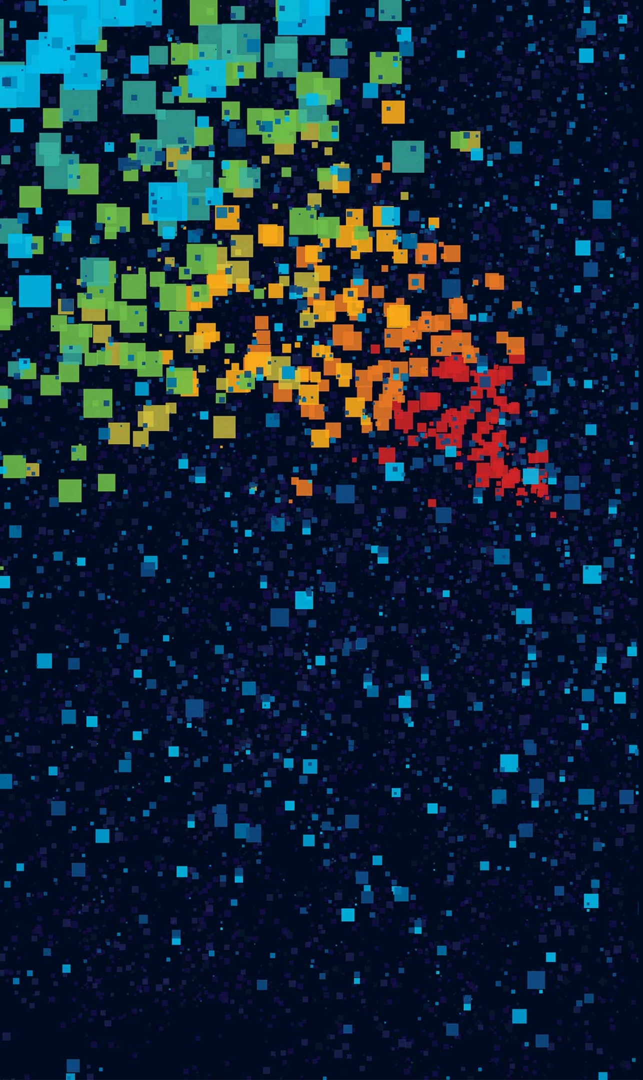
# Сетевой марафон Cisco: Catalyst 9800 - новая классика WLAN

## Сессия 2 – Миграция Flexconnect сети на беспроводной контроллер Catalyst 9800

Виктор Платов, CCIE #24288, CWNE #283



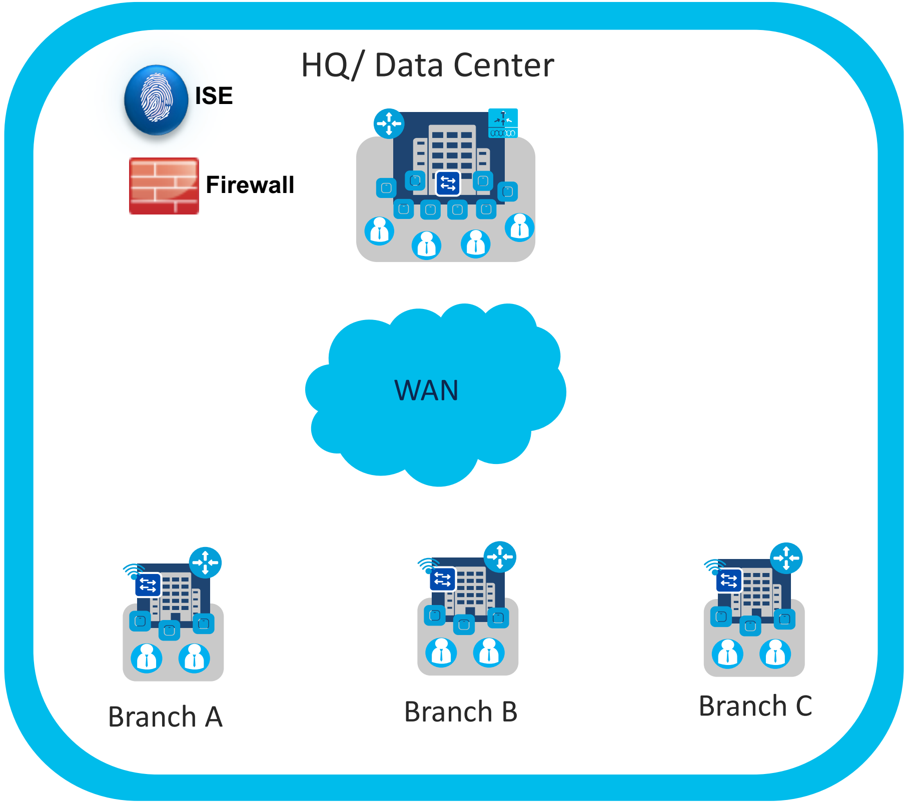
# Содержание

- Варианты разворачивания сети филиала
- Настройка FlexConnect local switching
- Что такое Site Tags и Flex Profiles
- Дизайн надежного беспроводного филиала
- Сегментация и безопасность
- Влияние WAN каналов на работу БЛВС
- Рекомендации

# Варианты разворачивания сети филиала

# Branch Design Considerations

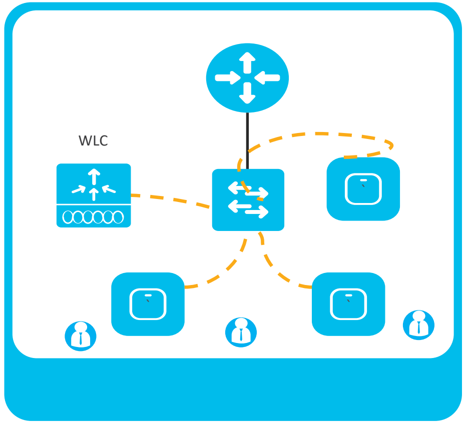
- Central IT / Local IT
- Single-site / Multi-site
- Number of Branches
- Employees/Devices per branch
- Local/central Internet breakout?
- WAN Bandwidth / resiliency
- Local AAA and backup AAA



# Branch Wireless Design Options

## Dedicated Local Controller

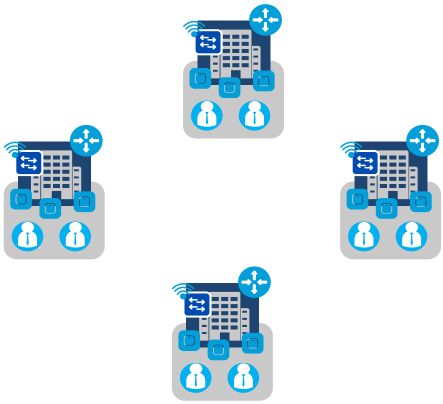
### Local Controller



Local WLAN Controller

## Embedded Local Controller

### Embedded Controller Options

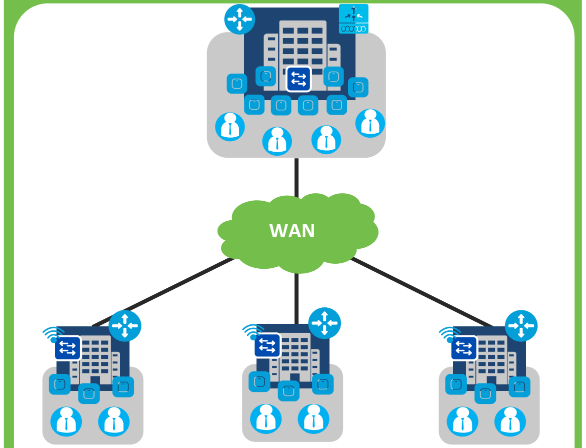


Single or Multi-Site

Single/Multi-site networks
Low IT footprints
Controller running on AP or Switch

## Remote Controller

### Flex Connect



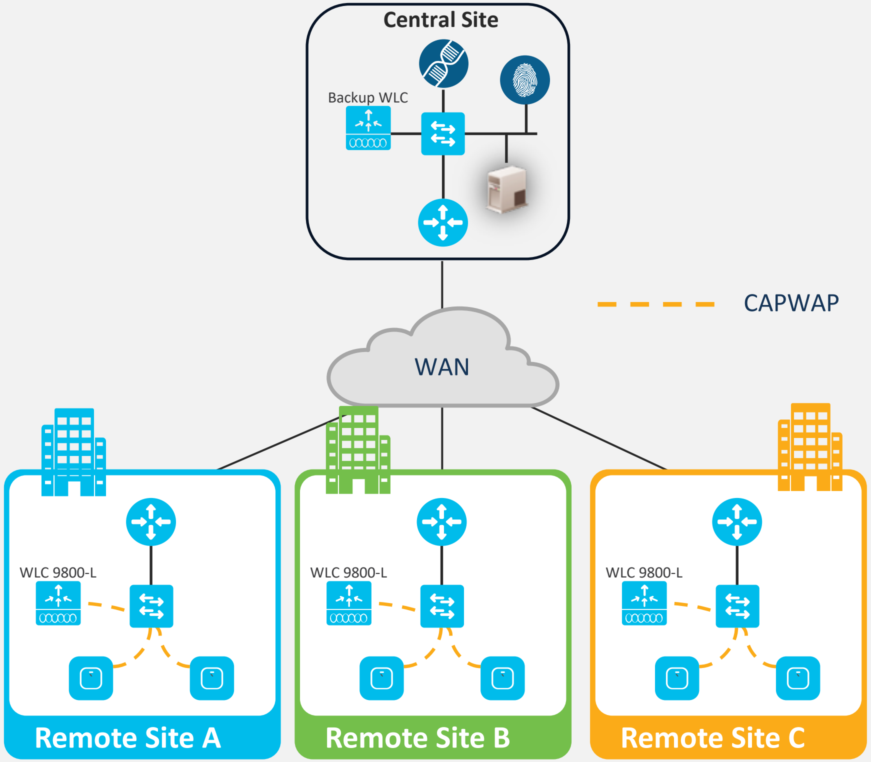
FlexConnect

Controller running in Data Center
Distributed Network
Highly Scalable

Cisco DNA Center

Policy
Automation
Assurance
Security
ISE
CMX

# Branch Office with dedicated WLAN Controller

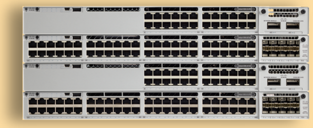


- Small or mid branch WLC 9800-L , 9800-CL  (NFVIS or Virtual)

- Layer-3 roaming with controller in each branch
- No limit of 100 APs per seamless roaming domain
- Full local control, no dependency on WAN

- WLC at each site, higher capital cost
- Higher OpEX costs (cabling, racking, managing it)

# Branch Office with Embedded WLAN Controllers



SDA: 9800 on Catalyst Switches

Scale to 200 APs and 4,000 Clients

SDA Fabric

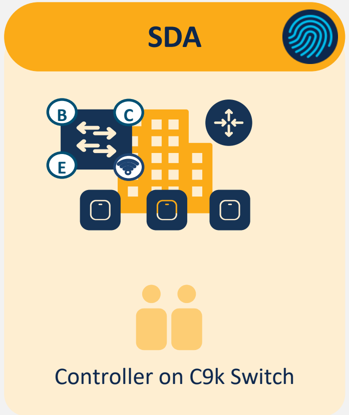
Supported on Catalyst 9300, 9400 and 9500 Series switches

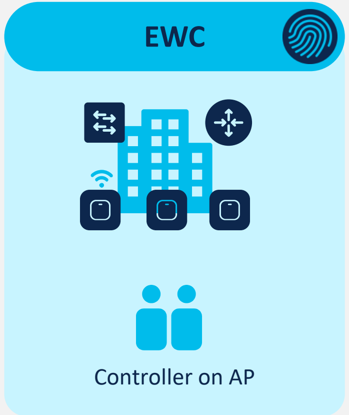
EWC: 9800 on Catalyst APs

Scale to 100 APs and 2,000 Clients

FlexConnect Local Switching

Support on Catalyst 9100 Series access points



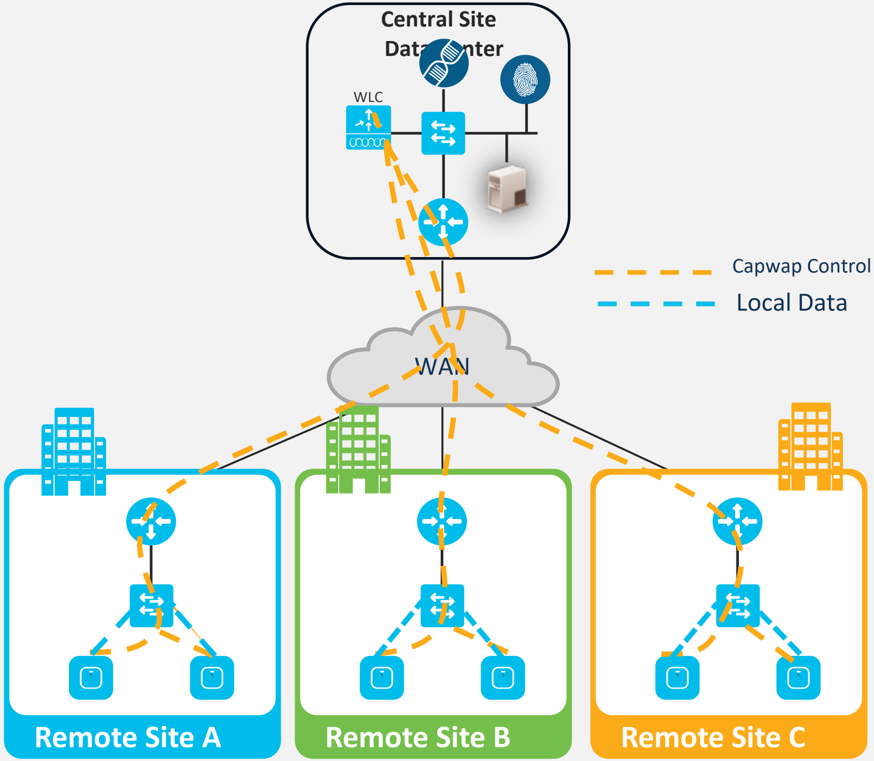


- Branches can have local embedded controllers
- No separate appliance

- Full local control, no dependency on WAN

- 9800 on Cat9k switch is for SDA Fabric
- 9800/EWC on AP has a limit of 100 APs max

# Branch Office with Flex Connect (Remote Controller)



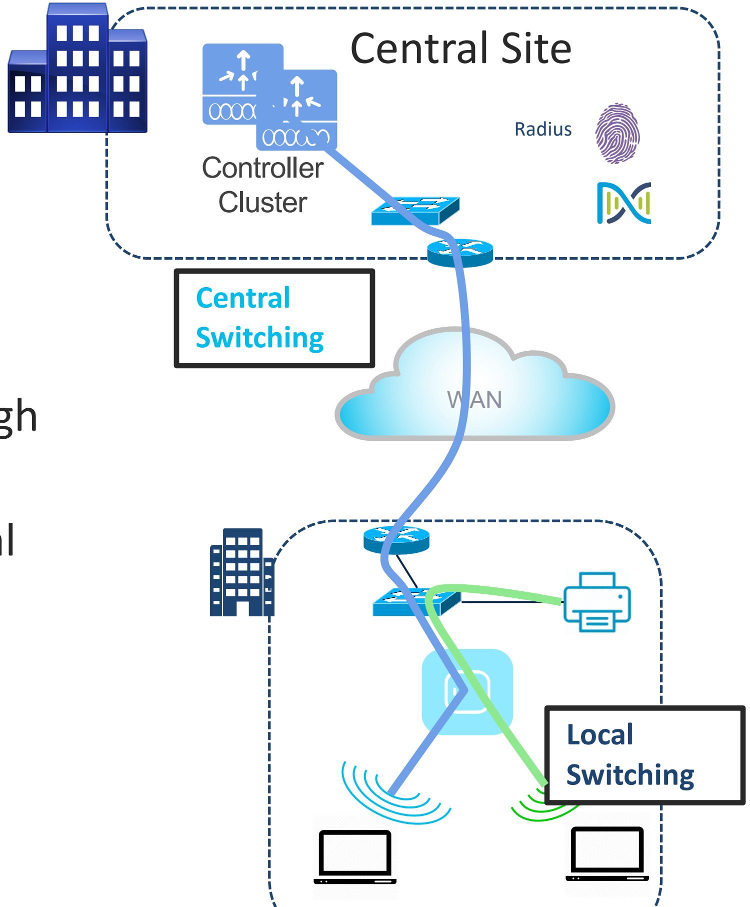
- Wireless Controller is at a central site managing AP's across sites/branches
- Clients in branch roam independently

- Each site can have up to 100 AP's in a Site Tag with a Flex Profile for seamless roaming
- L2 roaming only
- Supports standalone mode operations

- Highly Scalable
- Central management
- Ideal for cookiecutter branch configuration
- Supports optional central switching

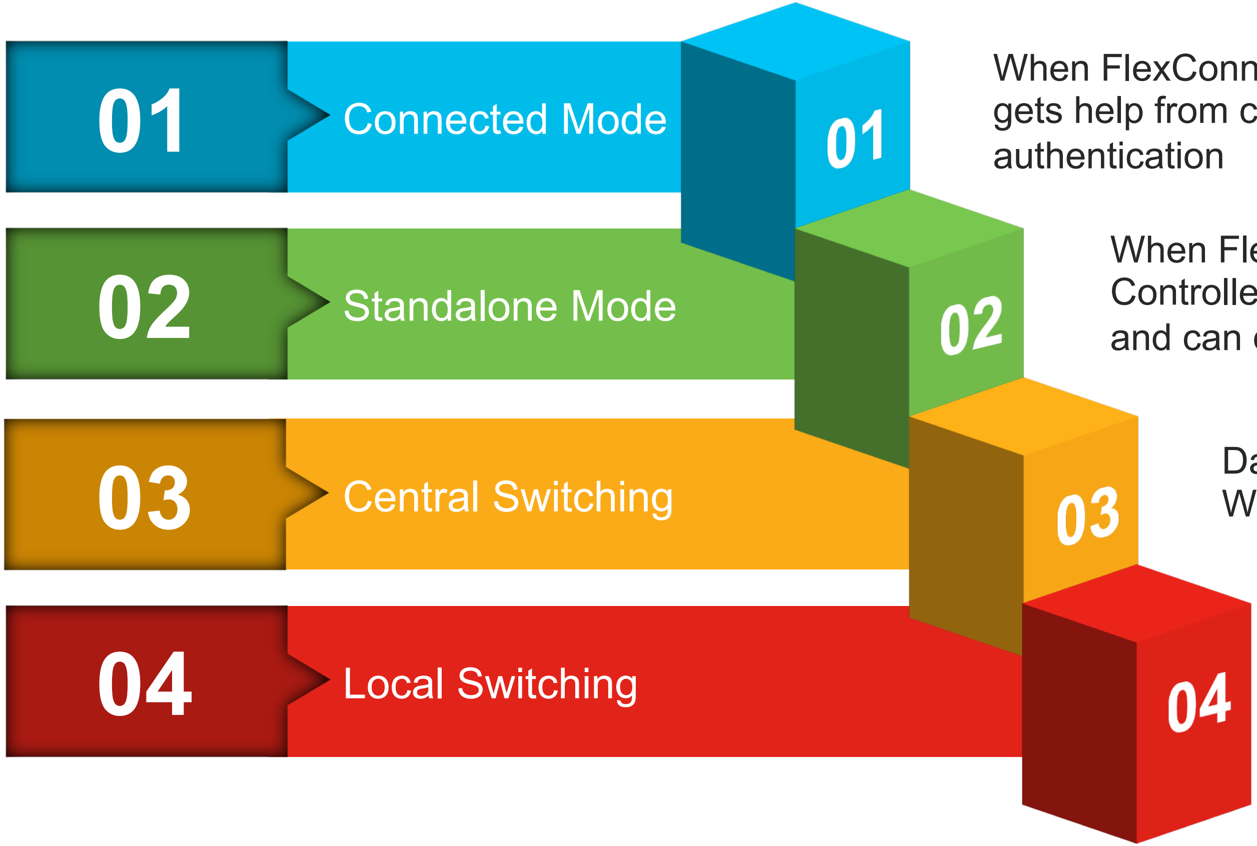
# Introducing FlexConnect

- Ease of Management via Controller
- Two traffic switching modes:
  - **Central Switching** (SSID data traffic tunneled through the WLC)
  - **Local Switching** (SSID data traffic switched to a local VLAN behind the AP’s switchport)
- Two states of operation from the AP’s perspective:
  - **Connected** (when WLC is reachable)
  - **Standalone** (when WLC is not reachable)



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

# FlexConnect Glossary



01 Connected Mode 01

When FlexConnect AP **can reach** Controller, it gets help from controller to complete client authentication

02 Standalone Mode 02

When FlexConnect AP **cannot reach** Controller, it goes into standalone mode and can do client authentication by itself

03 Central Switching 03

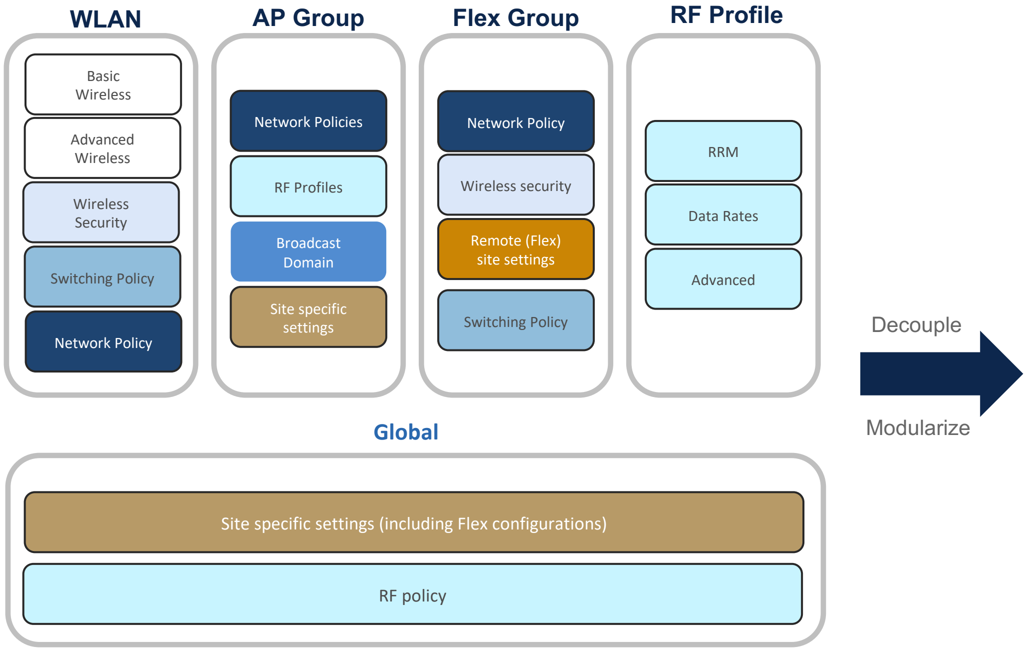
Data traffic **is tunneled back** to WLC for an SSID

04 Local Switching 04

Data traffic **is switched onto local VLANs** for an SSID

# Настройка FlexConnect local switching

# Catalyst 9800 vs. AireOS Configuration Model
# Modularized model



WLAN: Basic Wireless, Advanced Wireless, Wireless Security, Switching Policy, Network Policy

AP Group: Network Policies, RF Profiles, Broadcast Domain, Site specific settings

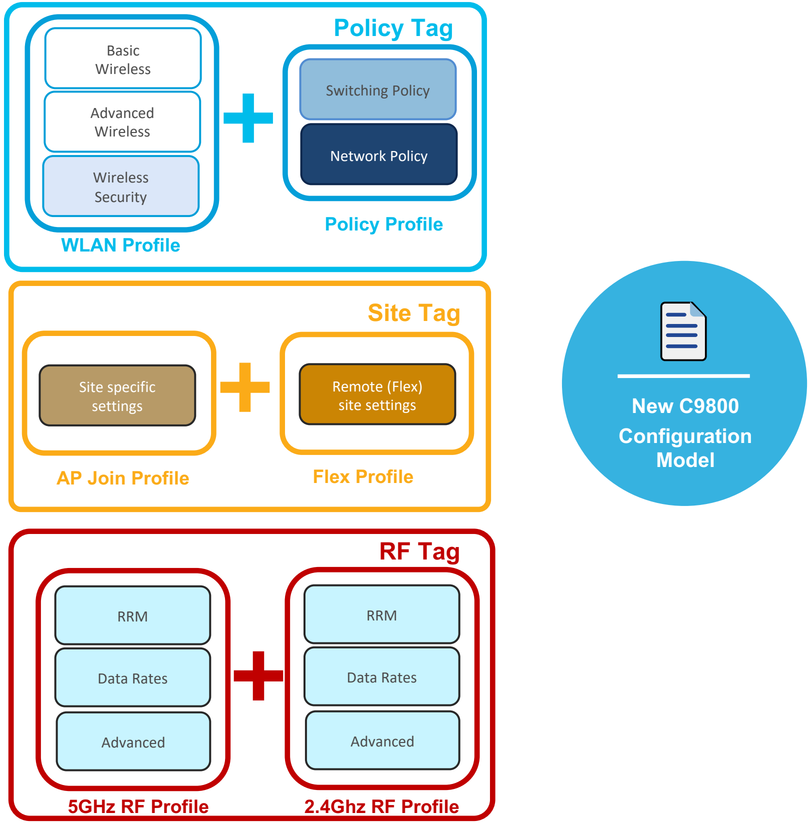
Flex Group: Network Policy, Wireless security, Remote (Flex) site settings, Switching Policy

RF Profile: RRM, Data Rates, Advanced

Global: Site specific settings (including Flex configurations), RF policy

Decouple

Modularize



Policy Tag: WLAN Profile (Basic Wireless, Advanced Wireless, Wireless Security) + Policy Profile (Switching Policy, Network Policy)

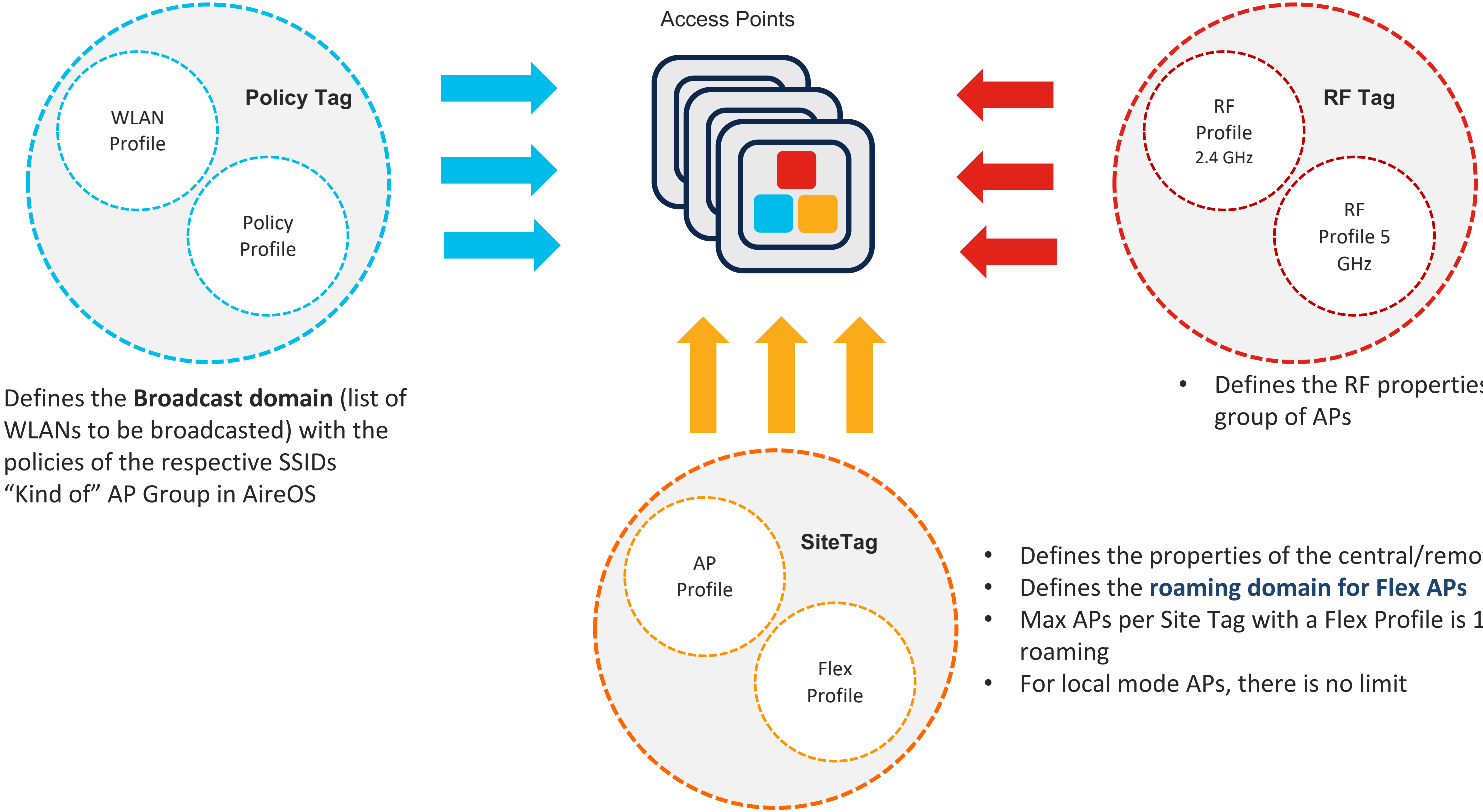
Site Tag: AP Join Profile (Site specific settings) + Flex Profile (Remote (Flex) site settings)

RF Tag: 5GHz RF Profile (RRM, Data Rates, Advanced) + 2.4Ghz RF Profile (RRM, Data Rates, Advanced)

New C9800 Configuration Model

AireOS configuration Model: same type of information is spread across multiple configuration constructs

# Cisco Catalyst 9800 Config Model



- Defines the **Broadcast domain** (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Kind of” AP Group in AireOS

- Defines the RF properties of the group of APs

- Defines the properties of the central/remote sites
- Defines the **roaming domain for Flex APs**
- Max APs per Site Tag with a Flex Profile is 100 for seamless roaming
- For local mode APs, there is no limit

# Steps to configure FlexConnect Local Switching

STEP **01**

**Access Point Mode**

- Configure the AP Join Profile, Flex Profile, the Site Tag and assign the Site Tag to the AP(s)

STEP **02**

**Configure the WLAN and the Policy Profile**

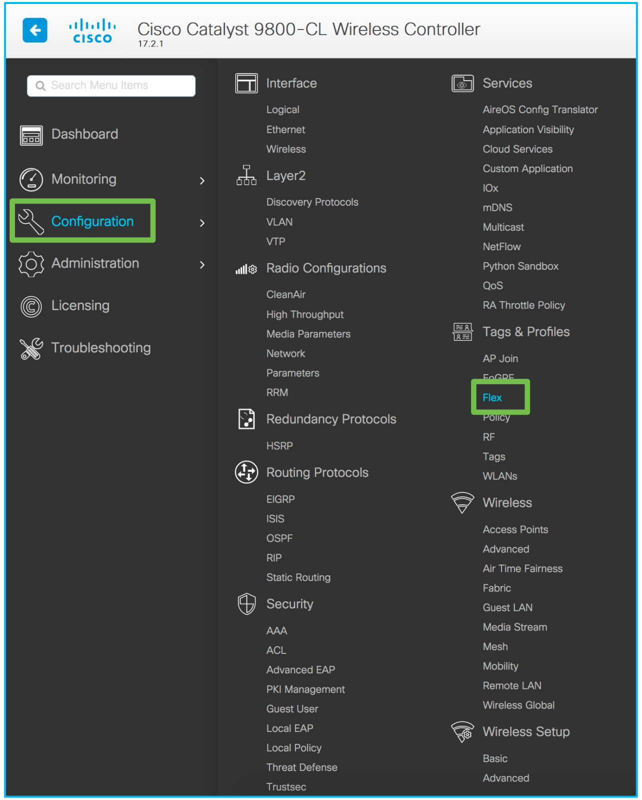
- Configure the WLAN and the Policy Profile, with local switching traffic options

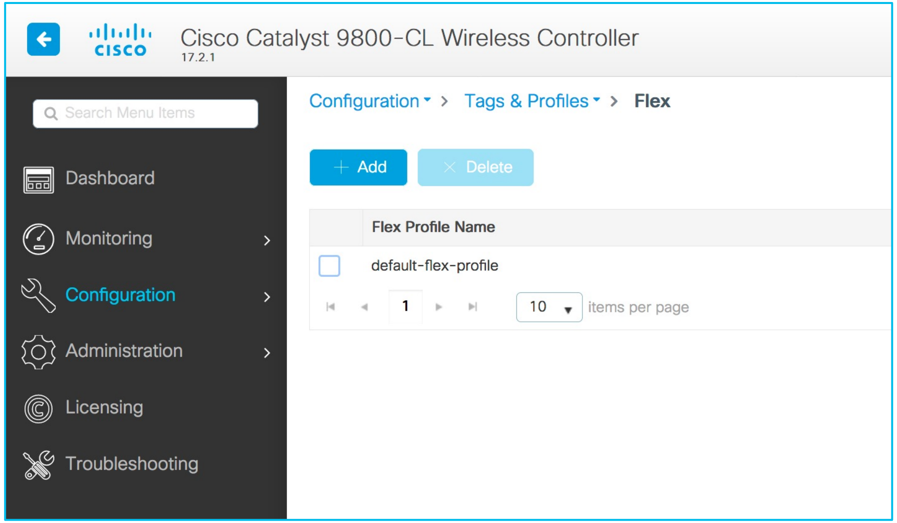
STEP **03**

**Assign the Policy Tag with WLAN+Profile**

- Link the WLAN with the Policy Profile under the Policy Tag and assign it to the AP(s)

# FlexConnect workflow example



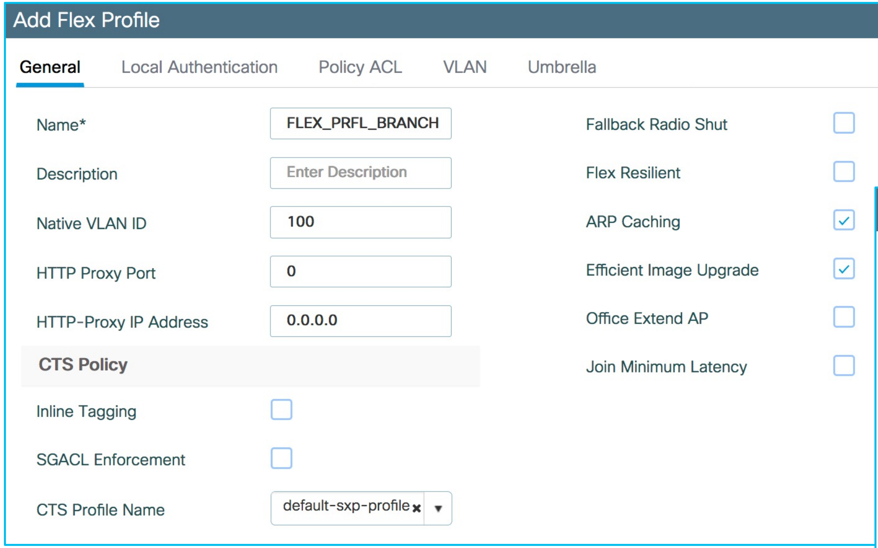


| | Flex Profile Name |
|---|---|
| □ | default-flex-profile |

1 | 10 items per page

Configuration > Tags & Profiles > Flex > Add Flex Profile

# FlexConnect workflow example

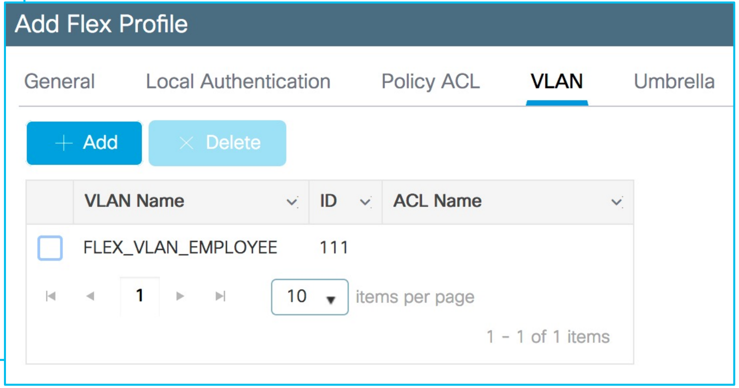


Add Flex Profile

General | Local Authentication | Policy ACL | VLAN | Umbrella

| | | | |
|---|---|---|---|
| Name* | FLEX_PRFL_BRANCH | Fallback Radio Shut | □ |
| Description | Enter Description | Flex Resilient | □ |
| Native VLAN ID | 100 | ARP Caching | ☑ |
| HTTP Proxy Port | 0 | Efficient Image Upgrade | ☑ |
| HTTP-Proxy IP Address | 0.0.0.0 | Office Extend AP | □ |
| **CTS Policy** | | Join Minimum Latency | □ |
| Inline Tagging | □ | | |
| SGACL Enforcement | □ | | |
| CTS Profile Name | default-sxp-profile × ▾ | | |

Not technically 100% mandatory, but better to be sure that the AP's native VLAN on the switchport trunk matches this configuration



Add Flex Profile

General | Local Authentication | Policy ACL | VLAN | Umbrella

+ Add | × Delete

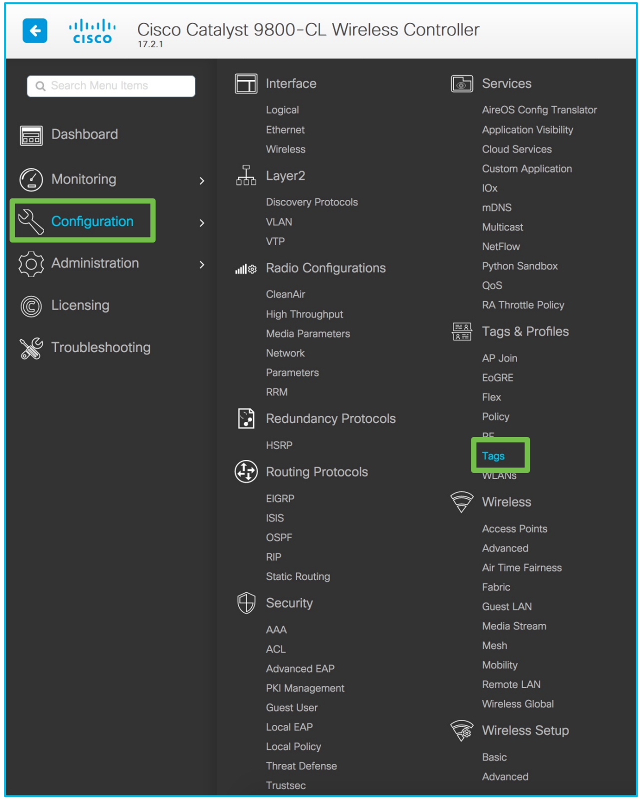
| | VLAN Name | ID | ACL Name |
|---|---|---|---|
| □ | FLEX_VLAN_EMPLOYEE | 111 | |

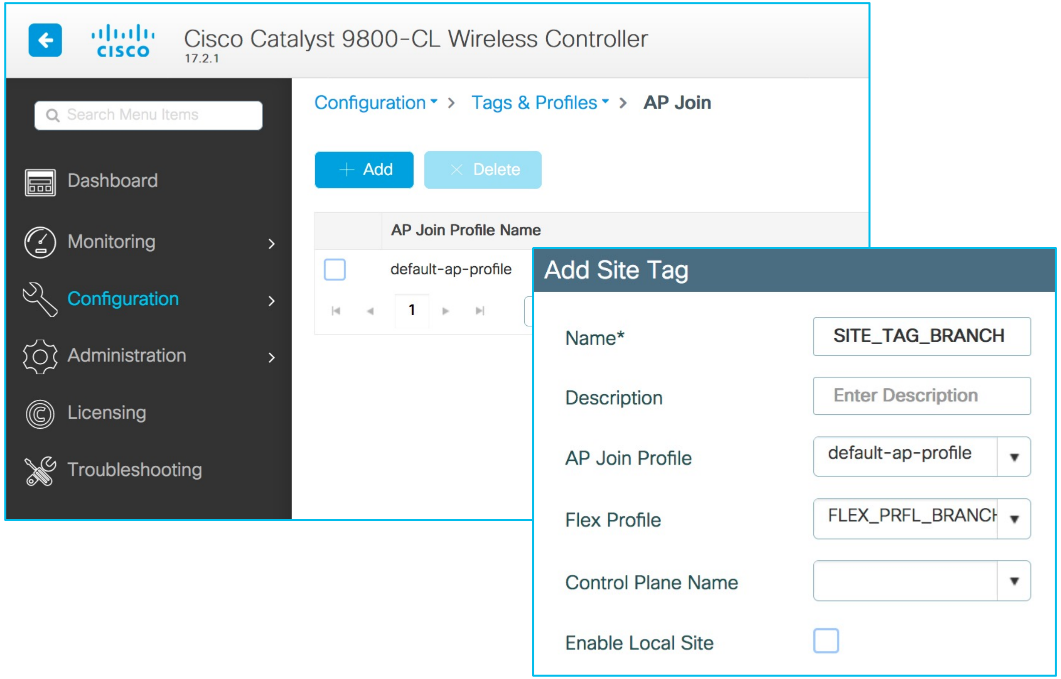
1 | 10 ▾ items per page

1 - 1 of 1 items

Adding VLANs in the Flex Profile is needed only if you wish to dynamically assign them via RADIUS attributes, or after also declaring them in the 9800's VLAN database

# FlexConnect workflow example



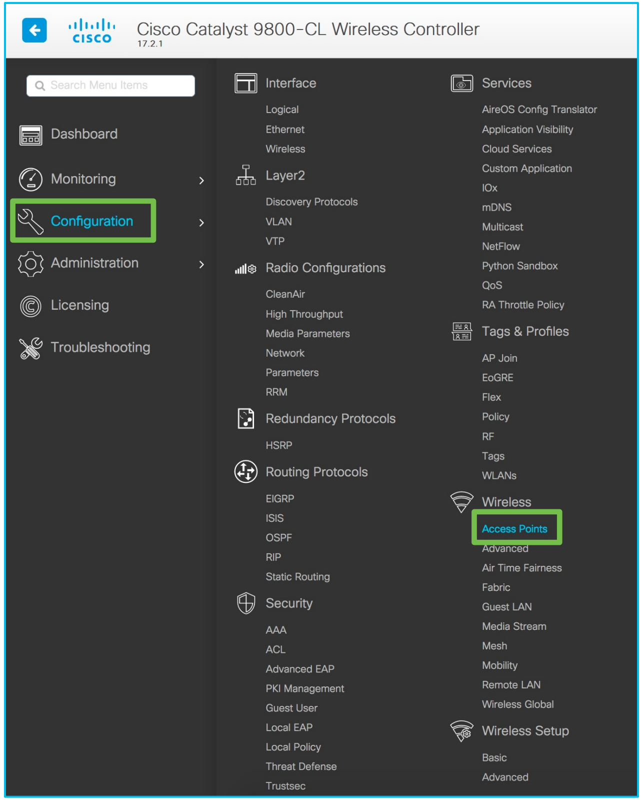


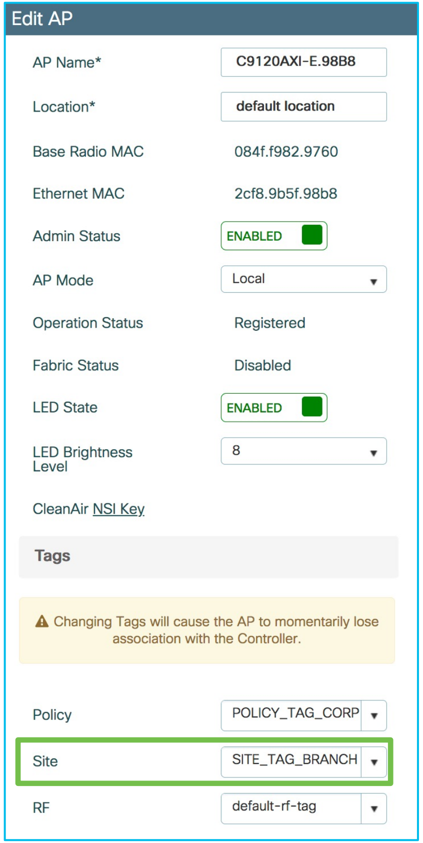
## Add Site Tag

| | |
|---|---|
| Name* | SITE_TAG_BRANCH |
| Description | Enter Description |
| AP Join Profile | default-ap-profile ▾ |
| Flex Profile | FLEX_PRFL_BRANCH ▾ |
| Control Plane Name | ▾ |
| Enable Local Site | □ |

Configuration > Tags & Profiles > Tags
> Add a Site Tag with “Enable Local Site” unchecked
and the previously configured Flex Profile

# FlexConnect workflow example





Edit AP

| | |
|---|---|
| AP Name* | C9120AXI-E.98B8 |
| Location* | default location |
| Base Radio MAC | 084f.f982.9760 |
| Ethernet MAC | 2cf8.9b5f.98b8 |
| Admin Status | ENABLED |
| AP Mode | Local |
| Operation Status | Registered |
| Fabric Status | Disabled |
| LED State | ENABLED |
| LED Brightness Level | 8 |
| CleanAir NSI Key | |

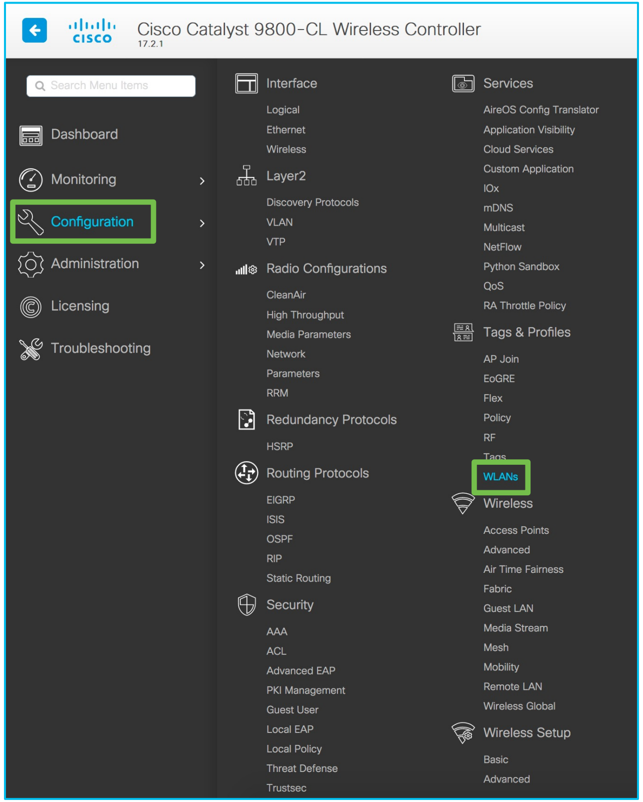
Tags

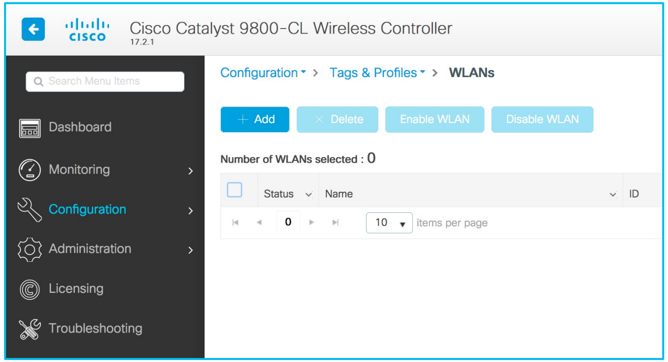
⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

| | |
|---|---|
| Policy | POLICY_TAG_CORP |
| Site | SITE_TAG_BRANCH |
| RF | default-rf-tag |

Configuration > Wireless > Access Points > Edit AP > Site

# FlexConnect workflow example

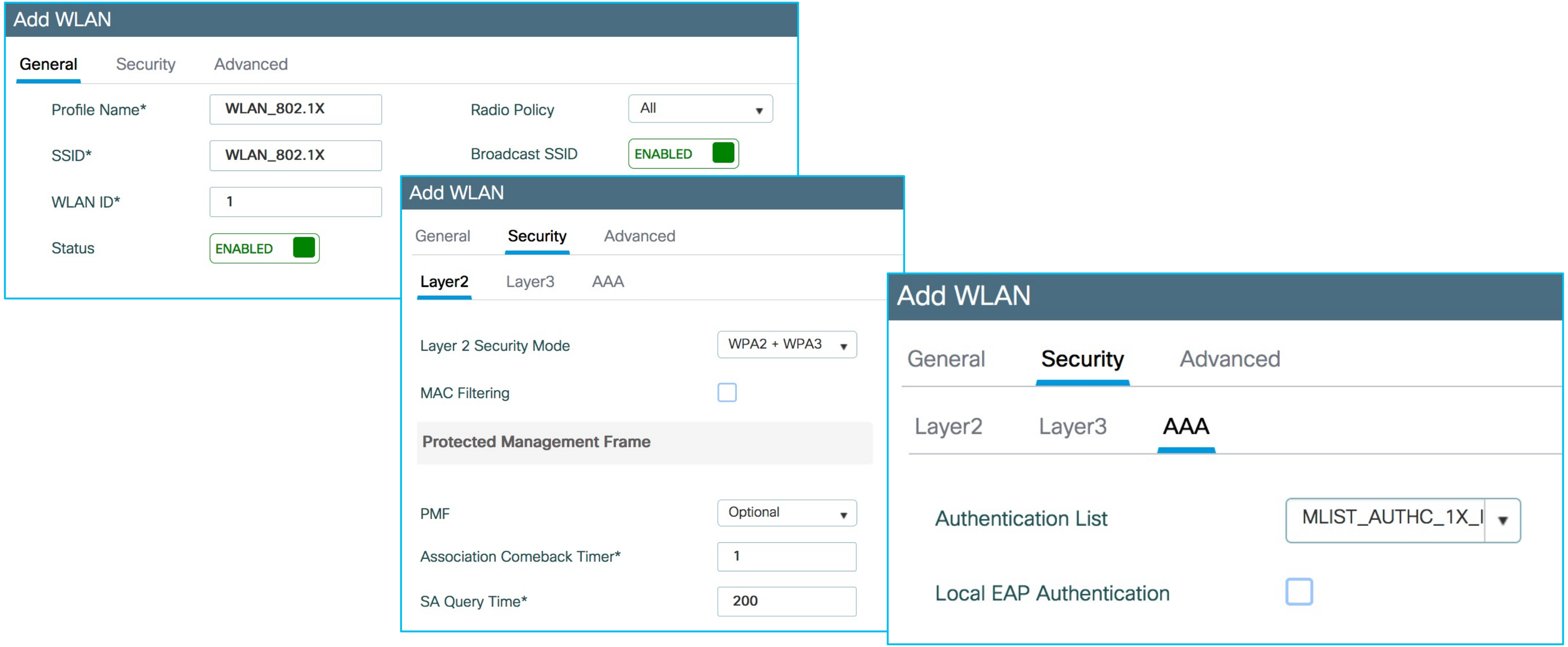




Number of WLANs selected : 0

Configuration > Tags & Profiles > WLANs > Add WLAN

# FlexConnect workflow example



Add WLAN

General | Security | Advanced

| | |
|---|---|
| Profile Name* | WLAN_802.1X |
| SSID* | WLAN_802.1X |
| WLAN ID* | 1 |
| Status | ENABLED |
| Radio Policy | All |
| Broadcast SSID | ENABLED |

Add WLAN

General | Security | Advanced

Layer2 | Layer3 | AAA

| | |
|---|---|
| Layer 2 Security Mode | WPA2 + WPA3 |
| MAC Filtering | □ |

**Protected Management Frame**

| | |
|---|---|
| PMF | Optional |
| Association Comeback Timer* | 1 |
| SA Query Time* | 200 |

Add WLAN

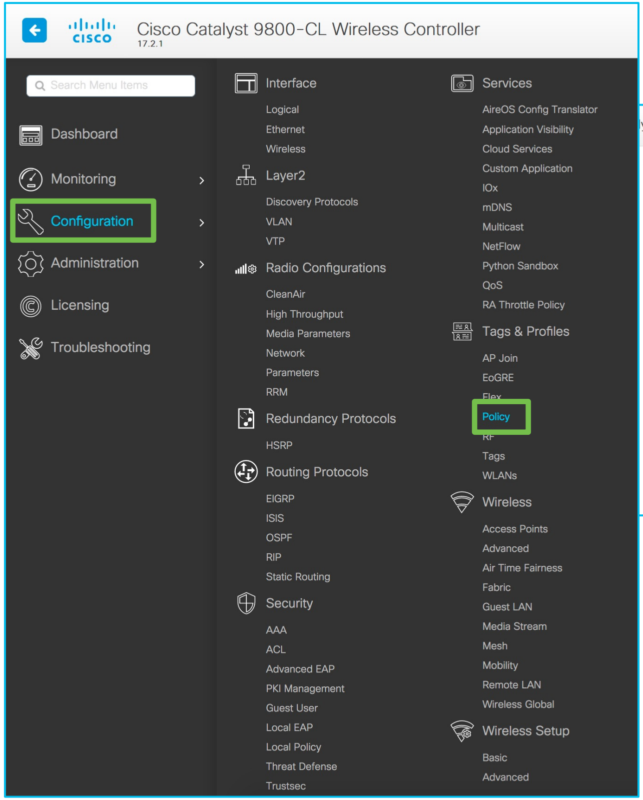
General | Security | Advanced

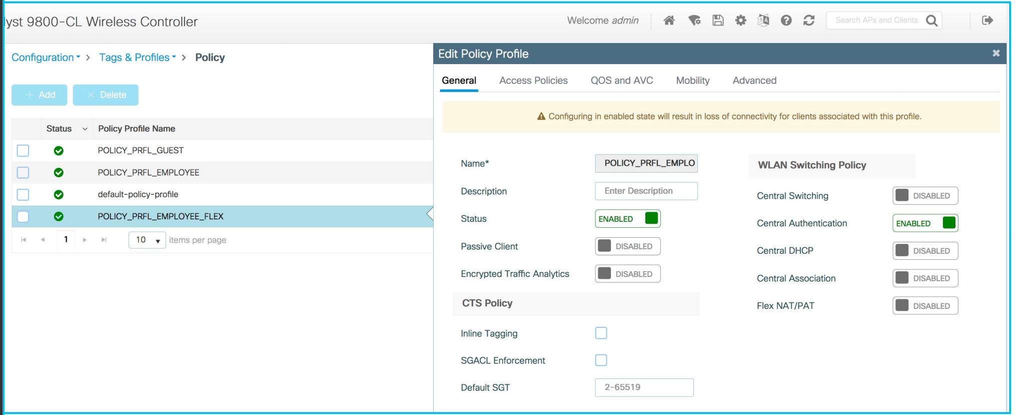
Layer2 | Layer3 | AAA

| | |
|---|---|
| Authentication List | MLIST_AUTHC_1X_I |
| Local EAP Authentication | □ |

Configuration > Tags & Profiles > WLANs
> Add WLAN (with 802.1X in this example)

# FlexConnect workflow example





| | Status | Policy Profile Name |
|---|---|---|
| □ | ✓ | POLICY_PRFL_GUEST |
| □ | ✓ | POLICY_PRFL_EMPLOYEE |
| □ | ✓ | default-policy-profile |
| □ | ✓ | POLICY_PRFL_EMPLOYEE_FLEX |

1 | 10 items per page

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* POLICY_PRFL_EMPLO

Description Enter Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging □

SGACL Enforcement □

Default SGT 2-65519

WLAN Switching Policy

Central Switching DISABLED

Central Authentication ENABLED

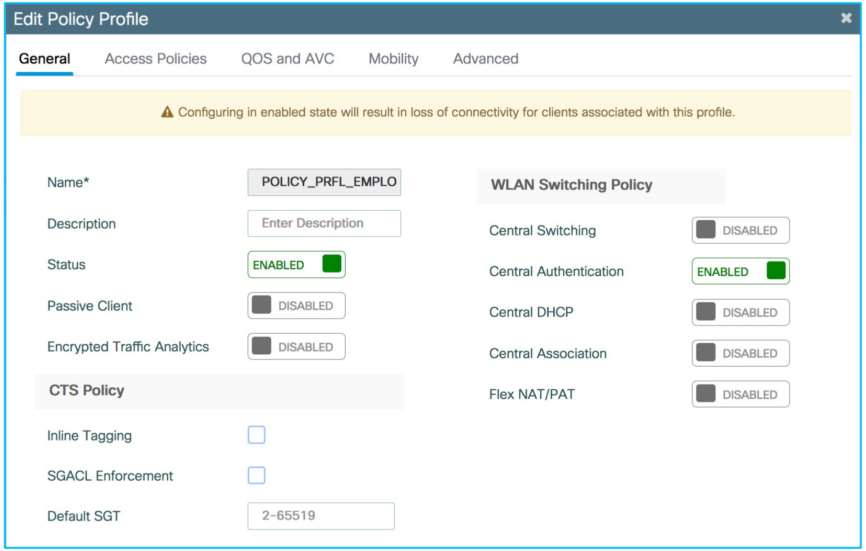
Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Configuration > Tags & Profiles > Policy
> Create the Policy Profile for FlexConnect

# FlexConnect workflow example



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

| | |
|---|---|
| Name* | POLICY_PRFL_EMPLO |
| Description | Enter Description |
| Status | ENABLED |
| Passive Client | DISABLED |
| Encrypted Traffic Analytics | DISABLED |

**CTS Policy**

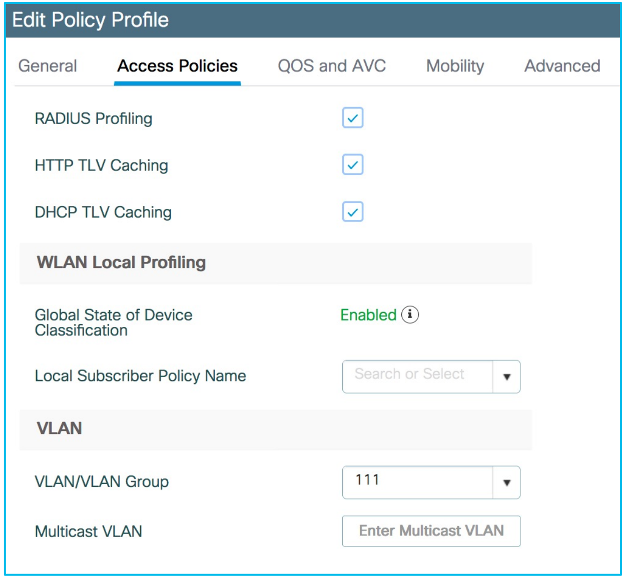
| | |
|---|---|
| Inline Tagging | □ |
| SGACL Enforcement | □ |
| Default SGT | 2-65519 |

**WLAN Switching Policy**

| | |
|---|---|
| Central Switching | DISABLED |
| Central Authentication | ENABLED |
| Central DHCP | DISABLED |
| Central Association | DISABLED |
| Flex NAT/PAT | DISABLED |

Disable:

- Central Switching
- Central DHCP
- Central Association



| | |
|---|---|
| RADIUS Profiling | ☑ |
| HTTP TLV Caching | ☑ |
| DHCP TLV Caching | ☑ |

**WLAN Local Profiling**

| | |
|---|---|
| Global State of Device Classification | Enabled ⓘ |
| Local Subscriber Policy Name | Search or Select ▾ |

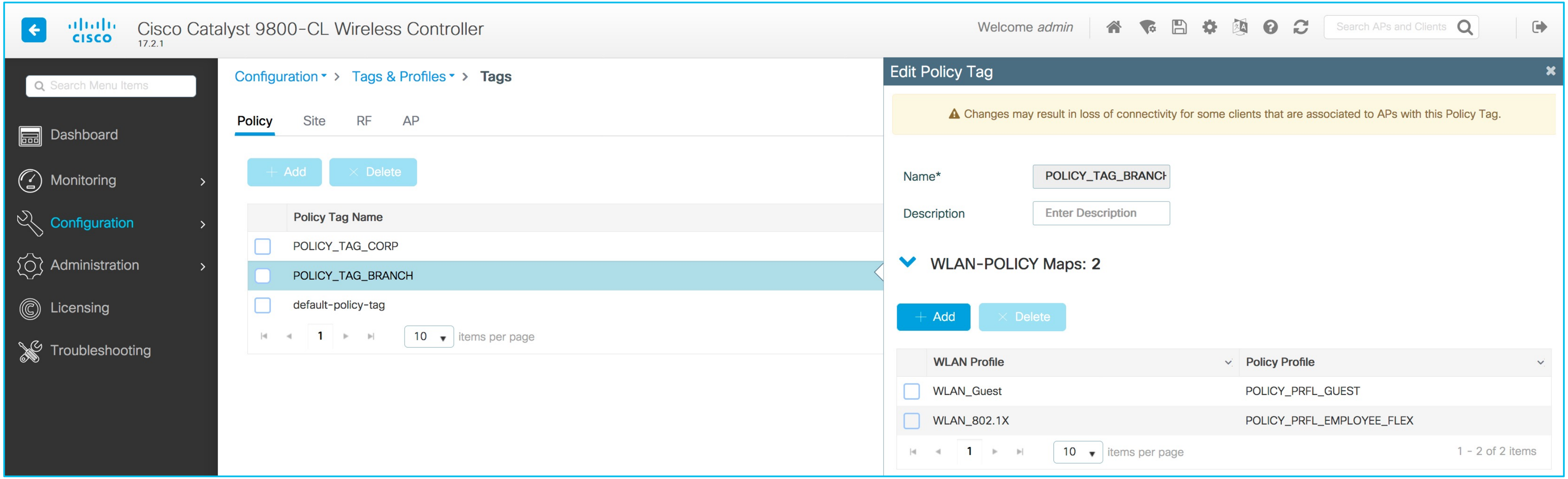
**VLAN**

| | |
|---|---|
| VLAN/VLAN Group | 111 ▾ |
| Multicast VLAN | Enter Multicast VLAN |

VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.
If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- when typing a VLAN number, this VLAN must not exist in the 9800's VLAN database;
- when using a VLAN name from the drop-down option, this VLAN must exist both in the 9800's local database and under the Flex Profile, with the exact same name and ID.

# FlexConnect workflow example



| | Policy Tag Name |
|---|---|
| □ | POLICY_TAG_CORP |
| □ | POLICY_TAG_BRANCH |
| □ | default-policy-tag |

1 · 10 items per page

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: POLICY_TAG_BRANCH

Description: Enter Description

WLAN-POLICY Maps: 2

| | WLAN Profile | Policy Profile |
|---|---|---|
| □ | WLAN_Guest | POLICY_PRFL_GUEST |
| □ | WLAN_802.1X | POLICY_PRFL_EMPLOYEE_FLEX |

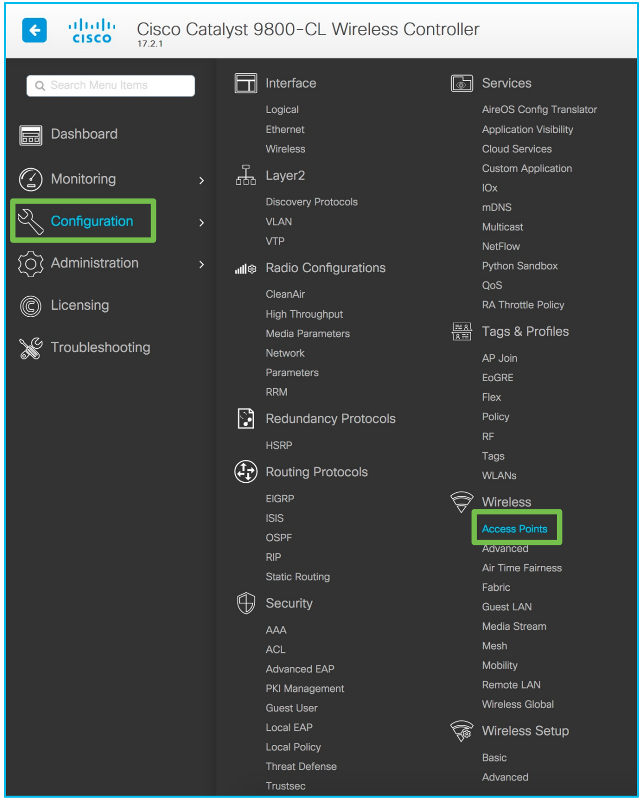
1 · 10 items per page · 1 - 2 of 2 items

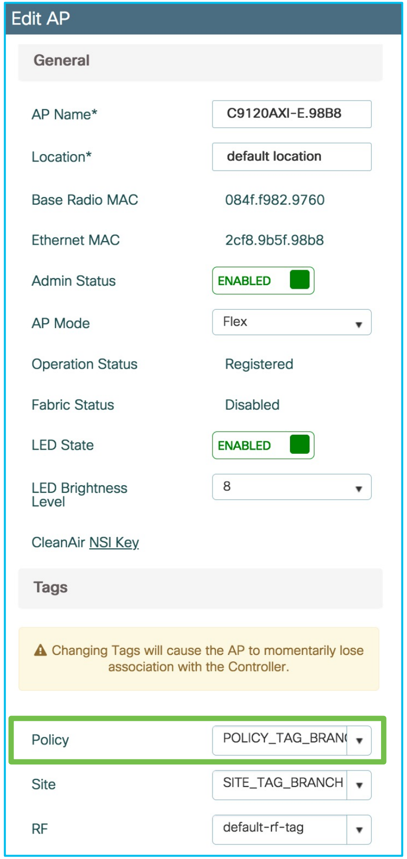
Configuration > Tags & Profiles > Tags

> Create a dedicated Policy Tag for the branch

> Under the new Policy Tag, associate the WLAN to the Policy Profile

# FlexConnect workflow example





Edit AP

General

| | |
|---|---|
| AP Name* | C9120AXI-E.98B8 |
| Location* | default location |
| Base Radio MAC | 084f.f982.9760 |
| Ethernet MAC | 2cf8.9b5f.98b8 |
| Admin Status | ENABLED |
| AP Mode | Flex |
| Operation Status | Registered |
| Fabric Status | Disabled |
| LED State | ENABLED |
| LED Brightness Level | 8 |
| CleanAir NSI Key | |

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

| | |
|---|---|
| Policy | POLICY_TAG_BRAN( |
| Site | SITE_TAG_BRANCH |
| RF | default-rf-tag |

Configuration > Wireless > Access Points > Edit AP > Policy

Assign the new Policy Tag to the AP

# Что такое Site Tags и Flex Profiles

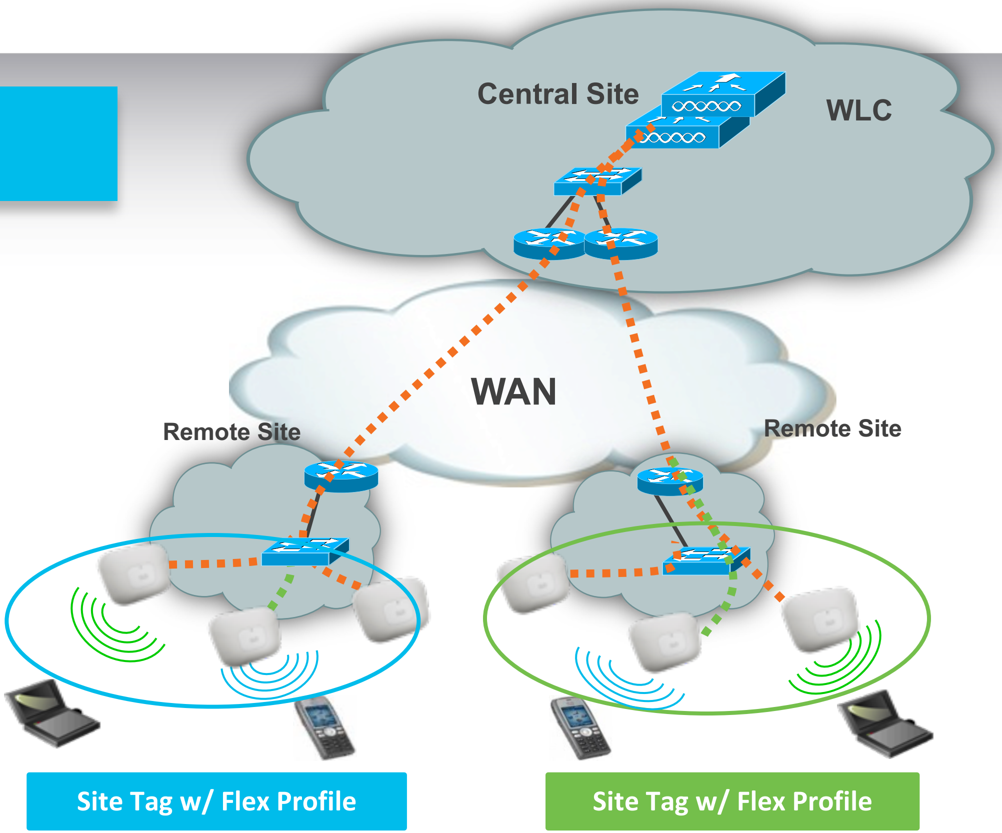
# Site Tag with a Flex Profile (aka Flex Group)

## Overview

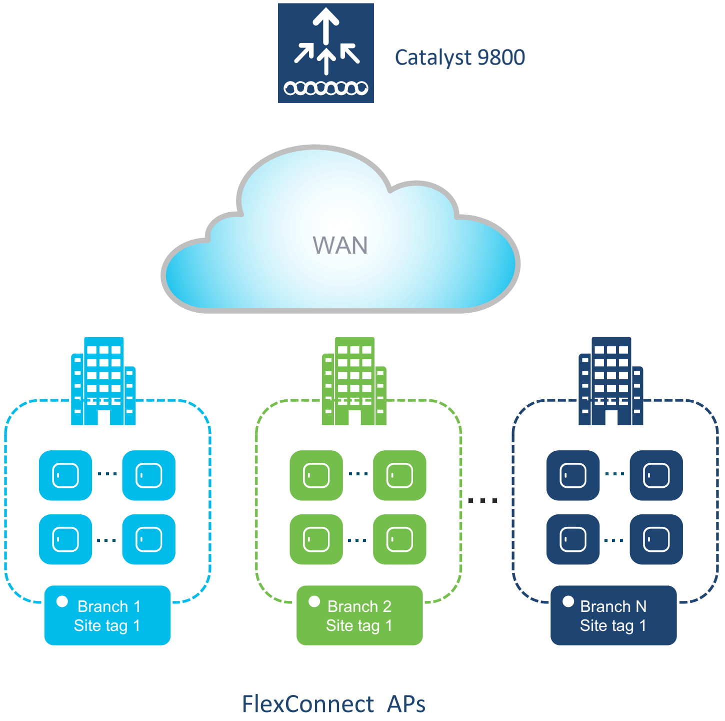
Each Site Tag with a Flex Profile is a (Flex) group of APs sharing the following:

- 802.11r fast roaming keys
- Local/backup RADIUS servers IP/keys
- Local EAP authentication settings
- AAA Override for Local Switching
- Smart Image Upgrade
- FlexConnect  AVC/QoS Policies

| Scaling | 9800-80<br>9800-CL | 9800-40 | 9800-L |
|---|---|---|---|
| FlexConnect Profiles | 6000 | 2000 | 250/500 |
| AP per Site Tag (with a Flex Profile assigned) | 100 | 100 | 100 |

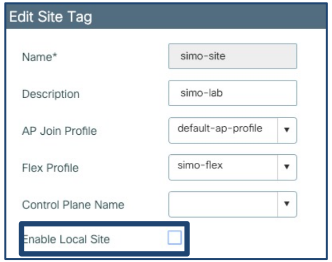


# Site Tag with a Flex Profile



## Important facts:

- For a Site Tag to have a Flex Profile, disable the option for “Local Site” (i.e. APs in Local mode)



Edit Site Tag

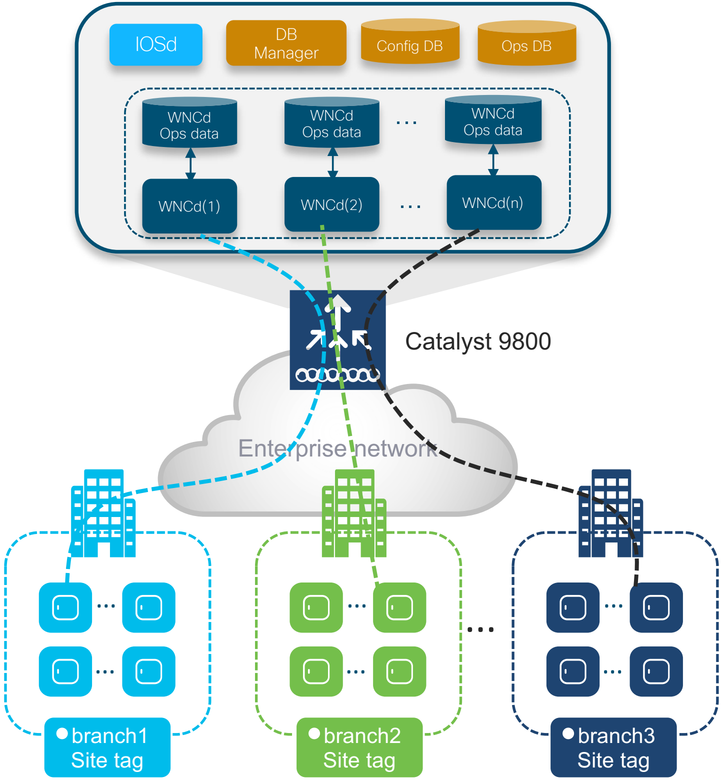
| | |
|---|---|
| Name* | simo-site |
| Description | simo-lab |
| AP Join Profile | default-ap-profile |
| Flex Profile | simo-flex |
| Control Plane Name | |
| Enable Local Site | □ |

- In this case the Site Tag is equivalent to a FlexConnect Group in AireOS

- As with AireOS, there is a limit of **100 APs** per **Site Tag** with a **Flex Profile** for supporting seamless roaming

- Roaming across Site Tags with Flex Profiles will result in a client full re-authentication

# Site Tags: some design tips for branches



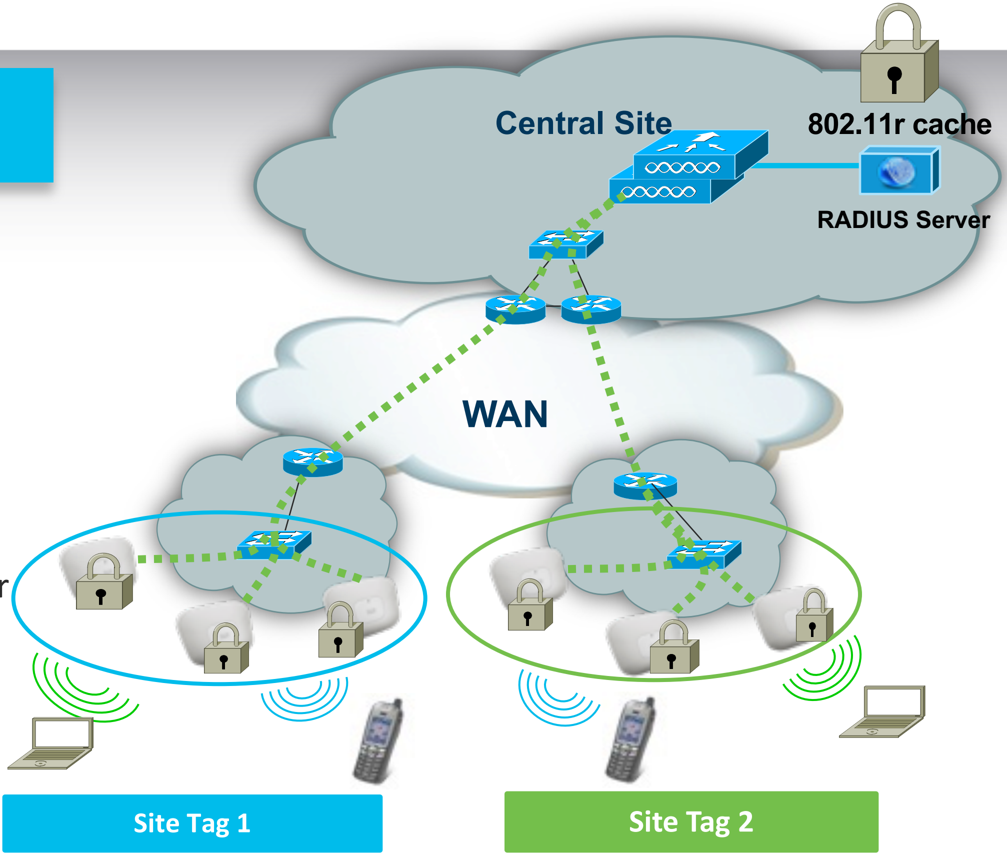
**Recommendations:**

- For FlexConnect, Site Tag is the roaming domain. Fast roaming happens only within a single Flex enabled Site Tag
- A good "principle" is a Site Tag per... site/branch
- **Don't use the same Site Tag across multiple branches** (this includes the default-site-tag ☺)
- If support for fast seamless roaming (802.11r, CCKM, OKC) is needed, then the **max number of APs per Site Tag with a Flex Profile is 100**
- If the branch has more than 100 APs, define at least two Site Tags and design APs-to-Site Tag assignment so that each Site Tag has less than 100 APs. Roaming across the two site tags will not be a fast roam (client will need to go through a full re-authentication) – same as AireOS with Flex Groups

# Site Tags and 802.11r

## Overview

- 802.11r cache stored on FlexConnect APs for Layer 2 fast roaming
- The FlexConnect APs receives the 802.11r cache from WLC
- If a FlexConnect AP boots up in standalone mode, it will not get the 802.11r keys from the WLC
- FlexConnect supports 802.11r Fast Transition with local key caching

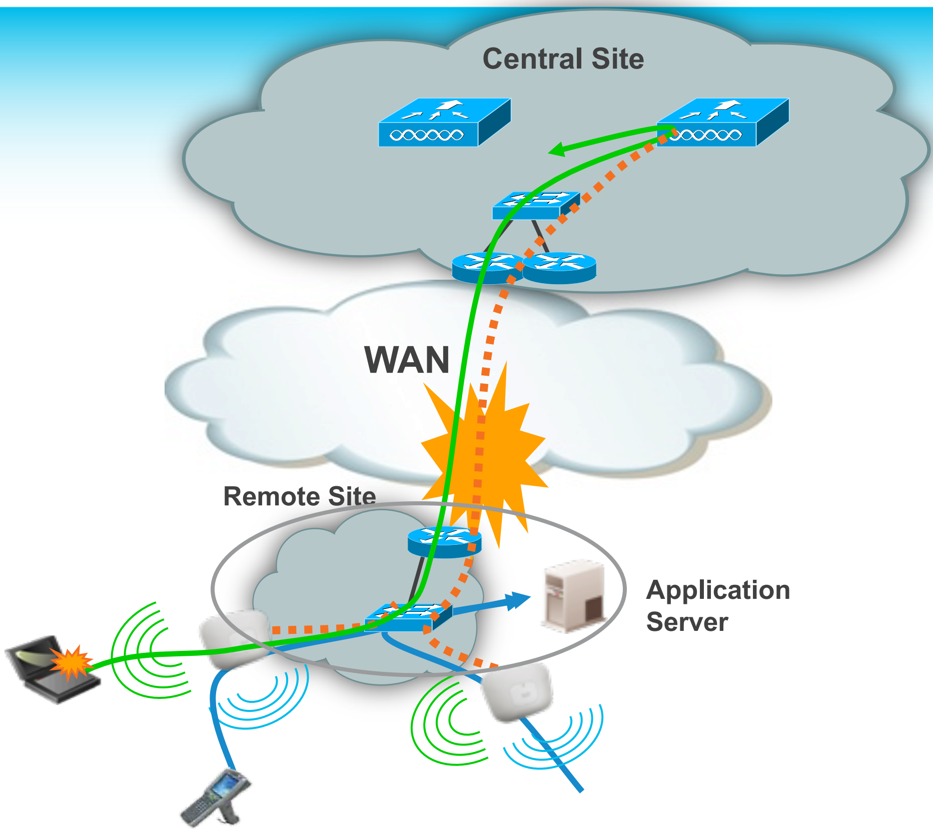


# Дизайн надежного беспроводного филиала

# FlexConnect Resiliency - WAN Failure

## WAN Failure

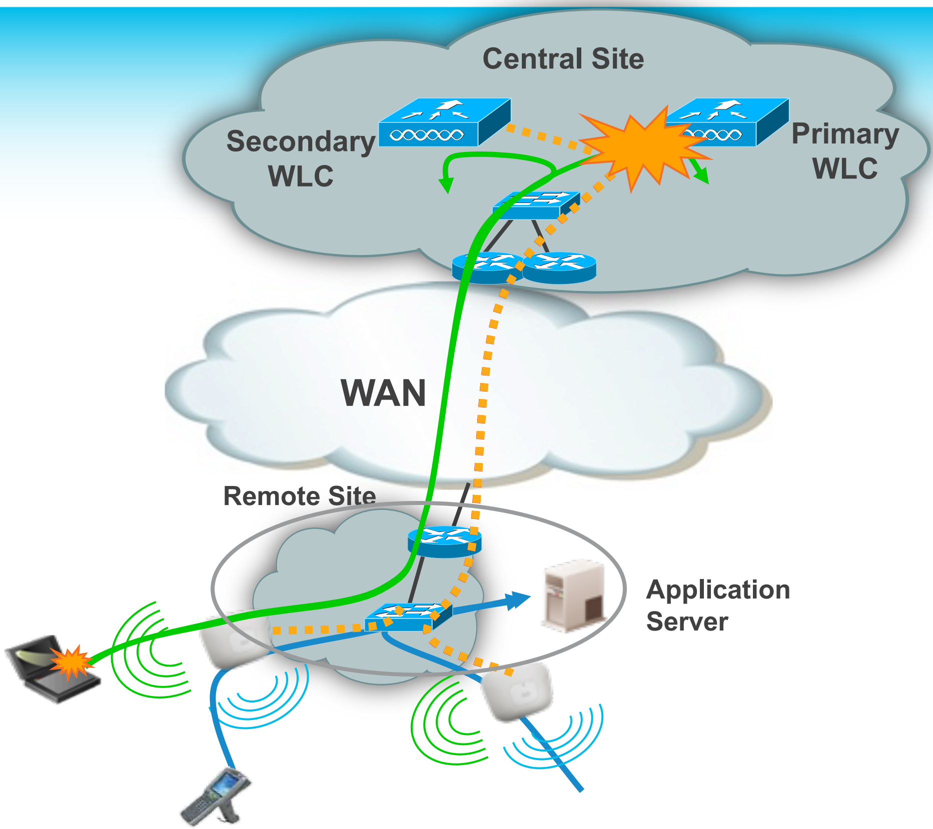
- FlexConnect APs will go to Standalone mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- Static authentication keys are locally stored in FlexConnect AP
- Lost Features
  - RRM, WIPS, location, etc.
  - URL Redirection (guest, BYOD, posture, MDM)



# FlexConnect Resiliency – N+1 HA Scenario

## WLC Failure scenario with N+1 HA

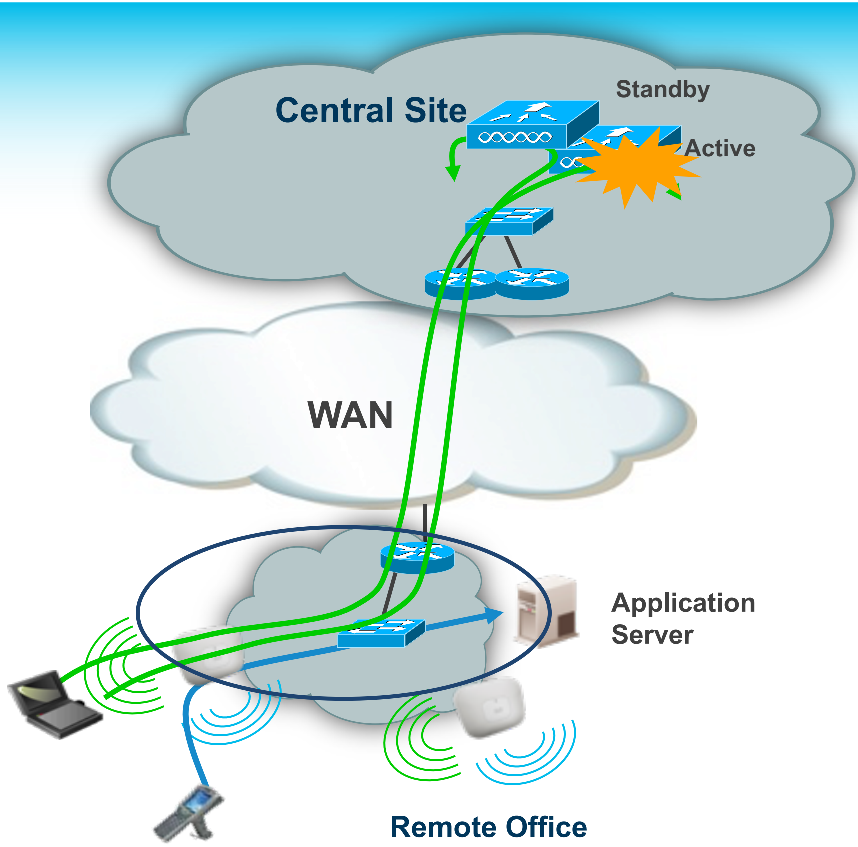
- FlexConnect APs will go to Standalone mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- Roaming allowed within the Site Tag
- FlexConnect AP will then search for a secondary WLC; when the secondary WLC is found, FlexConnect AP will resync with it and resume client sessions for central switching
- Locally switched client sessions are not impacted during resync with the secondary WLC (which needs to have the same config as the primary WLC)



# FlexConnect Resiliency – SSO HA  Scenario

## WLC failure scenario with SSO

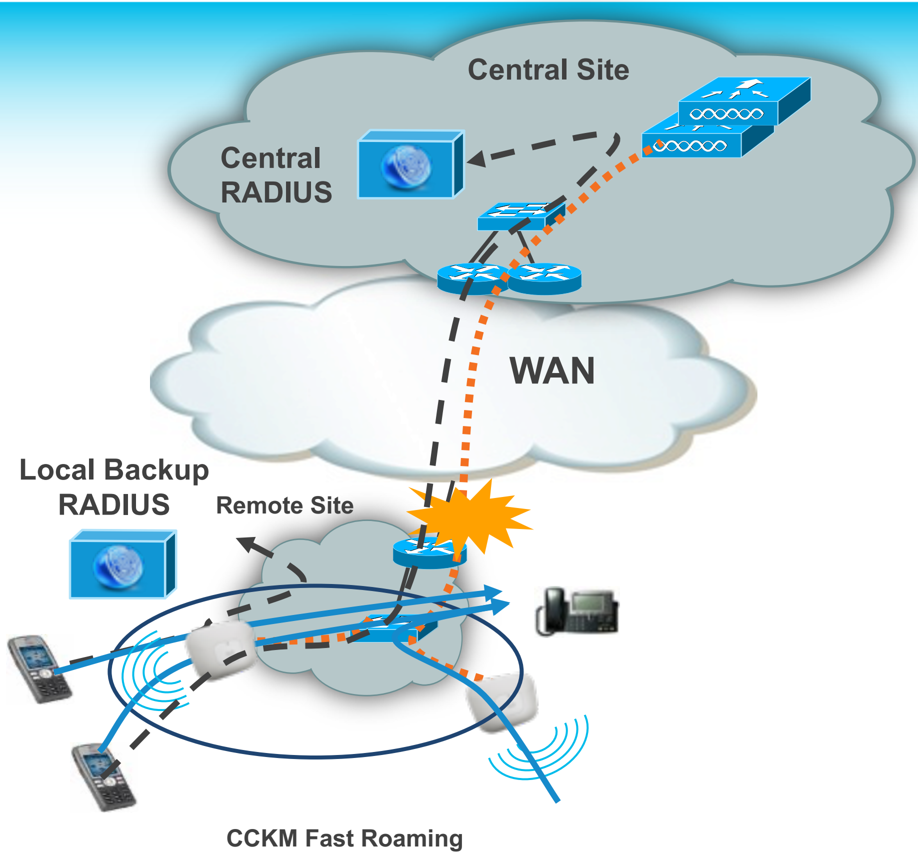
- True high availability with sub-second failover to a standby WLC
- AP/client sessions are synched between active and standby WLCs
- FlexConnect APs will not need to transition to standalone thanks to SSO
- **APs will continue to be in connected mode with the standby (new active) WLC**
- **Centrally switched SSIDs will always stay up**



# FlexConnect – AAA Survivability
# Local Backup RADIUS

## Local Backup RADIUS

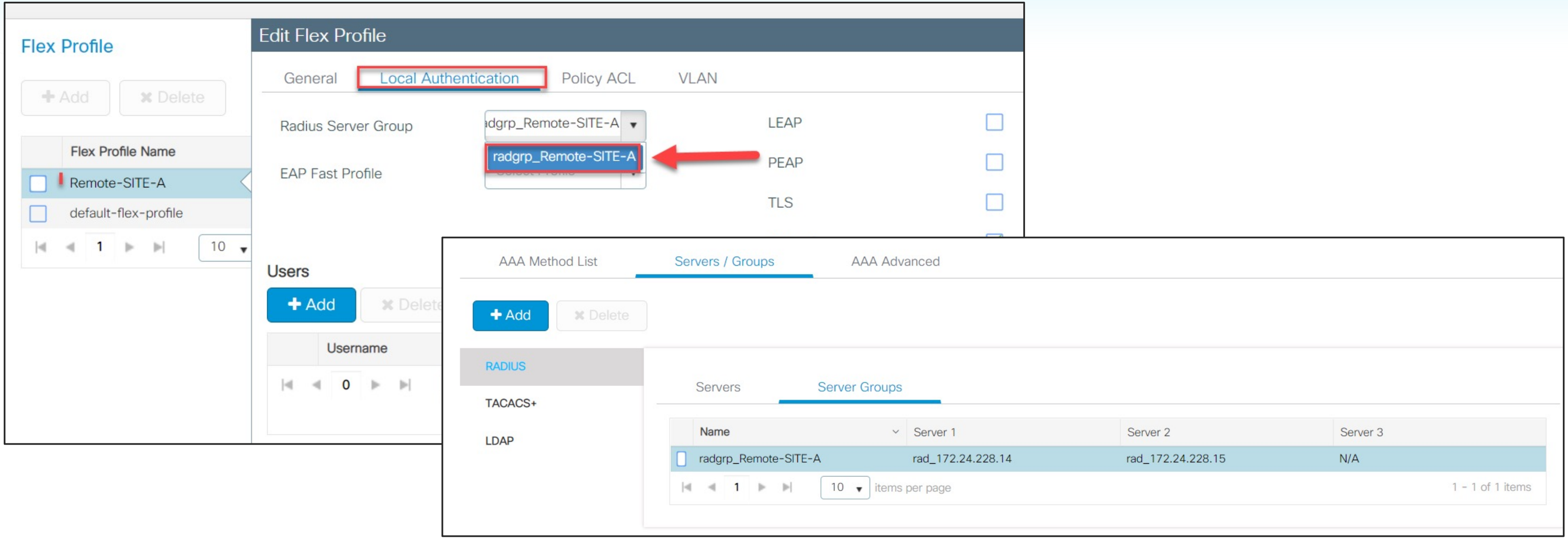
- Authentications done centrally through the WLC by default
- On WAN failure, the AP goes to standalone mode and can authenticate new clients with a locally defined RADIUS server
- Existing connected clients stay connected
- Clients can roam with
  - 802.11r fast roaming
  - Re-authentication



# Radius Server Group option under the Flex Profile

## Configuration

Define local backup RADIUS servers under the Flex Profile’s Local Authentication tab



| | Flex Profile Name |
|---|---|
| □ | Remote-SITE-A |
| □ | default-flex-profile |

1 | 10

Radius Server Group: radgrp_Remote-SITE-A

EAP Fast Profile

LEAP □

PEAP □

TLS □

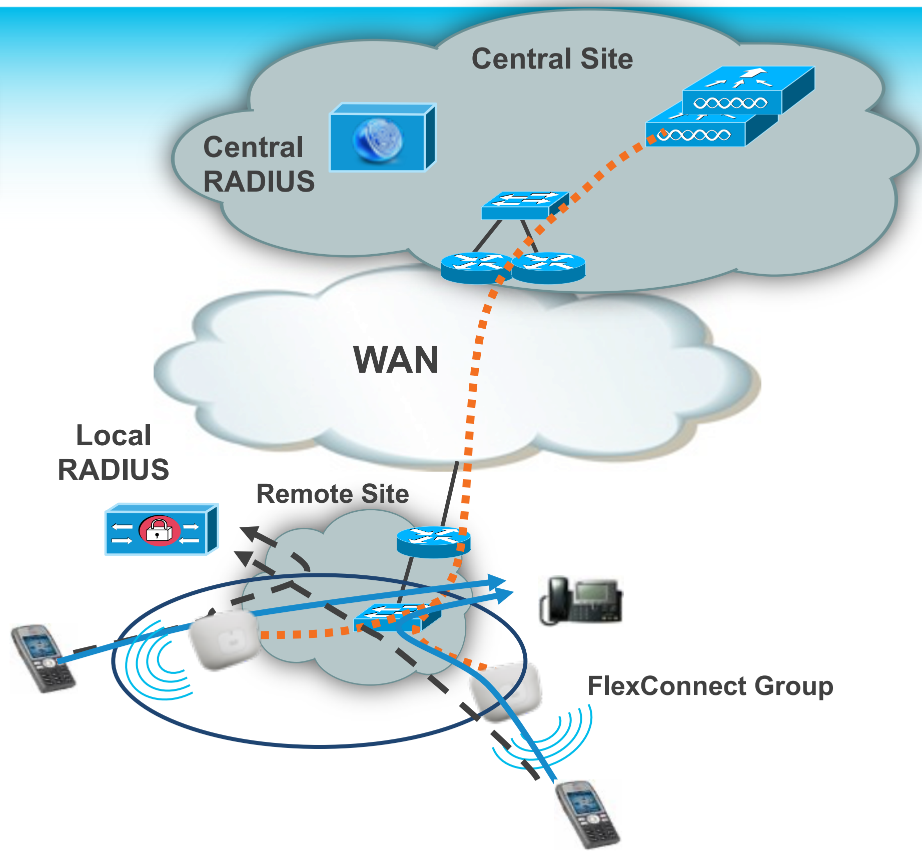
| | Name | Server 1 | Server 2 | Server 3 |
|---|---|---|---|---|
| □ | radgrp_Remote-SITE-A | rad_172.24.228.14 | rad_172.24.228.15 | N/A |

1 | 10 items per page | 1 - 1 of 1 items

# FlexConnect - Local Authentication

## Local Authentication

- By default FlexConnect AP authenticates clients through the central controller
- Local Authentication allows the use of local RADIUS server directly from the FlexConnect AP even when **WAN is UP**, or else even a local database at the AP's level (generally recommended as a last resort option)



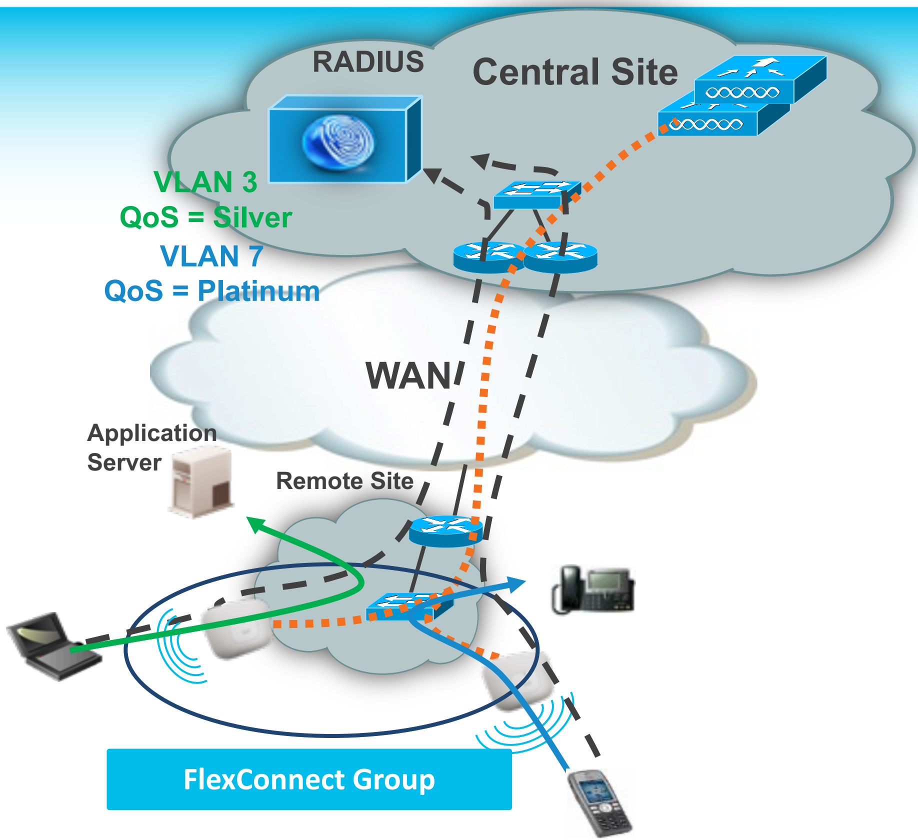
# Сегментация и безопасность

# FlexConnect AAA VLAN assignment

# FlexConnect AAA VLAN Override

## Description

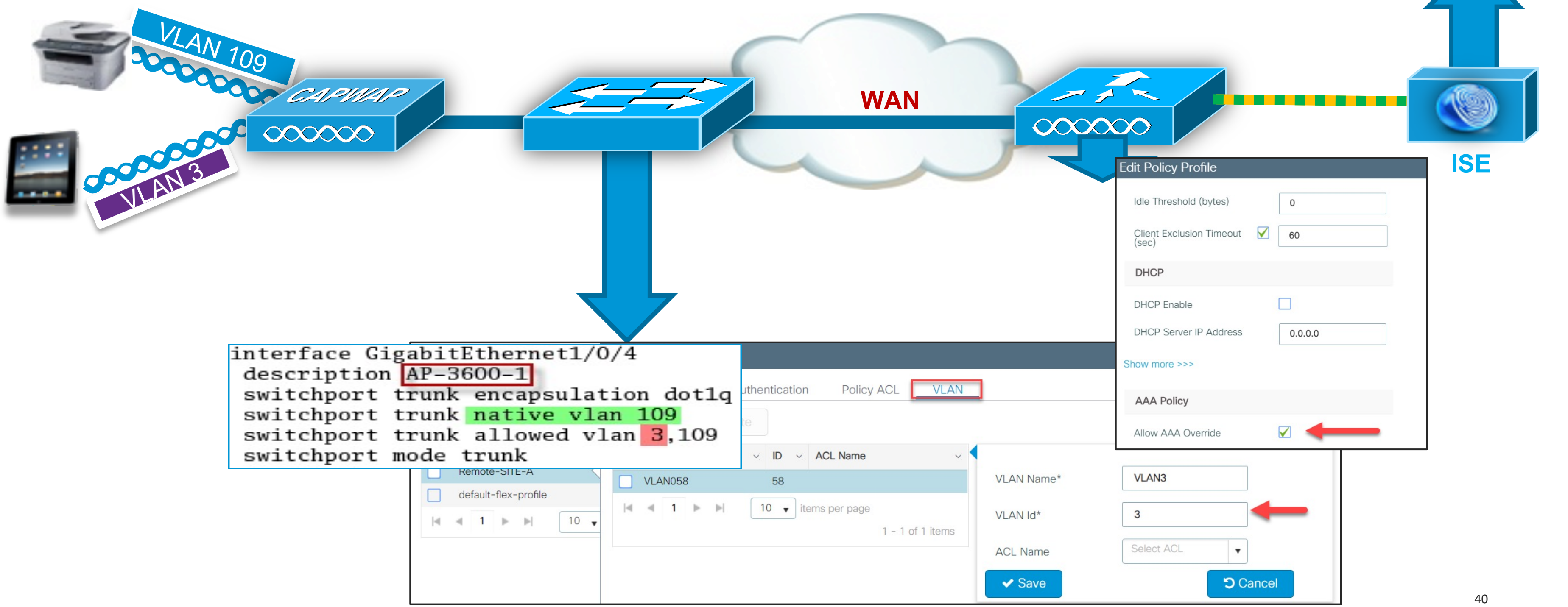
- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group



# FlexConnect AAA VLAN Override

## Configuration

| | 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
```

Edit Policy Profile

| | |
|---|---|
| Idle Threshold (bytes) | 0 |
| Client Exclusion Timeout (sec) ☑ | 60 |

DHCP

| | |
|---|---|
| DHCP Enable | ☐ |
| DHCP Server IP Address | 0.0.0.0 |

Show more >>>

AAA Policy

Allow AAA Override ☑

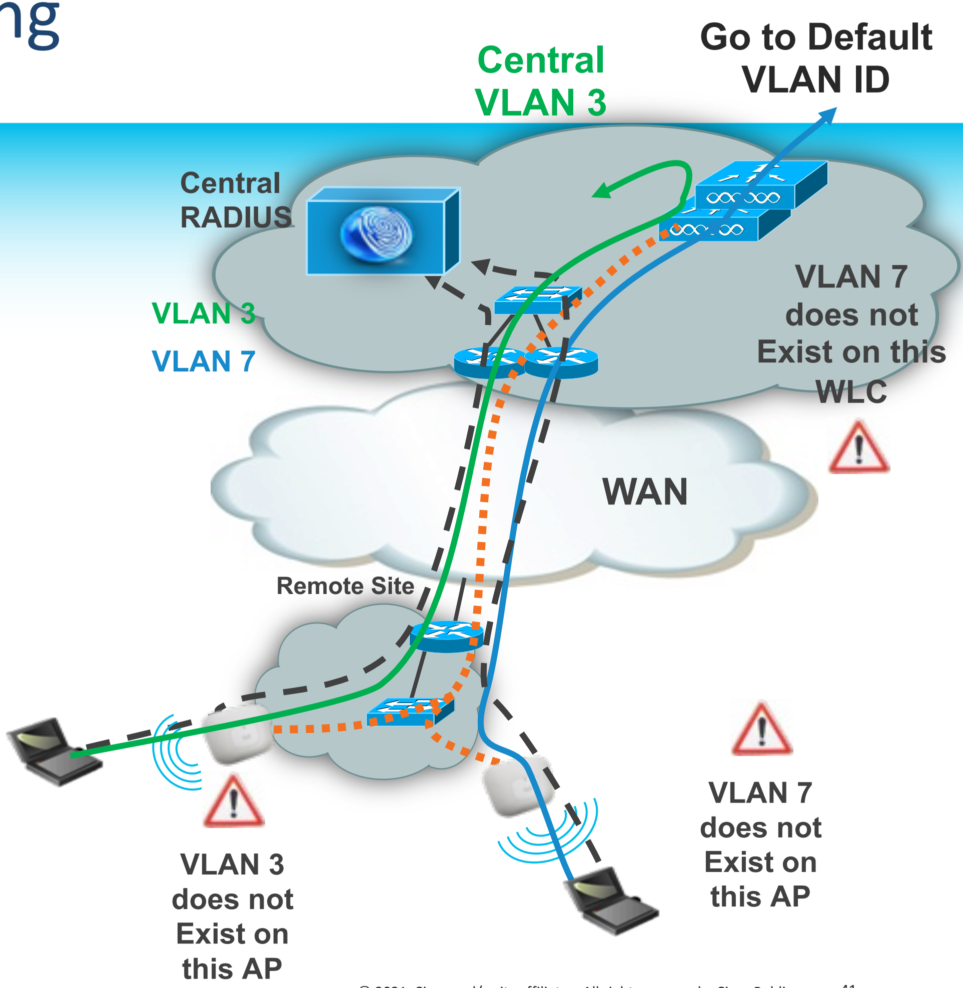
| ID | ACL Name |
|---|---|
| VLAN058 | 58 |

| | |
|---|---|
| VLAN Name* | VLAN3 |
| VLAN Id* | 3 |
| ACL Name | Select ACL |

# VLAN Based Central Switching

## Overview

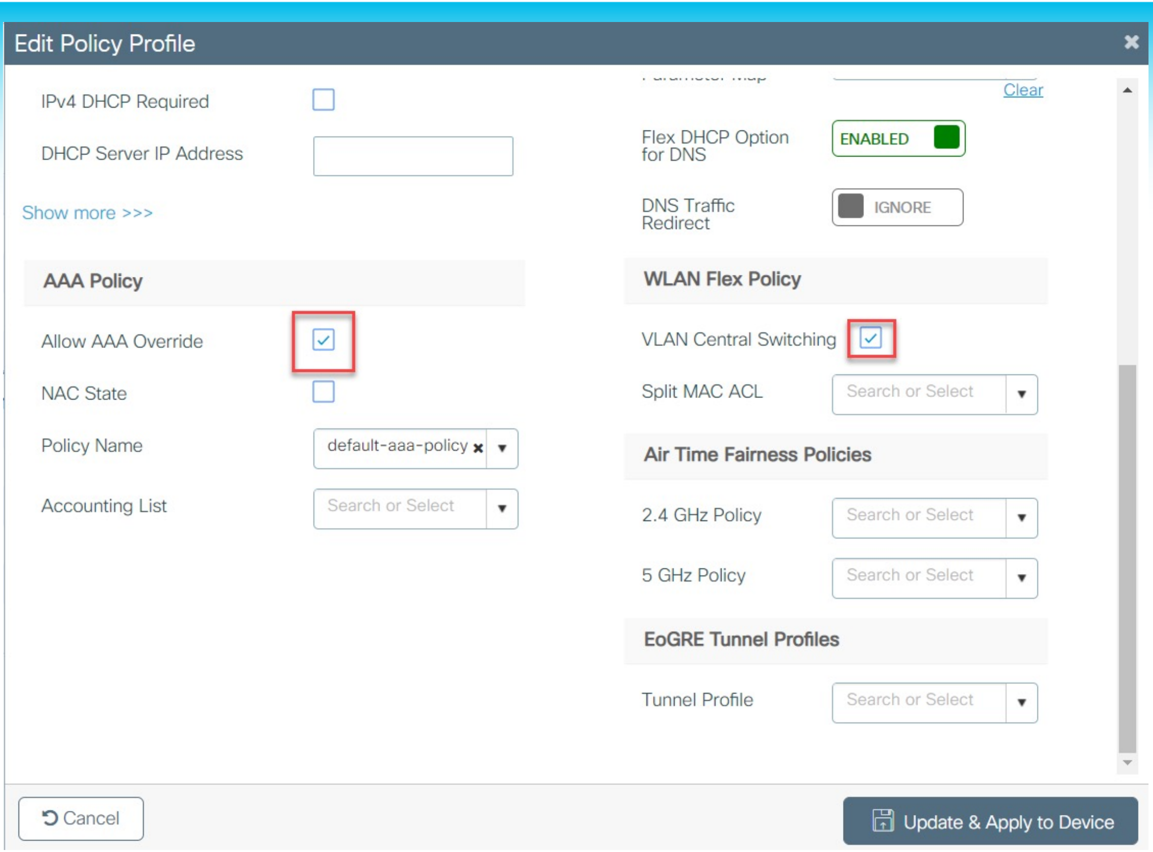
- While doing AAA VLAN Override with local switching:
- If VLAN ID does not exist at the AP, the traffic is central switched to the central VLAN ID
- If the central VLAN ID does not exist, the traffic is centrally switched to the default VLAN ID of the WLAN / Policy Profile



Central VLAN 3
Go to Default VLAN ID
Central RADIUS
VLAN 3
VLAN 7
VLAN 7 does not Exist on this WLC
WAN
Remote Site
VLAN 3 does not Exist on this AP
VLAN 7 does not Exist on this AP

# VLAN Based Central Switching

- This can be enabled on the Policy Profile
- Enable AAA Overide
- Enable VLAN Central switching



Edit Policy Profile

IPv4 DHCP Required □

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override ☑

NAC State □

Policy Name: default-aaa-policy

Accounting List: Search or Select

Clear

Flex DHCP Option for DNS: ENABLED

DNS Traffic Redirect: IGNORE

WLAN Flex Policy

VLAN Central Switching ☑

Split MAC ACL: Search or Select

Air Time Fairness Policies

2.4 GHz Policy: Search or Select

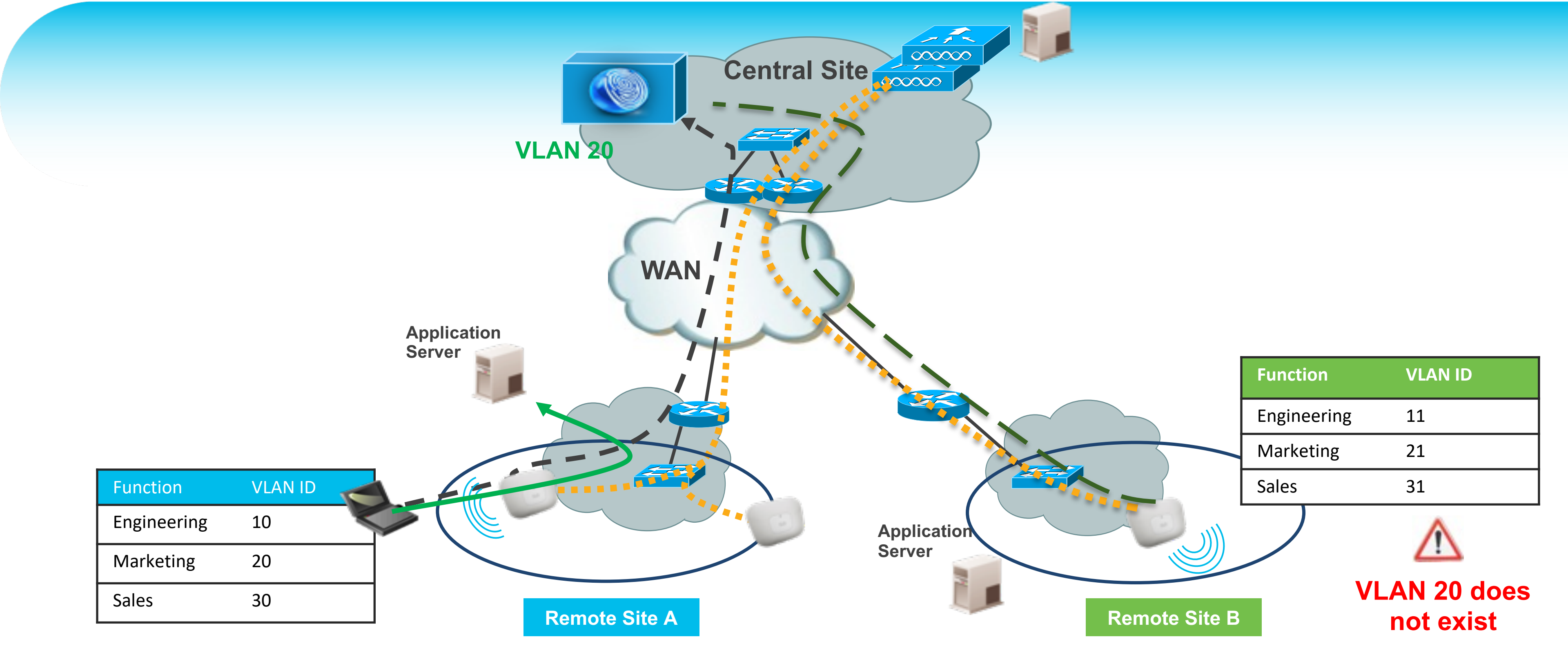
5 GHz Policy: Search or Select

EoGRE Tunnel Profiles

Tunnel Profile: Search or Select

# AAA Override Deployment Scenario

## Problem Statement – Map clients to specific vlans based on their function

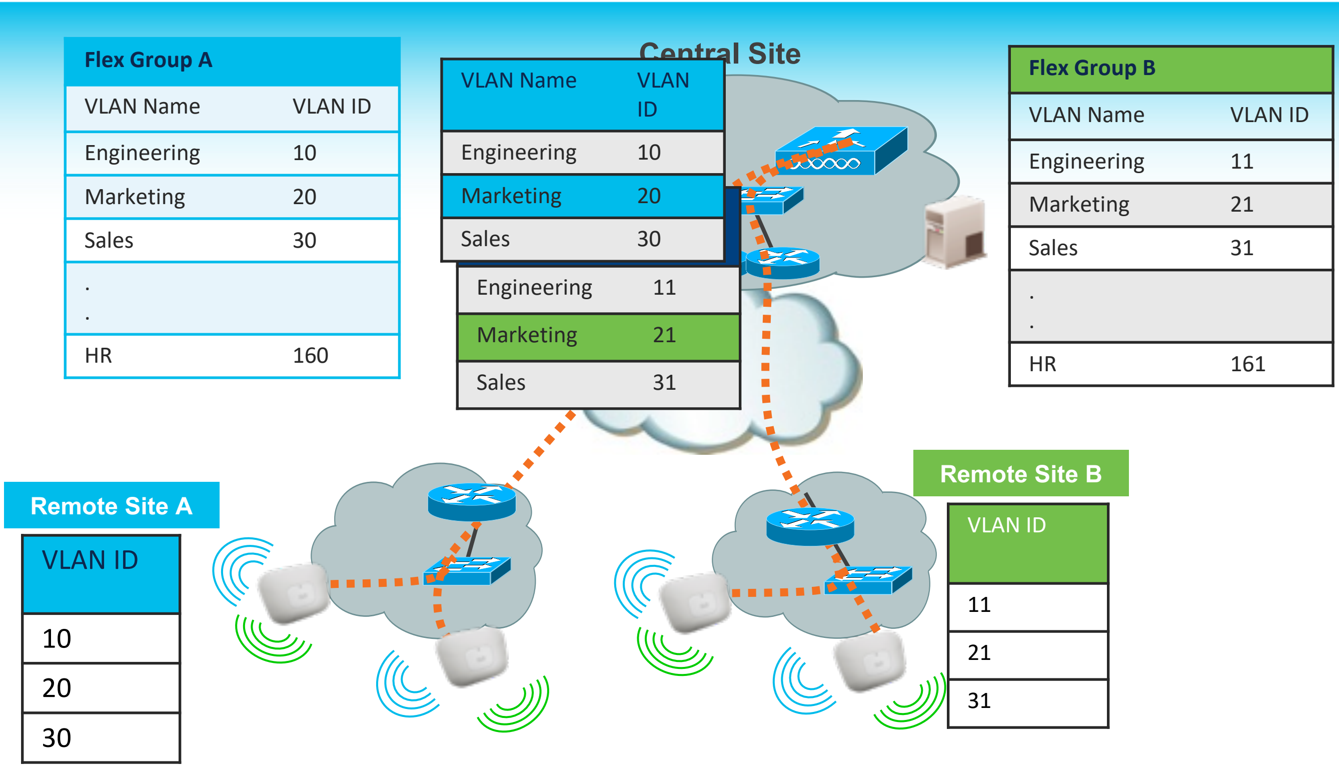


| Function | VLAN ID |
|---|---|
| Engineering | 10 |
| Marketing | 20 |
| Sales | 30 |

| Function | VLAN ID |
|---|---|
| Engineering | 11 |
| Marketing | 21 |
| Sales | 31 |

⚠ VLAN 20 does not exist

# VLAN Name Mapping at FlexConnect Group /Profile



**Flex Group A**

| VLAN Name | VLAN ID |
|---|---|
| Engineering | 10 |
| Marketing | 20 |
| Sales | 30 |
| .<br>. | |
| HR | 160 |

**Central Site**

| VLAN Name | VLAN ID |
|---|---|
| Engineering | 10 |
| Marketing | 20 |
| Sales | 30 |
| Engineering | 11 |
| Marketing | 21 |
| Sales | 31 |

**Flex Group B**

| VLAN Name | VLAN ID |
|---|---|
| Engineering | 11 |
| Marketing | 21 |
| Sales | 31 |
| .<br>. | |
| HR | 161 |

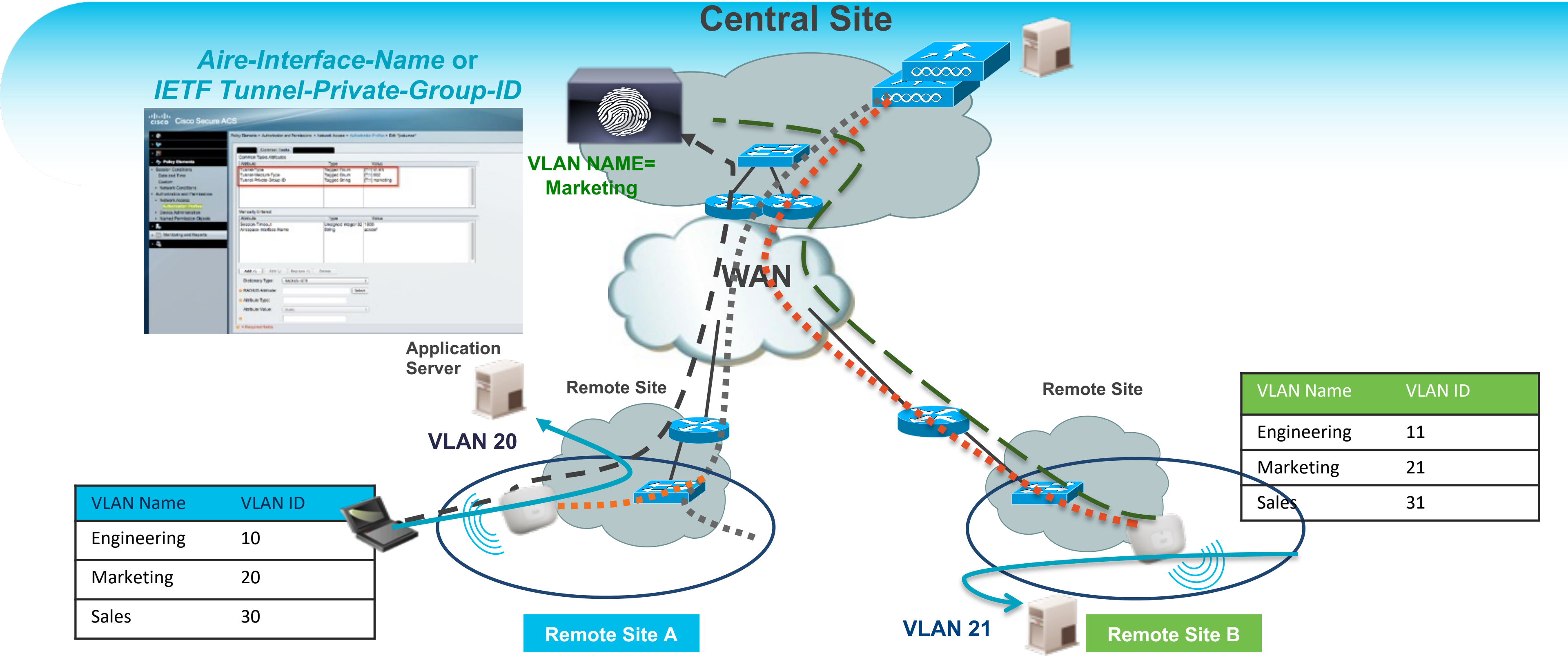
**Remote Site A**

| VLAN ID |
|---|
| 10 |
| 20 |
| 30 |

**Remote Site B**

| VLAN ID |
|---|
| 11 |
| 21 |
| 31 |

# VLAN Name AAA Override - Solution



*Aire-Interface-Name or*
*IETF Tunnel-Private-Group-ID*

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit "[illegible]"

Common Tasks

Common Tasks Attributes

| Attribute | Type | Value |
|---|---|---|
| Tunnel-Type | Tagged Enum | [T:1] VLAN |
| Tunnel-Medium-Type | Tagged Enum | [T:1] 802 |
| Tunnel-Private-Group-ID | Tagged String | [T:1] marketing |

Manually Entered

| Attribute | Type | Value |
|---|---|---|
| Session-Timeout | Unsigned Integer 32 | 1800 |
| Airespace-Wireless-Name | String | [illegible] |

Dictionary Type: RADIUS-IETF

RADIUS Attribute:

Attribute Type:

Attribute Value: Static

= Required fields

| VLAN Name | VLAN ID |
|---|---|
| Engineering | 10 |
| Marketing | 20 |
| Sales | 30 |

| VLAN Name | VLAN ID |
|---|---|
| Engineering | 11 |
| Marketing | 21 |
| Sales | 31 |

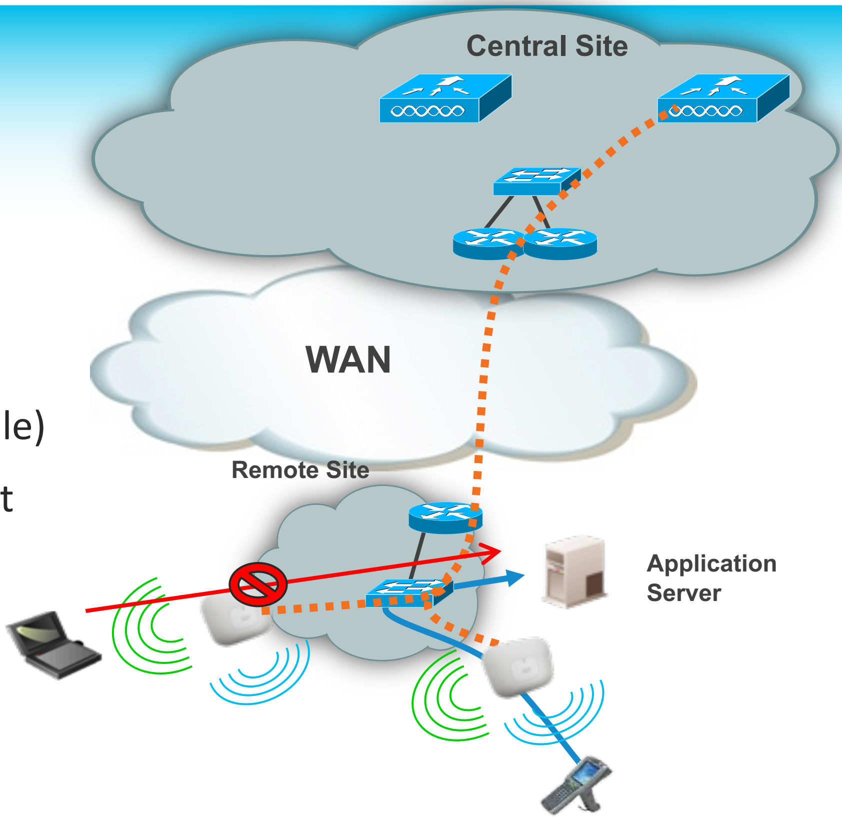
# FlexConnect Access-Control (ACL)

# FlexConnect ACL

Overview

1. Download ACL on to AP

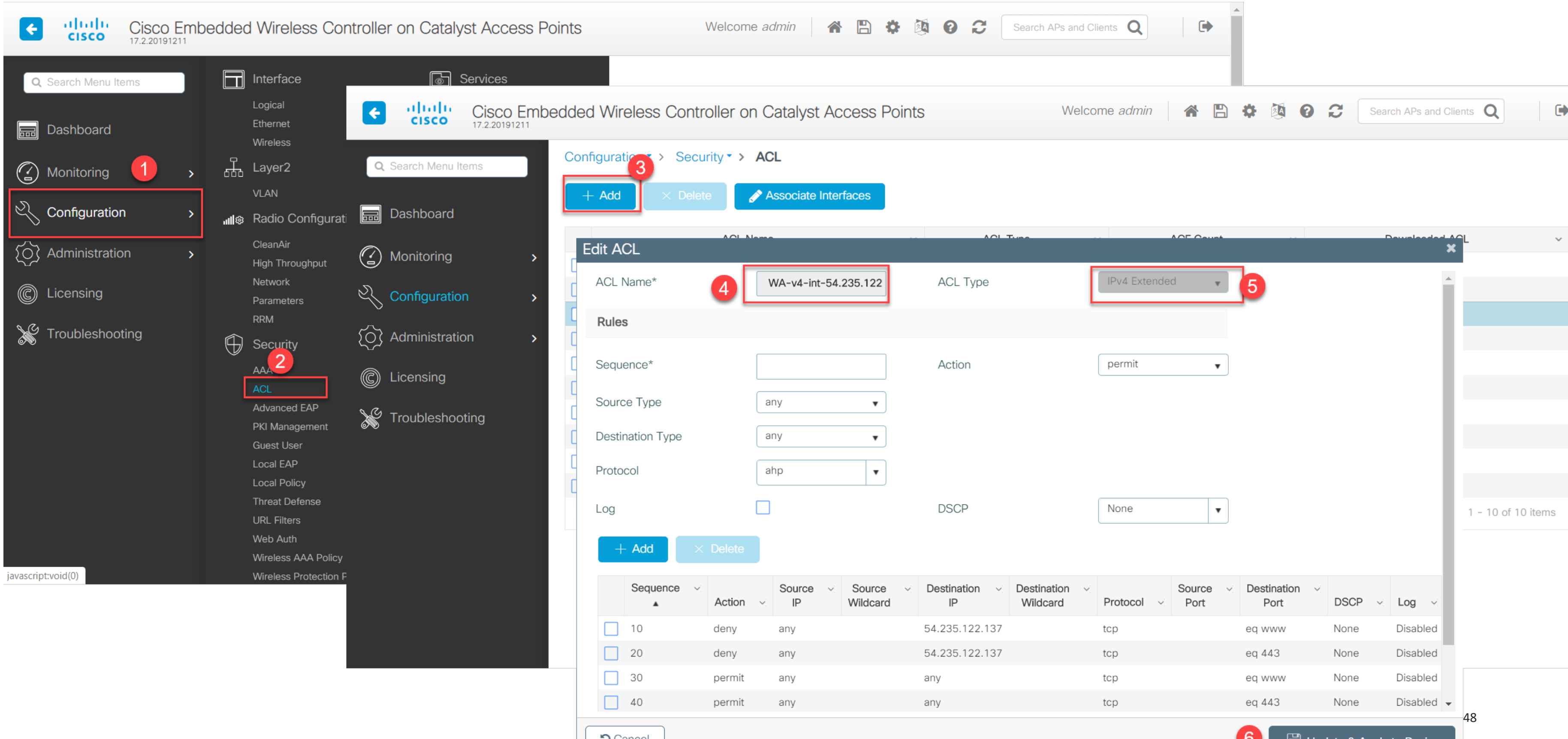
2. Apply ACL on AP



- ACL can be applied on WLAN (configured on Policy Profile)
- ACL can be applied on a VLAN (configured in flex connect profile)
- FlexConnect ACL support AAA-returned Client ACL

# Create Access Lists

## Configuration – Create IPv4 or Ipv6 ACL on WLC



Edit ACL

| | | | |
|---|---|---|---|
| ACL Name* | WA-v4-int-54.235.122 | ACL Type | IPv4 Extended |

Rules

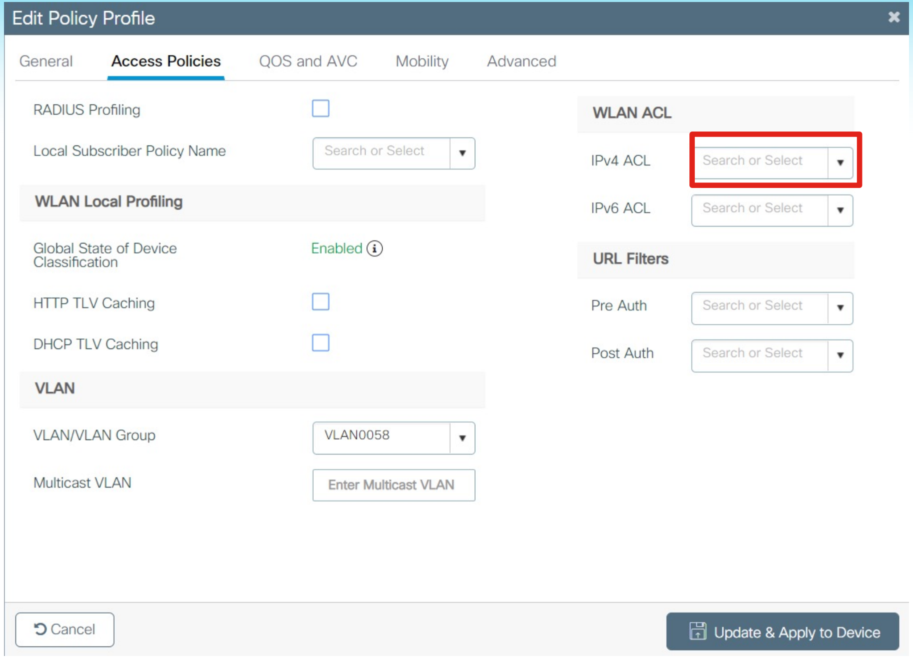
| | | | |
|---|---|---|---|
| Sequence* | | Action | permit |
| Source Type | any | | |
| Destination Type | any | | |
| Protocol | ahp | | |
| Log | □ | DSCP | None |

| | Sequence | Action | Source IP | Source Wildcard | Destination IP | Destination Wildcard | Protocol | Source Port | Destination Port | DSCP | Log |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 10 | deny | any | | 54.235.122.137 | | tcp | | eq www | None | Disabled |
| □ | 20 | deny | any | | 54.235.122.137 | | tcp | | eq 443 | None | Disabled |
| □ | 30 | permit | any | | any | | tcp | | eq www | None | Disabled |
| □ | 40 | permit | any | | any | | tcp | | eq 443 | None | Disabled |

# ACL – Policy Profile Mapping

- Configuration – Map it to the Policy Profile

- For the ACL to be applied the ACL needs to be downloaded to AP
- Any ACL mapped to Policy Profile mapped to wlan in the policy tag will be downloaded to AP Automatically



Edit Policy Profile

General | **Access Policies** | QOS and AVC | Mobility | Advanced

RADIUS Profiling □

Local Subscriber Policy Name: Search or Select ▾

**WLAN Local Profiling**

Global State of Device Classification: Enabled ⓘ

HTTP TLV Caching □

DHCP TLV Caching □

**VLAN**

VLAN/VLAN Group: VLAN0058 ▾

Multicast VLAN: Enter Multicast VLAN

**WLAN ACL**

IPv4 ACL: Search or Select ▾

IPv6 ACL: Search or Select ▾

**URL Filters**

Pre Auth: Search or Select ▾

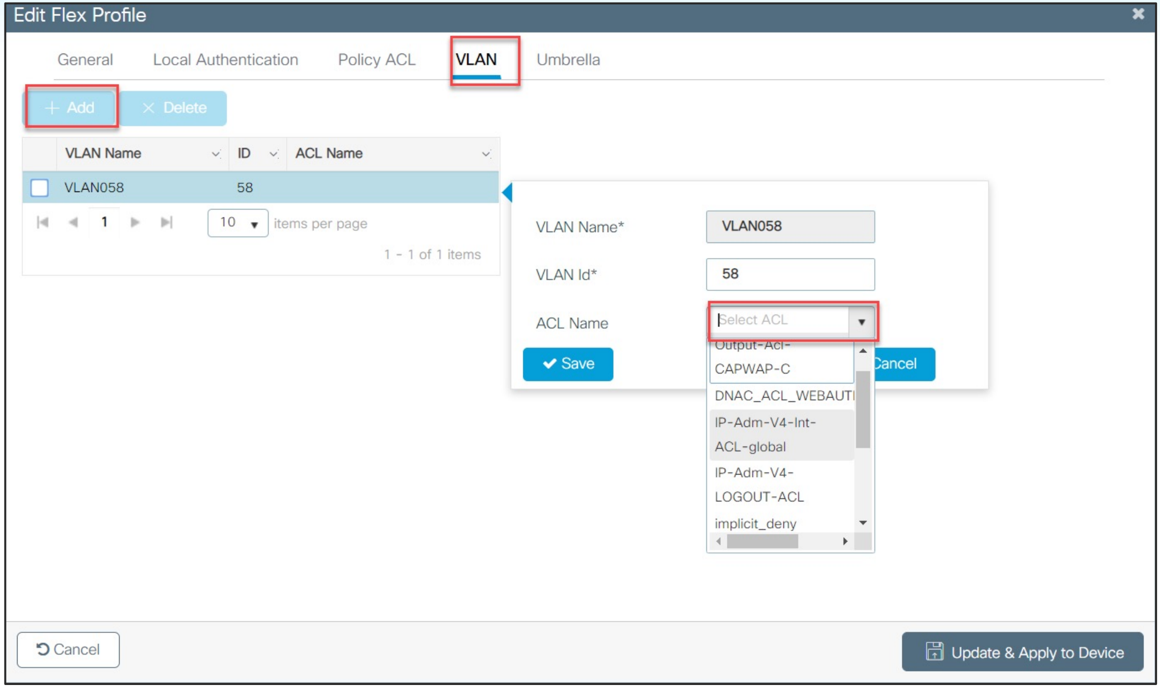
Post Auth: Search or Select ▾

# ACL – VLAN Mapping

- Configuration – Map it to the Flex Connect Profile on

- For the ACL to be applied the ACL needs to be downloaded to AP

- Any ACL mapped to VLANs on Flex connect profile will be downloaded to AP's in the flex connect profile Automatically



| | VLAN Name | ID | ACL Name |
|---|---|---|---|
| □ | VLAN058 | 58 | |

10 items per page

1 - 1 of 1 items

VLAN Name*: VLAN058

VLAN Id*: 58

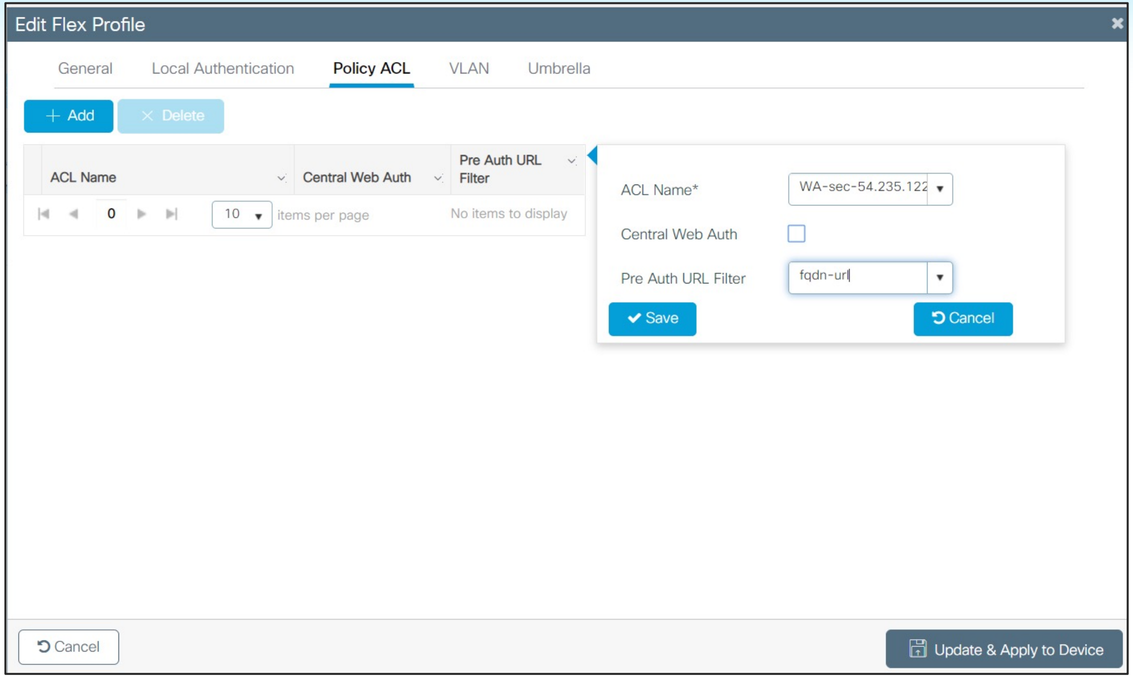
ACL Name: Select ACL

Output-Acl-CAPWAP-C
DNAC_ACL_WEBAUTI
IP-Adm-V4-Int-ACL-global
IP-Adm-V4-LOGOUT-ACL
implicit_deny

# Policy ACL

- For a AAA Override ACL to work on an AP in Flex Connect , the ACL should present  on AP

- The ACL is Provisioned on AP using the Flex Connect Profile
- This is done as part of Policy ACL configuration on Flex Profile
- MAP the ACL and optionally any PreAuth FQDN Filters as well to be downloaded to the AP
- If the ACL Used is a WebAuth ACL that is returned by AAA Check the “Central Web Auth”
- Central Web Auth indicates that deny to be used for redirect and Permit to Allow



| ACL Name | Central Web Auth | Pre Auth URL Filter |
|---|---|---|

0 | 10 items per page | No items to display

ACL Name*: WA-sec-54.235.122

Central Web Auth: □

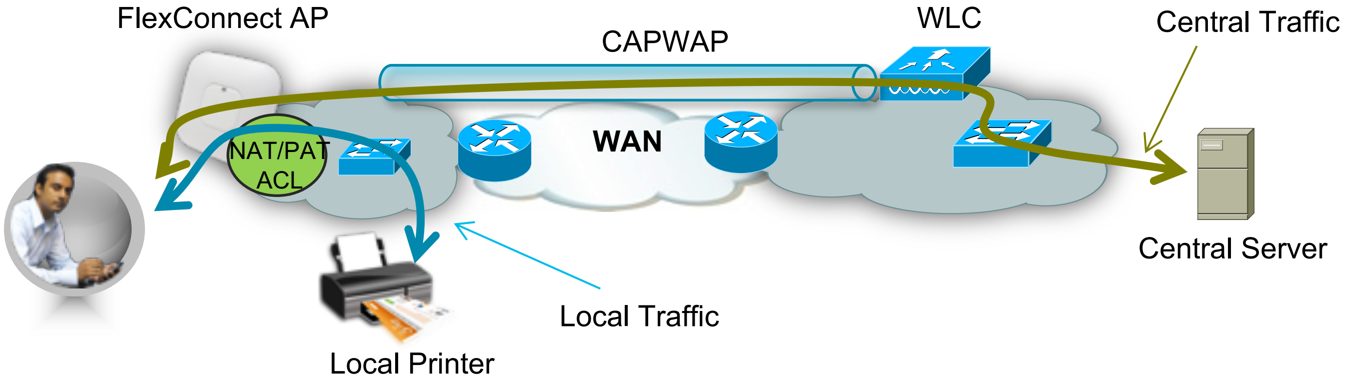
Pre Auth URL Filter: fqdn-url

# FlexConnect Split Tunneling (Using FlexConnect Split ACL)

# FlexConnect ACL – Split Tunneling

## Overview

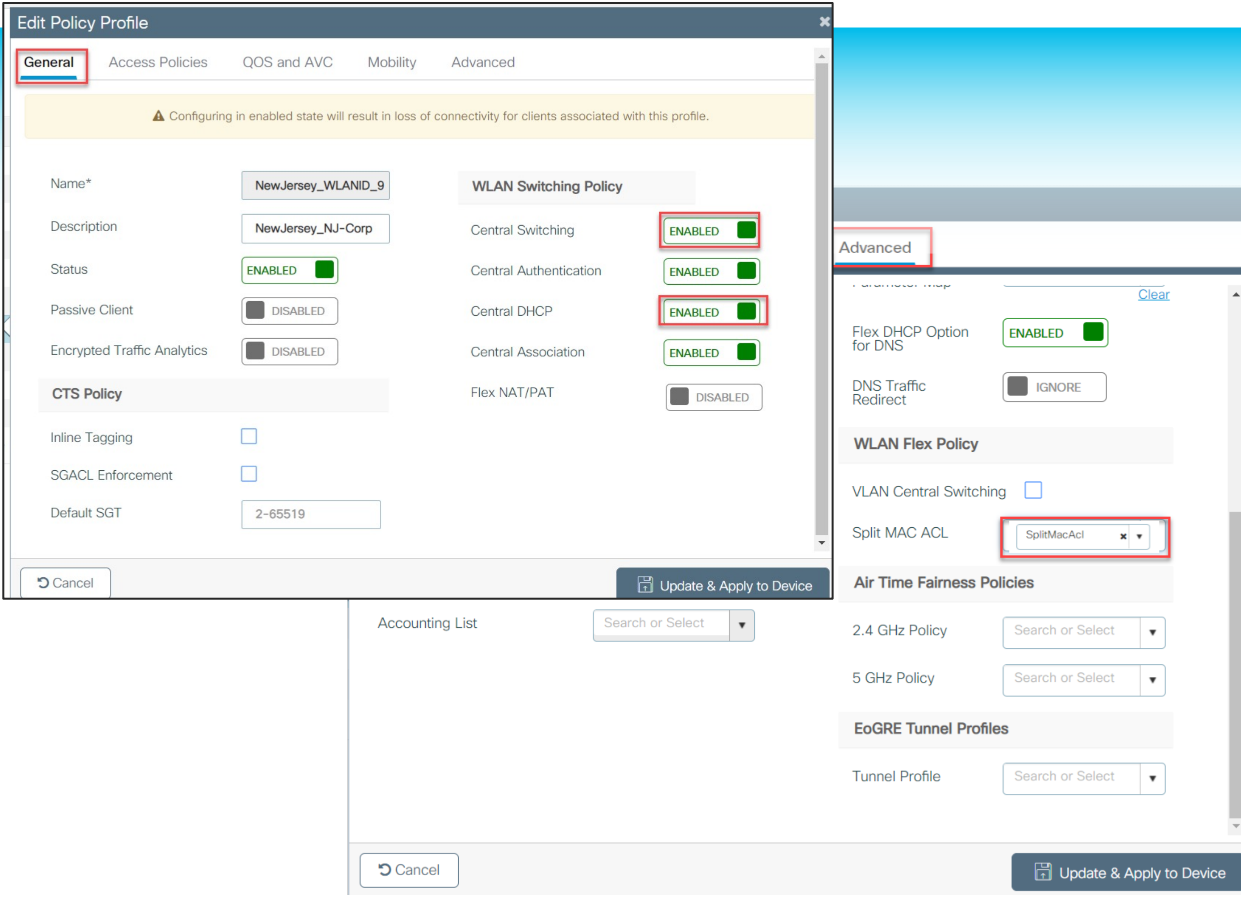
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP @ for the NAT/PAT feature



# FlexConnect ACL – Split Tunneling

## Configuration

- Create a centrally switched WLAN in policy Profile along with Central DHCP
- DHCP Required should be enabled
- Attach ACL in Policy Profile to match traffic to be locally switched
- Traffic Permitted will be switched locally
- Traffic Denied in ACL will be Switched Centrally



Edit Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

| | |
|---|---|
| Name* | NewJersey_WLANID_9 |
| Description | NewJersey_NJ-Corp |
| Status | ENABLED |
| Passive Client | DISABLED |
| Encrypted Traffic Analytics | DISABLED |

CTS Policy

| | |
|---|---|
| Inline Tagging | □ |
| SGACL Enforcement | □ |
| Default SGT | 2-65519 |

WLAN Switching Policy

| | |
|---|---|
| Central Switching | ENABLED |
| Central Authentication | ENABLED |
| Central DHCP | ENABLED |
| Central Association | ENABLED |
| Flex NAT/PAT | DISABLED |

| | |
|---|---|
| Flex DHCP Option for DNS | ENABLED |
| DNS Traffic Redirect | IGNORE |

WLAN Flex Policy

| | |
|---|---|
| VLAN Central Switching | □ |
| Split MAC ACL | SplitMacAcl |

Air Time Fairness Policies

| | |
|---|---|
| 2.4 GHz Policy | Search or Select |
| 5 GHz Policy | Search or Select |

EoGRE Tunnel Profiles

| | |
|---|---|
| Tunnel Profile | Search or Select |
| Accounting List | Search or Select |

# Влияние WAN каналов на работу БЛВС

# Flex Connect Design Considerations

## WAN Limitation 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 |

**It is highly recommended that the minimum bandwidth restriction remains 24 Kbps per AP with the round trip latency no greater than 300 ms for data deployments and 100 ms for Data + Voice deployments.**

# 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 ~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

**Goal is to minimize downloads over WAN**

# Efficient AP join (enabled by default) in flex connect profile

## Feature

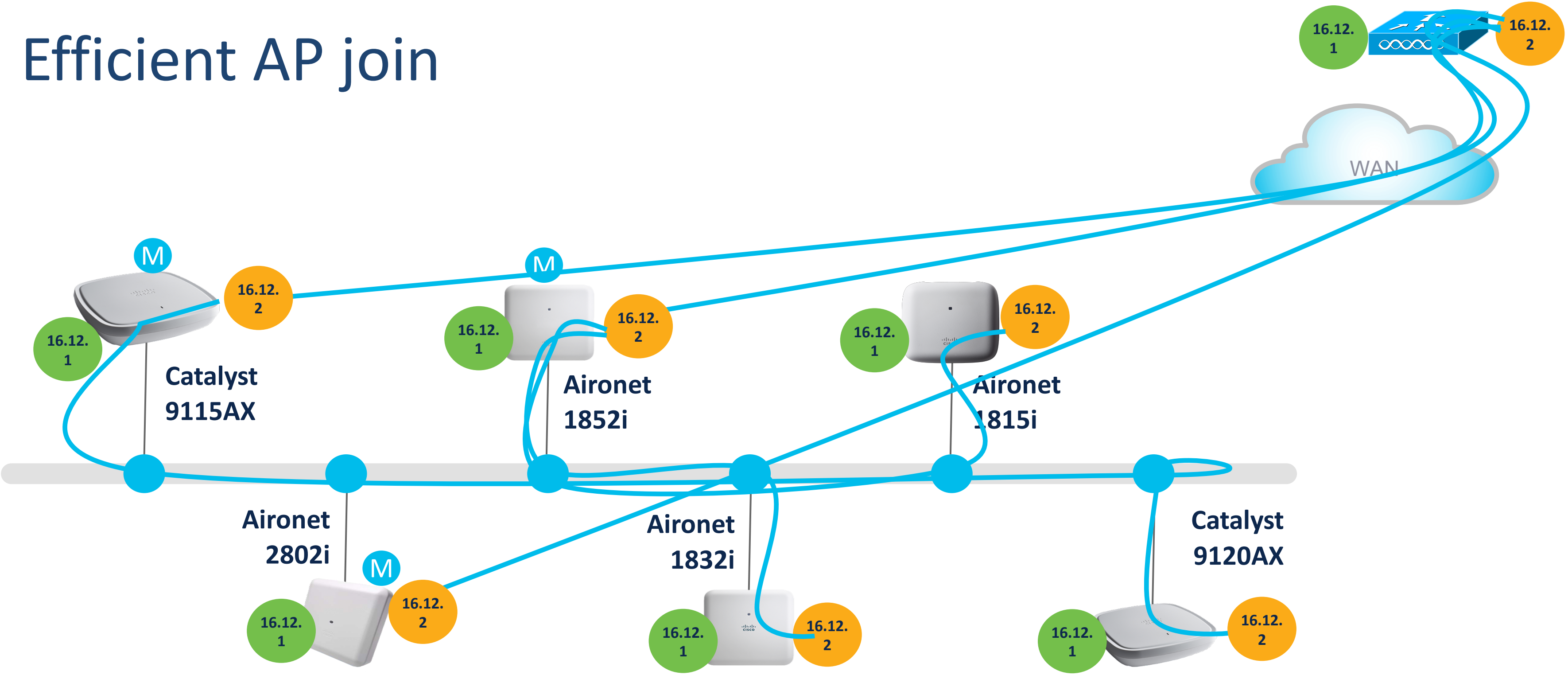
- Enables an CAPWAP to download the code from another AP in the network as long as **it is of the same AP family.**
- For example, If you add a 9120AX and a 9115AX is present, code will be downloaded from the 9115AX
- This feature minimizes the data sent on WAN at the time of AP join or AP Image Pre-download
- WLC elects a master AP in each FlexConnect Group for each Model /Type

## Supported AP models

- Supported on **all** 802.11ax and 802.11ac Wave 2 APs (indoor and outdoor)
- AP families sharing the same image:
  - ap3g3: Aironet® 4800, 3800, 2800, 1560 Series
  - ap1g5: Aironet 1815i, 1815w,1815m,1540, 1840 Series
  - ap1g4: Aironet 1852, 1832
  - ap1g7: Catalyst 9115AX, 9120AX Series
  - ap1g6: Catalyst 9117AX Series
  - ap1g6a: Catalyst 9130AX Series

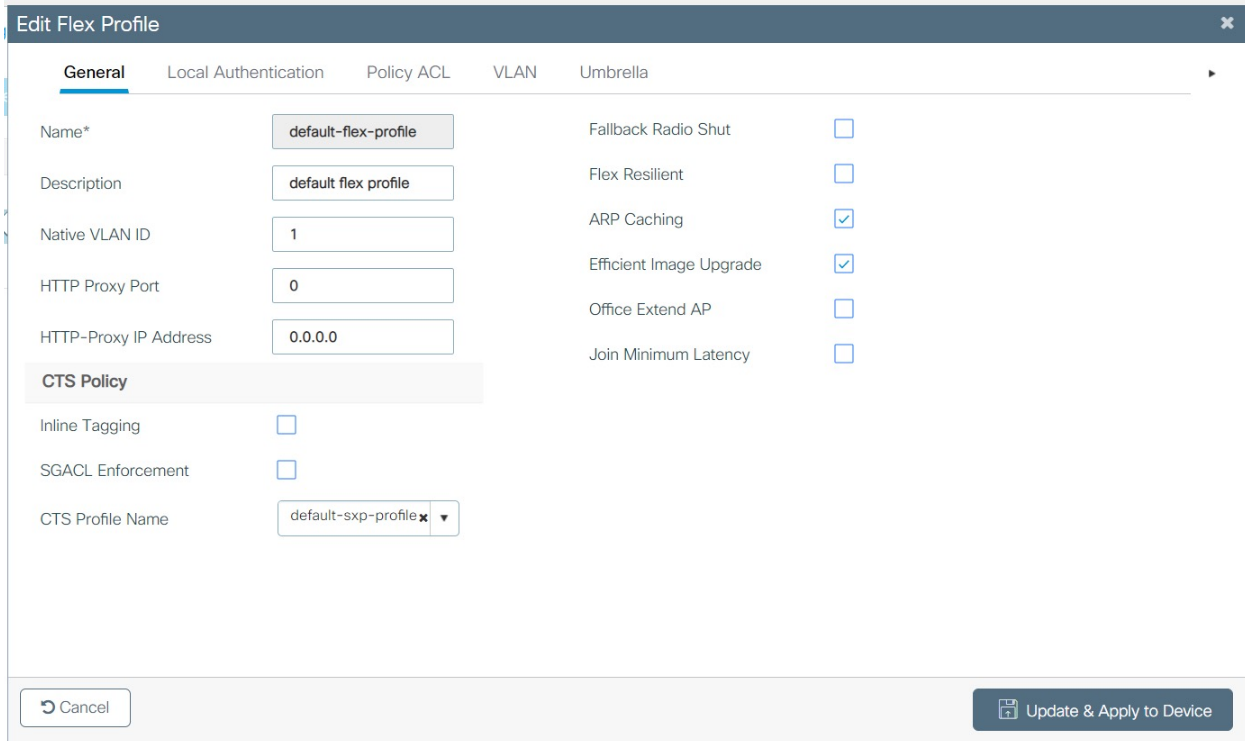
Not supported on Wave 1 APs

# Efficient AP join



**Works for all 802.11ax and 802.11ac Wave 2 APs**

# FlexConnect Efficient AP Image Upgrade



| | |
|---|---|
| Name* | default-flex-profile |
| Description | default flex profile |
| Native VLAN ID | 1 |
| HTTP Proxy Port | 0 |
| HTTP-Proxy IP Address | 0.0.0.0 |

**CTS Policy**

| | |
|---|---|
| Inline Tagging | ☐ |
| SGACL Enforcement | ☐ |
| CTS Profile Name | default-sxp-profile |

| | |
|---|---|
| Fallback Radio Shut | ☐ |
| Flex Resilient | ☐ |
| ARP Caching | ☑ |
| Efficient Image Upgrade | ☑ |
| Office Extend AP | ☐ |
| Join Minimum Latency | ☐ |

# Рекомендации

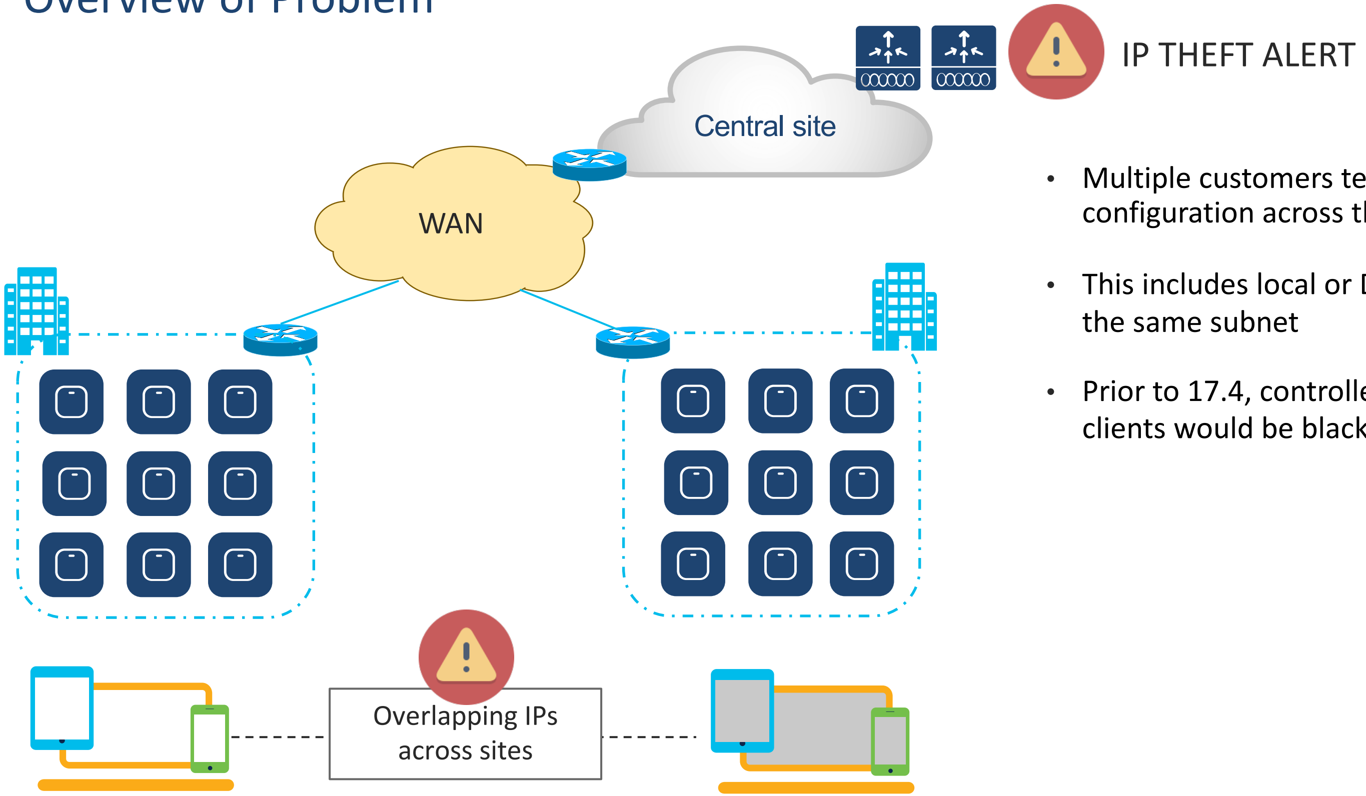
# FlexConnect Best Practices

- Enable FlexConnect Profile
- 802.11r/CCKM/OKC Key sharing for Voice deployments
- VLAN Support and configure Native VLAN at Group
- VLAN-WLAN Mappings at FlexConnect Profile
- VLAN Name override
- Consistent configuration across Primary and Backup WLCs
- Design for Resiliency
- Enable Efficient AP Image Upgrade

# FlexConnect IOS-XE Enhancements

# Overlapping IP across Flex sites

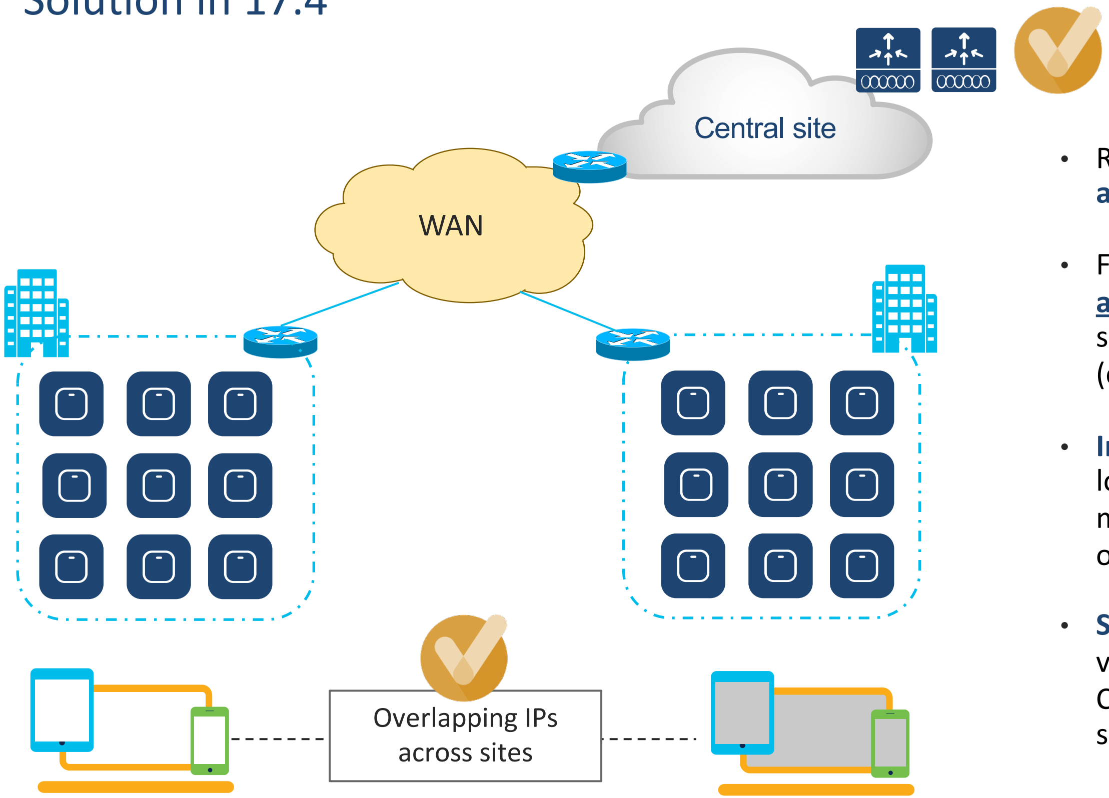
## Overview of Problem



- Multiple customers tend to use cookie cutter configuration across the sites and branches
- This includes local or DHCP servers configured with the same subnet
- Prior to 17.4, controller detected this is IP THEFT and clients would be blacklisted.

# Overlapping IP across Flex sites

## Solution in 17.4



- Release 17.4 adds support for **overlapping IP addresses** across different flex sites

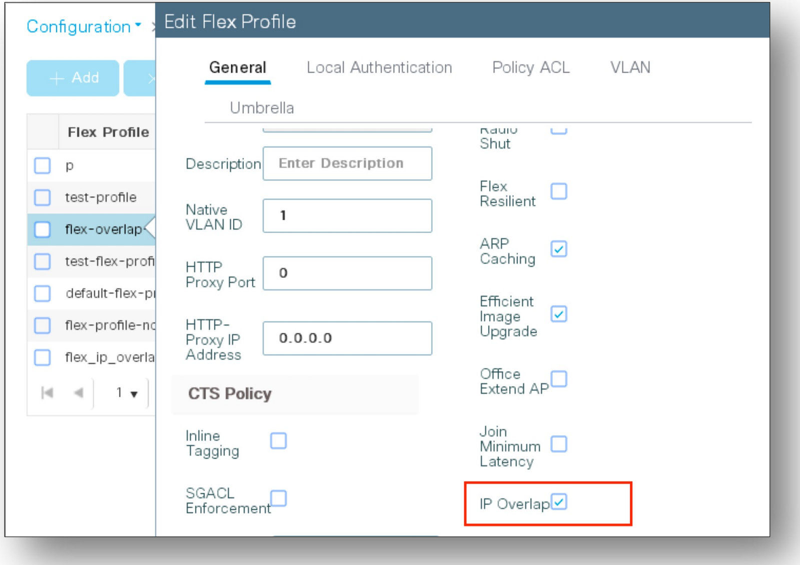
- For this to work, **every site needs to be assigned to a unique site-tag** > C9800 uses the combination of site-tag + IP address as a unique ID for the client (called zone-id)

- **Important**: this is only available for Flex local DHCP/ local switching; for all other deployments (local mode, central switching, central DHCP, etc.), overlapping IPs are still not supported

- **Supported on all C9800 appliances** (physical and virtual). Not supported on EWC on Catalyst AP and Catalyst 9k switch because these are meant for single site deployments.

# Configuration – IP Overlap

```
(config)#wireless profile flex flex1
(config-wireless-flex-profile)#ip overlap
```



Configuration

Flex Profile

- □ p
- □ test-profile
- □ flex-overlap
- □ test-flex-profi
- □ default-flex-pr
- □ flex-profile-nc
- □ flex_ip_overla

Edit Flex Profile

General | Local Authentication | Policy ACL | VLAN | Umbrella

Description: Enter Description

Native VLAN ID: 1

HTTP Proxy Port: 0

HTTP-Proxy IP Address: 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □

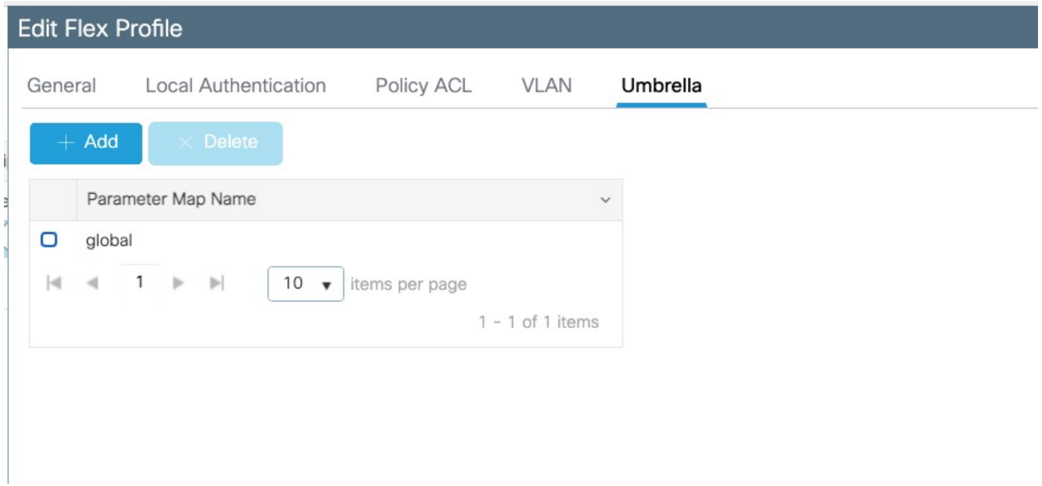
IP Overlap ☑

- Following configuration should be done to enable/disable feature.
- Flex local switching mode should also be enabled.

# FlexConnect and Umbrella

# Flexconnect - Umbrella

- Policy Profile
- Flex Profile – Enable Umbrella for Flex

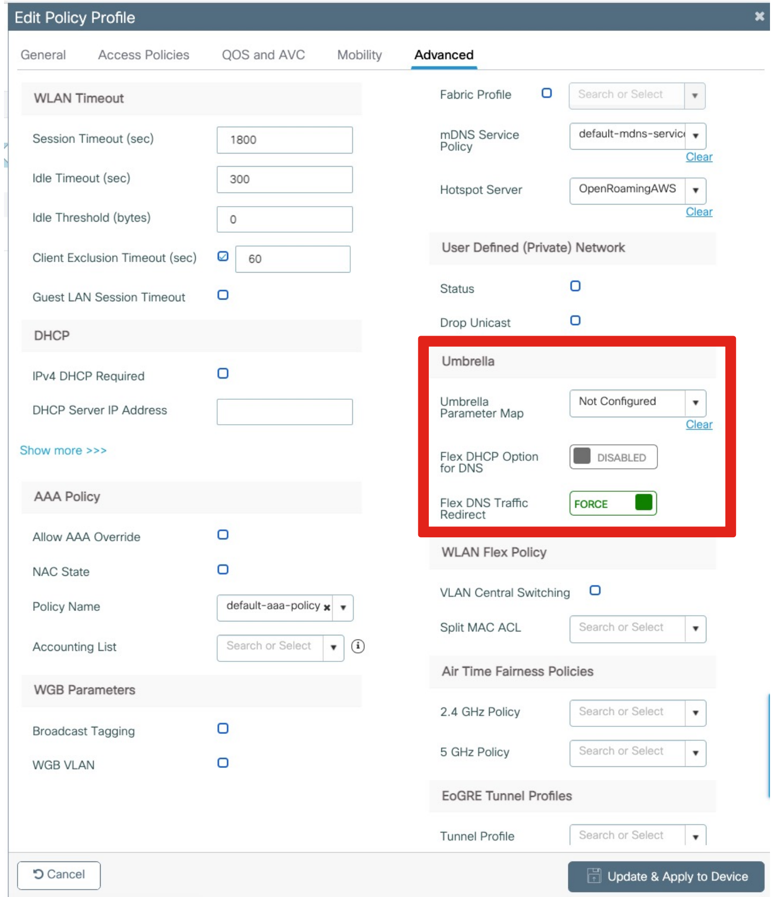


Edit Flex Profile

General | Local Authentication | Policy ACL | VLAN | **Umbrella**

|  | Parameter Map Name |
|---|---|
| □ | global |

1 - 1 of 1 items



Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | **Advanced**

**WLAN Timeout**

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

**DHCP**

IPv4 DHCP Required: □

DHCP Server IP Address:

Show more >>>

**AAA Policy**

Allow AAA Override: □

NAC State: □

Policy Name: default-aaa-policy ×

Accounting List: Search or Select

**WGB Parameters**

Broadcast Tagging: □

WGB VLAN: □

Fabric Profile: □ Search or Select

mDNS Service Policy: default-mdns-servic Clear

Hotspot Server: OpenRoamingAWS Clear

**User Defined (Private) Network**

Status: □

Drop Unicast: □

**Umbrella**

Umbrella Parameter Map: Not Configured Clear

Flex DHCP Option for DNS: DISABLED

Flex DNS Traffic Redirect: FORCE

**WLAN Flex Policy**

VLAN Central Switching: □

Split MAC ACL: Search or Select

**Air Time Fairness Policies**

2.4 GHz Policy: Search or Select

5 GHz Policy: Search or Select

**EoGRE Tunnel Profiles**

Tunnel Profile: Search or Select

# Заключение

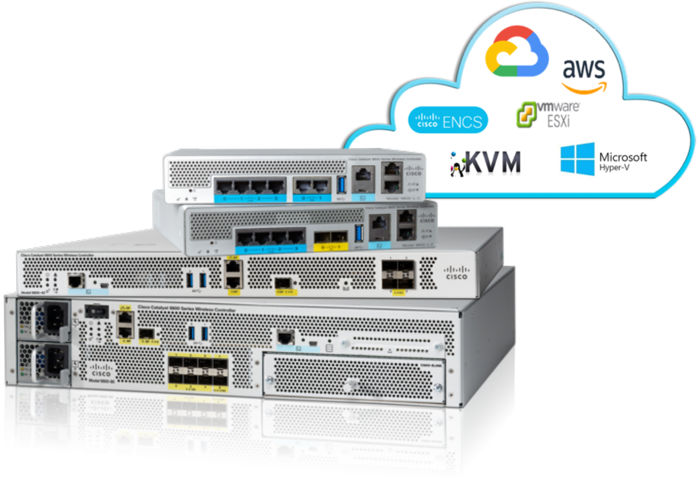
# Что нужно запомнить

Определите лучший для себя вариант внедрения филиальной сети

Максимум 100 ТД на Site Tag

Не забывайте о High Availability

Используйте сегментацию где требуется



# Полезные ссылки

Design and Deployment of Wireless for Branch and Remote Offices – BRKEWN-2016

Campus LAN and WLAN Solution Design CVD

C9800 Release Notes

C9800 Configuration Guides

C9800 Technical References

C9800 Configuration Examples and Tech Notes

C9800 Command References

C9800 Deployment Best Practices

C9800 WLC Configuration Model

WLC Configuration Converter

WLC Compatibility Matrix

AireOS to IOS-XE Command Mapping

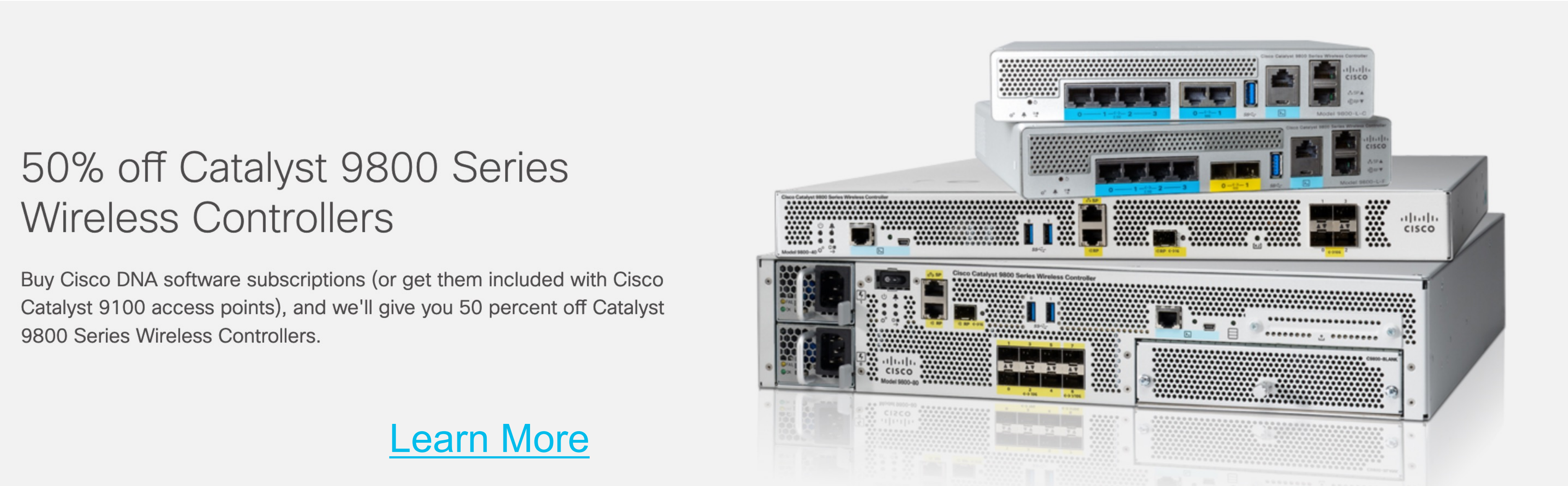
AireOS to C9800 Wireless Controller Feature Comparison Matrix

Understand FlexConnect on a 9800 WLC

Cisco Learning Partners

Cisco WLAN YouTube Channel

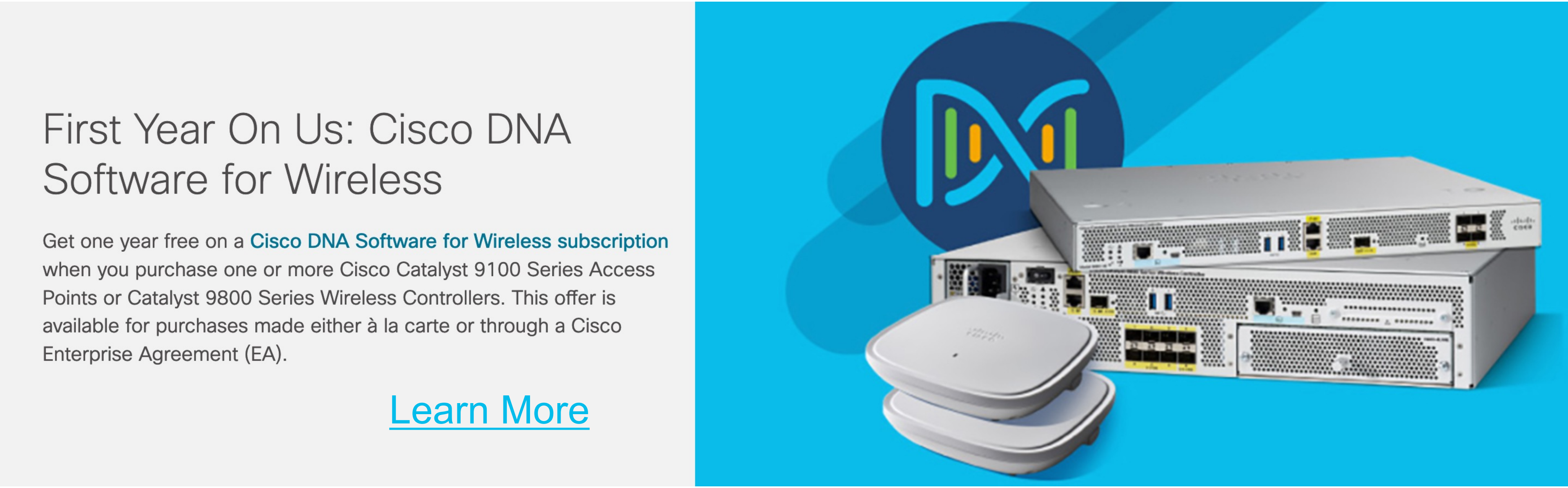
# Wireless Promotions



## 50% off Catalyst 9800 Series Wireless Controllers

Buy Cisco DNA software subscriptions (or get them included with Cisco Catalyst 9100 access points), and we'll give you 50 percent off Catalyst 9800 Series Wireless Controllers.

# Wireless Promotions



## First Year On Us: Cisco DNA Software for Wireless

Get one year free on a **Cisco DNA Software for Wireless subscription** when you purchase one or more Cisco Catalyst 9100 Series Access Points or Catalyst 9800 Series Wireless Controllers. This offer is available for purchases made either à la carte or through a Cisco Enterprise Agreement (EA).

Learn More

# Спасибо за внимание!