Branch Office Wireless LAN Design

BRKEWN-2016

Sujit Ghosh

Senior Manager Technical Marketing

Enterprise Networking Group

Cisco live!

Objective

Design & Deploy Branch Network That Increases Business Resiliency

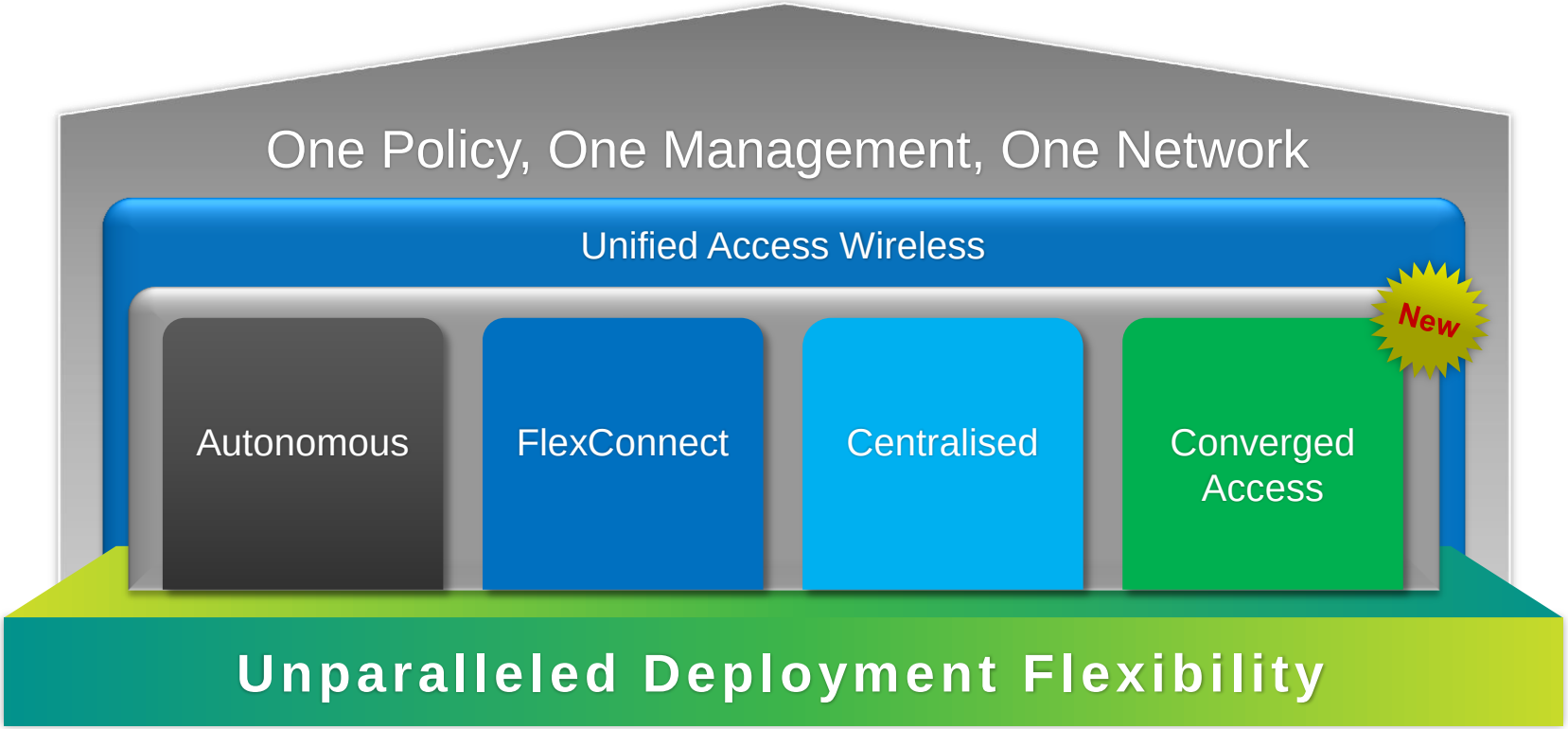
Agenda

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



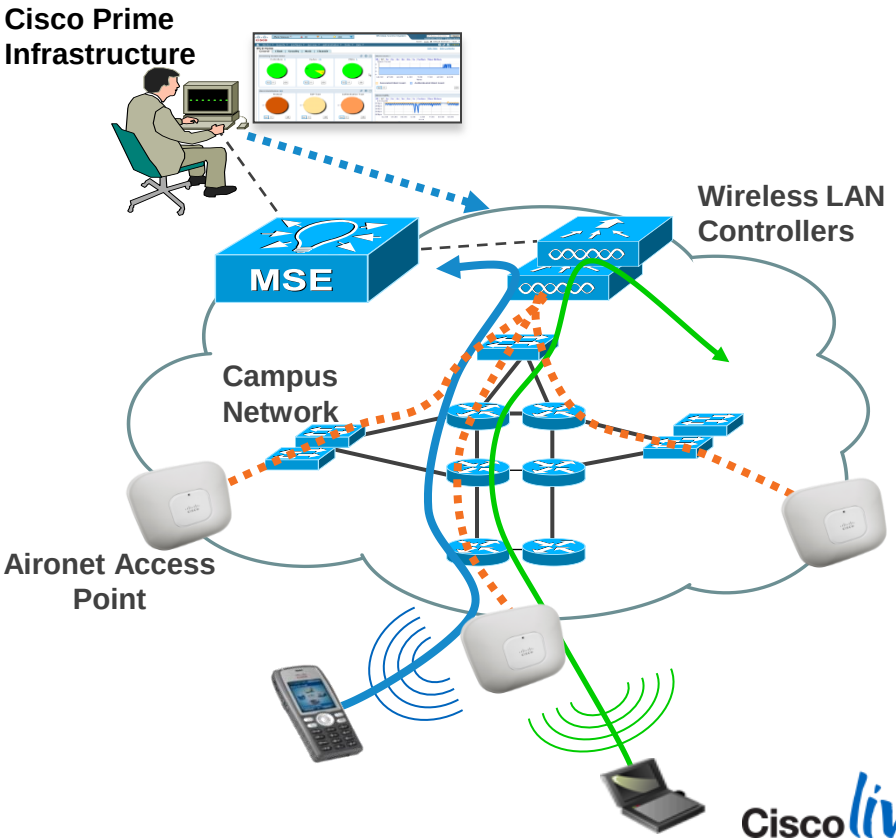

Cisco Unified Wireless LAN Principles

Cisco One Network : Wireless Deployment Modes



Cisco Unified Wireless Principles

- Components
  - Wireless LAN Controllers
  - Aironet Access Points
  - Management (Prime Infrastructure)
  - Mobility Services 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



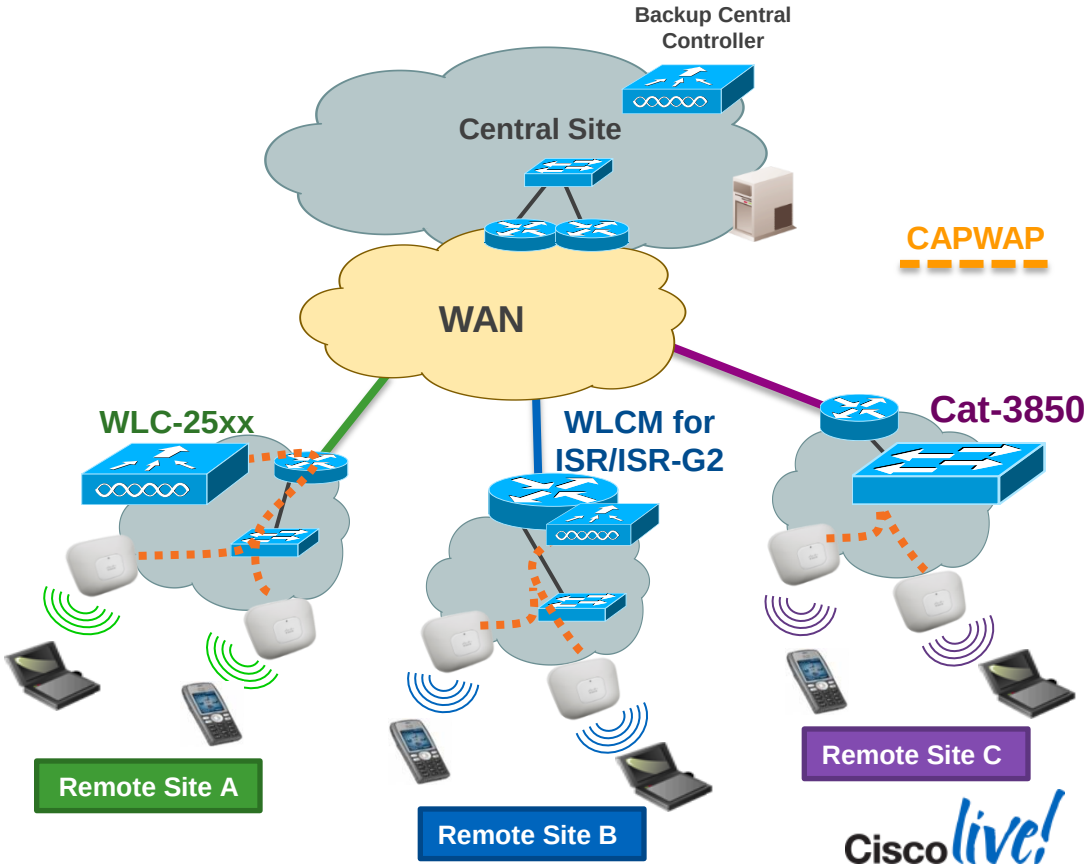



Wireless Branch Deployment Options

Branch Office with Local WLAN Controller

Overview

- Branches can also have local remote controllers
- Small or Mid-size Branch WLCs
  - CT-2504,
  - Integrated controller modules in ISR/ISR-G2
  - New Converged Access Cat-3850
- 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

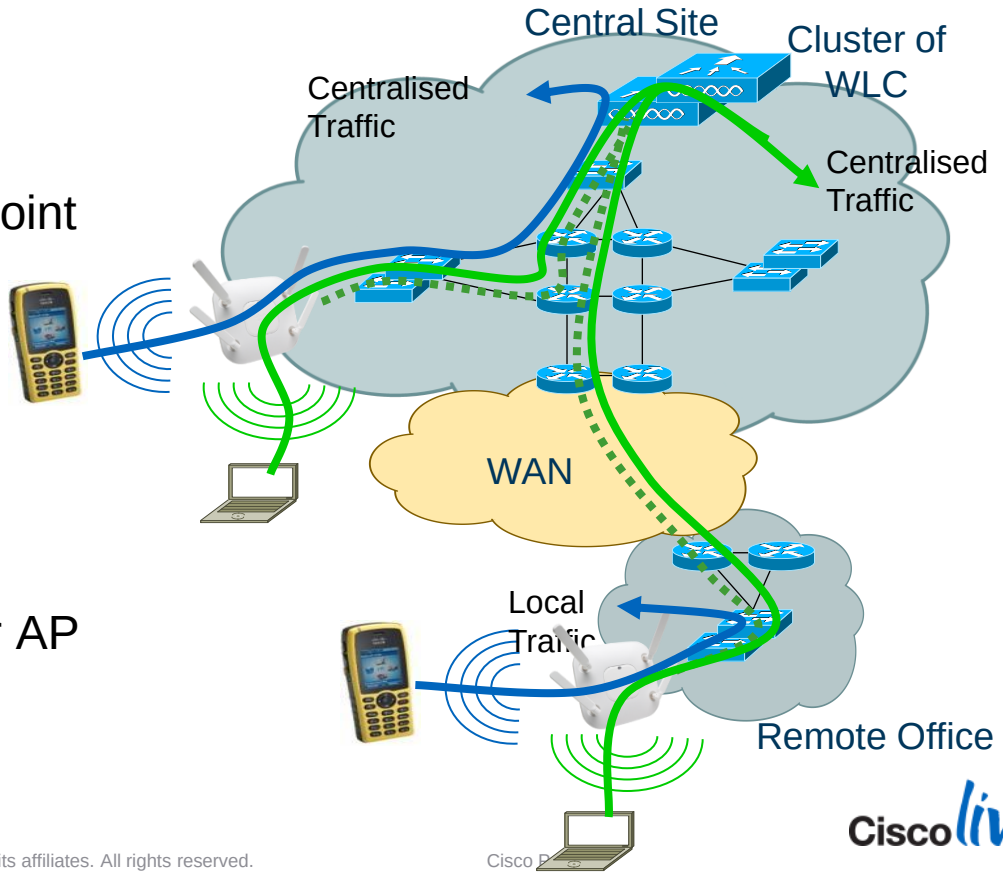
Note: If you have ISR/ISR G2 at branch site then it is recommended to use the IOS Firewall at edge for unified access policies.

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

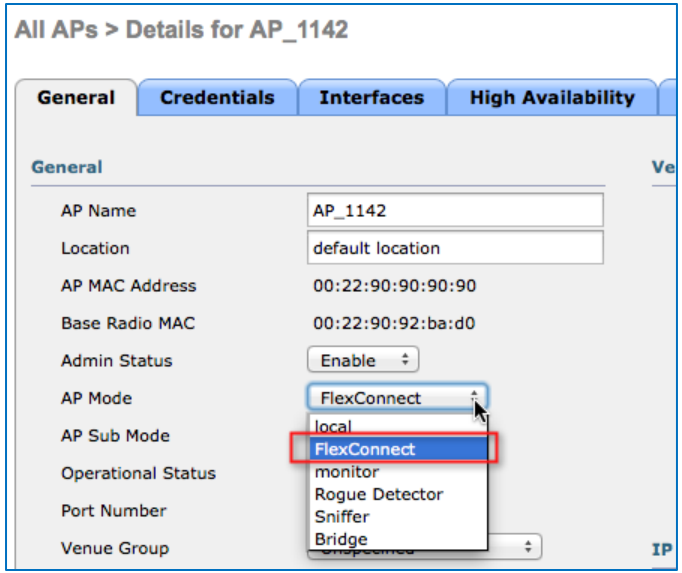
- **Connected Mode** – When FlexConnect can reach Controller (connected state), it gets help from controller to complete client authentication.
- **Standalone mode** – When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.

- **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

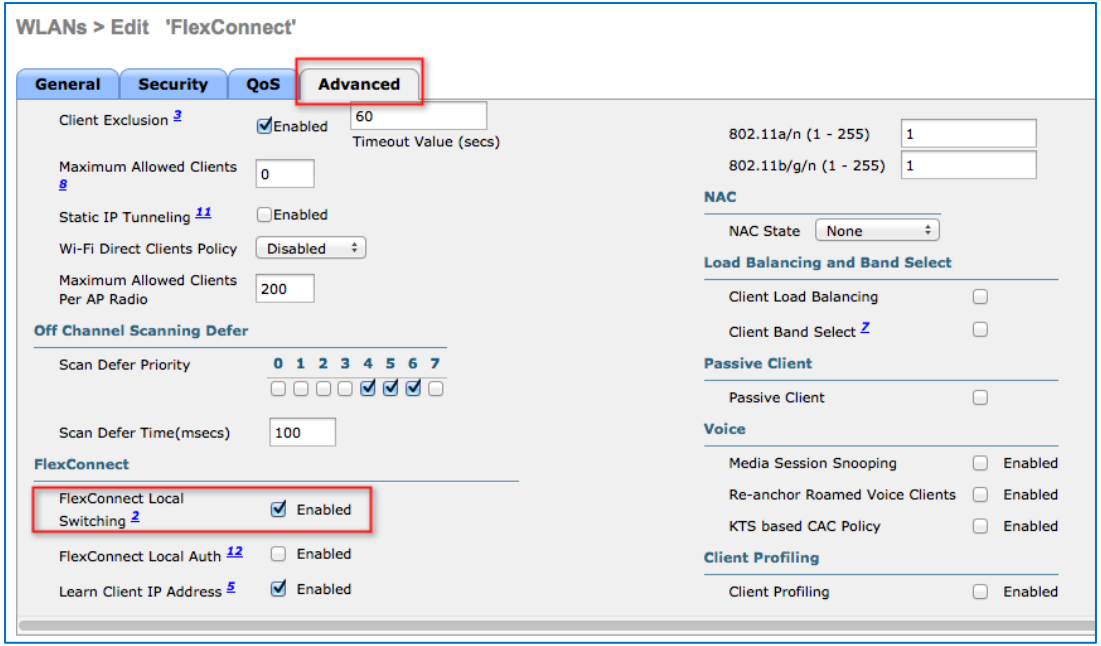
- Enable FlexConnect mode per AP
- Supported AP: AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600 , AP-2600 , AP-3600, AP-3700, AP-1520, AP-1530, AP-1550



Configure FlexConnect Local Switching

Step 2: Enable Local Switching per WLAN

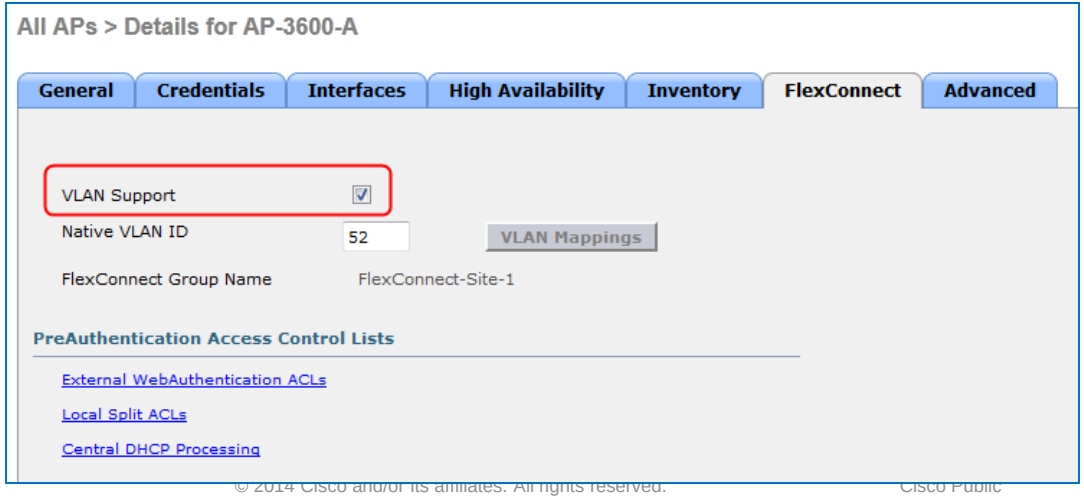
- Only WLAN with “FlexConnect Local Switching” enabled will allow local switching on the FlexConnect AP



Configure FlexConnect VLAN Mapping

Step 3: FlexConnect Specific Configuration

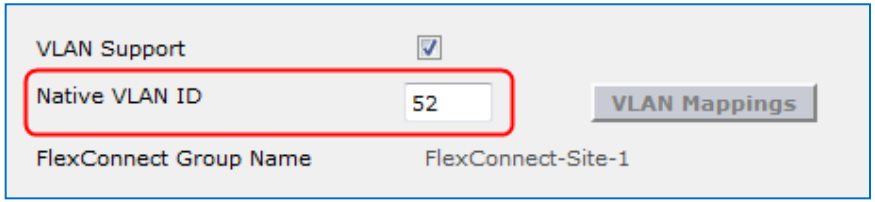
- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)
- VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using Cisco Prime Infrastructure templates



Configure FlexConnect VLAN Mapping

Step 4: FlexConnect Specific Configuration – Native Vlan

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

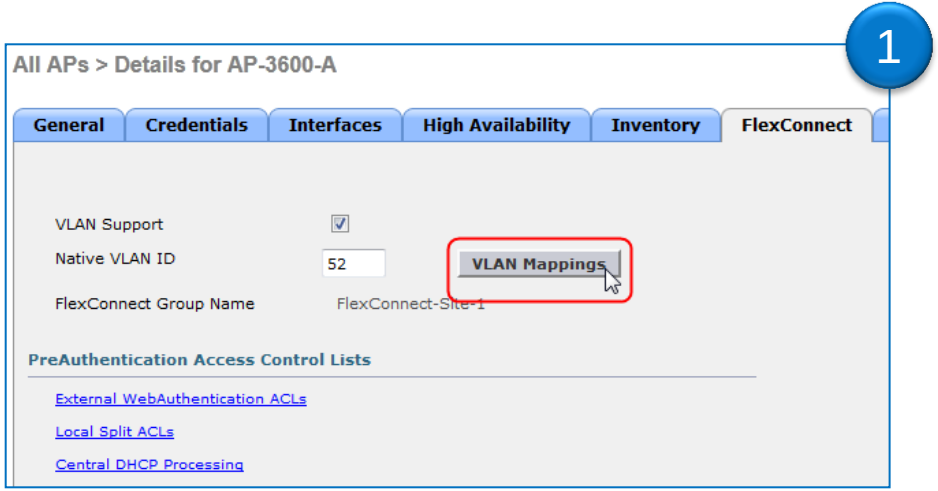


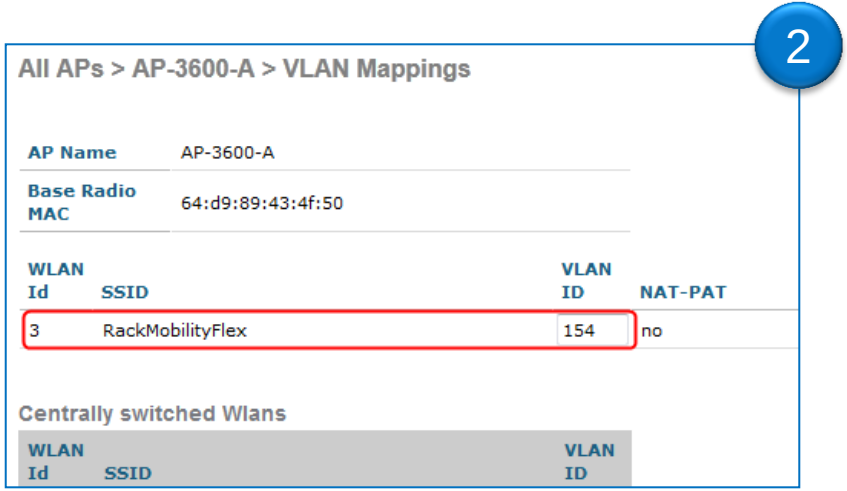

```
!
interface GigabitEthernet0/1
 switchport access vlan 52
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 52
 switchport trunk allowed vlan 52,154,155
 switchport mode trunk
 spanning-tree portfast
!
```

Configure FlexConnect SSID-VLAN Mapping

Step 5: Per AP SSID to VLAN Mapping

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





- Or use Cisco Prime Infrastructure (NCS) via configuration templates




Evaluate FlexConnect Architectural Requirements

FlexConnect Design Considerations

For Your Reference

WAN Limitations Apply

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	64 kbps	300 ms	5	25
Data	640 kbps	300 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Data+Voice	128 kbps	100 ms	5	25
Data+Voice	1.44 Mbps	100 ms	50	1000
Monitor	64 kbps	2 sec	5	N/A
Monitor	640 kbps	2 sec	50	N/A

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

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

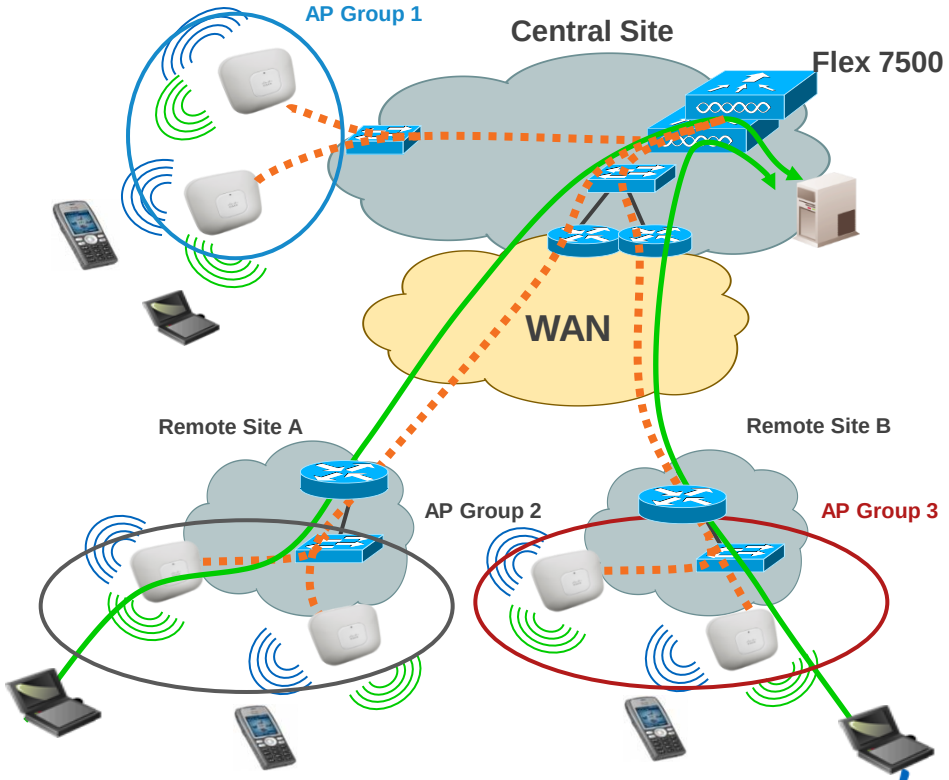



Why do we need FlexConnect & AP Groups?

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 group

Scaling	Flex 7500	CT-5508	WiSM-2	CT-2504
# AP Groups	6000	500	1000	50
# WLAN (SSID)	512	512	512	16
# VLAN (Interfaces)	4095	512	512	16



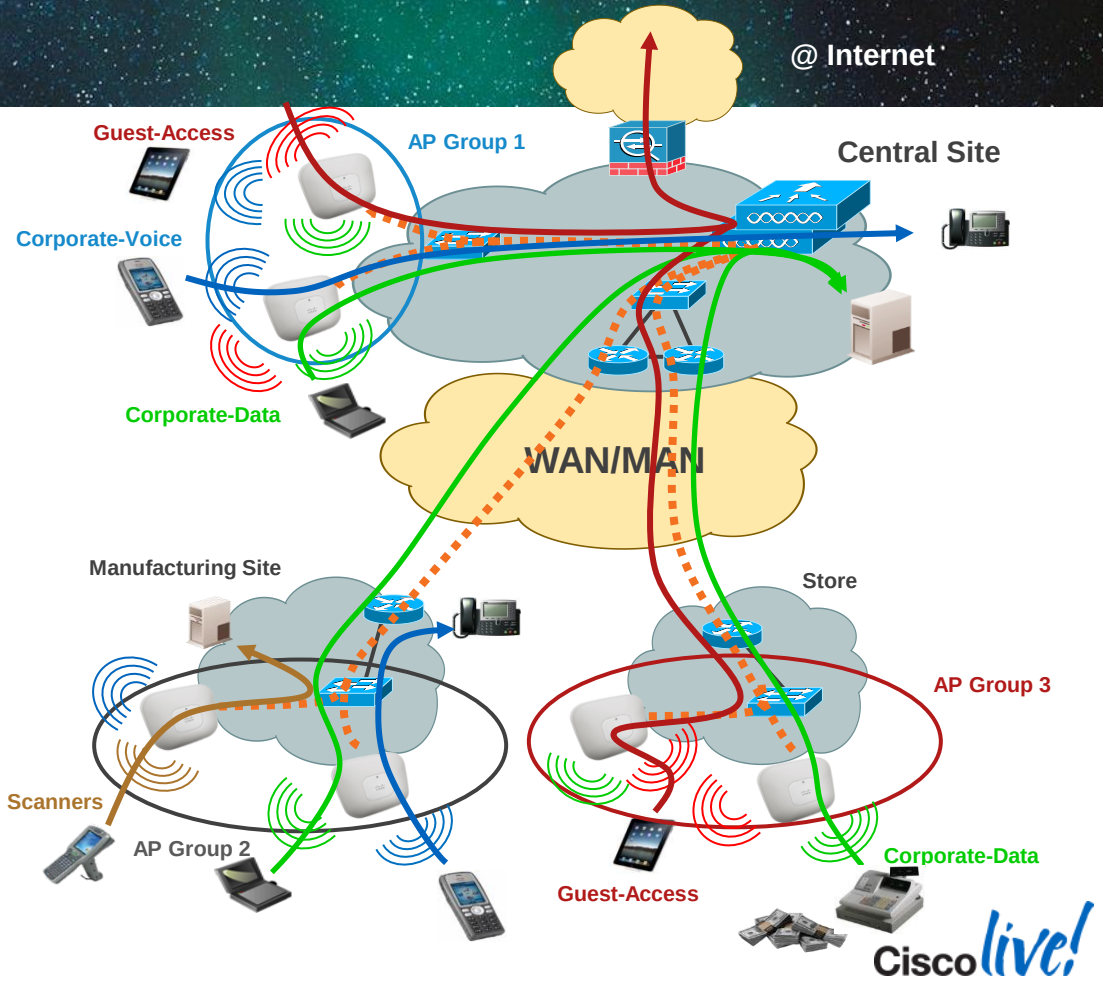
AP Groups Usage
Per Location SSID

- 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 Site**

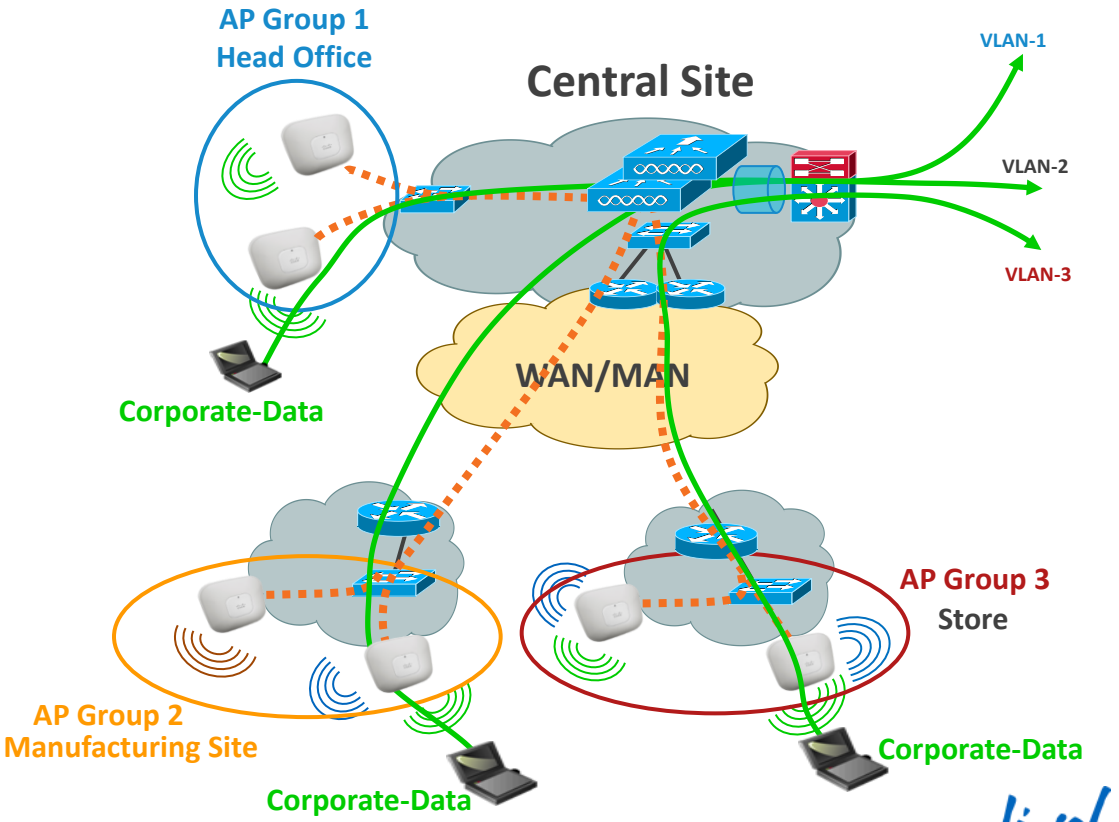
    Corporate-Voice, Corporate-Data, Scanners
  - **Store**

    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.
- Admin can monitor and filter based on different IP@ each site
- 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

Add New

WLAN SSID: RackMobility(1)

Interface /Interface Group(G): partenaires 1

SNMP NAC State: Enabled

Add | Cancel

Ap Groups > Edit 'AP-Group-1'

< Back

General | WLANs | RF Profile | APs | 802.11u

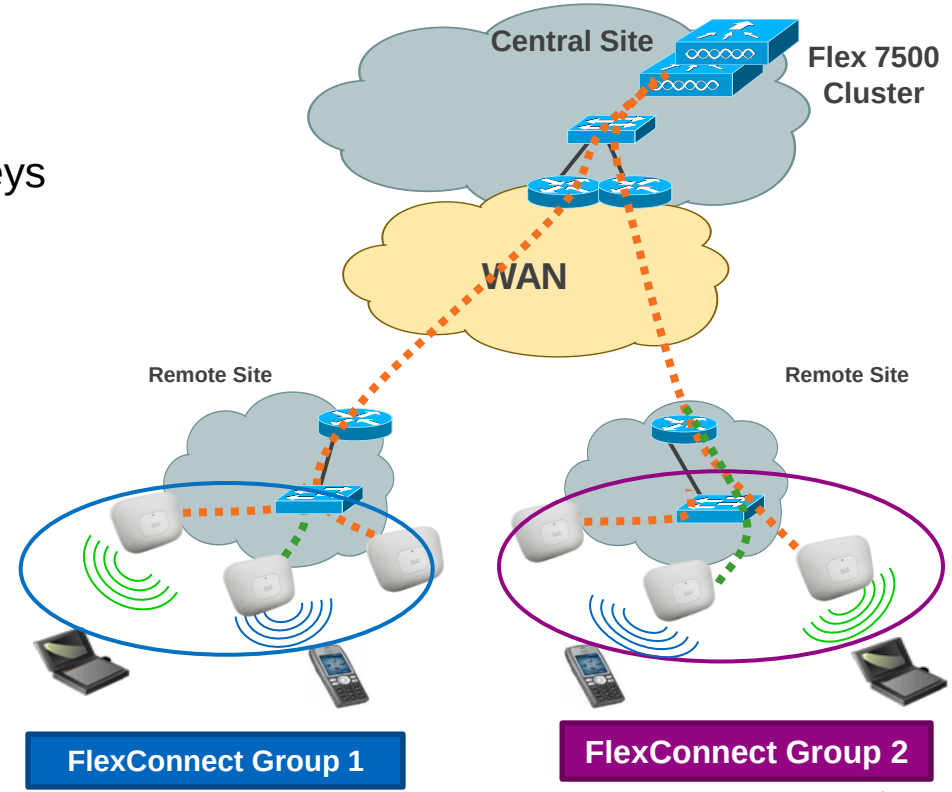
Add New

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

Understanding FlexConnect Groups
Overview

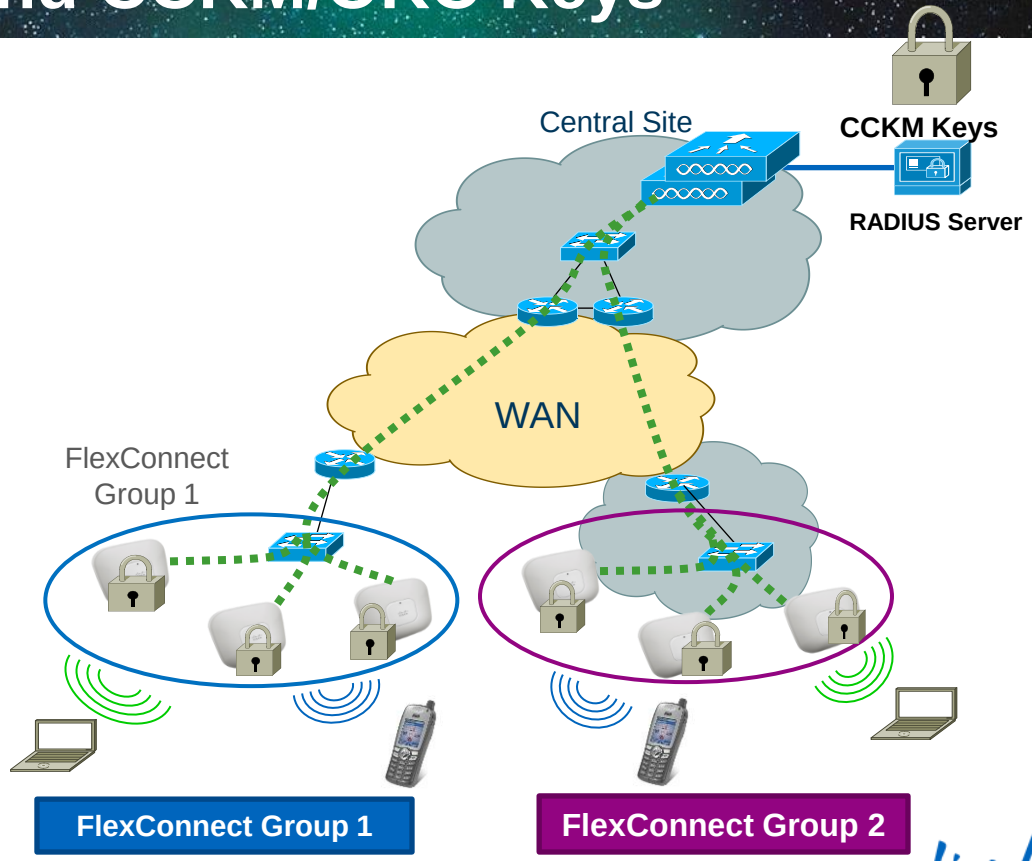
- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys
  - Local/backup RADIUS servers IP/keys
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade
- Scaling information

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



FlexConnect Groups and CCKM/OKC Keys

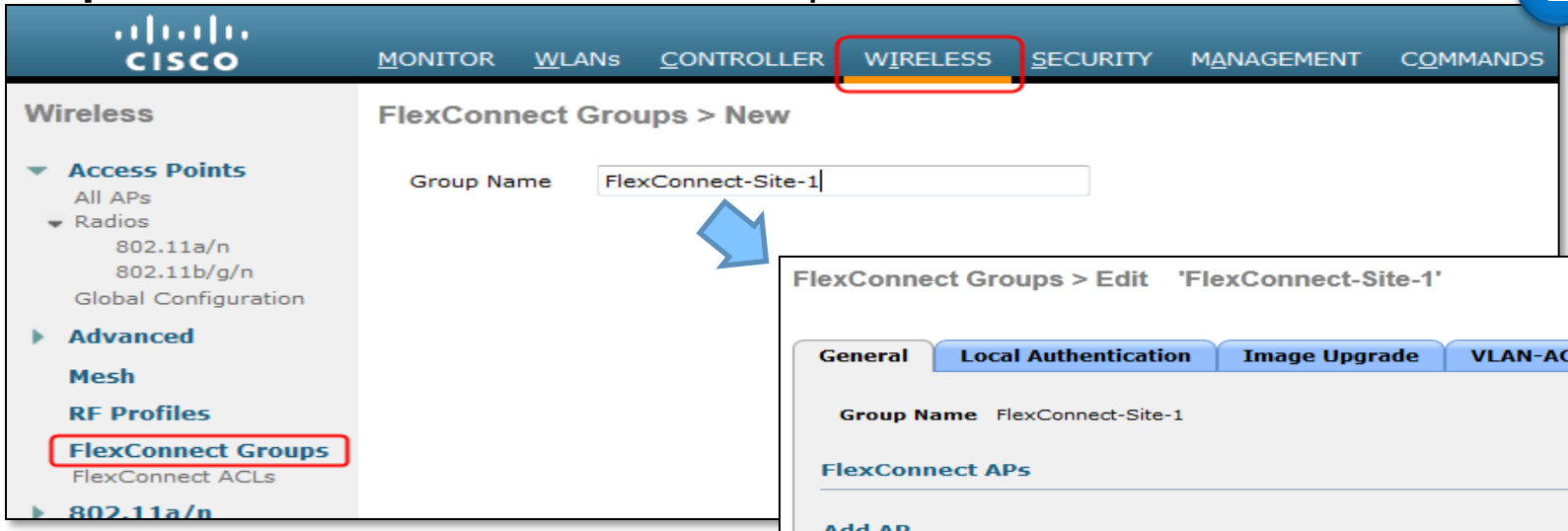
- CCKM/OKC keys are stored on FlexConnect APs for Layer 2 fast roaming
- The FlexConnect APs will receive the CCKM/OKC keys from the WLC
- If a FlexConnect AP boots up in standalone mode, it will not get the OKC/CCKM keys from the WLC and fast roaming will not be supported
- FlexConnect supports 802.11r Fast Transition with local key caching.



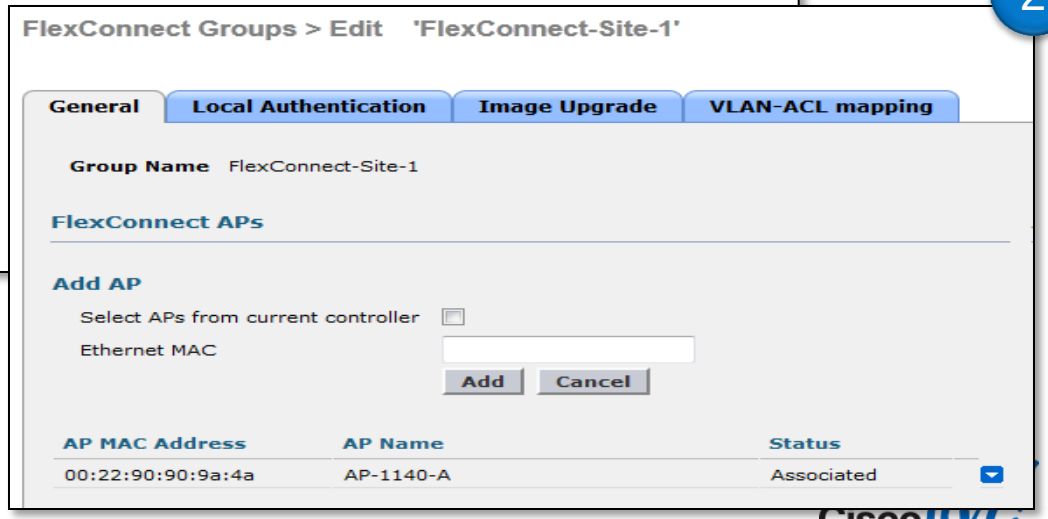
FlexConnect Groups Creation

Step 1: Add a New FlexConnect Group

1



2



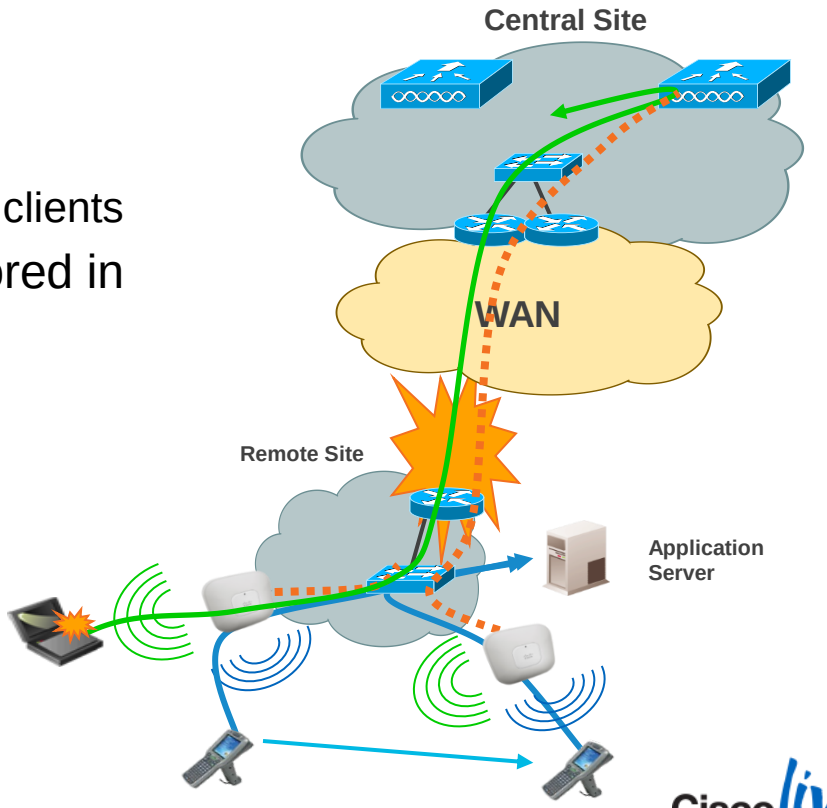
Step 2: Add APs to the FlexConnect Group




Designing a Resilient Wireless Branch Network

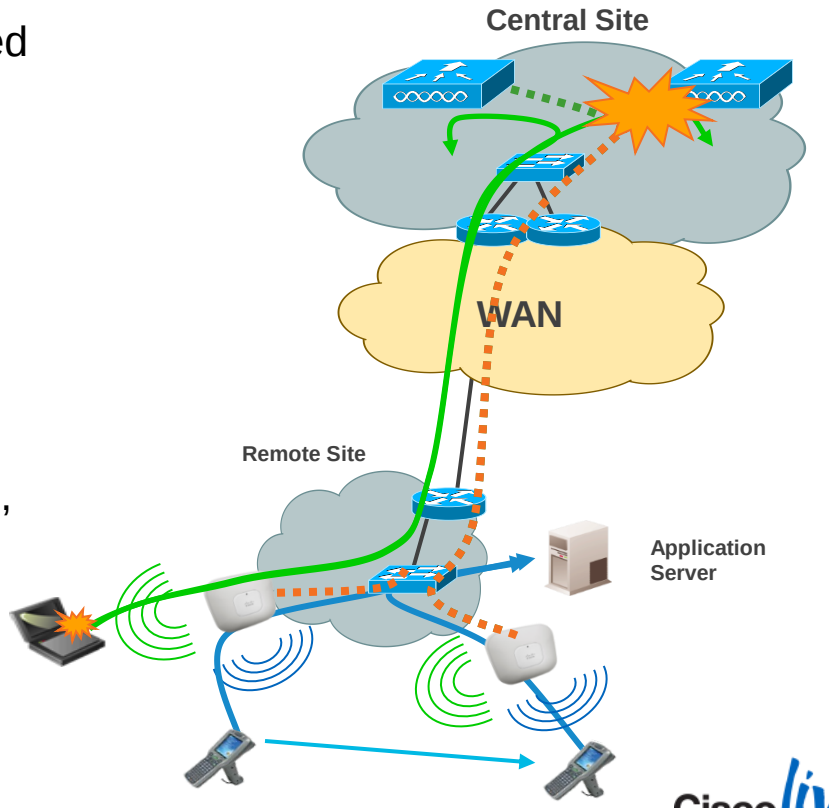
FlexConnect Backup Scenario
WAN Failure

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



FlexConnect Backup Scenario - *WLC Failure*

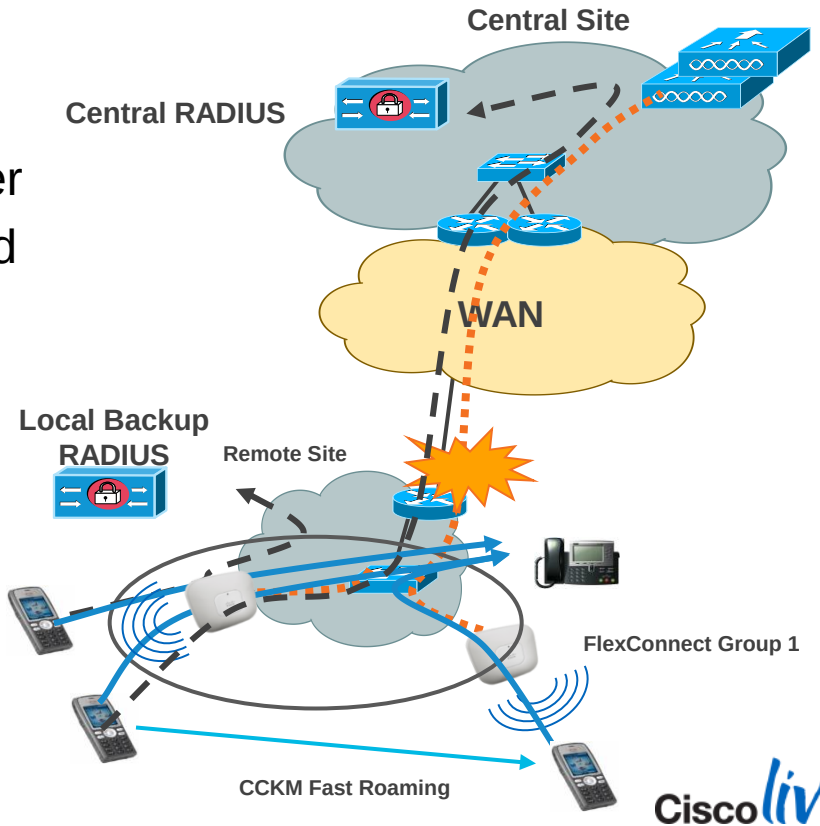
- FlexConnect will first backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with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



FlexConnect Group: Local Backup RADIUS

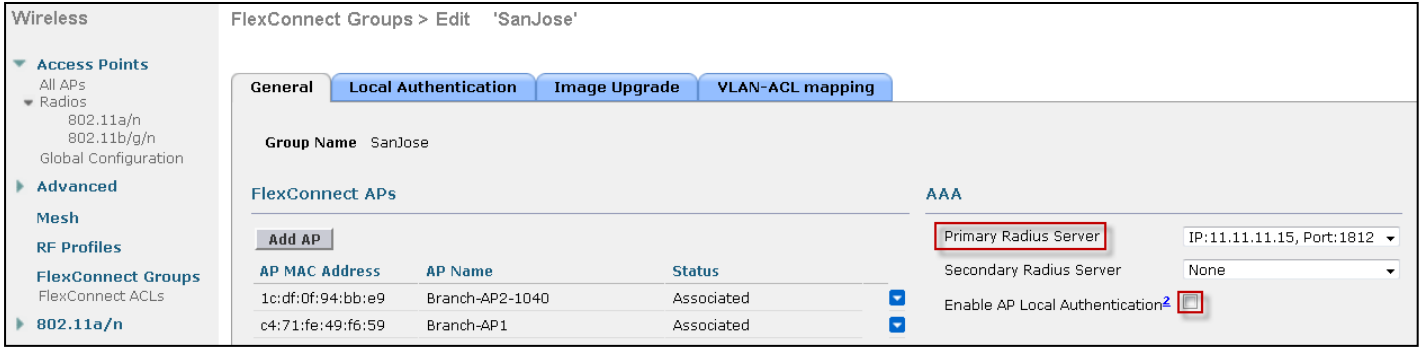
Backup Scenario

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



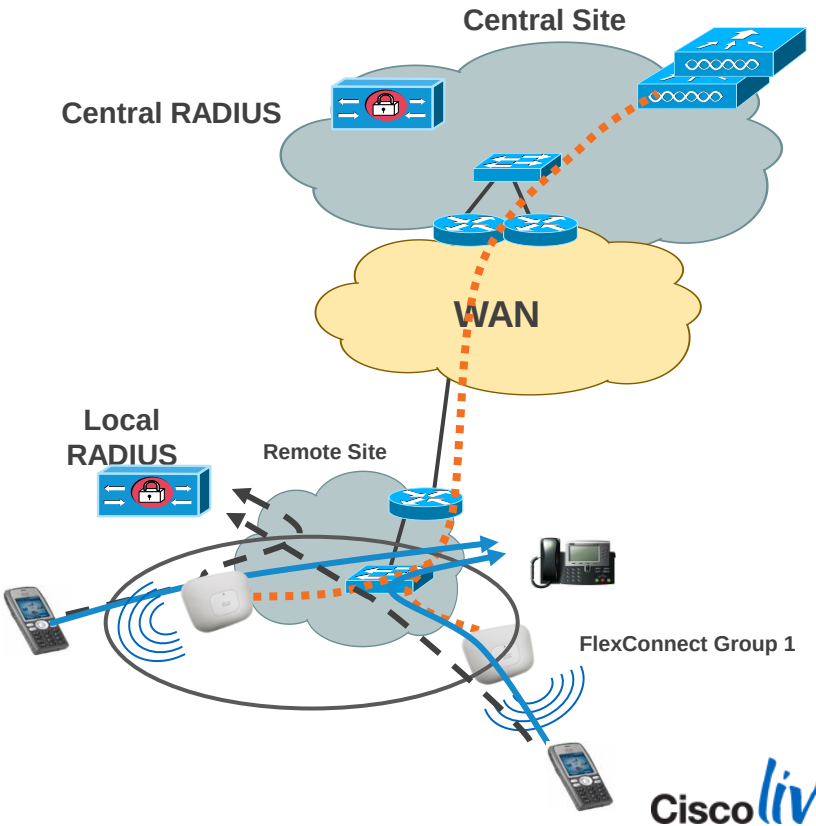
FlexConnect Group: Local Backup RADIUS
Configuration

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



Local Authentication

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



New in 7.0.116

Local Authentication
Configuration

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

WLANs > Edit 'RackMobility'

< Back | Apply

General | Security | QoS | Advanced

Maximum Allowed Clients [8]: 0

Static IP Tunneling [11]: Enabled

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Off Channel Scanning Defer

Scan Defer Priority: 0 1 2 3 4 5 6 7

Scan Defer Time(msecs): 100

FlexConnect

FlexConnect Local Switching [2]: Enabled

FlexConnect Local Auth [12]: Enabled

Learn Client IP Address [5]: Enabled

802.11b/g/n (1 - 255): 1

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing

Client Band Select [7]

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

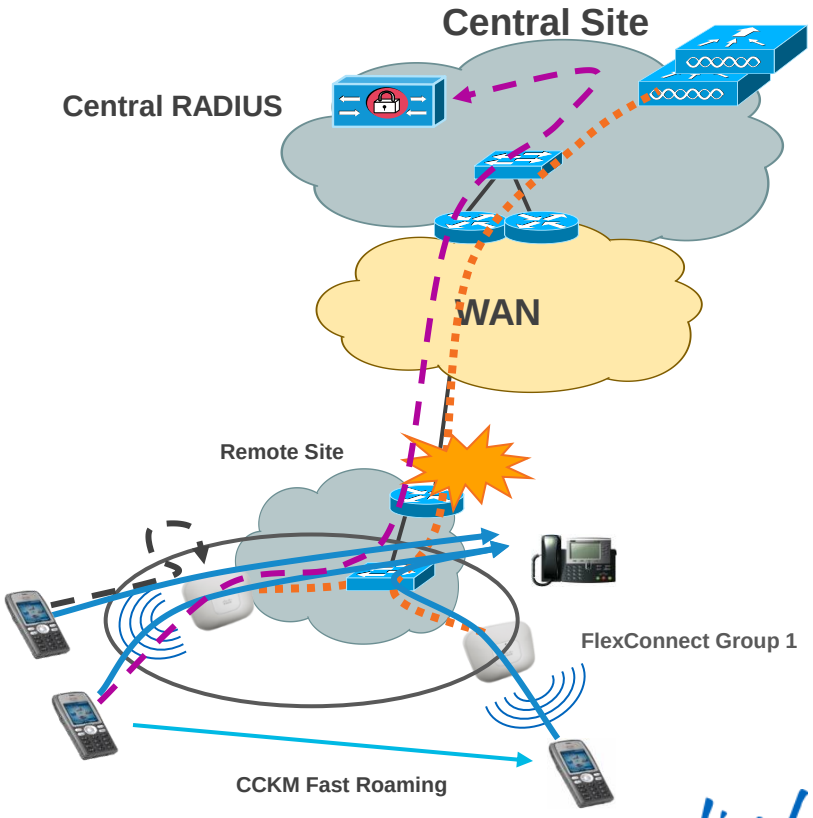
Backup Scenario

- 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

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

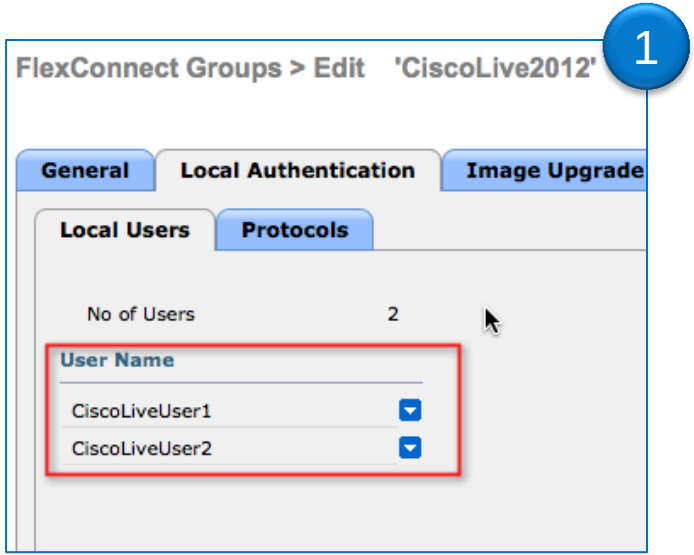
New

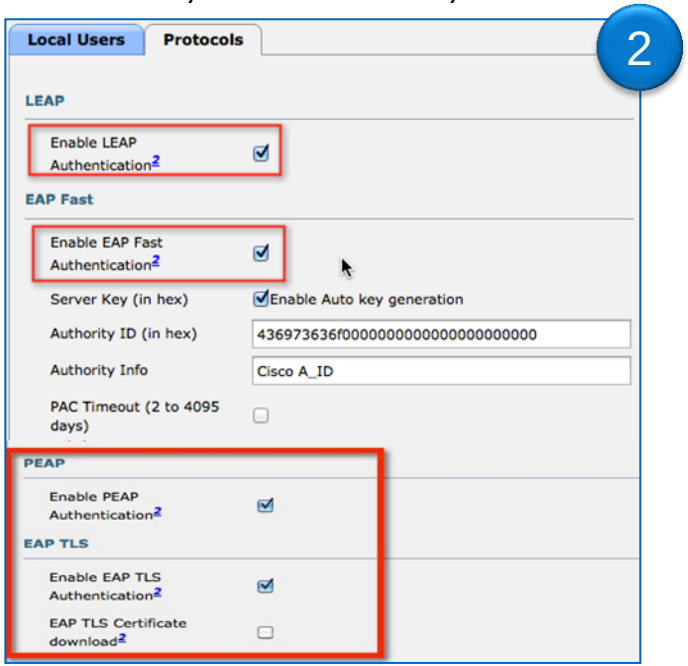
New



FlexConnect Group: Local Backup Authentication
Configuration

- Define users (max 100) and passwords
- Select supported Security protocols i.e. LEAP, EAP-FAST, PEAP or EAP-TLS








Designing Secure & BYOD Enabled Branch Network



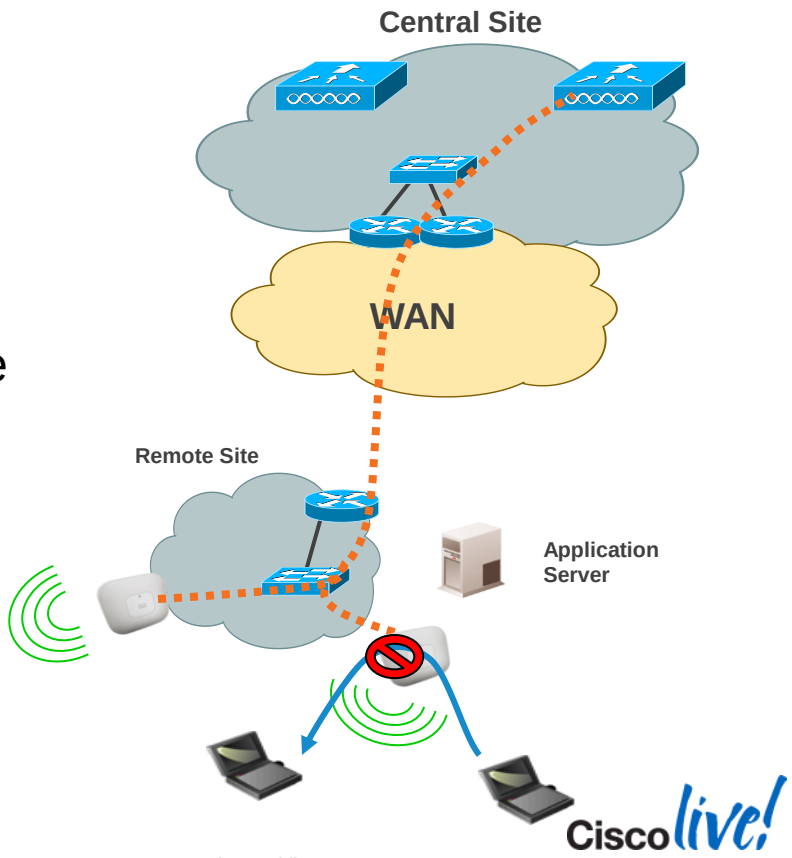

FlexConnect Peer-to-peer Blocking

Local Switching Peer-to-peer Blocking

Description

Starting from 7.2

- 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



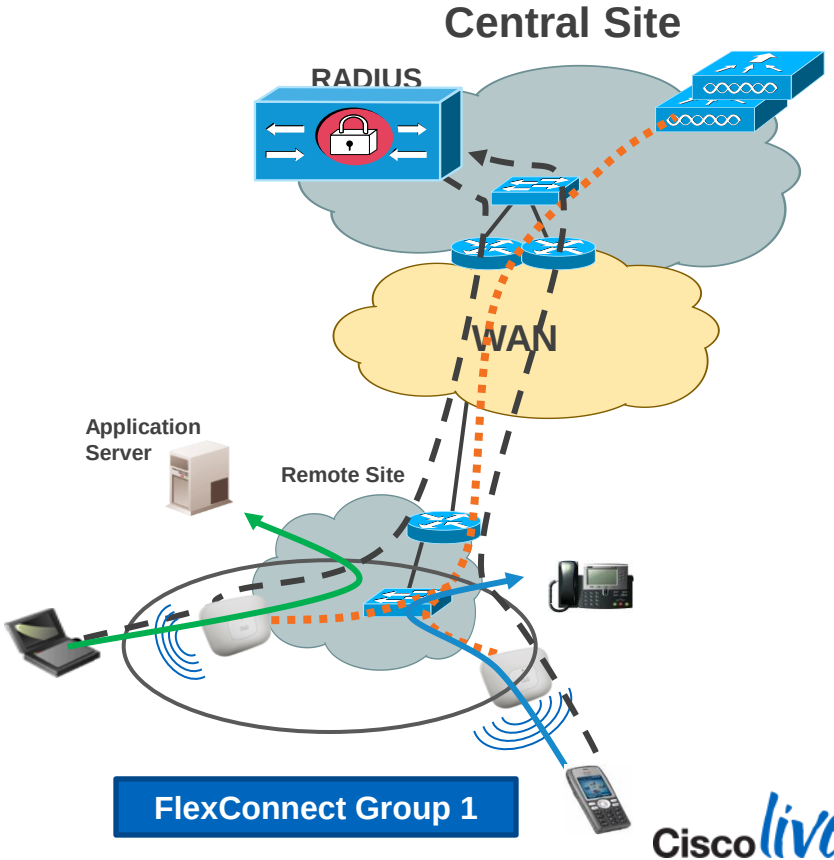



FlexConnect AAA VLAN & QoS Override

FlexConnect AAA VLAN Override
Description

Starting from 7.2

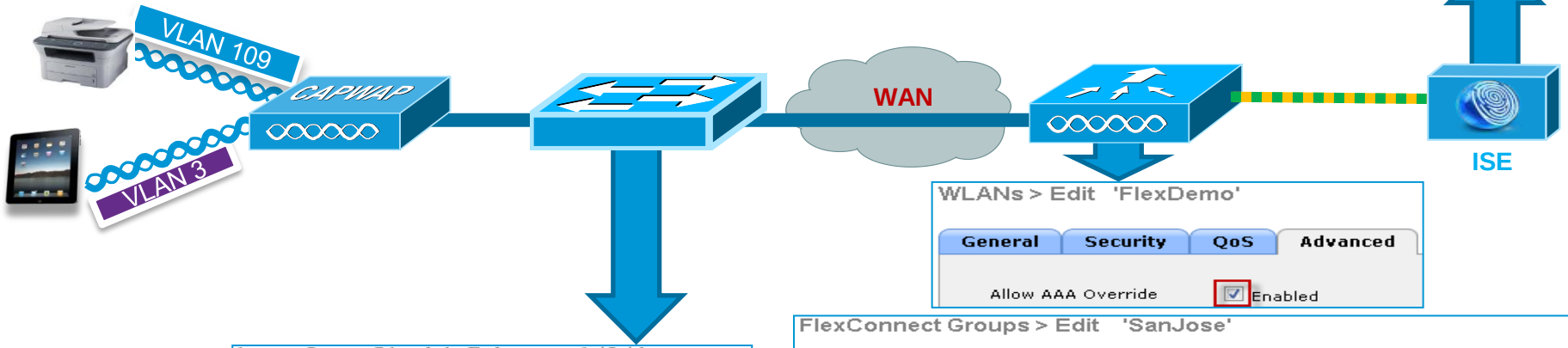
- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- If VLAN ID does not exist, default VLAN is used, unless « VLAN Based Central Switching » enabled
- **Starting from 7.5** AAA override for QoS is also supported.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



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

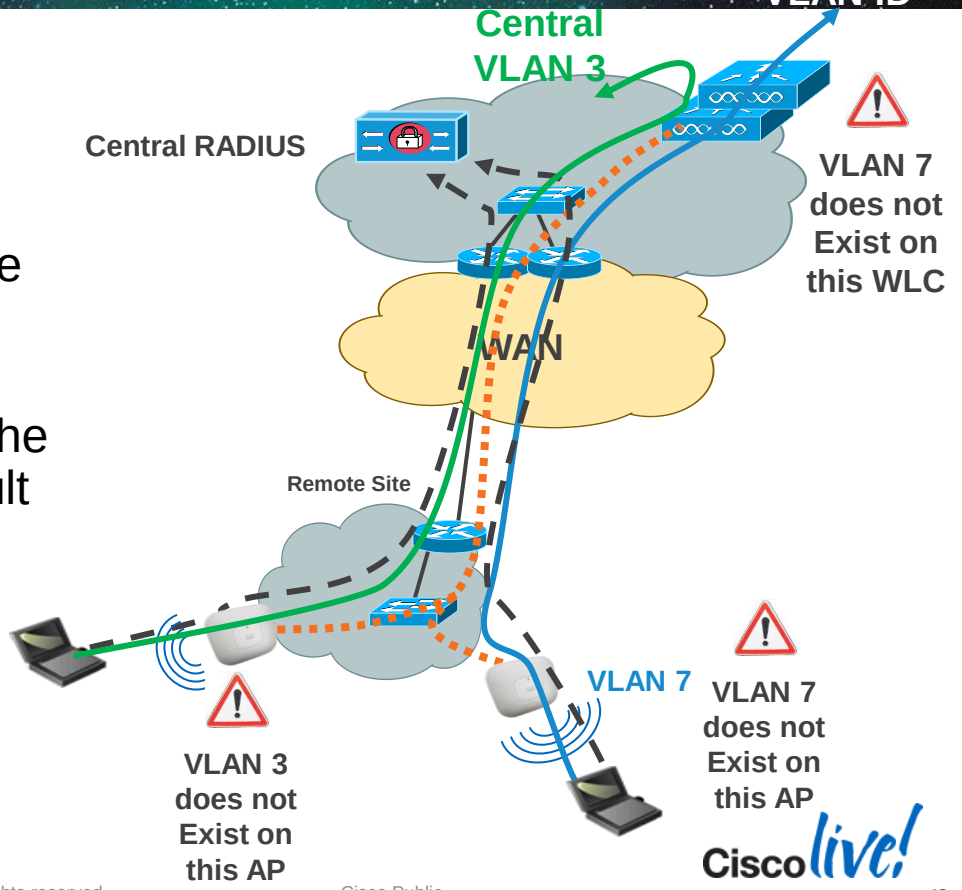
Egress ACL none

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 AAA QoS Override

Description

Starting from 7.5

- Dynamically assign QoS levels and/or bandwidth contracts for local switching, centrally authenticated WLANs
- Web-authenticated WLANs and 802.1X-authenticated WLANs supported
- Order of precedence for Rate Limiting parameters
  - AAA override
  - QoS Profile of AAA override
  - Local WLAN configuration
  - QoS Profile of local WLAN configuration

Vendor ID/Vendor Type	Attribute
[14179\002]	Aire-QoS-Level
[14179\004]	Aire-802.1P-Tag
[14179\007]	Aire-Data-Bandwidth-Average-Contract
[14179\008]	Aire-Real-Time-Bandwidth-Average-Contract
[14179\009]	Aire-Data-Bandwidth-Burst-Contract
[14179\0010]	Aire-Real-Time-Bandwidth-Burst-Contract

Supported on 802.11n non-mesh access points 1040,1140,1250,1260,1600,2600,3500,3600,3700

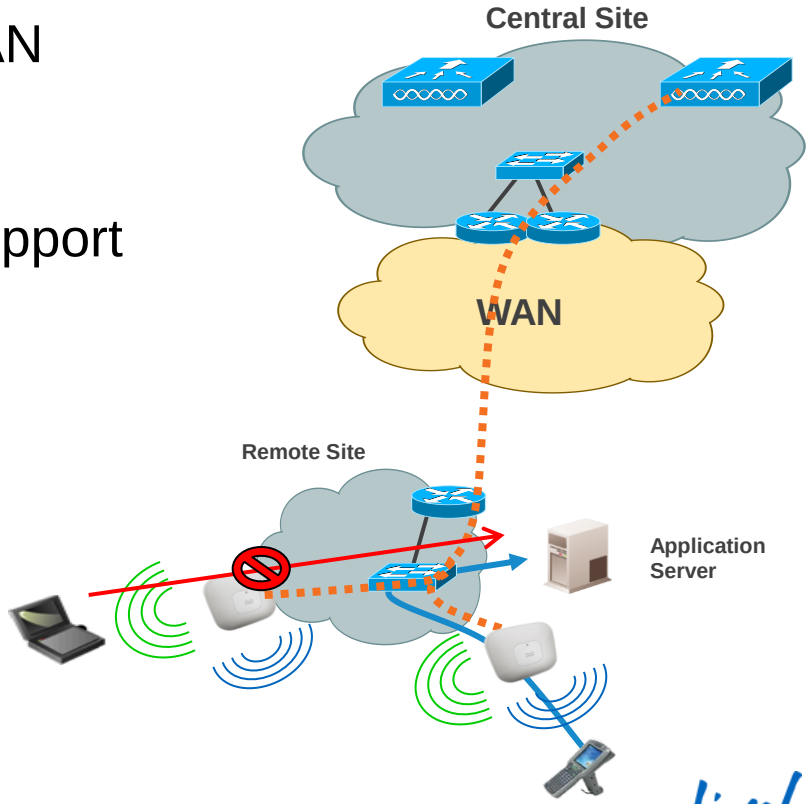



FlexConnect ACL VLAN Mapping & Per-Client ACL

FlexConnect ACL – VLAN Mapping
Overview

Starting from 7.2

- FlexConnects ACL are applied per VLAN
- FlexConnect ACL are Ingress / Egress oriented
- **Starting from 7.5** FlexConnect ACL support AAA-returned Client ACL New



Scale

512 FlexConnect ACL per WLC

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

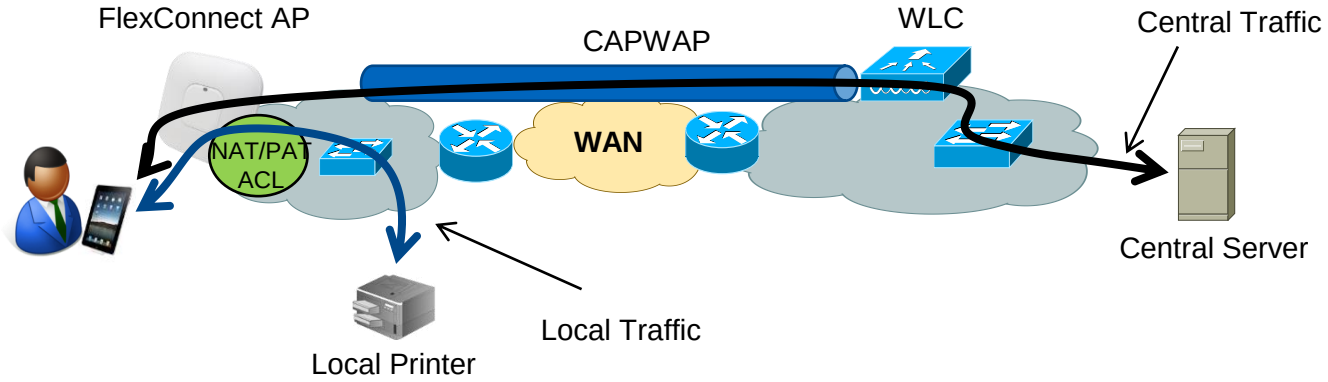



FlexConnect Split Tunnelling (Using FlexConnect Split ACL)

FlexConnect ACL – Split Tunnelling
Overview

Starting from 7.3

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



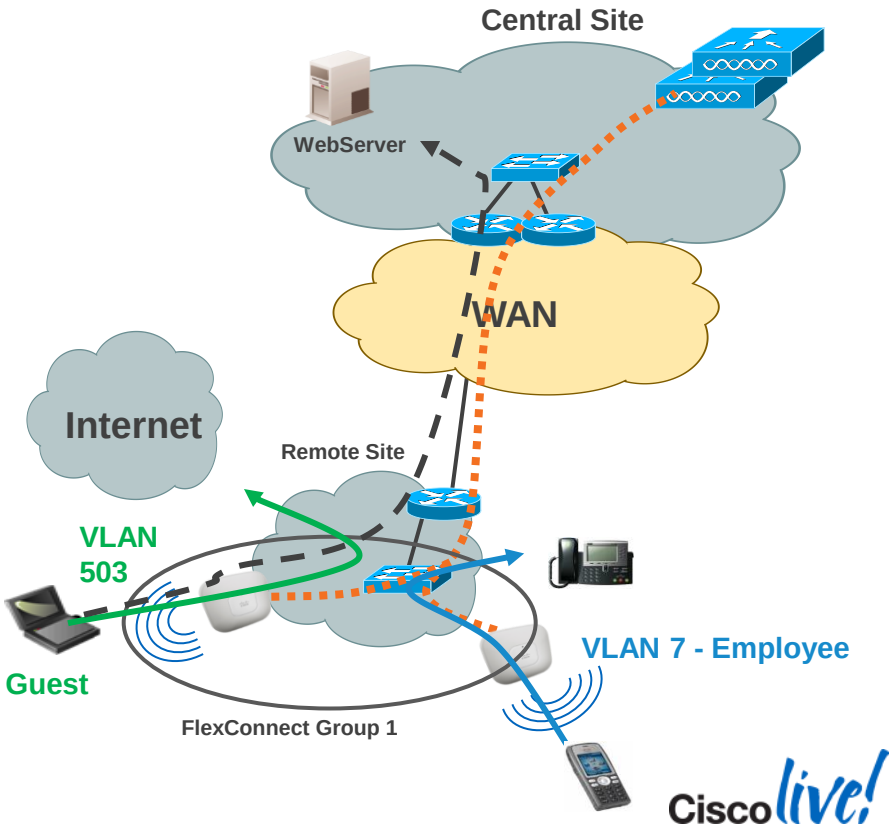



Deploying External WebAuth with FlexConnect Local Switching
(Using FlexConnect WebAuth ACL)

External WebAuth with Local Switching
Description

Starting from 7.2.110

- 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 for this functionality 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_Overide_ACL
Pre-WebAuthPolicy-ACL
WebAuth_ACL

Access Control Lists > Edit

General

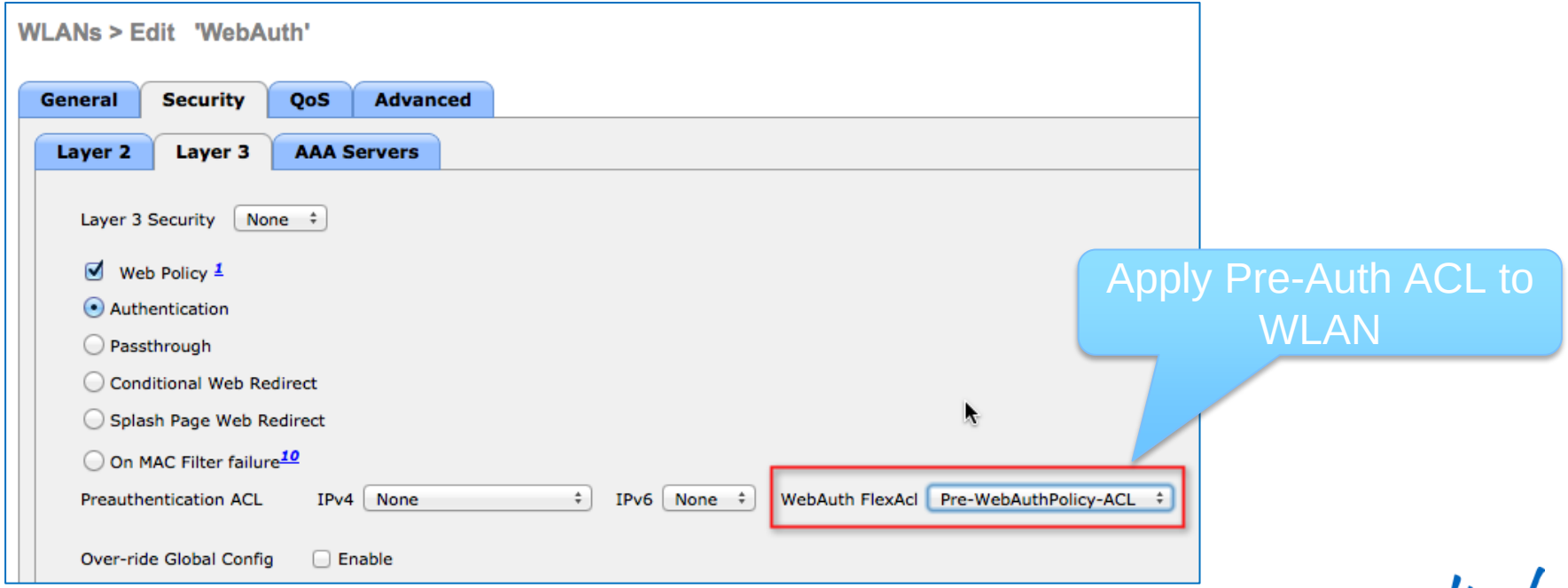
Access List Name: Pre-WebAuthPolicy-ACL

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0	/	192.168.1.11	/	Any	Any	Any	Any
		0.0.0.0		255.255.255.255					

External Web-Server IP

External WebAuth with Local Switching
Configuration

Step 2: Apply Pre-Auth ACL to WLAN



External WebAuth with Local Switching
Configuration – Per AP

Step 3: Apply Pre-Auth ACL to FlexConnect AP

All APs > Details for AP-3600-A

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

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

Map WLAN-Id to Pre-Auth ACL

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

External WebAuth with Local Switching
Configuration – Per FlexConnect Group

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 4

WebAuth ACL Pre-WebAuthPolicy-ACL

Add

Local Split ACL Mapping

WLAN Id 0

Local Split ACL FlexC… Acl-1

Add

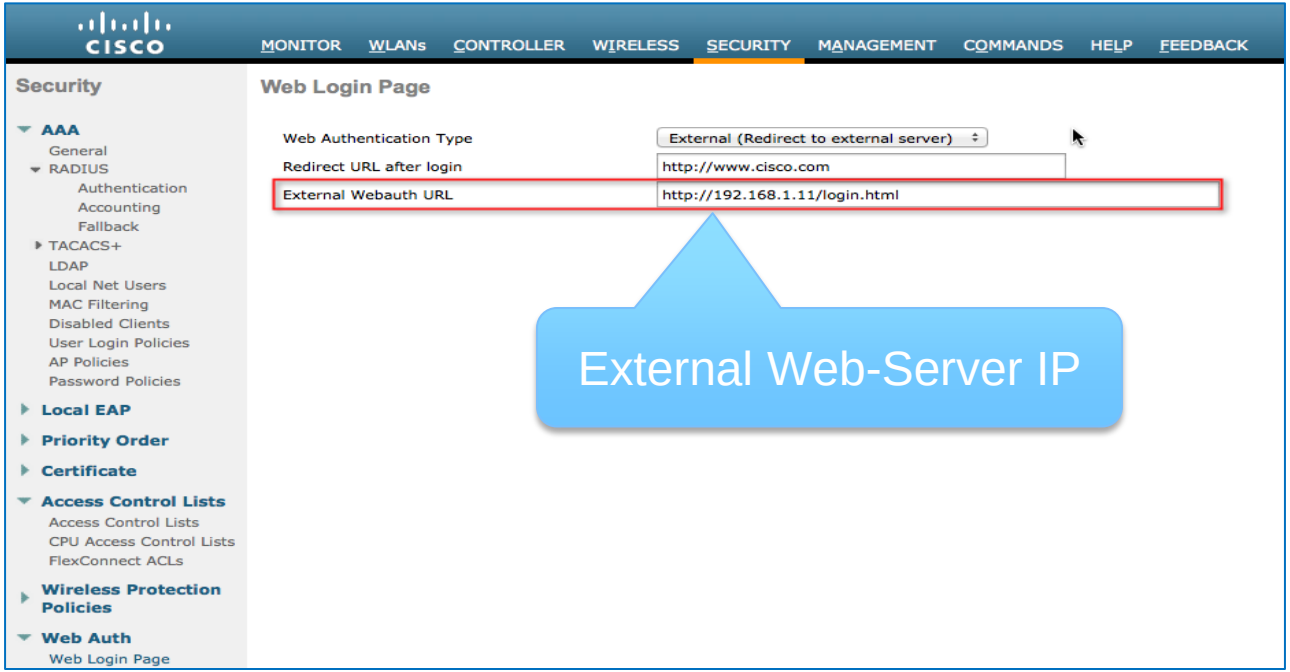
WLAN Id	WLAN Profile Name	WebAuth ACL
4	WebAuth	Pre-WebAuthPolicy-ACL

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



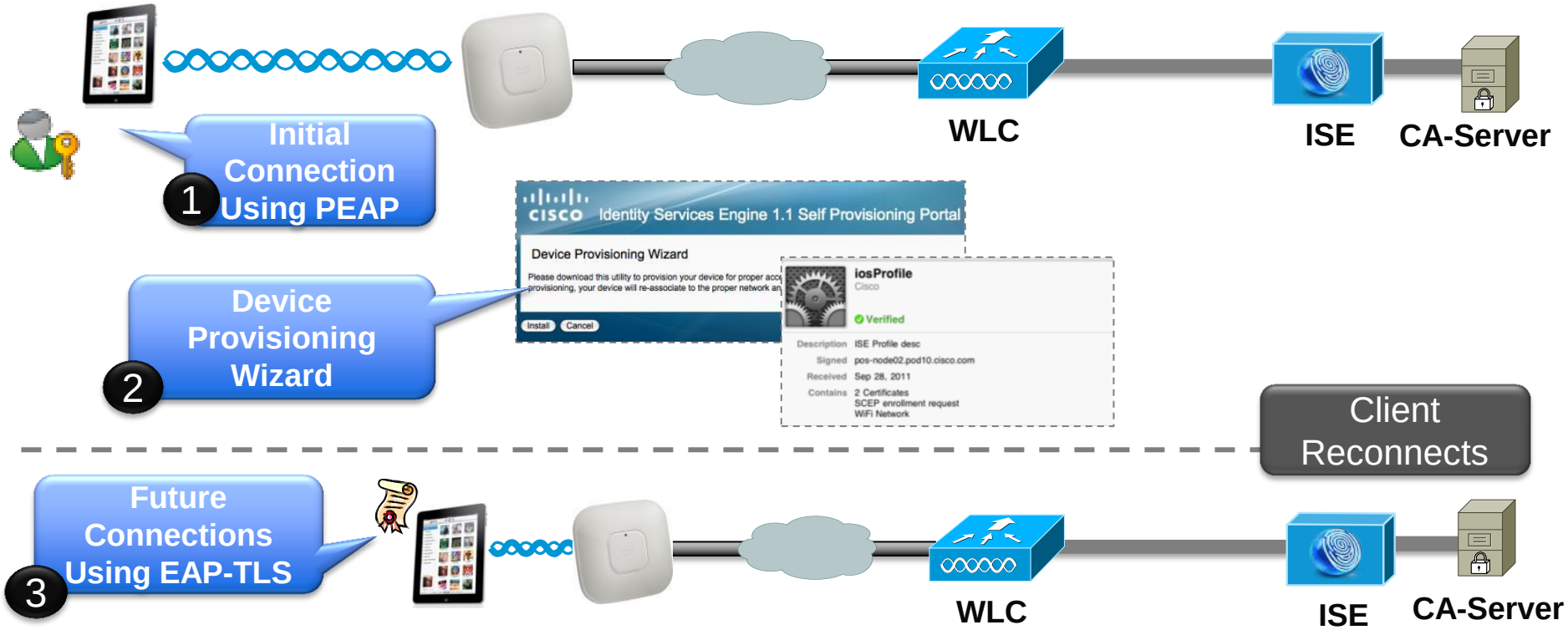



Deploying BYOD with FlexConnect Local Switching (Using FlexConnect WebPolicies ACL)

BYOD Device On-Boarding in FlexConnect

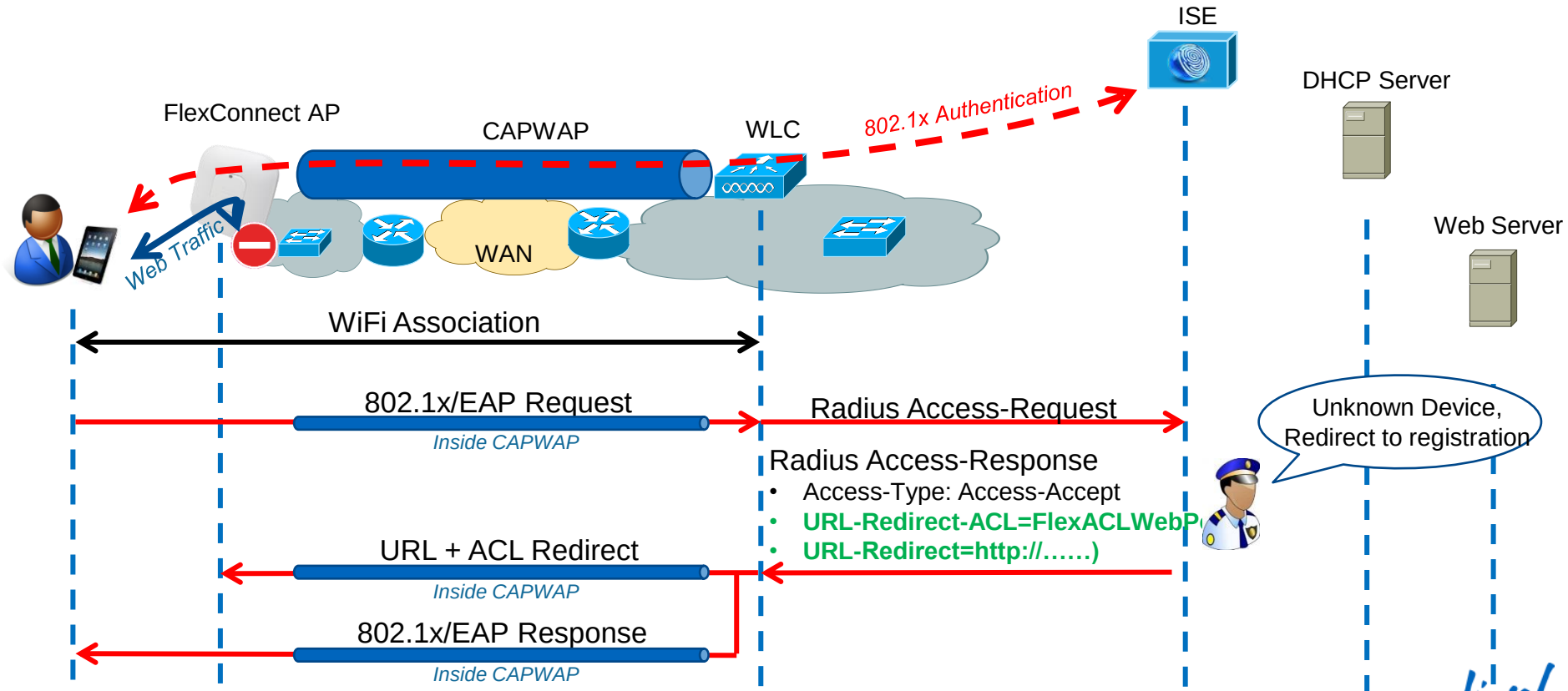
Example: Apple iOS Device Provisioning

Starting from 7.4



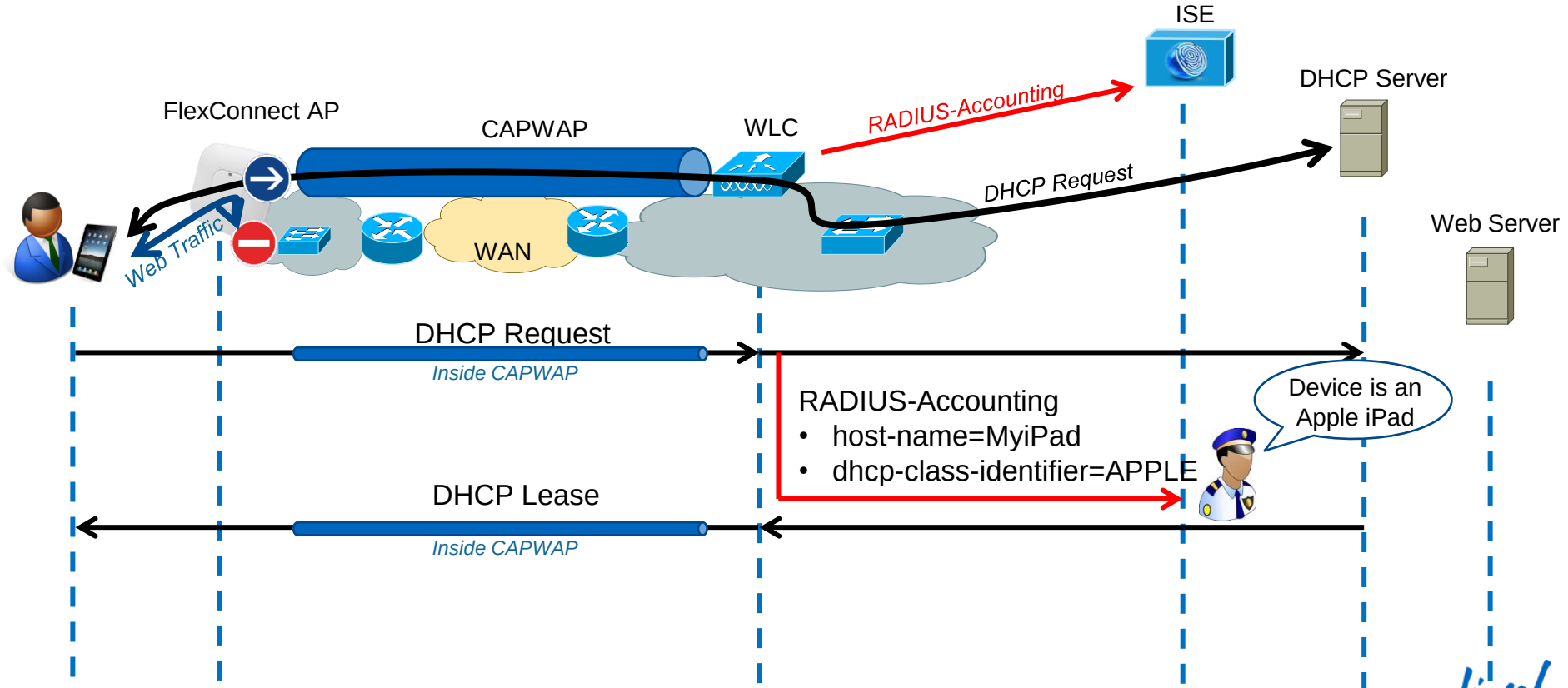
Deploying BYOD with FlexConnect Wireless

Summary – 802.1x/EAP Authentication



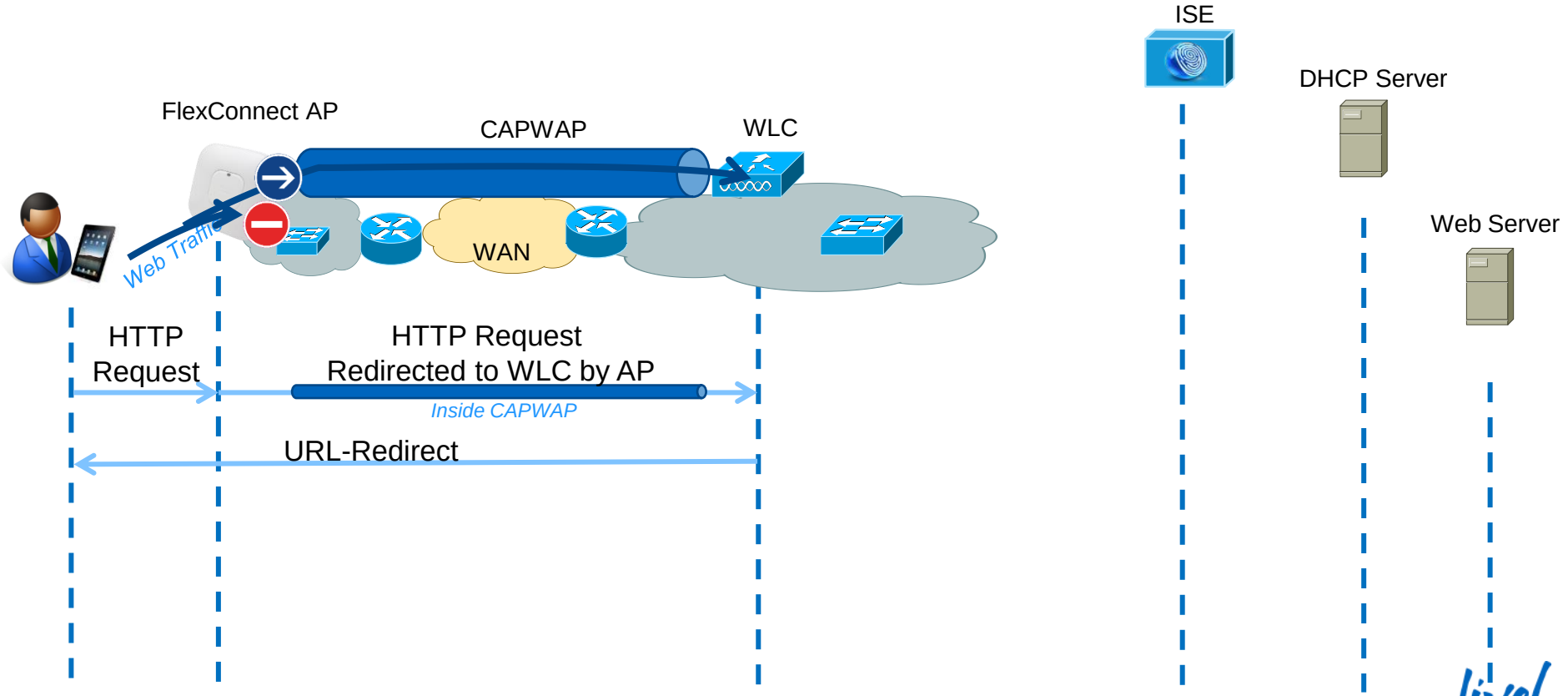
Deploying BYOD with FlexConnect Wireless

Summary – DHCP Request



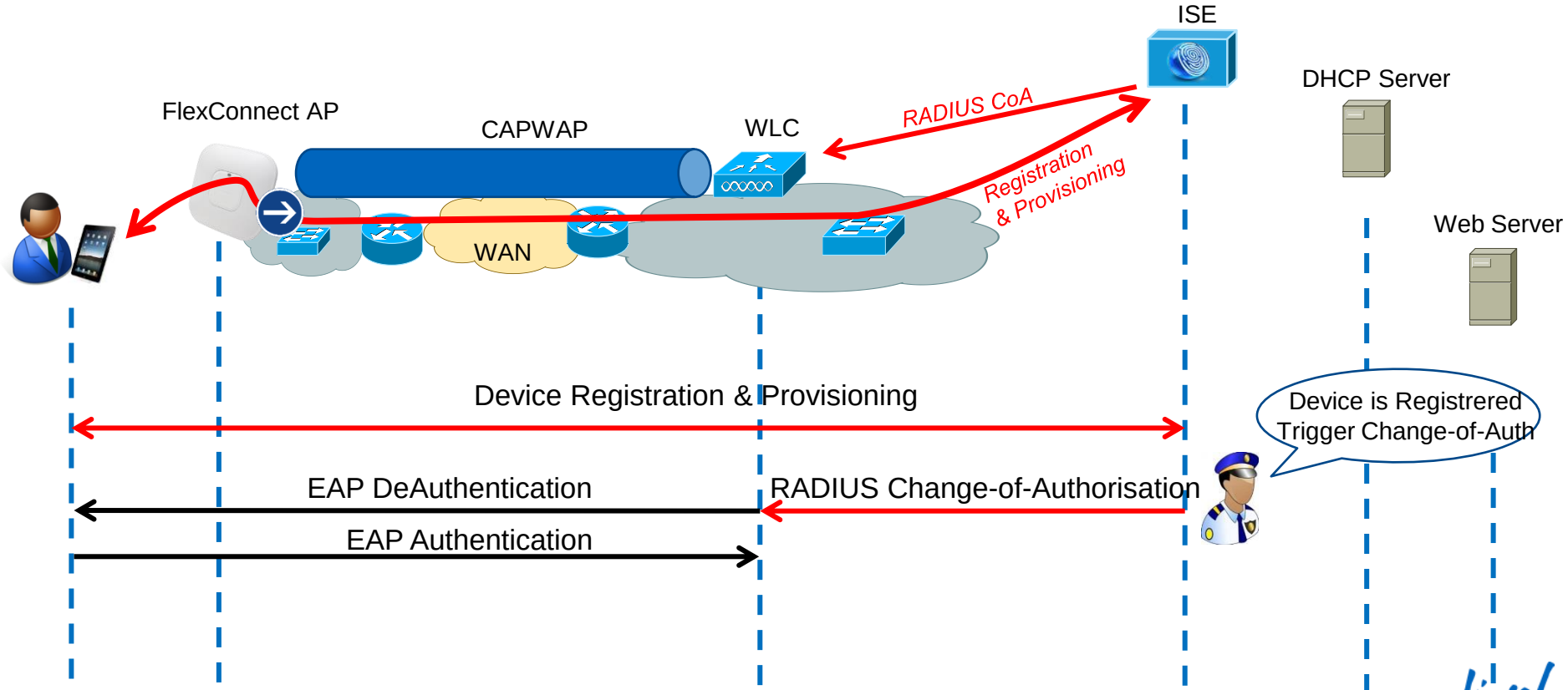
Deploying BYOD with FlexConnect Wireless

Summary – URL-Redirect



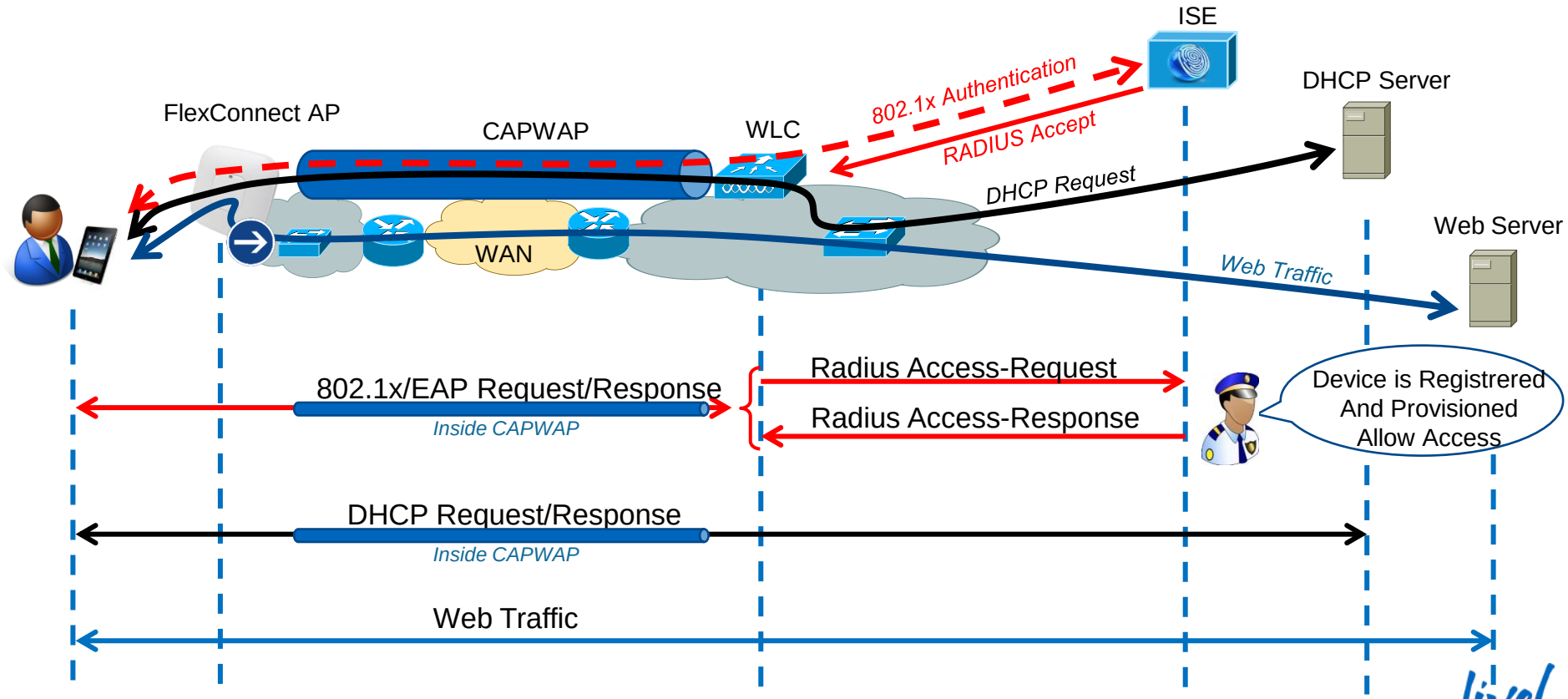
Deploying BYOD with FlexConnect Wireless

Summary – Registration & Provisioning



Deploying BYOD with FlexConnect Wireless

Summary – Device Access






Operating Wireless Branch Smart Upgrade over WAN

Upgrading a FlexConnect Deployment
Concerns

Starting from 7.2

- 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 ~6000 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

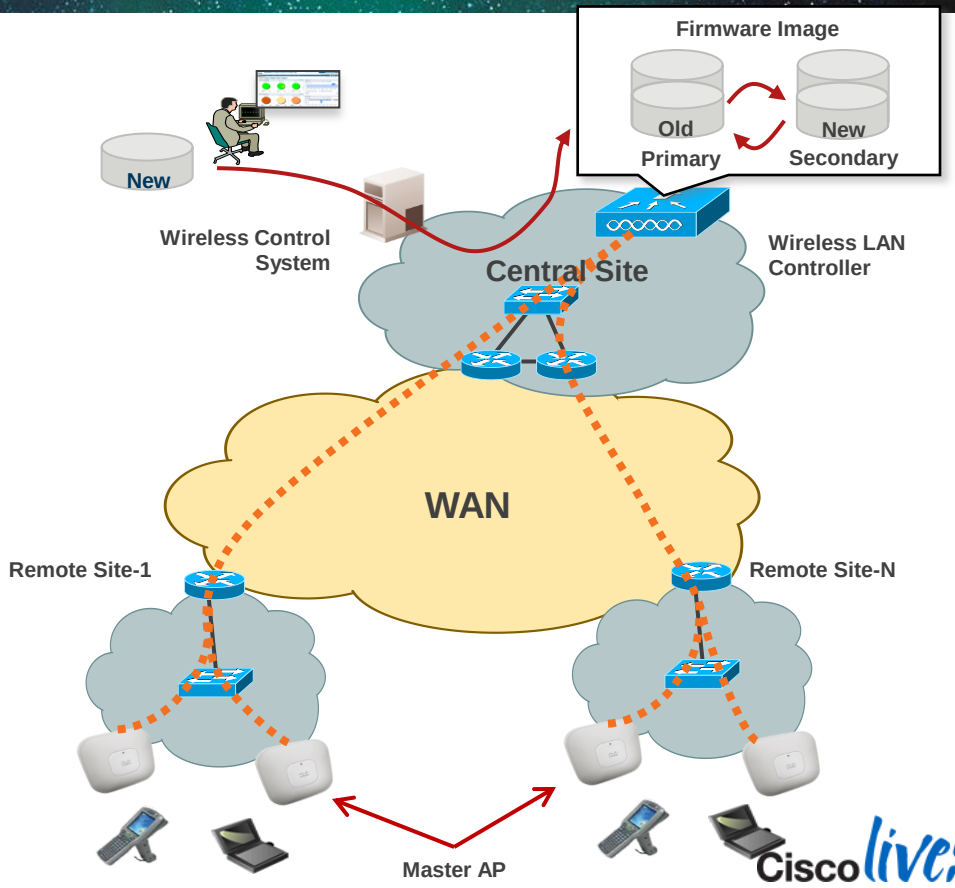
FlexConnect Smart AP Image Upgrade
Overview

Starting from 7.2

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

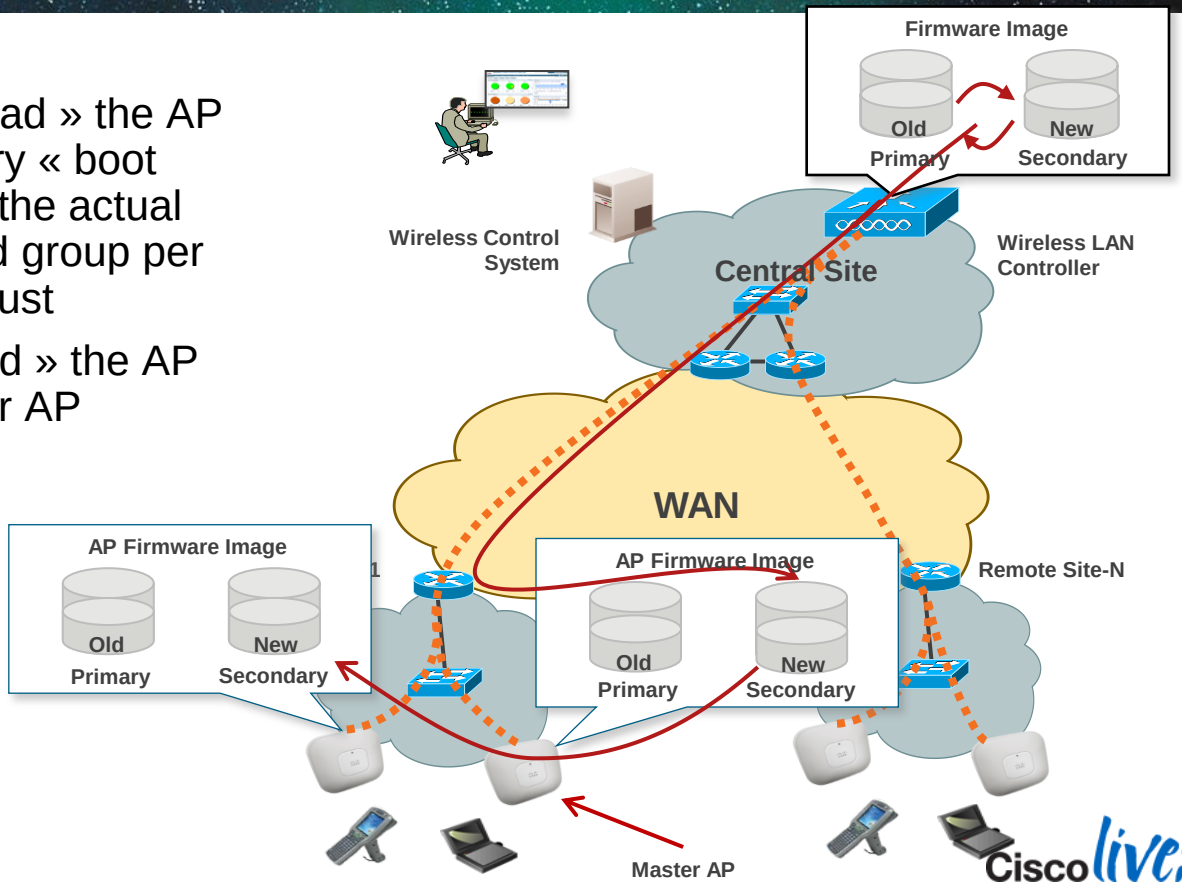
Other FlexConnect AP download the code from the master locally

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






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
- Wireless LAN Controller Scale Comparison Guide: http://www.cisco.com/en/US/products/hw/wireless/products_category_buyers_guide.html#controllers
- 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




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CISCO™