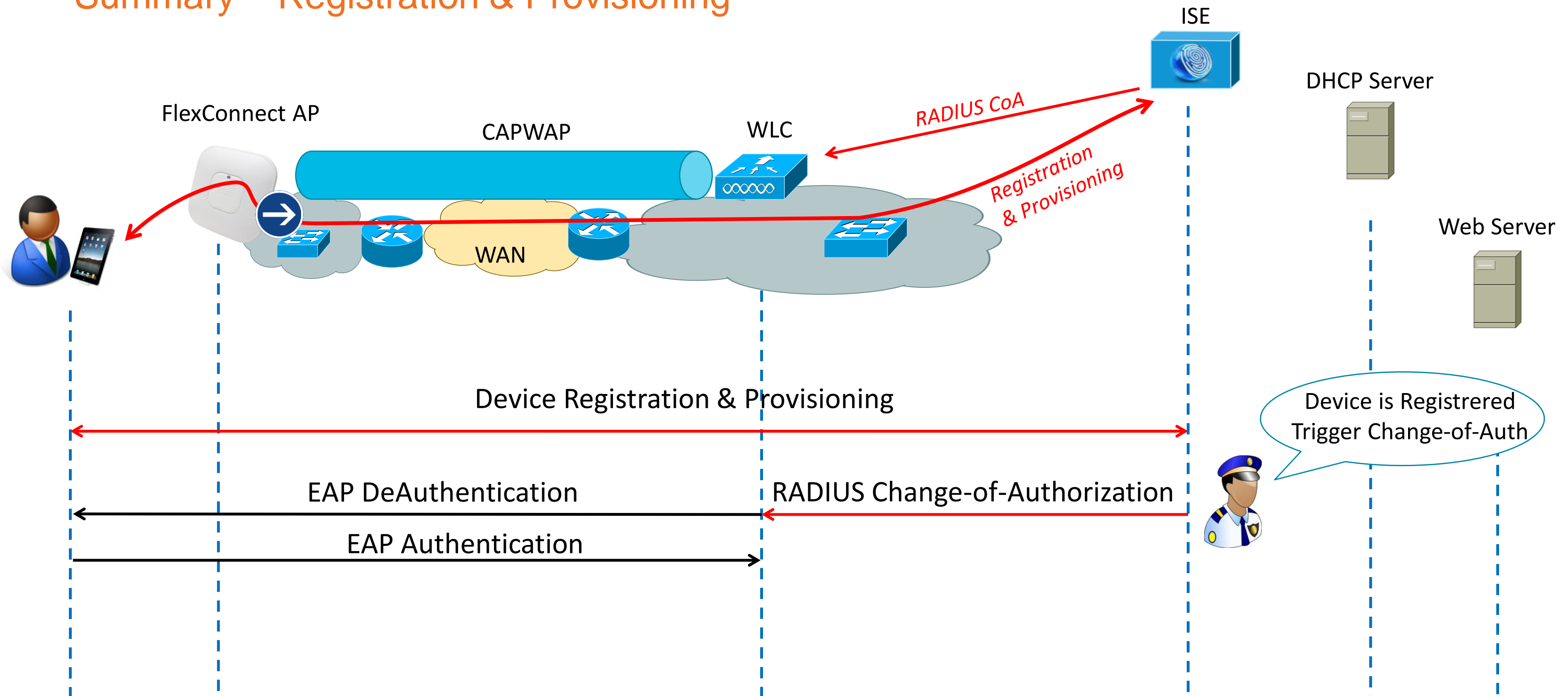
Deploying BYOD with FlexConnect Wireless

Summary – URL-Redirect



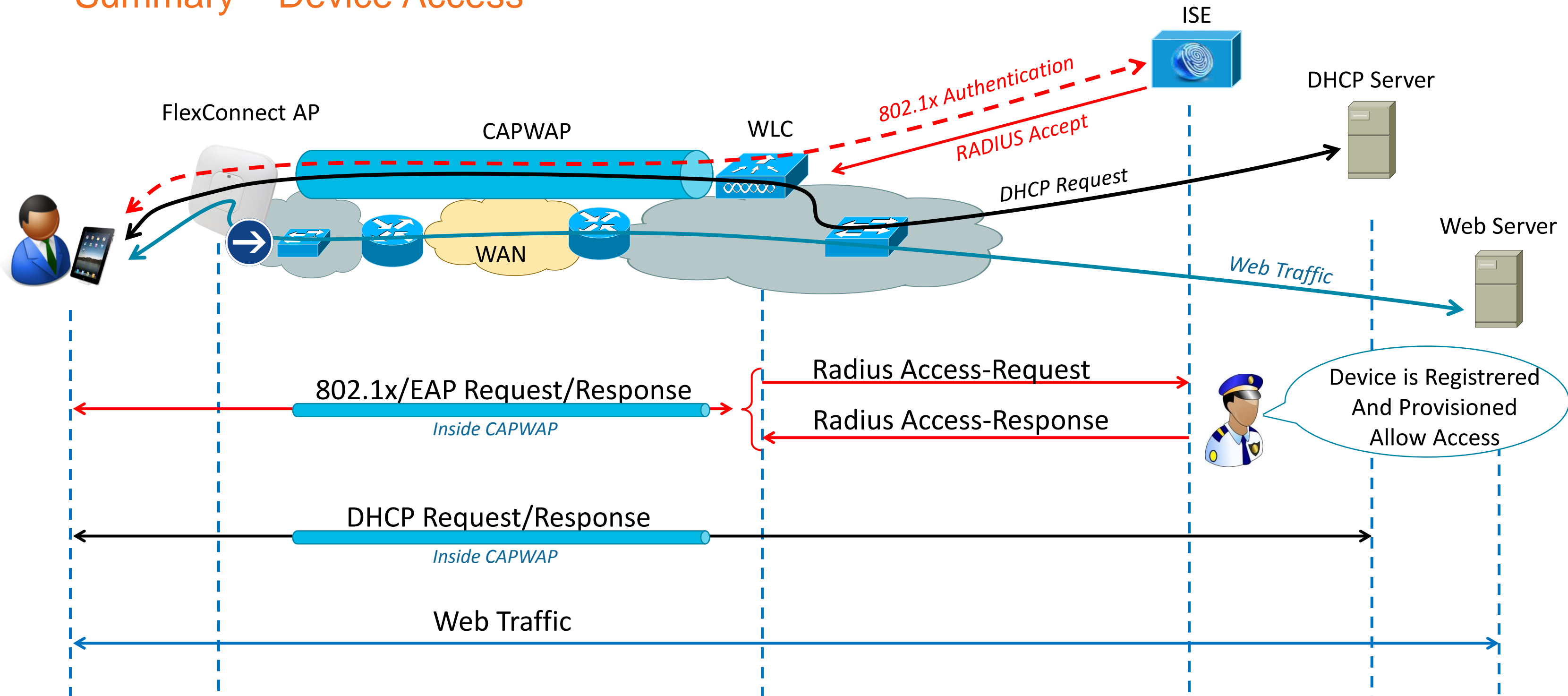
Deploying BYOD with FlexConnect Wireless

Summary – Registration & Provisioning



Deploying BYOD with FlexConnect Wireless

Summary – Device Access





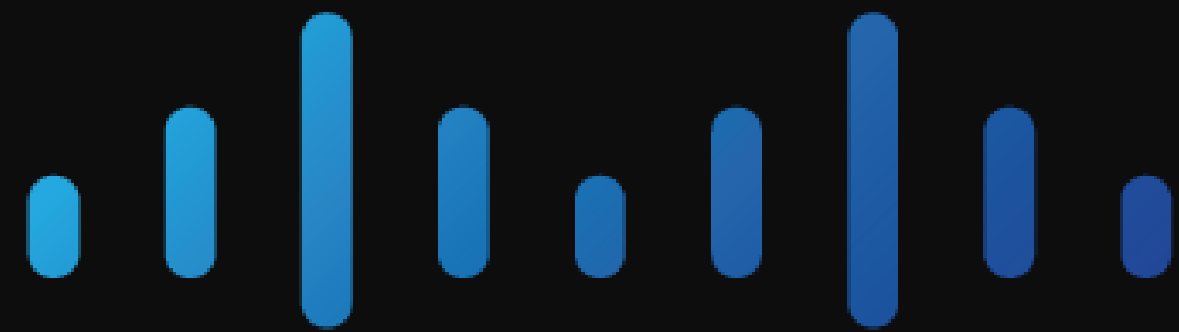
Summary

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