Guía de implementación del controlador de sucursal inalámbrico Flex 7500

Contenido

Introducción

Este documento describe cómo implementar un controlador de ramificación inalámbrico Cisco Flex 7500. El propósito de este documento es:

- Explique varios elementos de red de la solución Cisco FlexConnect, junto con su flujo de comunicación.
- Proporcione directrices generales de implementación para el diseño de la solución de sucursales inalámbricas Cisco FlexConnect.
- Explique las funciones de software de la versión de código 7.2.103.0 que refuerzan la base de información sobre el producto.

Nota: Antes de 7.2, FlexConnect se llamaba Hybrid REAP (HREAP). Ahora se denomina FlexConnect.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción general del producto

Figura 1: Cisco Flex 7500

El controlador de nube Cisco Flex serie 7500 es un controlador de sucursal altamente escalable

para implementaciones inalámbricas multisitio. Cisco Flex 7500 Series Controller, implementado en la nube privada, amplía los servicios inalámbricos a las sucursales distribuidas con un control centralizado que reduce el coste total de las operaciones.

Cisco Flex serie 7500 (Figura 1) puede gestionar puntos de acceso inalámbricos en hasta 500 sucursales y permite a los administradores de TI configurar, administrar y solucionar problemas de hasta 3000 puntos de acceso (AP) y 30 000 clientes del Data Center. El controlador Cisco Flex serie 7500 admite acceso seguro para invitados, detección no autorizada para el cumplimiento de la normativa de la industria de tarjetas de pago (PCI) y voz y vídeo Wi-Fi en la sucursal (conmutados localmente).

Esta tabla destaca las diferencias de escalabilidad entre el controlador Flex 7500, WiSM2 y WLC 5500:

Escalabilidad	Flex 7500	WiSM2	WLC 5500
Puntos de acceso totales	6,000	1000	500
Clientes totales	64,000	15,000	7,000
Máximo de grupos FlexConnect	2000	100	100
Número máximo de puntos de acceso por grupo FlexConnect	100	25	25
Máximo de grupos de puntos de acceso	6000	1000	500

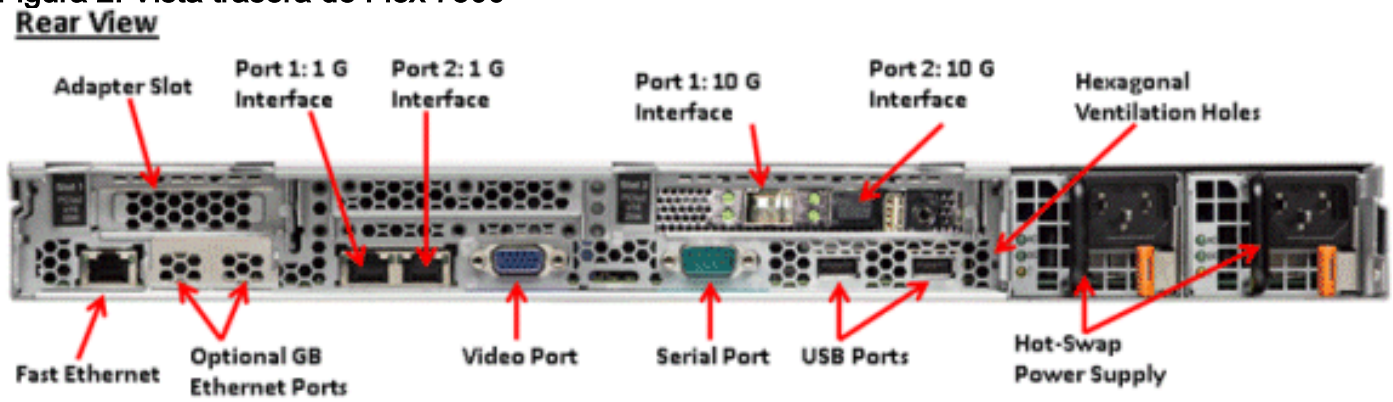
Especificaciones del producto

Ficha técnica

Consulte http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html.

Característica de la plataforma

Figura 2: Vista trasera de Flex 7500



Puertos de interfaz de red

Puertos de	Uso

interfaz	
Fast Ethernet	Módulo de gestión integrada (IMM)
Port 1: 1 G	Puerto de servicio WLC
Port 2: 1 G	Puerto redundante WLC (RP)
Port 1: 10G	Interfaz de administración de WLC
Port 2: 10G	Puerto de Interfaz de Administración de Respaldo WLC (Fallo de Puerto)
Puertos Ethernet Gb opcionales	N/A

Nota:

- La compatibilidad con LAG para interfaces 2x10G permite el funcionamiento de link activo-activo con redundancia de link de failover rápido. Un enlace activo adicional de 10 G con LAG no cambia el rendimiento inalámbrico del controlador.
- 2 interfaces de 10 G
- Las interfaces 2x10G sólo admiten cables ópticos con el producto SFP N.º SFP-10G-SR.
- Switch side SFP Product # X2-10GB-SR

Direcciones MAC del sistema

Port 1: 10 G (interfaz de gestión)	Dirección MAC del sistema/base
Port 2: 10G(Interfaz de administración de copias de seguridad)	Dirección MAC base + 5
Port 1: 1G (puerto de servicio)	Dirección MAC base + 1
Port 2: 1G (puerto redundante)	Dirección MAC base + 3

Redirección de consola serie

El WLC 7500 habilita la redirección de la consola de forma predeterminada a la velocidad en baudios de 9600, simulando el terminal Vt100 sin control de flujo.

Información de inventario

Figura 3: Consola WLC 7500

```
(Cisco Controller) >show inventory

Burned-in MAC Address.......................... E4:1F:13:65:DB:6C
Maximum number of APs supported................ 2000
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: AIR-CT7510-K9,  VID: V01,  SN: KQZZXWL
```

La tabla Interfaz de administración de escritorios (CSI) contiene información de BIOS y hardware de servidor.

El WLC 7500 muestra la versión del BIOS, PID/VID y el número de serie como parte del inventario.

Arranque Flex 7500

Las opciones del cargador de arranque de Cisco para el mantenimiento del software son idénticas a las plataformas de controlador existentes de Cisco.

Figura 4: Orden de arranque

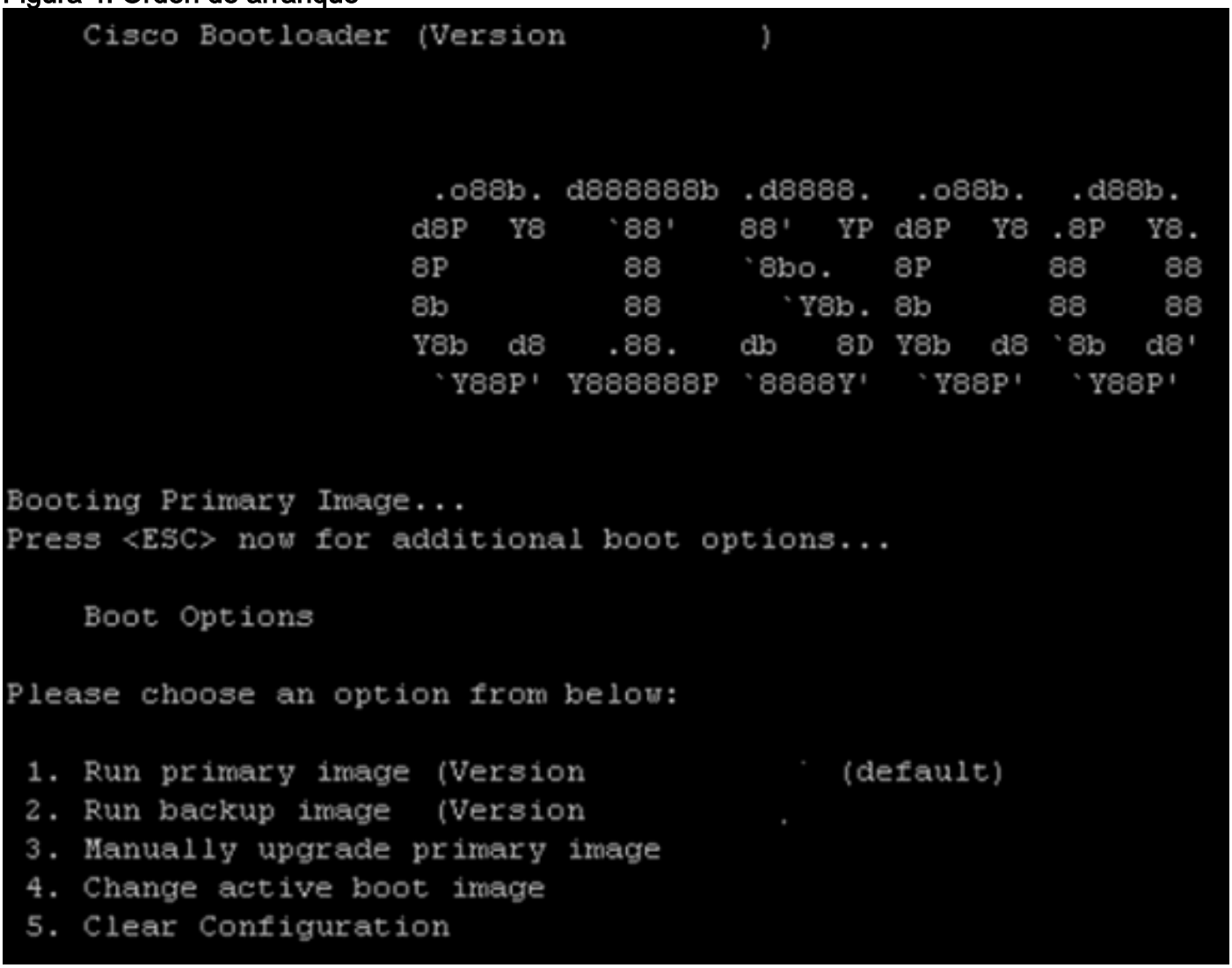


Figura 5: Asistente de configuración WLC

```
Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password                  : *******

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```


Nota: La secuencia de arranque Flex 7500 es equivalente y coherente con las plataformas de controlador existentes. El inicio inicial requiere la configuración del WLC mediante el asistente.

Licencias de Flex 7500

Licencias de recuento de base de AP

SKU de recuento de base de puntos de acceso
300

500
1000
2000
3000
6000

Licencias de actualización de AP

SKU de actualización de PA
100
250
500
1000

A excepción de los conteos de base y actualización, todo el procedimiento de licencia que cubre pedidos, instalación y visualización es similar al WLC 5508 existente de Cisco.

Refiérase a la guía de configuración de WLC 7.3, que cubre todo el procedimiento de licencia.

Soporte de la versión de software

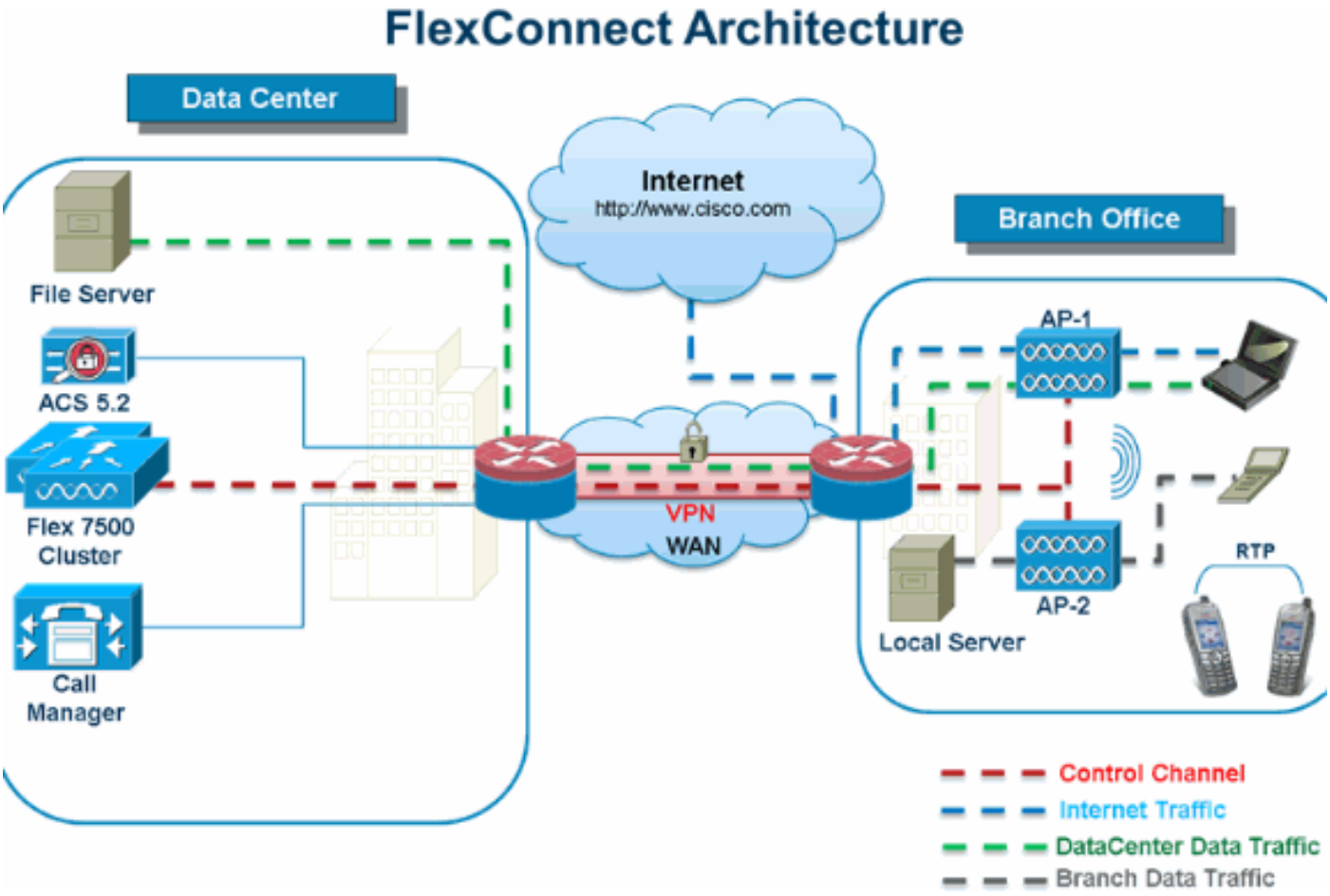
El Flex 7500 soporta solamente la versión 7.0.116.x del código WLC y posterior.

Puntos de acceso admitidos

Puntos de acceso 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 e ISR 881 son compatibles con Flex 7500.

Arquitectura FlexConnect

Figura 6: Topología típica de sucursal inalámbrica



FlexConnect es una solución inalámbrica para implementaciones en sucursales y oficinas remotas. También se denomina solución Híbrida REAP, pero en este documento se hace referencia a ella como FlexConnect.

La solución FlexConnect permite al cliente:

- Centralice el control y la gestión del tráfico de los AP desde el Data Center.El tráfico de control está marcado por guiones rojos en la Figura 6.
- Distribuya el tráfico de datos del cliente en cada sucursal.El tráfico de datos se marca con guiones azul, verde y púrpura en la Figura 6.Cada flujo de tráfico va a su destino final de la manera más eficiente.

Ventajas de Centralizar el Tráfico de Control de Punto de Acceso

- Un único panel de supervisión y solución de problemas
- Facilidad de gestión
- Acceso móvil seguro y sin problemas a los recursos del Data Center
- Reducción del espacio físico de las sucursales
- Aumento del ahorro operativo

Ventajas de la distribución del tráfico de datos del cliente

- Sin tiempo de inactividad operativo (supervivencia) frente a fallos completos de enlaces WAN o falta de disponibilidad del controlador
- Resistencia de la movilidad dentro de la sucursal durante fallos de enlaces WAN

- Aumento de la escalabilidad de las sucursales. Admite el tamaño de la sucursal que puede ampliarse hasta 100 AP y 250 000 pies cuadrados (5000 pies cuadrados). pies por AP).

La solución Cisco FlexConnect también es compatible con el tráfico de datos de clientes centrales, pero debe limitarse únicamente al tráfico de datos de invitados. En esta tabla siguiente se describen las restricciones de los tipos de seguridad WLAN L2 sólo para clientes no invitados cuyo tráfico de datos también se conmuta centralmente en el Data Center.

Soporte de seguridad L2 para usuarios no invitados conmutados centralmente

Seguridad WLAN L2	Tipo	Resultado
Ninguno	N/A	Permitido
WPA + WPA2	802.1x	Permitido
	CCKM	Permitido
	802.1x + CCKM	Permitido
	PSK	Permitido
802.1x	WEP	Permitido
WEP estática	WEP	Permitido
WEP + 802.1x	WEP	Permitido
CKIP		Permitido

Nota: Estas restricciones de autenticación no se aplican a clientes cuyo tráfico de datos se distribuye en la sucursal.

Soporte de seguridad L3 para usuarios conmutados centralmente y localmente

Seguridad WLAN L3	Tipo	Resultado
Autenticación Web	Interno	Permitido
	Externo	Permitido
	Personalizado	Permitido
Paso a través de la Web	Interno	Permitido
	Externo	Permitido
	Personalizado	Permitido
Redirección web condicional	Externo	Permitido
Redirección web de la página Splash	Externo	Permitido

Para obtener más información sobre la implementación de WebAuth externa de Flexconnect, consulte la Guía de implementación de WebAuth Externa de Flexconnect

Para obtener más información sobre los estados de HREAP/FlexConnect AP y las opciones de switching del tráfico de datos, consulte Configuración de FlexConnect.

Modos de funcionamiento de FlexConnect

Modo	Descripción

FlexConnect	
Conectado	Se dice que FlexConnect se encuentra en modo conectado cuando su plano de control CAPWAP de vuelta al controlador está activo y en funcionamiento, lo que significa que el link WAN no está inactivo.
Independiente	El modo autónomo se especifica como el estado operativo en el que entra FlexConnect cuando ya no tiene la conectividad de vuelta al controlador. Los AP FlexConnect en modo autónomo seguirán funcionando con la última configuración conocida, incluso en caso de fallo de alimentación y falla de WLC o WAN.

Para obtener más información sobre la teoría de operaciones de FlexConnect, consulte la Guía de diseño e implementación de H-Reap / FlexConnect.

Requisitos de WAN

Los puntos de acceso FlexConnect se implementan en el sitio de la sucursal y se administran desde el Data Center a través de un enlace WAN. Se recomienda encarecidamente que la restricción mínima de ancho de banda siga siendo de 12,8 kbps por AP, con una latencia de ida y vuelta no superior a 300 ms para implementaciones de datos y 100 ms para implementaciones de datos y voz. La unidad máxima de transmisión (MTU) debe tener al menos 500 bytes.

Tipo de implementación	Ancho de banda WAN (mín.)	Latencia de RTT de WAN (máx.)	Máximo de puntos de acceso por sucursal	Clientes máximos por sucursal
Datos	64 kbps	300 m	5	25
Datos + Voz	128 kbps	100 m	5	25
Monitor	64 kbps	2 seg.	5	N/A
Datos	640 kbps	300 m	50	1000
Datos + Voz	1.44 Mbps	100 m	50	1000
Monitor	640 kbps	2 seg.	50	N/A

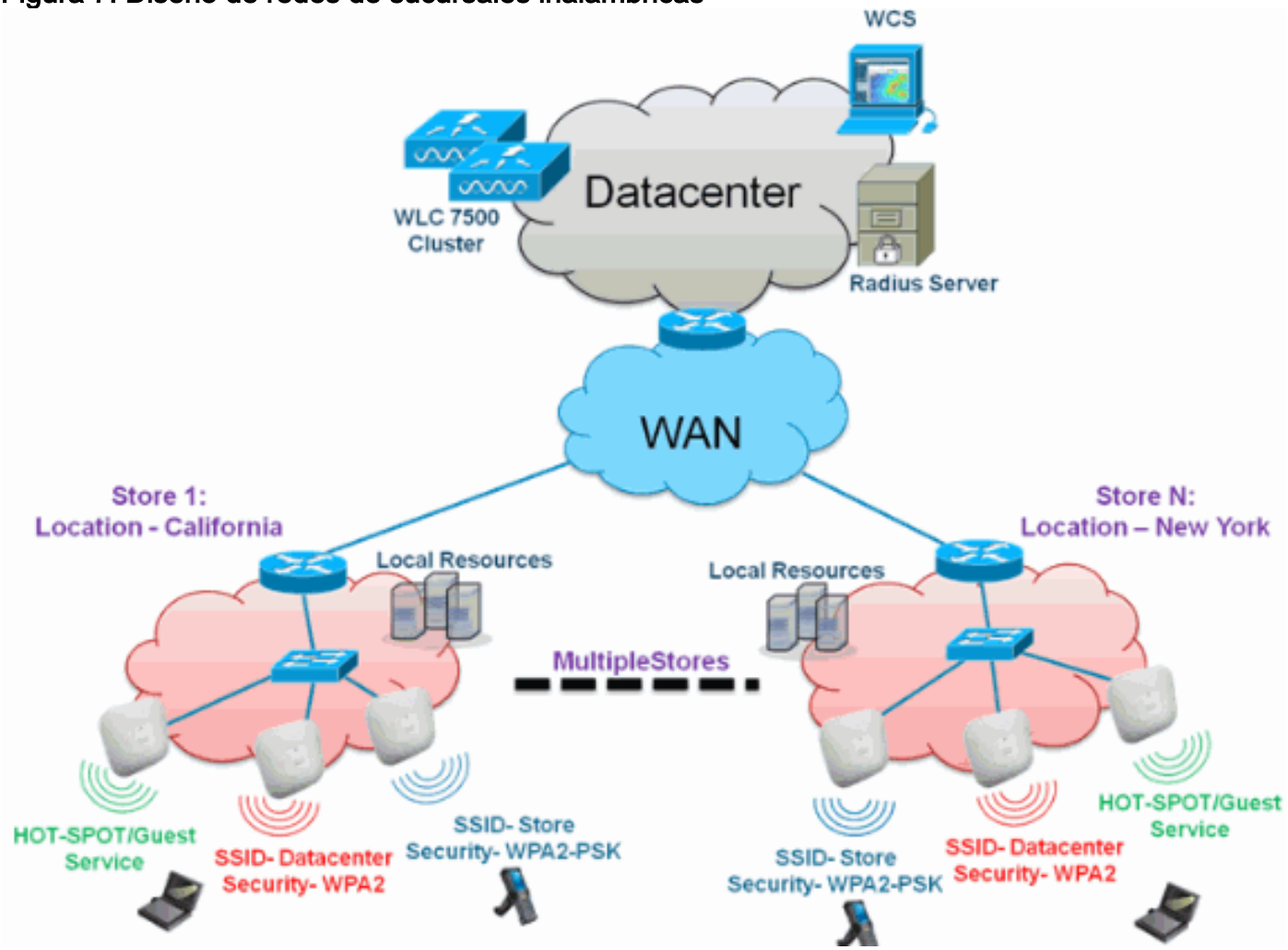
Diseño de redes de sucursales inalámbricas

El resto de este documento destaca las directrices y describe las mejores prácticas para implementar redes de sucursales distribuidas seguras. Se recomienda la arquitectura FlexConnect para redes de sucursales inalámbricas que cumplan estos requisitos de diseño.

Requisitos de diseño principales

- Tamaño de la sucursal que puede ampliarse hasta 100 puntos de acceso y 250 000 pies cuadrados (5000 pies cuadrados). pies por AP)
- Gestión central y resolución de problemas
- Sin tiempo de inactividad operativo
- Segmentación del tráfico basada en el cliente
- Conectividad inalámbrica segura y fluida a los recursos corporativos
- Compatible con PCI
- Soporte para invitados

Figura 7: Diseño de redes de sucursales inalámbricas



Overview

A los clientes de las sucursales les resulta cada vez más difícil y costoso ofrecer servicios de red seguros y escalables con todas las funciones en todas las ubicaciones geográficas. Para ayudar a los clientes, Cisco está haciendo frente a estos retos mediante la introducción de Flex 7500.

La solución Flex 7500 virtualiza las complejas operaciones de seguridad, gestión, configuración y solución de problemas del Data Center y, a continuación, extiende estos servicios de forma transparente a cada sucursal. Las implementaciones que utilizan Flex 7500 son más fáciles de configurar, gestionar y, lo que es más importante, escalar para el departamento de TI.

Ventajas

- Aumente la escalabilidad con compatibilidad con 6000 puntos de acceso
- Mayor resistencia gracias a la tolerancia a fallos de FlexConnect
- Aumentar la segmentación del tráfico mediante FlexConnect (switching central y local)
- Facilidad de gestión al replicar los diseños de las tiendas mediante grupos de puntos de acceso y grupos de FlexConnect.

Funciones que abordan el diseño de redes de sucursales

El resto de las secciones de la guía capturan el uso de la función y las recomendaciones para realizar el diseño de red que se muestra en la Figura 7.

Funciones:

Características principales	Aspectos destacados
Grupos de AP	Proporciona facilidad operativa/de gestión al gestionar varias sucursales. Además, ofrece la flexibilidad de replicar configuraciones para sucursales similares.
Grupos de FlexConnect	Los grupos FlexConnect proporcionan la funcionalidad de RADIUS de copia de seguridad local, itinerancia rápida CCKM/OKC y autenticación local.
Tolerancia de fallas	Mejora la resistencia de la sucursal inalámbrica y no ofrece tiempo de inactividad operativo.
ELM (modo local mejorado para wIPS adaptable)	Proporcione la funcionalidad wIPS adaptable cuando atienda a clientes sin ningún impacto en el rendimiento del cliente.
Límite de cliente por WLAN	Limitación del número total de clientes invitados en la red de la sucursal.
Descarga previa a la imagen de AP	Reduce el tiempo de inactividad al actualizar su sucursal.
Conversión automática de puntos de acceso en FlexConnect	Funcionalidad para convertir automáticamente los AP en FlexConnect para su sucursal.
Acceso de invitado	Continúe con la arquitectura de acceso de invitado de Cisco existente con FlexConnect.

Matriz de Soporte de IPv6

Funciones	Conmutado centralmente		Conmutado localmente	
	5500/WiSM-2	Flex 7500	5500/WiSM-2	Flex 7500
IPv6 (movilidad del cliente)	Supported	Not Supported	Not Supported	Not Supported
Protección de RA IPv6	Supported	Supported	Supported	Supported
Protección DHCP IPv6	Supported	Not Supported	Not Supported	Not Supported
Protección de origen IPv6	Supported	Not Supported	Not Supported	Not Supported
Regulación de RA / Límite de velocidad	Supported	Not Supported	Not Supported	Not Supported
ACL IPv6	Supported	Not Supported	Not Supported	Not Supported
Visibilidad del cliente IPv6	Supported	Not Supported	Not Supported	Not Supported
Almacenamiento en caché de detección de vecino IPv6	Supported	Not Supported	Not Supported	Not Supported
Puente IPv6	Supported	Not Supported	Supported	Supported

Matriz de características

Consulte Matriz de funciones de FlexConnect para obtener una matriz de características para la función FlexConnect.

Grupos de AP

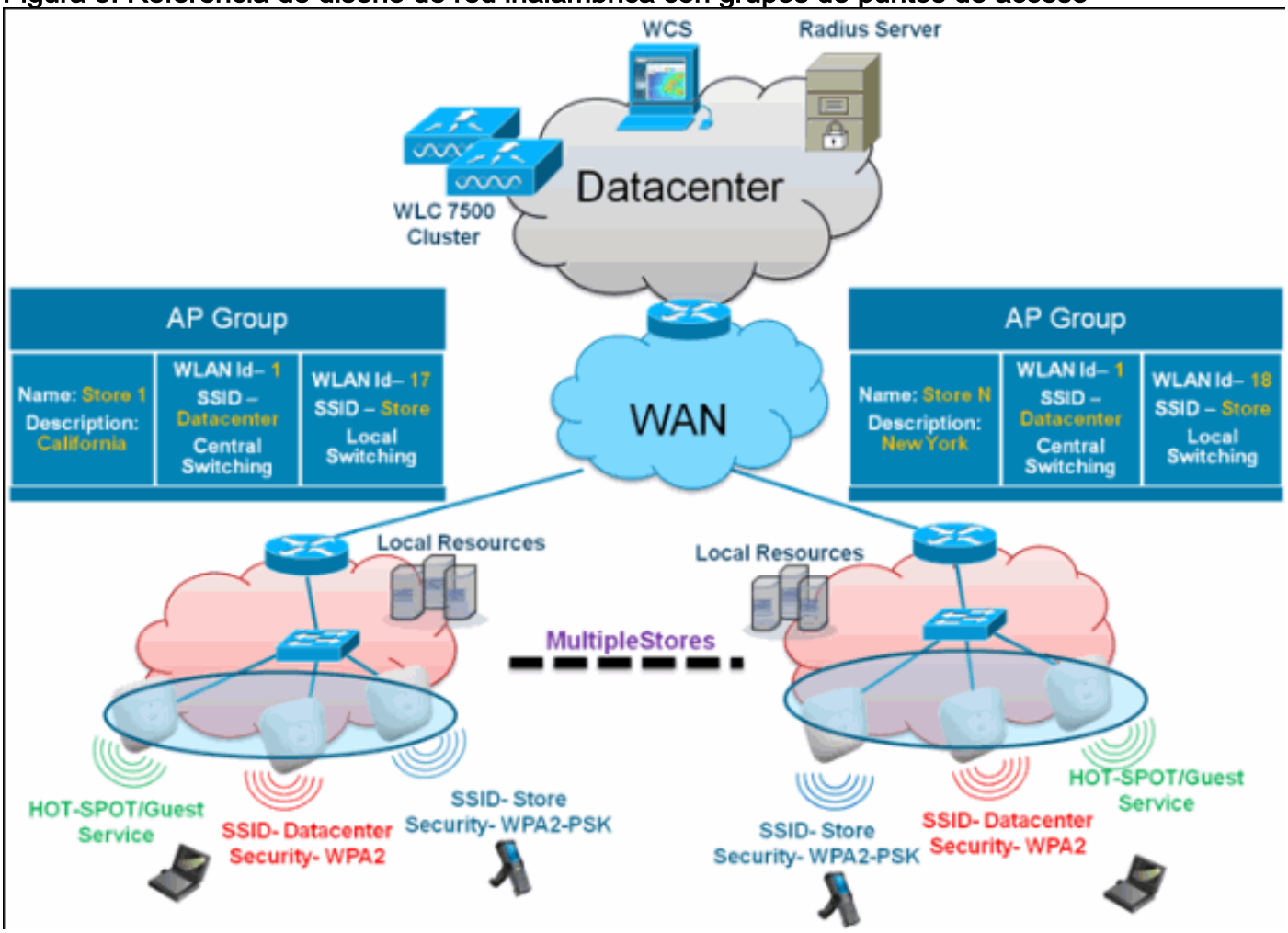
Después de crear WLAN en el controlador, puede publicarlas selectivamente (usando grupos de puntos de acceso) en diferentes puntos de acceso para gestionar mejor su red inalámbrica. En una implementación típica, todos los usuarios en una WLAN se asignan a una sola interfaz en el controlador. Por lo tanto, todos los usuarios asociados con esa WLAN están en la misma subred o VLAN. Sin embargo, puede optar por distribuir la carga entre varias interfaces o a un grupo de usuarios según criterios específicos, como departamentos individuales (como marketing, ingeniería o operaciones), creando grupos de puntos de acceso. Además, estos grupos de puntos

de acceso se pueden configurar en VLAN separadas para simplificar la administración de la red.

Este documento utiliza grupos AP para simplificar la administración de la red cuando se administran varios almacenes a través de ubicaciones geográficas. Para facilitar el funcionamiento, el documento crea un grupo AP por almacén para satisfacer estos requisitos:

- SSID **Datacenter** conmutado centralmente en todas las tiendas para el acceso administrativo de Local Store Manager.
- **Almacén** de SSID conmutado localmente con diferentes claves WPA2-PSK en todas las tiendas para los escáneres portátiles.

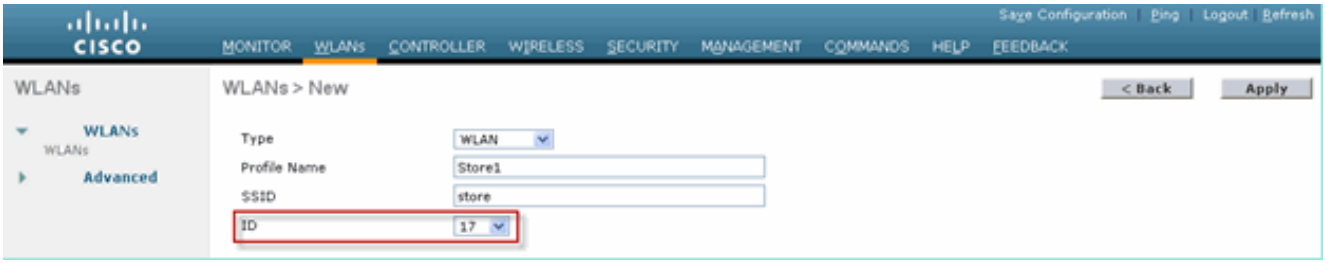
Figura 8: Referencia de diseño de red inalámbrica con grupos de puntos de acceso



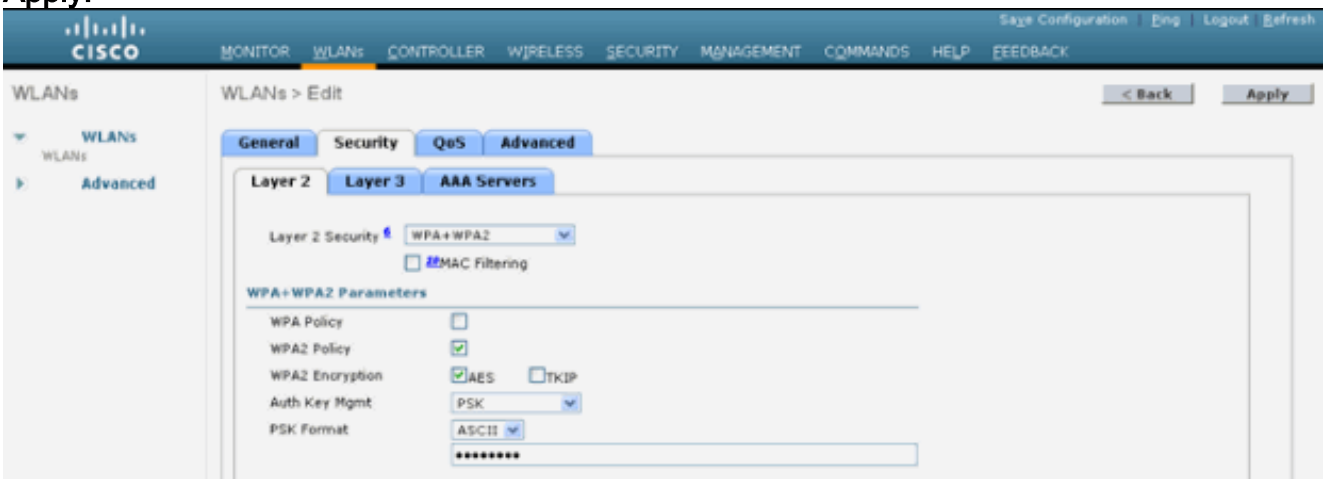
Configuraciones de WLC

Complete estos pasos:

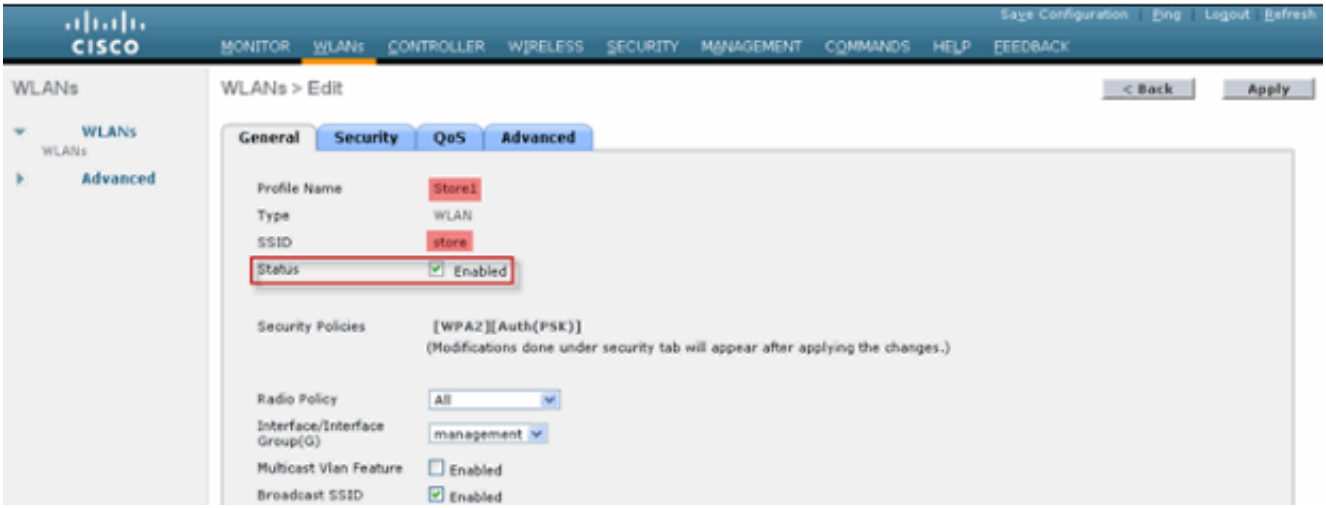
1. En la página WLANs > New, ingrese **Store1** en el campo Profile Name, ingrese **store** en el campo SSID y elija **17** en la lista desplegable ID.**Nota:** Los ID de WLAN 1-16 son parte del grupo predeterminado y no se pueden eliminar. Para satisfacer nuestro requisito de utilizar el mismo almacén SSID por tienda con un WPA2-PSK diferente, necesita utilizar el ID de WLAN 17 y posterior porque no forman parte del grupo predeterminado y pueden limitarse a cada
tienda.



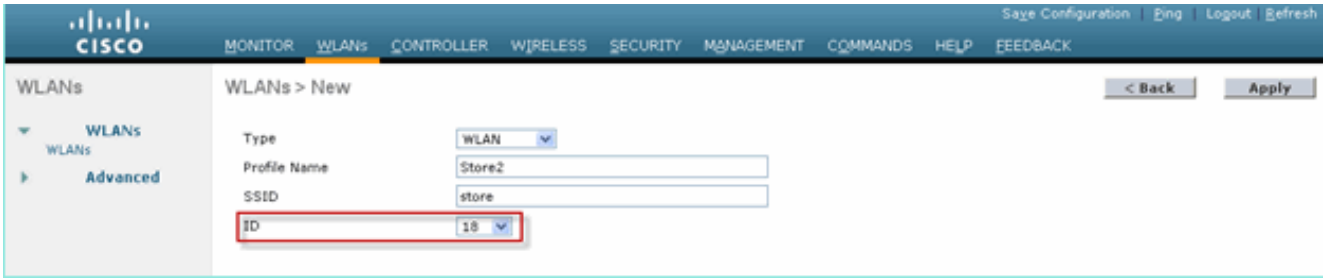
2. En WLAN > Security, elija **PSK** en la lista desplegable Auth Key Mgmt, elija **ASCII** en la lista desplegable PSK Format y haga clic en **Apply.**

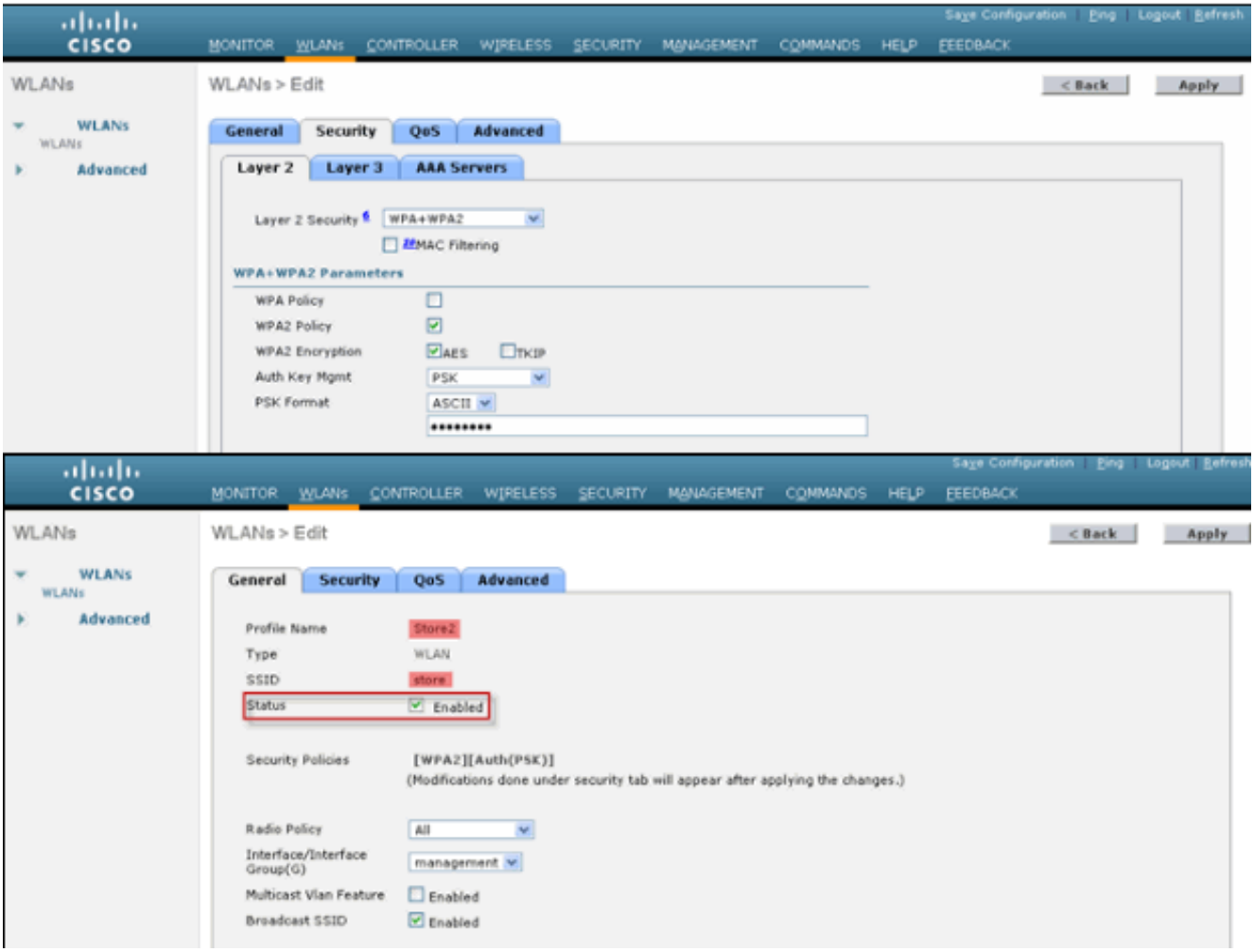


3. Haga clic en **WLAN > General**, verifique el cambio de las políticas de seguridad y marque la casilla **Status** para habilitar la WLAN.



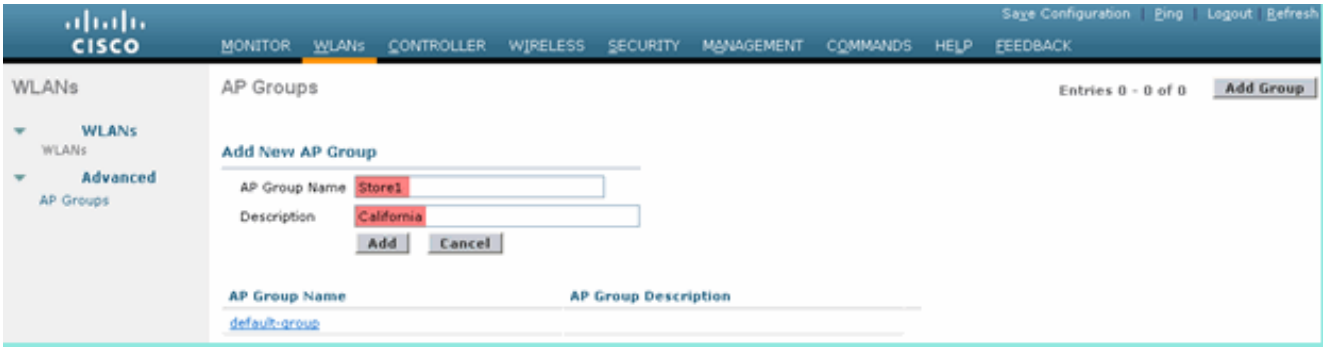
4. Repita los pasos 1, 2 y 3 para el nuevo **almacén de** perfiles WLAN**2**, con **almacén** SSID e ID 18.



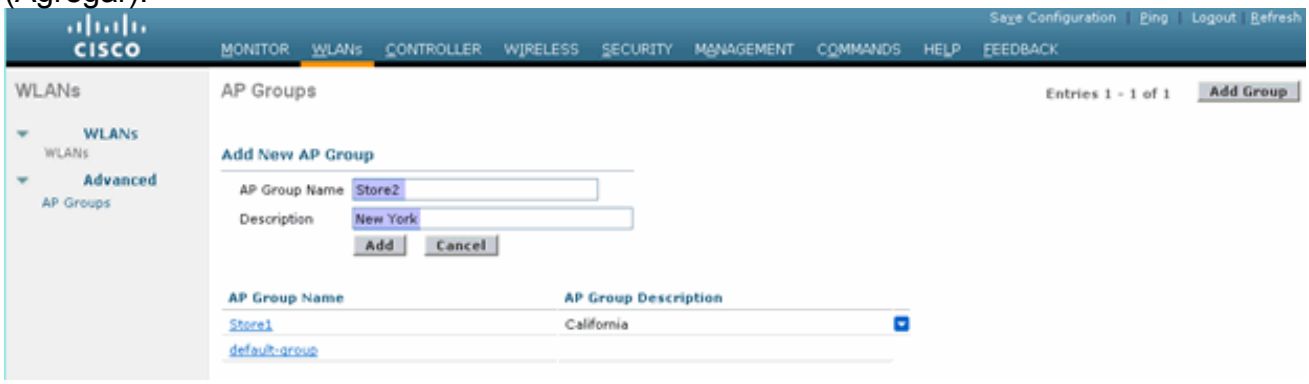


5. Cree y habilite el perfil WLAN con el nombre del perfil **DataCenter**, SSID **DataCenter** e ID 1.**Nota:** Al crear, los ID de WLAN del 1 al 16 forman automáticamente parte del grupo ap predeterminado.
6. En WLAN, verifique el estado de los ID de WLAN 1, 17 y 18.

7. Haga clic en **WLAN > Advanced > AP group > Add Group**.
8. Agregue AP Group Name **Store1**, igual que el **Store1 del perfil WLAN**, y Description as Location of the Store. En este ejemplo, California se utiliza como ubicación de la tienda.
9. Haga clic en **Agregar** cuando haya terminado.

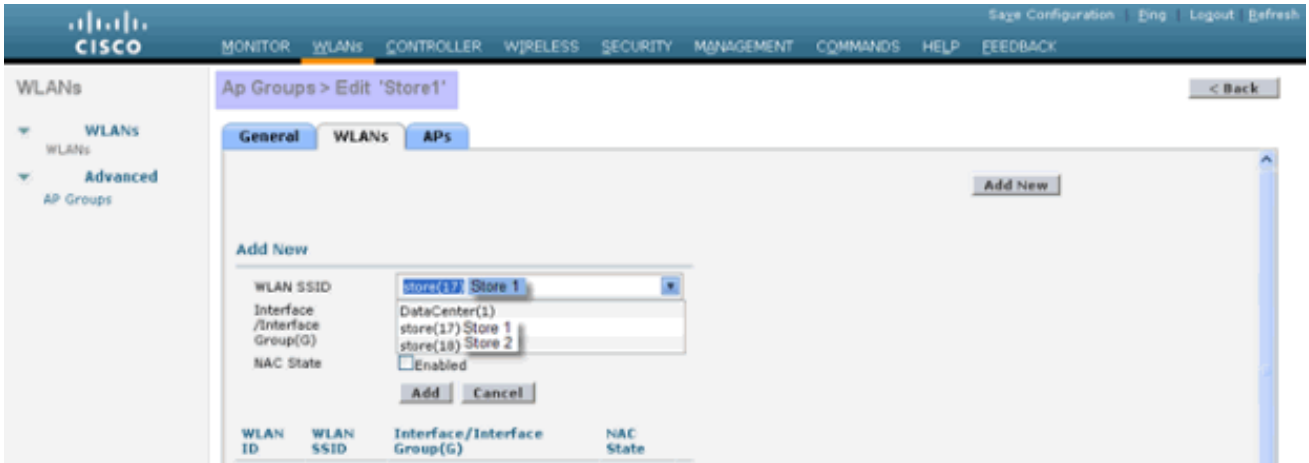


10. Haga clic en **Add Group** y cree AP Group Name **Store2** y Description New York.
11. Haga clic en Add (Agregar).



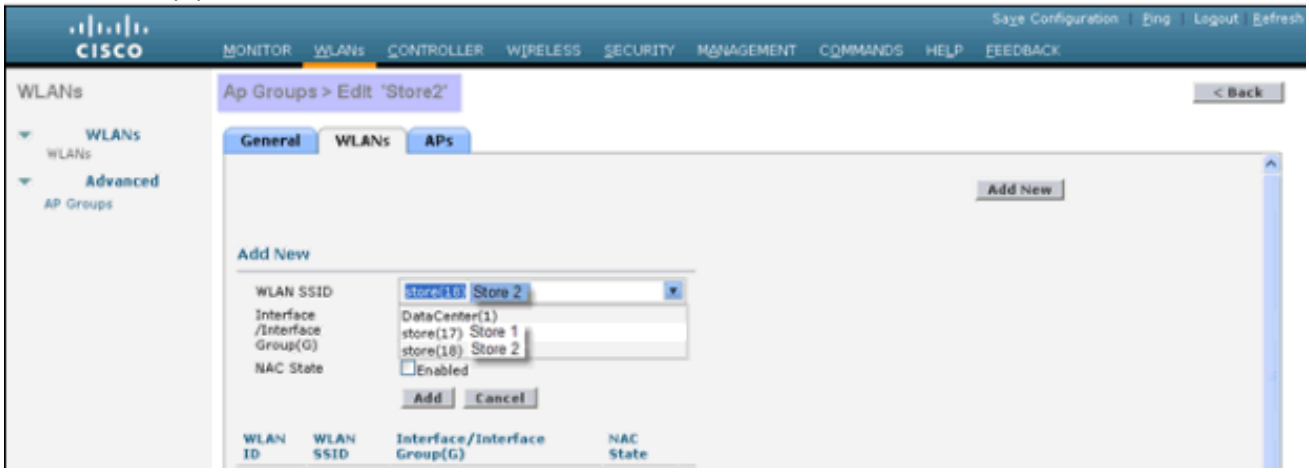
12. Verifique la creación del grupo haciendo clic en **WLAN > Advanced > AP Groups**.

13. Haga clic en AP Group Name **Store1** para agregar o editar la WLAN.
14. Haga clic en **Add New** para seleccionar la WLAN.
15. En WLAN, en el menú desplegable WLAN SSID, elija **WLAN ID 17 store(17)**.
16. Haga clic en **Agregar** después de seleccionar el ID WLAN 17.
17. Repita los pasos 14-16 para el ID de WLAN 1 DataCenter(1). Este paso es opcional y sólo se necesita si desea permitir el acceso a recursos remotos.

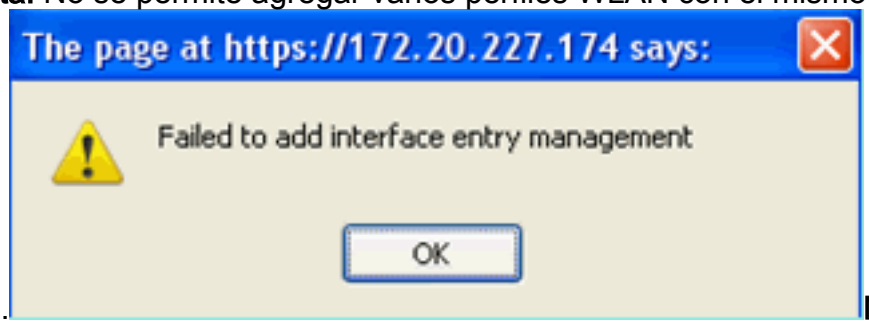


18. Vuelva a la pantalla **WLAN > Advanced > AP Groups**.
19. Haga clic en AP Group Name **Store2** para agregar o editar WLAN.

20. Haga clic en **Add New** para seleccionar la WLAN.
21. En WLAN, en el menú desplegable WLAN SSID, elija **WLAN ID 18 store(18)**.
22. Haga clic en **Agregar** después de seleccionar el ID de WLAN 18.
23. Repita los pasos 14-16 para el ID de WLAN 1 DataCenter(1).



Nota: No se permite agregar varios perfiles WLAN con el mismo SSID bajo un único grupo AP.



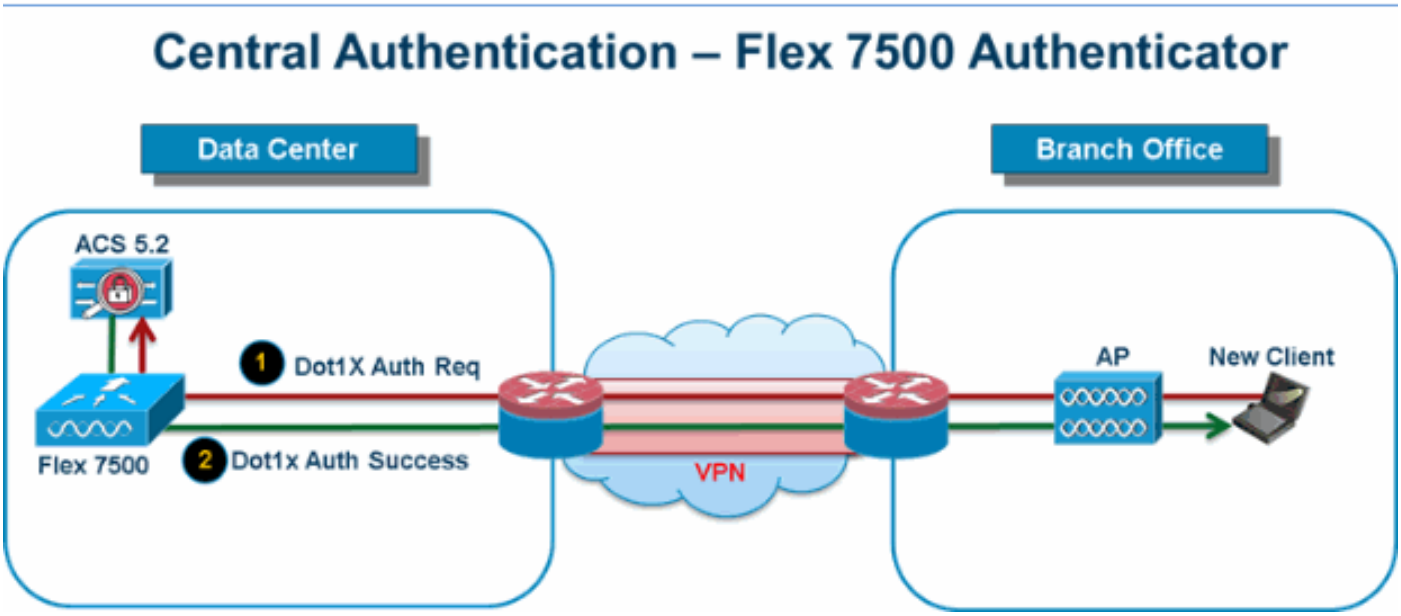
Nota: La adición de AP al grupo AP no se captura en este documento, pero es necesaria para que los clientes accedan a los servicios de red.

Summary

- Los grupos AP simplifican la administración de la red.
- Solución de problemas sencillos con granularidad por sucursal
- Mayor flexibilidad

Grupos de FlexConnect

Figura 9: Autenticación de Dot1X central (Flex 7500 actúa como autenticador)



En la mayoría de las implementaciones típicas de sucursales, es fácil prever que la autenticación del cliente 802.1X se realice de forma centralizada en el Data Center, como se muestra en la Figura 9. Dado que el escenario anterior es perfectamente válido, plantea estas preocupaciones:

- ¿Cómo pueden los clientes inalámbricos realizar la autenticación 802.1X y acceder a los servicios del Data Center si falla Flex 7500?
- ¿Cómo pueden los clientes inalámbricos realizar la autenticación 802.1X si falla el enlace WAN entre la sucursal y el Data Center?
- ¿Hay algún impacto en la movilidad de las sucursales durante los fallos de la WAN?
- ¿La solución FlexConnect no ofrece tiempo de inactividad en las sucursales?

FlexConnect Group se ha diseñado principalmente y debe crearse para afrontar estos retos. Además, facilita la organización de cada sucursal, ya que todos los puntos de acceso FlexConnect de cada sucursal forman parte de un único grupo FlexConnect.

Nota: Los grupos FlexConnect no son análogos a los grupos AP.

Objetivos principales de los grupos FlexConnect

Failover del Servidor RADIUS de Respaldo

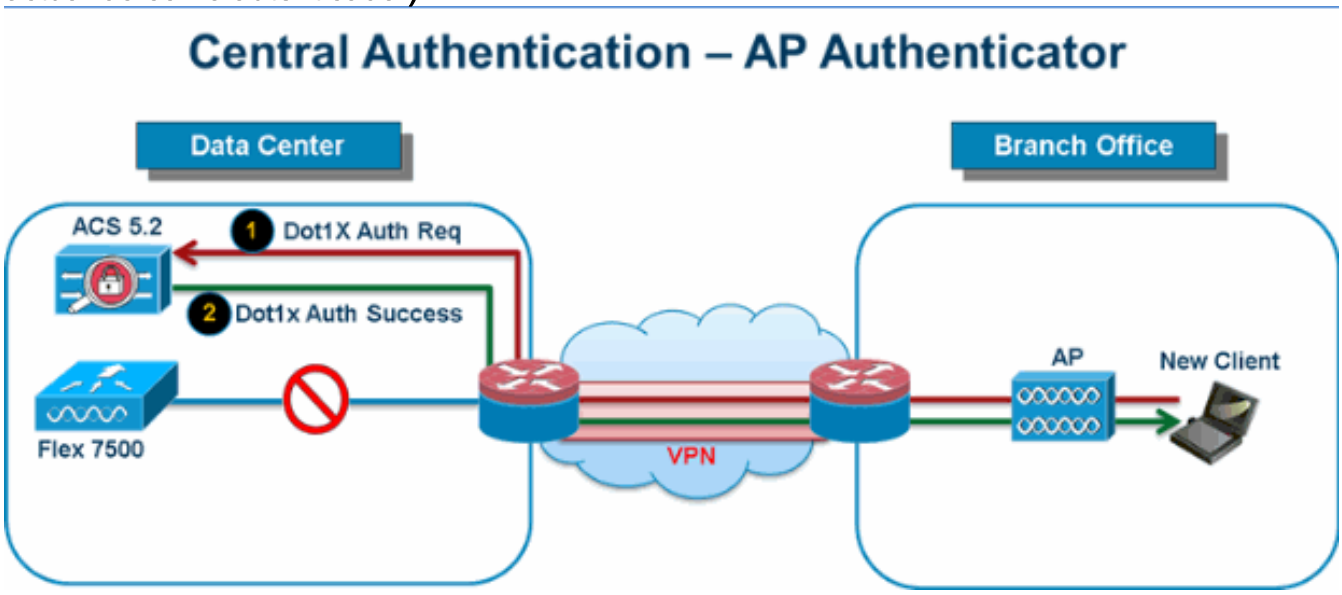
- Puede configurar el controlador para permitir que un punto de acceso FlexConnect en modo independiente realice la autenticación 802.1X completa a un servidor RADIUS de respaldo. Para aumentar la resistencia de la sucursal, los administradores pueden configurar un servidor RADIUS de respaldo primario o un servidor RADIUS de respaldo primario y secundario. Estos servidores se utilizan únicamente cuando el punto de acceso FlexConnect no está conectado al controlador.

Nota: No se admite la contabilización RADIUS de respaldo.

Autenticación local

- Antes de la versión de código 7.0.98.0, la autenticación local sólo se admitía cuando FlexConnect se encontraba en modo independiente para garantizar que la conectividad del cliente no se viera afectada durante una falla de enlace WAN. Con la versión 7.0.116.0, esta función se admite ahora incluso cuando los puntos de acceso FlexConnect se encuentran en

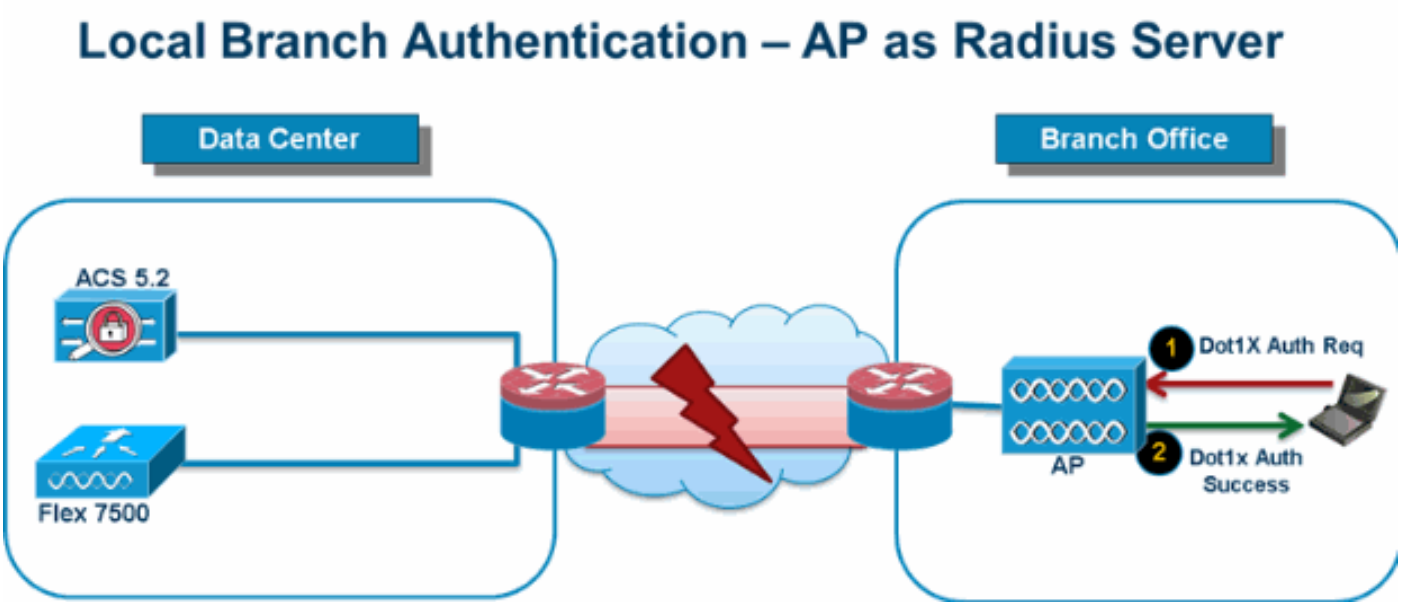
modo conectado.**Figura 10: Autenticación de Dot1X central (puntos de acceso FlexConnect actuando como autenticador)**



Como se muestra en la Figura 10, los clientes de sucursales pueden continuar realizando la autenticación 802.1X cuando los AP de sucursal FlexConnect pierden conectividad con Flex 7500. Mientras el servidor RADIUS/ACS esté accesible desde el sitio de la sucursal, los clientes inalámbricos seguirán autenticando y accediendo a los servicios inalámbricos. En otras palabras, si RADIUS/ACS se encuentra dentro de la sucursal, los clientes autenticarán y accederán a los servicios inalámbricos incluso durante una interrupción de la WAN.**Nota:** Esta función se puede utilizar junto con la función de servidor RADIUS de respaldo FlexConnect. Si se configura un grupo FlexConnect con el servidor RADIUS de respaldo y la autenticación local, el punto de acceso FlexConnect siempre intenta autenticar a los clientes utilizando primero el servidor RADIUS de respaldo primario, seguido por el servidor RADIUS de respaldo secundario (si el primario no es accesible) y, finalmente, el servidor EAP local en el punto de acceso FlexConnect en sí mismo (si el primario y el secundario no son accesibles).

EAP local (continuación de autenticación local)

Figura 11: Autenticación Dot1X (puntos de acceso FlexConnect que actúan como servidor EAP local)



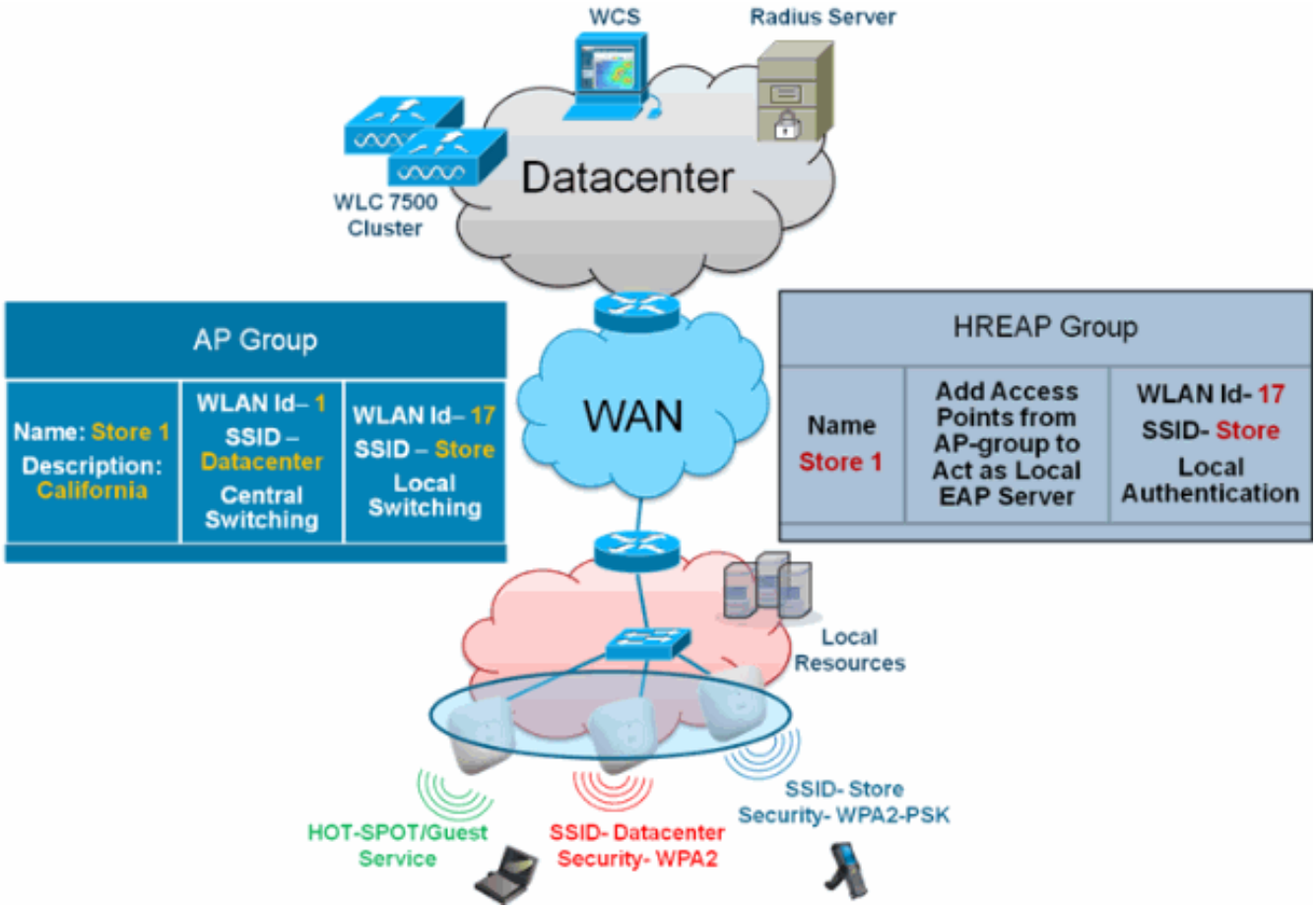
- Puede configurar el controlador para permitir que un punto de acceso FlexConnect en modo

independiente o conectado realice la autenticación LEAP o EAP-FAST para hasta 100 usuarios configurados estáticamente. El controlador envía la lista estática de nombres de usuario y contraseñas a cada punto de acceso FlexConnect de ese grupo FlexConnect concreto cuando se une al controlador. Cada punto de acceso del grupo autentifica solamente a sus propios clientes asociados.

- Esta función es ideal para clientes que migran desde una red de punto de acceso autónomo a una red de punto de acceso FlexConnect ligera y no están interesados en mantener una base de datos de usuarios de gran tamaño o en agregar otro dispositivo de hardware para sustituir la funcionalidad del servidor RADIUS disponible en el punto de acceso autónomo.
- Como se muestra en la Figura 11, si el servidor RADIUS/ACS dentro del Data Center no es accesible, entonces los AP FlexConnect actúan automáticamente como un servidor EAP local para realizar la autenticación Dot1X para los clientes de sucursales inalámbricas.

CCKM/OKC Fast Roaming

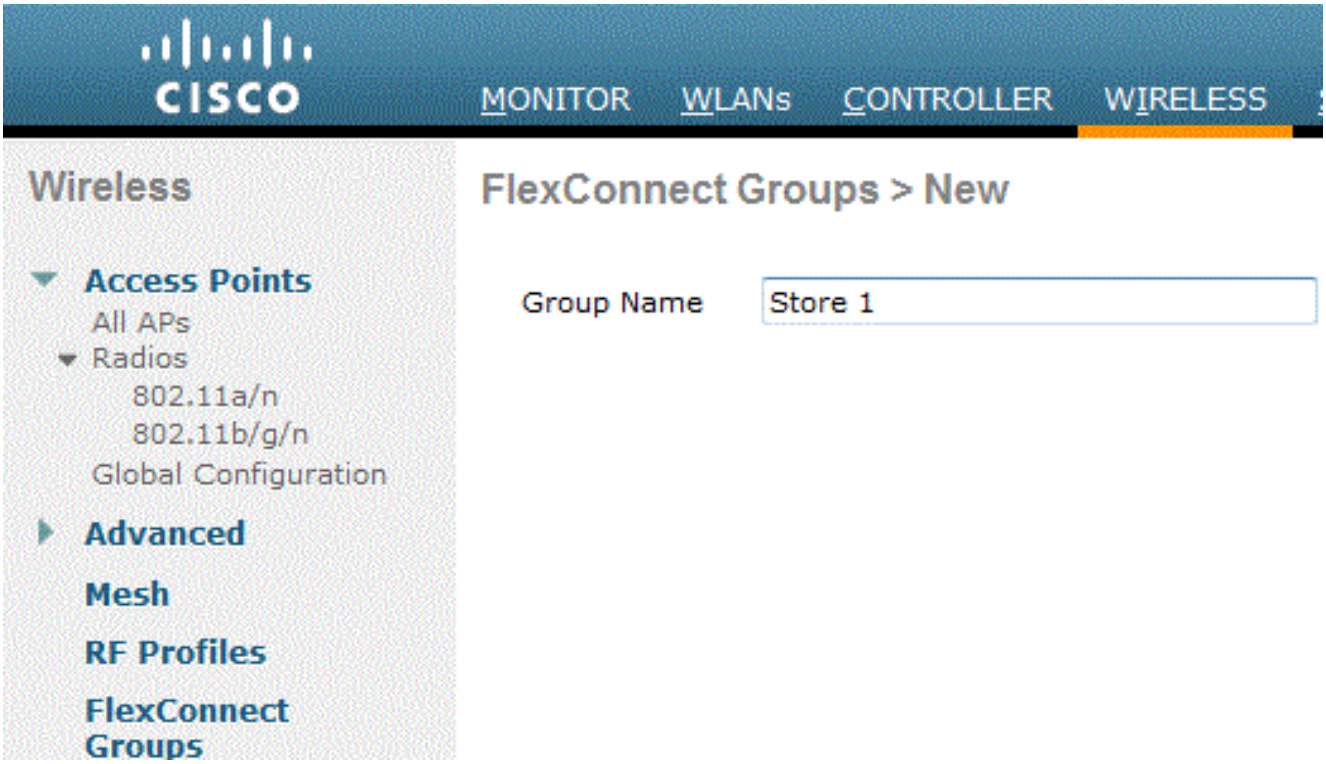
- Se requieren grupos FlexConnect para que CCKM/OKC funcione con puntos de acceso FlexConnect. El roaming rápido se logra almacenando en caché un derivado de la clave maestra desde una autenticación EAP completa para que pueda producirse un intercambio de claves simple y seguro cuando un cliente inalámbrico se desplaza a un punto de acceso diferente. Esta función evita la necesidad de realizar una autenticación RADIUS EAP completa mientras el cliente avanza de un punto de acceso a otro. Los puntos de acceso FlexConnect necesitan obtener la información de caché de CCKM/OKC para todos los clientes que puedan asociarse, de modo que puedan procesarla rápidamente en lugar de enviarla de vuelta al controlador. Si, por ejemplo, tiene un controlador con 300 puntos de acceso y 100 clientes que podrían asociarse, enviar la memoria caché CCKM/OKC para los 100 clientes no es práctico. Si crea un grupo FlexConnect que comprenda un número limitado de puntos de acceso (por ejemplo, crea un grupo para cuatro puntos de acceso en una oficina remota), los clientes sólo se desplazan entre esos cuatro puntos de acceso y la caché CCKM/OKC se distribuye entre esos cuatro puntos de acceso sólo cuando los clientes se asocian a uno de ellos.
- Esta función, junto con Backup Radius y Local Authentication (Local-EAP), **no** garantiza **tiempo de inactividad operativo** para las sucursales.**Nota:** No se admite el roaming rápido CCKM/OKC entre puntos de acceso FlexConnect y no FlexConnect.**Figura 12: Referencia de diseño de red inalámbrica con grupos FlexConnect**



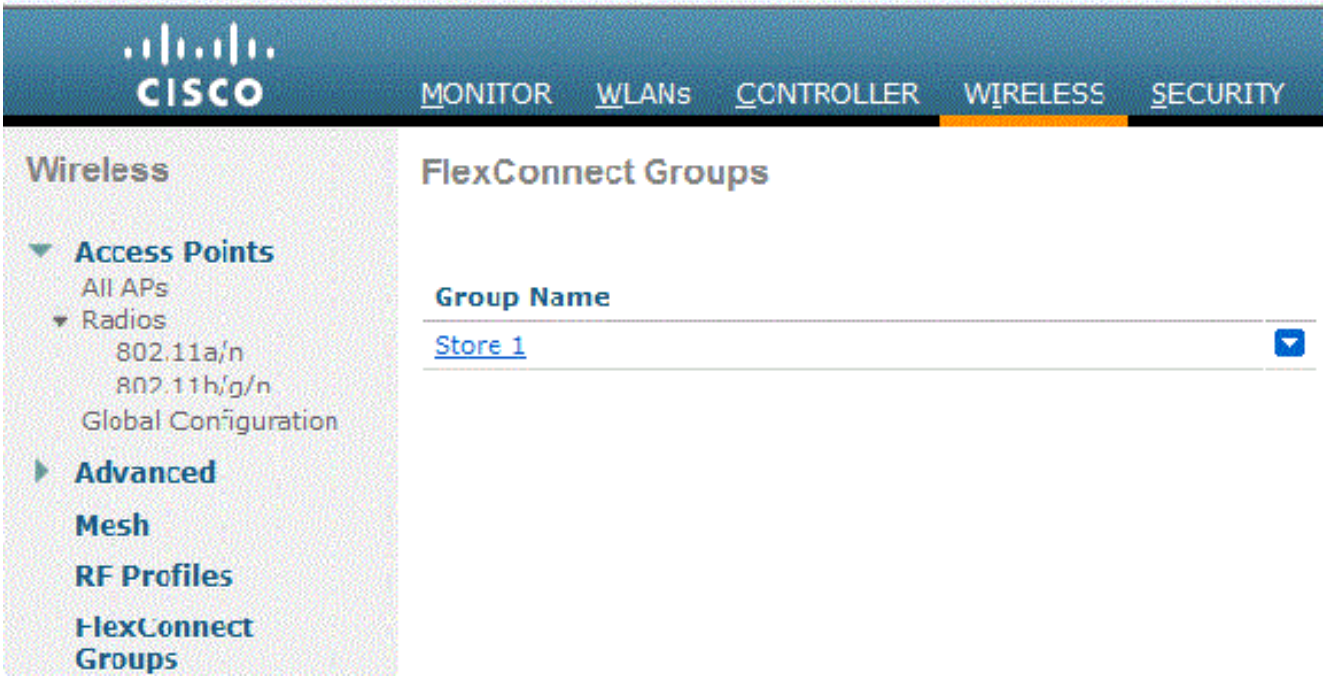
Configuración del grupo FlexConnect desde WLC

Complete los pasos de esta sección para configurar los grupos FlexConnect para que admitan la autenticación local mediante LEAP, cuando FlexConnect se encuentre en modo conectado o independiente. El ejemplo de configuración de la Figura 12 ilustra las diferencias objetivas y la asignación 1:1 entre el grupo AP y el grupo FlexConnect.

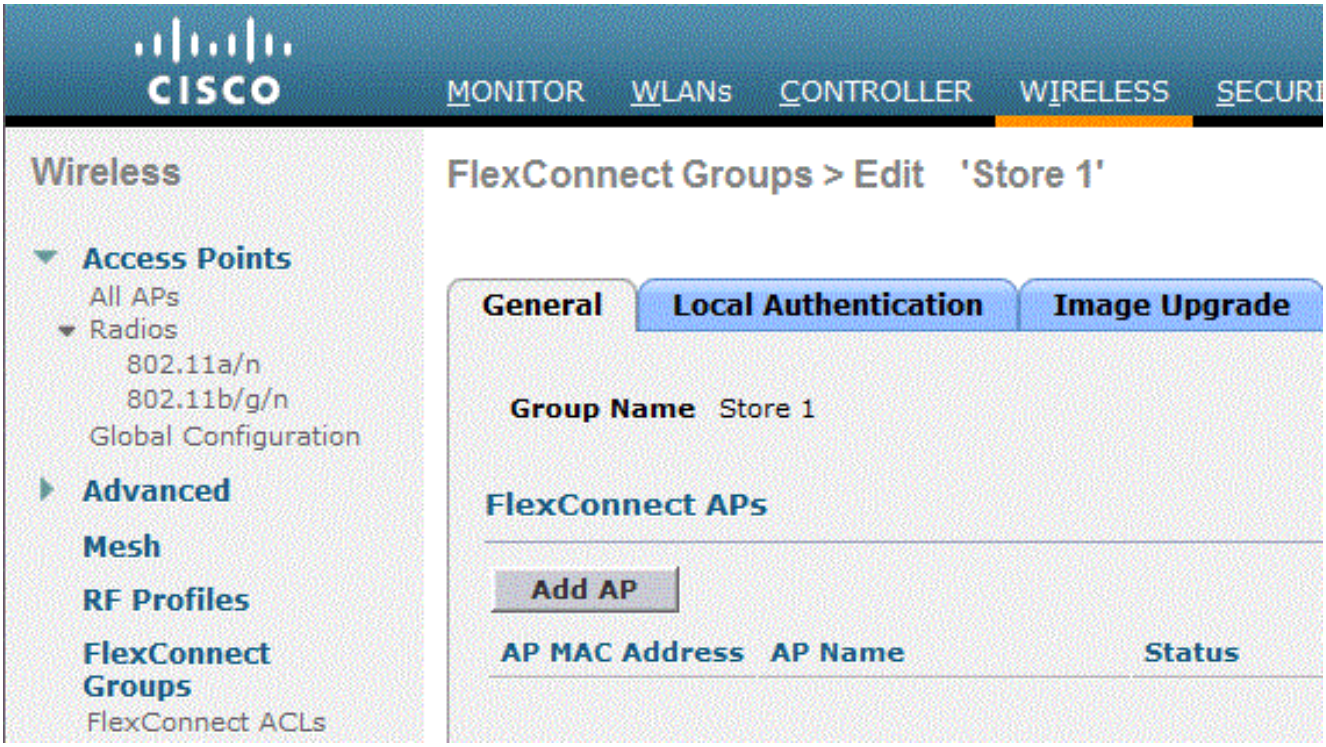
1. Haga clic en **Nuevo** en Inalámbrico > Grupos FlexConnect.
2. Asigne Group Name Store 1, de forma similar a la configuración de ejemplo, como se muestra en la Figura 12.
3. Haga clic en **Aplicar** cuando se establezca el nombre del grupo.



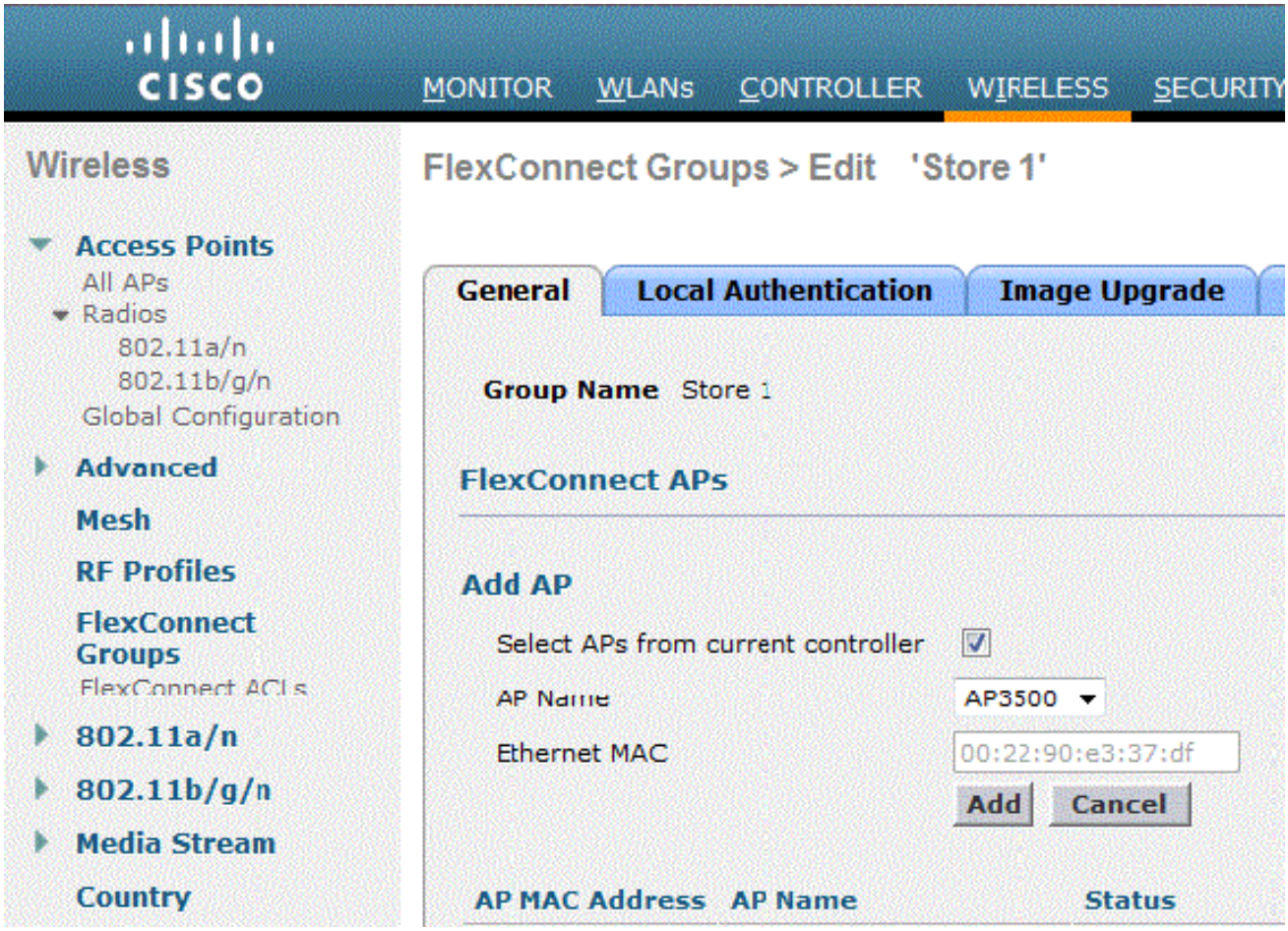
4. Haga clic en el **Almacén de** nombres de grupo **1** que acaba de crear para una configuración adicional.



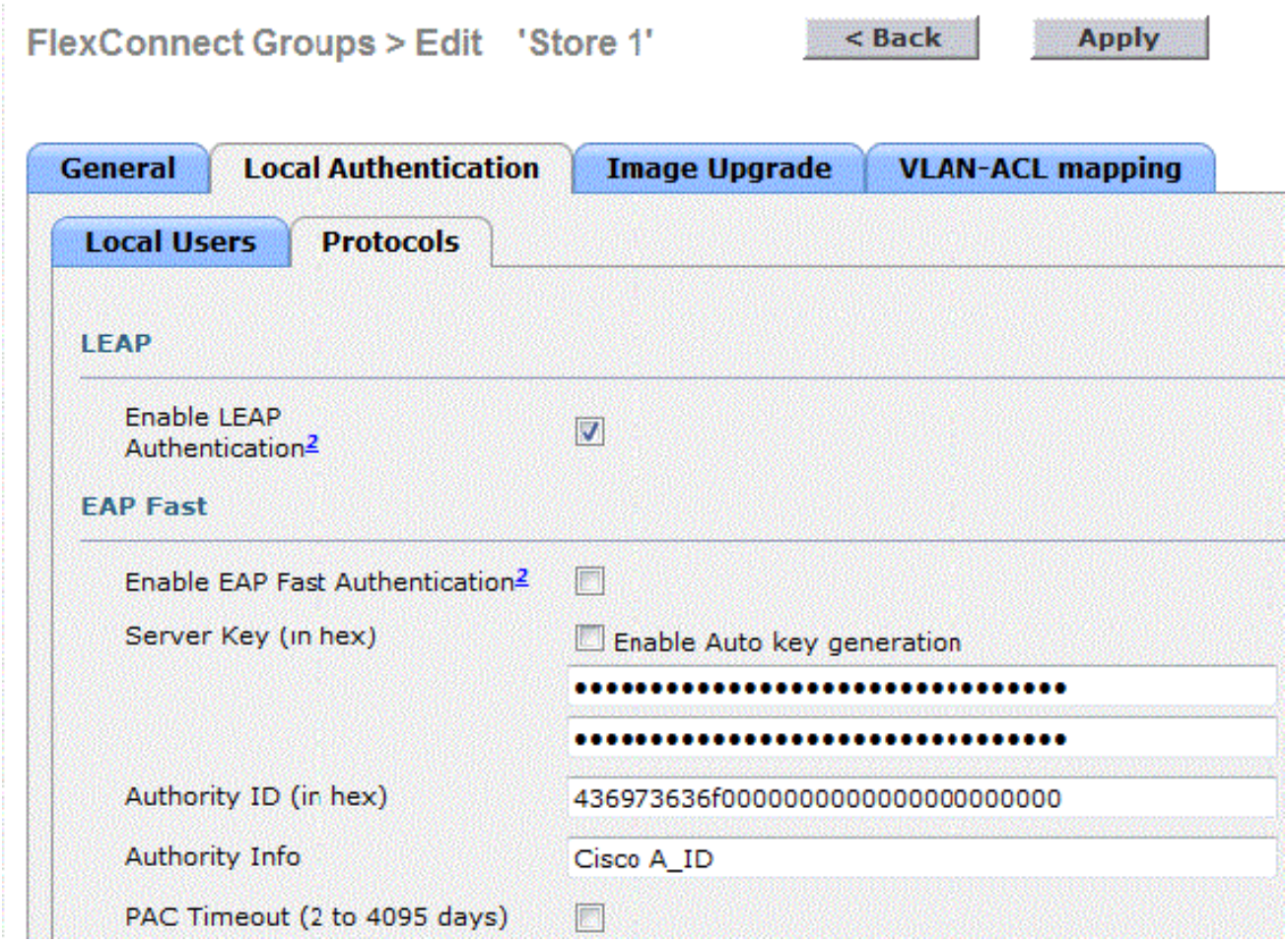
5. Haga clic en **Agregar AP**.



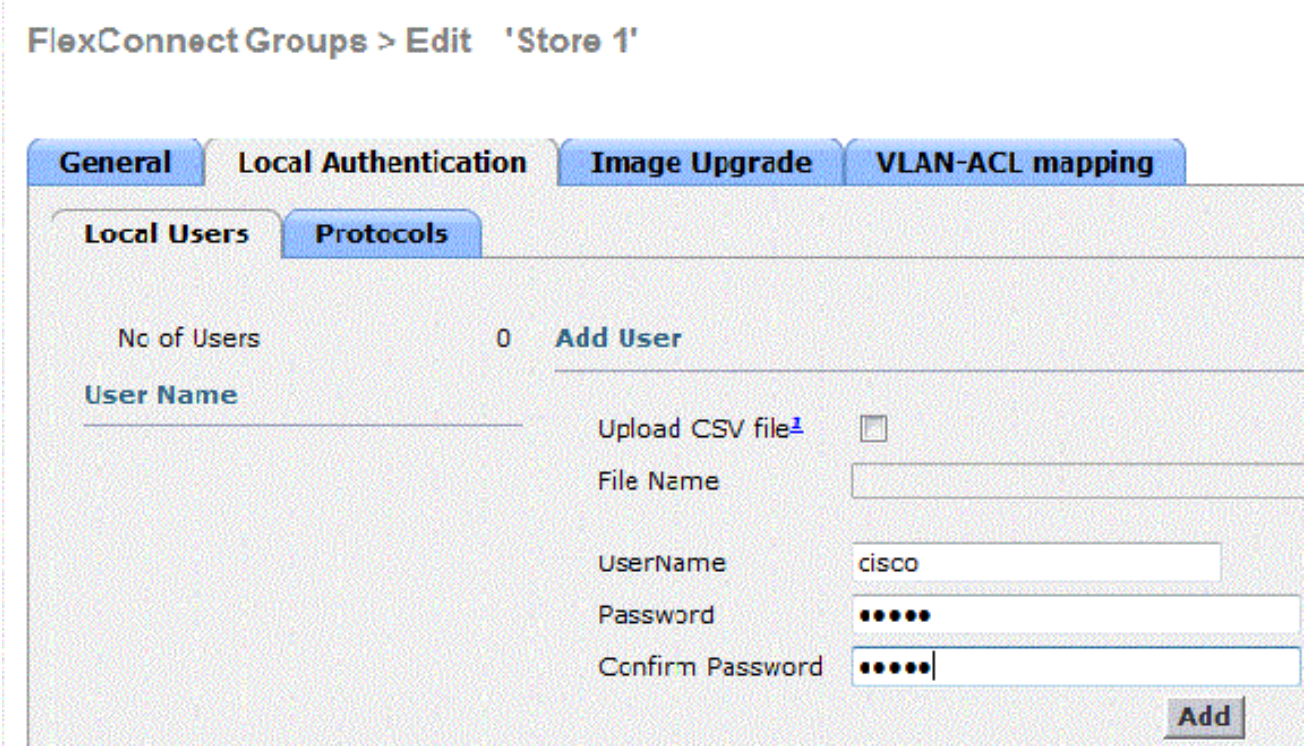
6. Marque la casilla **Enable AP Local Authentication** para habilitar la Autenticación Local cuando el AP está en el Modo Independiente.**Nota:** El Paso 20 muestra cómo habilitar la autenticación local para AP de modo conectado.
7. Marque la casilla **Select APs from current controller** para habilitar el menú desplegable AP Name .
8. Elija el AP de la lista desplegable que debe formar parte de este grupo FlexConnect.
9. Haga clic en **Agregar** después de seleccionar el AP en la lista desplegable.
10. Repita los pasos 7 y 8 para agregar todos los AP a este grupo de FlexConnect que también forman parte de AP-Group Store 1. Consulte la Figura 12 para comprender el mapping 1:1 entre el grupo AP y el grupo FlexConnect.Si ha creado un grupo AP por almacén (Figura 8), idealmente todos los AP de ese grupo AP deberían formar parte de este grupo FlexConnect (Figura 12). El mantenimiento de la relación 1:1 entre el grupo AP y el grupo FlexConnect simplifica la administración de la
red.



11. Haga clic en **Autenticación local > Protocolos** y marque la casilla **Habilitar autenticación LEAP**.
12. Haga clic en **Aplicar** después de establecer la casilla de verificación.**Nota:** Si tiene un controlador de respaldo, asegúrese de que los grupos de FlexConnect son idénticos y de que se incluyen las entradas de dirección MAC de AP por grupo de FlexConnect.

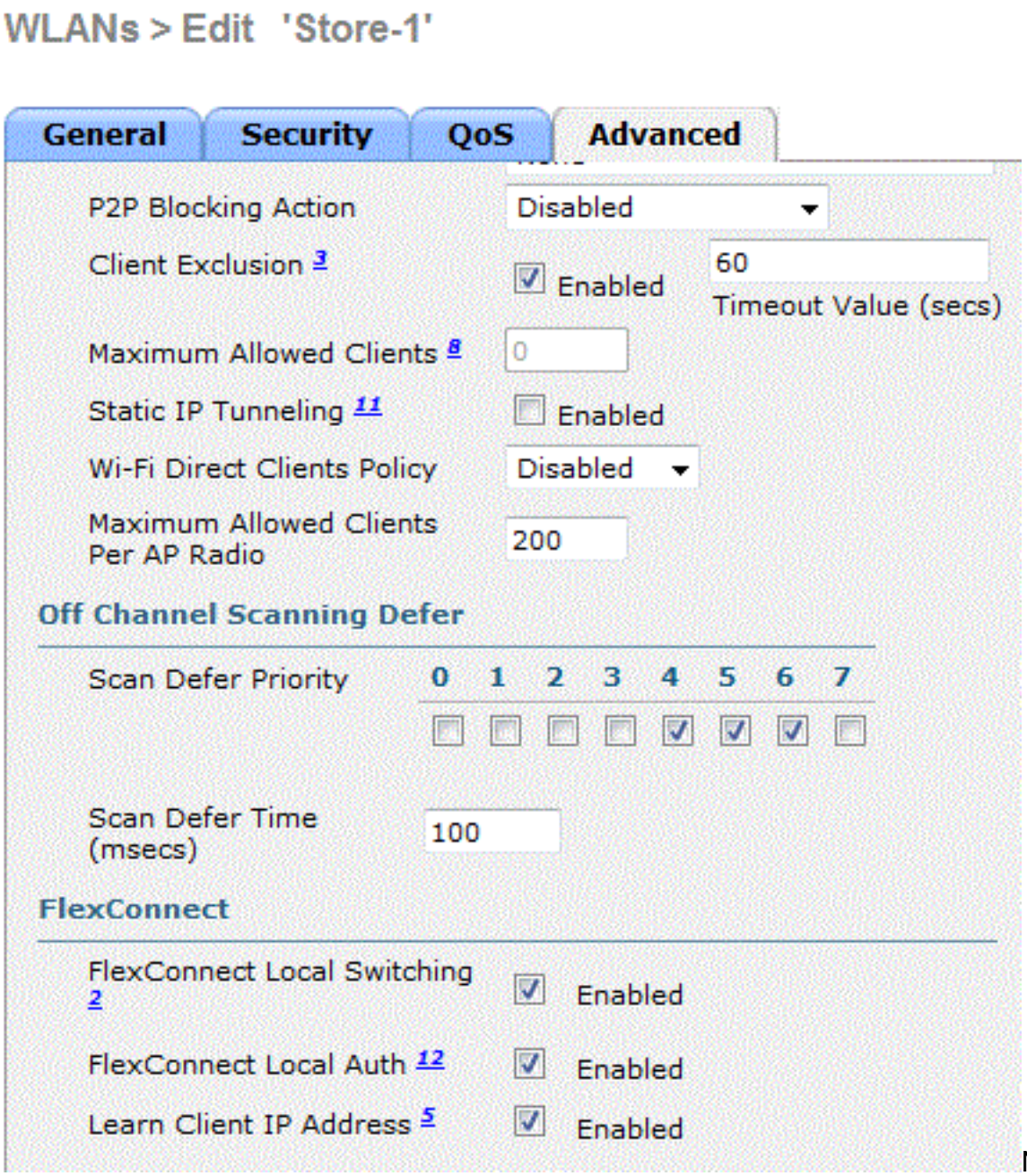


13. En Autenticación local, haga clic en **Usuarios locales**.
14. Establezca los campos Nombre de usuario, Contraseña y Confirmar contraseña, luego haga clic en **Agregar** para crear la entrada de usuario en el servidor EAP local que reside en el AP.
15. Repita el paso 13 hasta que se agote la lista de nombres de usuario local. No puede configurar ni agregar más de 100 usuarios.
16. Haga clic en **Aplicar** después de que se complete el paso 14 y se verifique el número de usuarios.

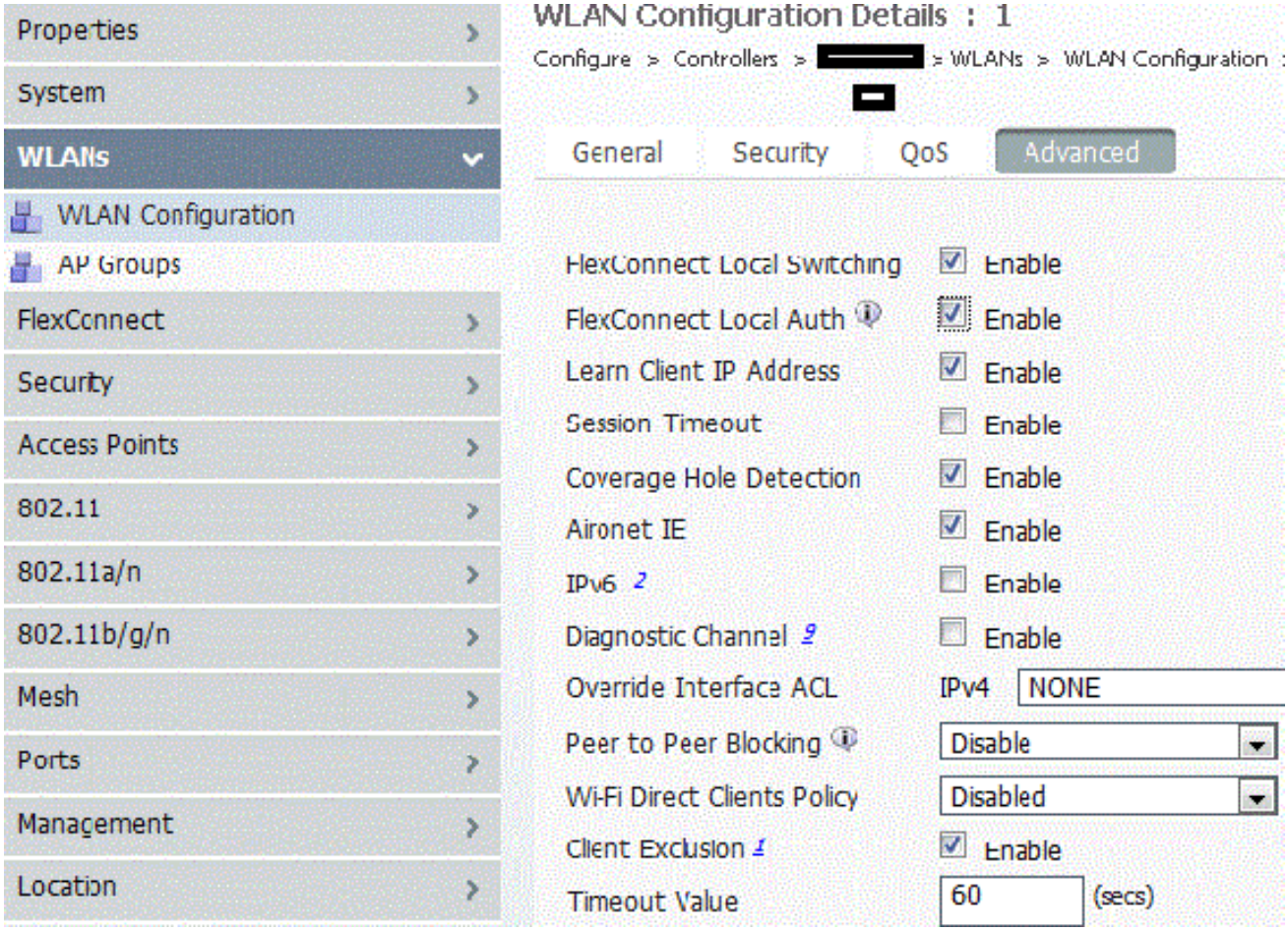


17. En el panel superior, haga clic en **WLAN**.
18. Haga clic en **WLAN ID 17**. Esto se creó durante la creación del grupo AP. Consulte la Figura 8.

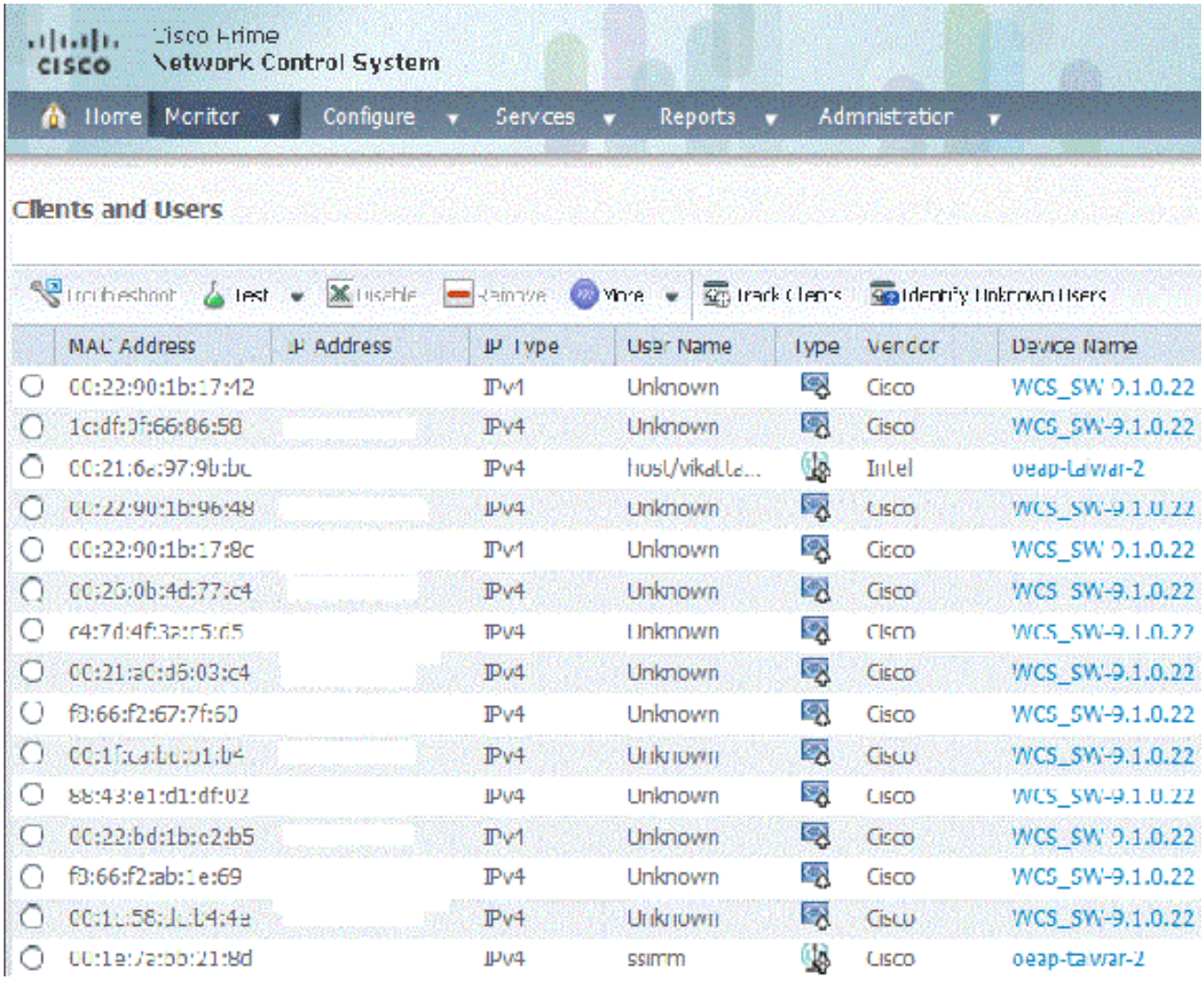
19. En WLAN > Edit for WLAN ID 17, haga clic en **Advanced**.
20. Marque la casilla **FlexConnect Local Auth** para habilitar la autenticación local en el modo conectado.**Nota:** La autenticación local sólo se admite para FlexConnect con conmutación local.**Nota:** Asegúrese siempre de crear el grupo FlexConnect antes de activar la autenticación local en

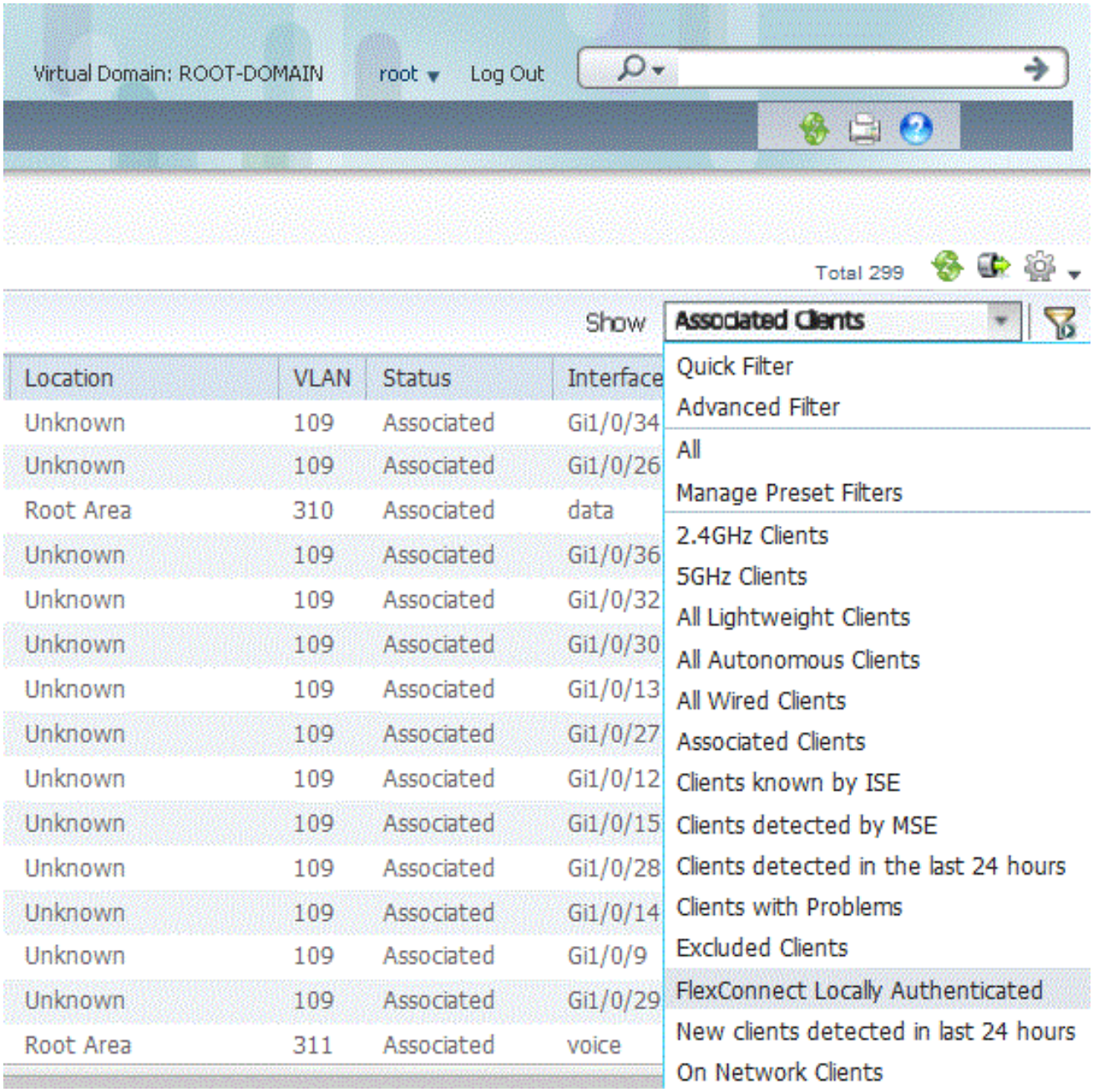


WLAN. NCS también proporciona la casilla de verificación FlexConnect Local Auth para habilitar la autenticación local en el modo conectado, como se muestra aquí:



NCS también proporciona funciones para filtrar y supervisar los clientes con autenticación local de FlexConnect, como se muestra a continuación:


Cisco Prime
Network Control System
Home
Monitor
Configure
Services
Reports
Administration
Clients and Users
Troubleshoot
Test
Disable
Remove
More
Track Clients
Identify Unknown Users
MAC Address
IP Address
IP Type
User Name
Type
Vendor
Device Name
00:22:90:1b:17:12 IPv4 Unknown Cisco WCS_SW 9.1.0.22
1c:df:0f:66:86:58 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:6a:97:9b:bc IPv4 host/vikalla... Intel deap-tavar-2
00:22:90:1b:96:48 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:90:1b:17:8c IPv4 Unknown Cisco WCS_SW 9.1.0.22
00:25:0b:4d:77:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
c4:7d:4f:3a:c5:c5 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:21:a0:d5:03:c4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
f0:66:f2:67:7f:50 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1f:ca:bc:b1:b4 IPv4 Unknown Cisco WCS_SW-9.1.0.22
88:43:e1:d1:df:02 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:22:bd:1b:e2:b5 IPv4 Unknown Cisco WCS_SW 9.1.0.22
f0:66:f2:ab:1e:69 IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1c:58:bc:b4:4a IPv4 Unknown Cisco WCS_SW-9.1.0.22
00:1e:7a:bb:21:8d IPv4 ssimm Cisco deap-tavar-2



Verificación mediante CLI

El estado de autenticación de cliente y el modo de conmutación pueden verificarse rápidamente usando esta CLI en el WLC:

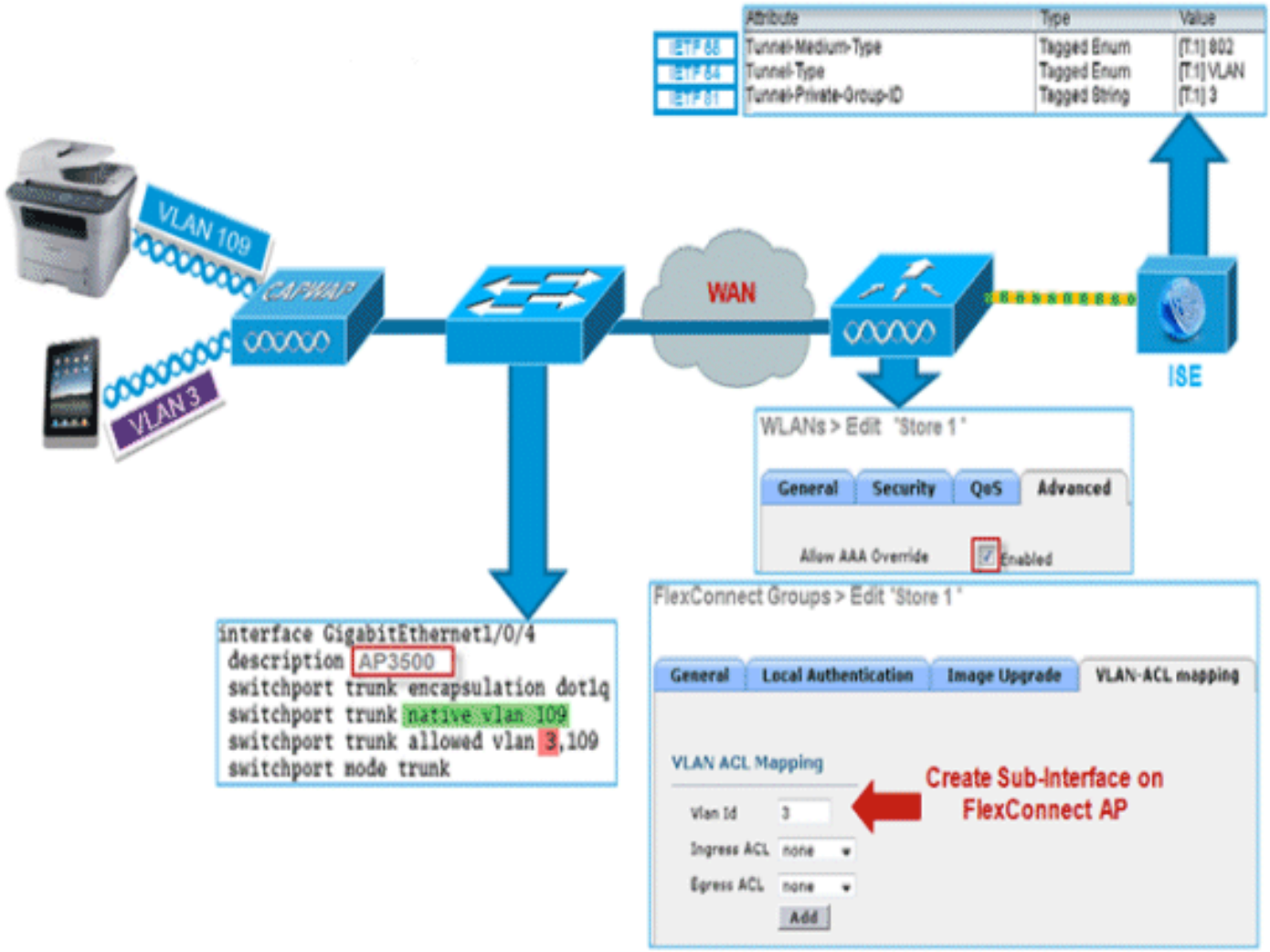
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address.............................. 00:24:d7:2b:7c:0c
Client Username ................................ N/A
AP MAC Address.................................. d0:57:4c:08:e6:70
Client State.................................... Associated
H-REAP Data Switching........................... Local
H-REAP Authentication........................... Local
```

Reemplazo de VLAN FlexConnect

En la arquitectura actual de FlexConnect, existe una asignación estricta de la WLAN a la VLAN y, por lo tanto, el cliente que se asocia en una WLAN determinada en el AP de FlexConnect debe

acatar una VLAN que se asigna a ella. Este método tiene limitaciones, porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes políticas basadas en VLAN.

A partir de la versión 7.2 en adelante, se soporta la invalidación AAA de VLAN en WLAN individual configurada para el switching local. Para tener una asignación de VLAN dinámica, AP tendría las interfaces para la VLAN previamente creadas basándose en una configuración usando el mapping de WLAN-VLAN existente para el AP de FlexConnect individual o usando el mapping de ACL-VLAN en un grupo de FlexConnect. El WLC se utiliza para precrear las subinterfaces en el AP.



Summary

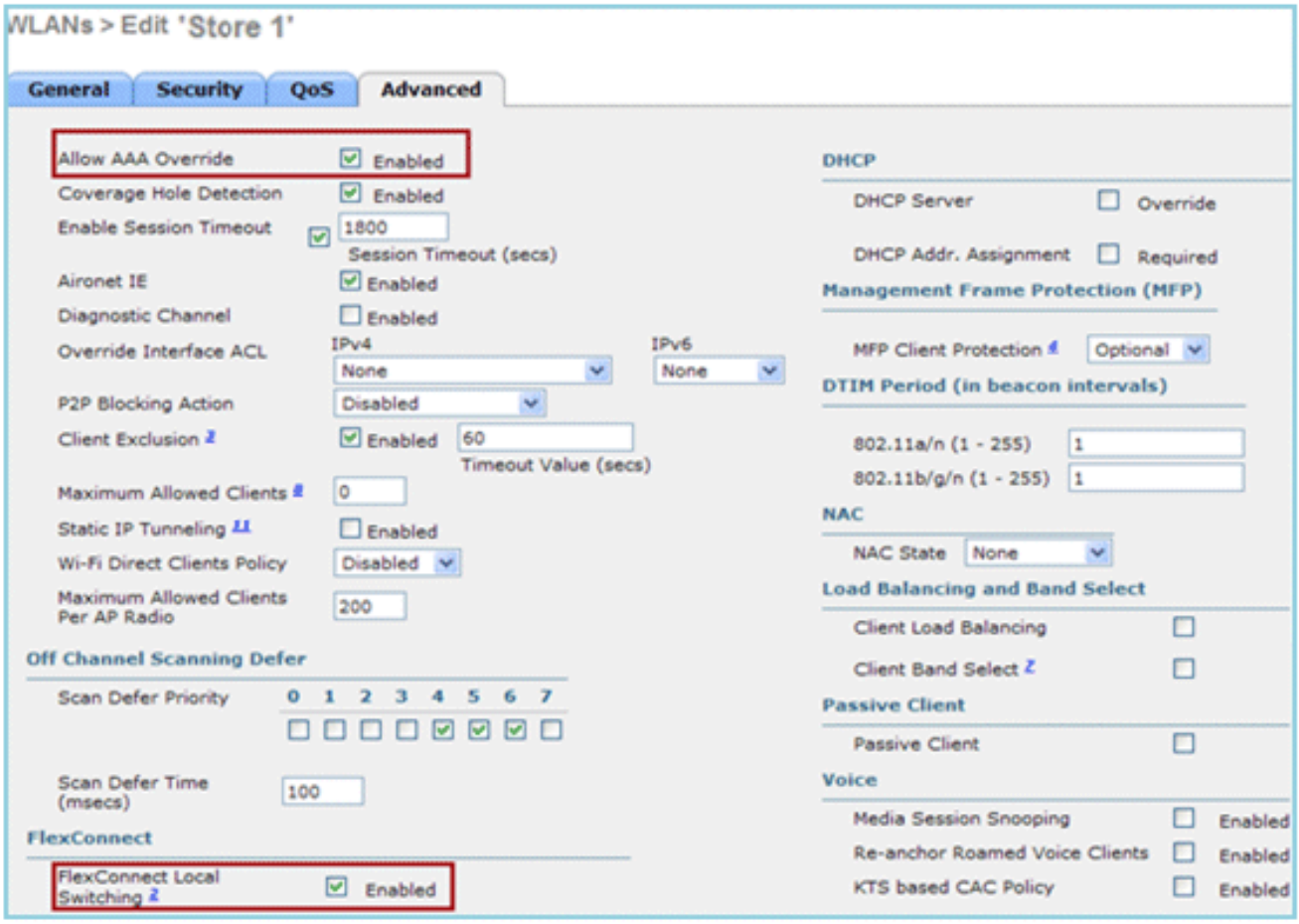
- La invalidación de VLAN AAA se soporta desde la versión 7.2 para las WLANs configuradas para el switching local en el modo de autenticación central y local.
- La anulación de AAA debe estar habilitada en la WLAN configurada para la conmutación local.
- El punto de acceso FlexConnect debe tener VLAN previamente creada desde el WLC para la asignación de VLAN dinámica.
- Si las VLAN devueltas por la invalidación AAA no están presentes en el cliente AP, obtendrán una IP de la interfaz VLAN predeterminada del AP.

Procedimiento

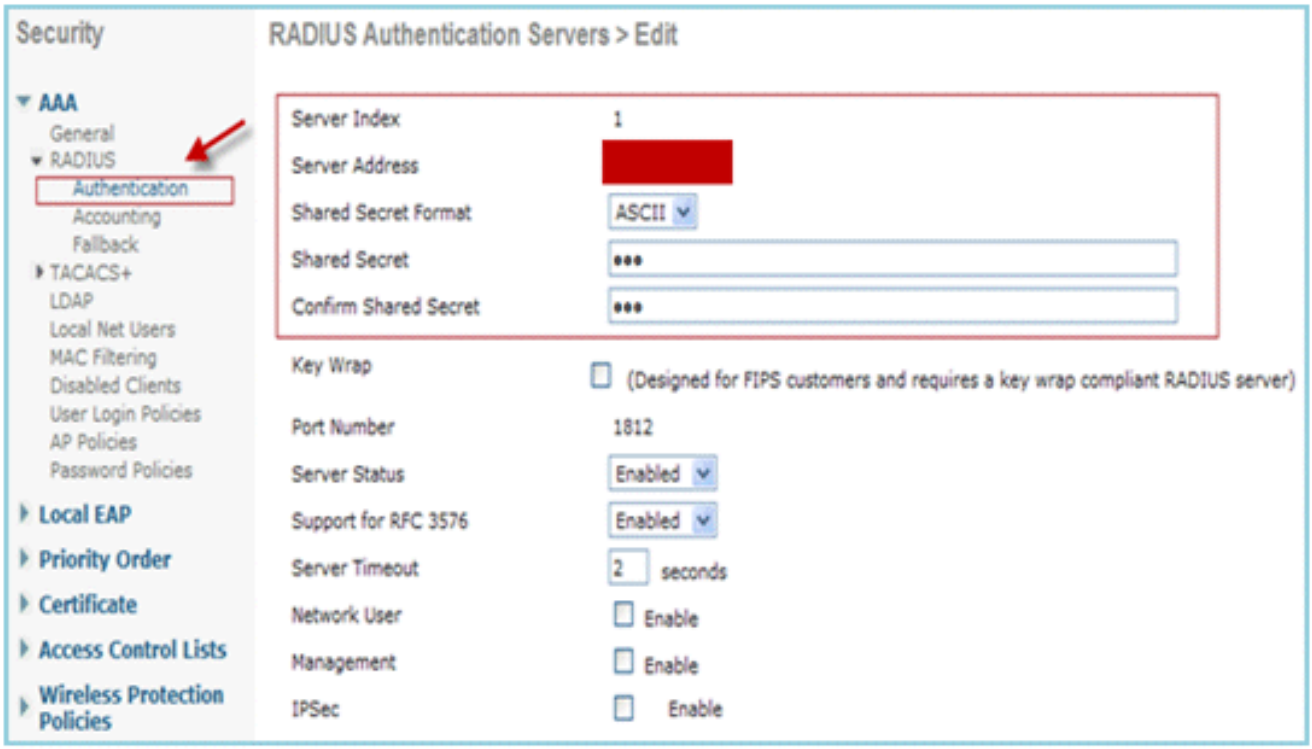
Complete estos pasos:

1. Cree una WLAN para la autenticación 802.1x.

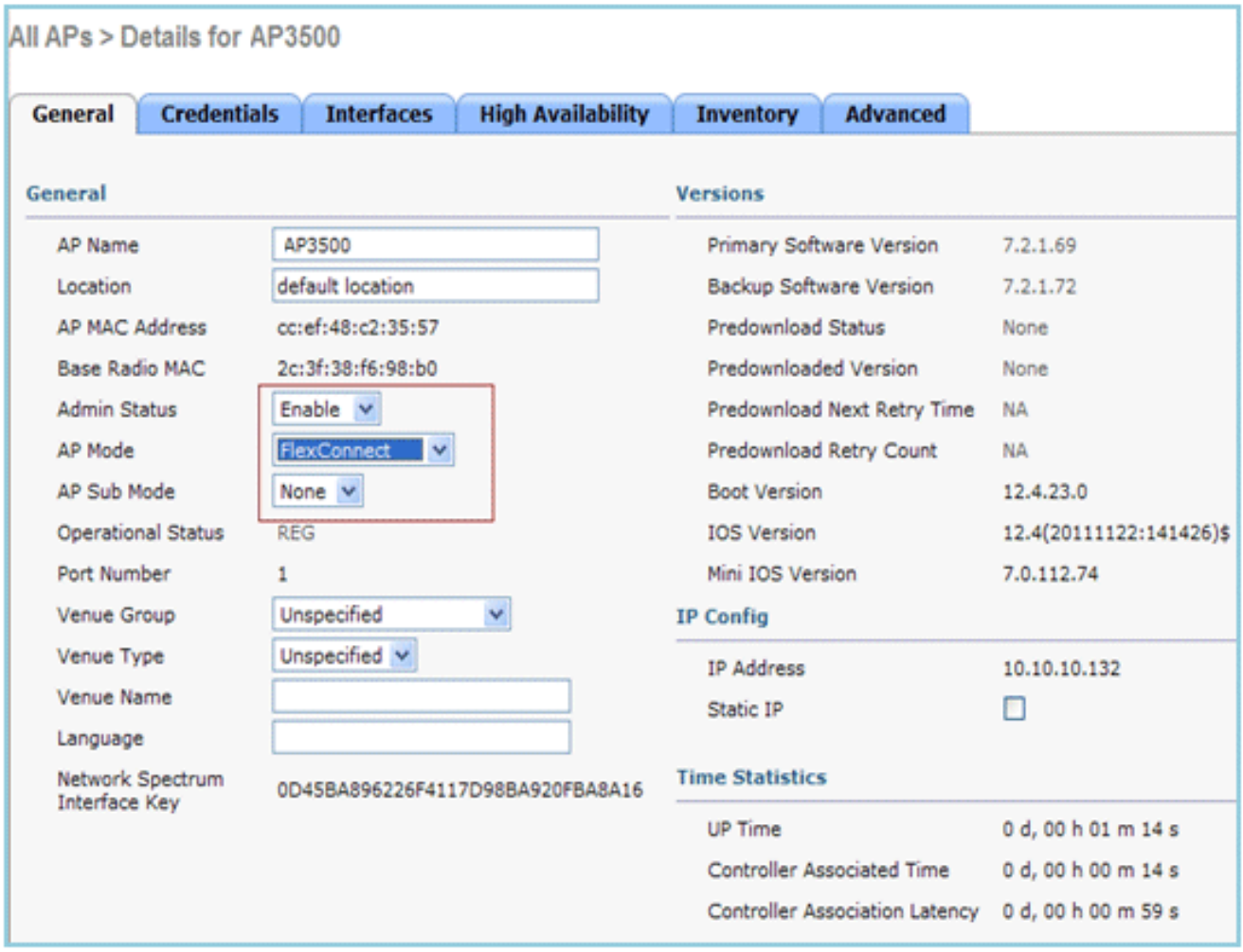
2. Habilite el soporte de invalidación AAA para la WLAN de conmutación local en el WLC. Navegue hasta **GUI de WLAN > WLAN > ID de WLAN >** pestaña **Advance**.



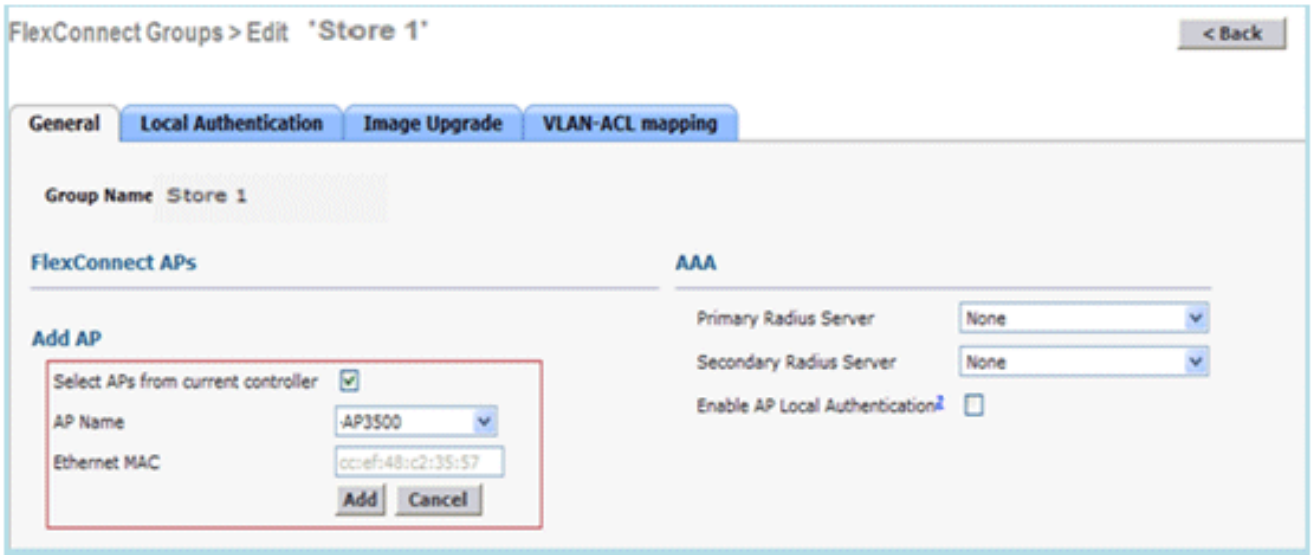
3. Agregue los detalles del servidor AAA en el controlador para la autenticación 802.1x. Para agregar el servidor AAA, navegue a WLC GUI > Security > AAA > **Radius** > **Authentication** > **New**.



4. El AP se encuentra en el modo local de forma predeterminada, por lo que el modo es el modo FlexConnect. Los AP de modo local se pueden convertir al modo FlexConnect yendo a **Wireless** > **All APs**, y haga clic en el AP individual.



5. Agregue los puntos de acceso FlexConnect al grupo FlexConnect.Navegue bajo WLC GUI > Wireless > FlexConnect Groups > **Select FlexConnect Group** > **General** pestaña > **Add AP**.



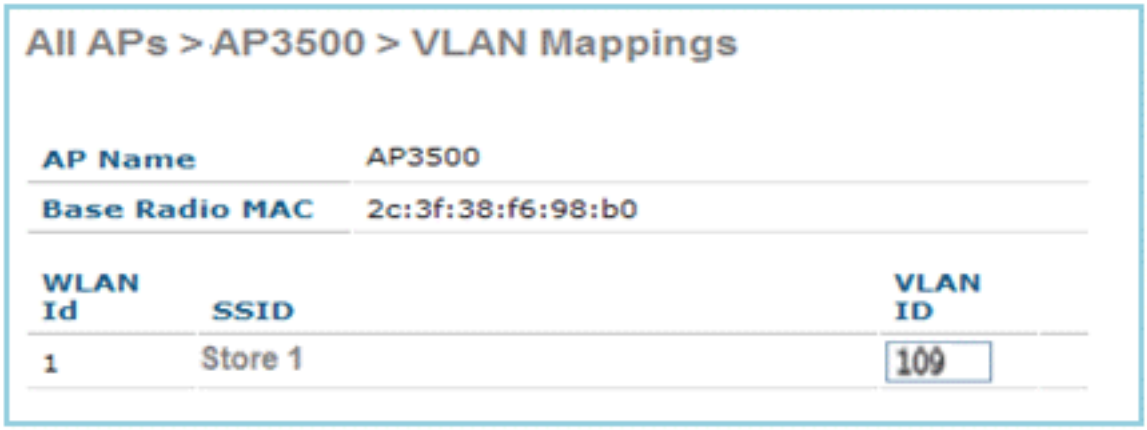
6. El punto de acceso FlexConnect debe estar conectado en un puerto troncal y la VLAN asignada a WLAN y la VLAN anulada por AAA deben estar permitidas en el puerto

troncal.

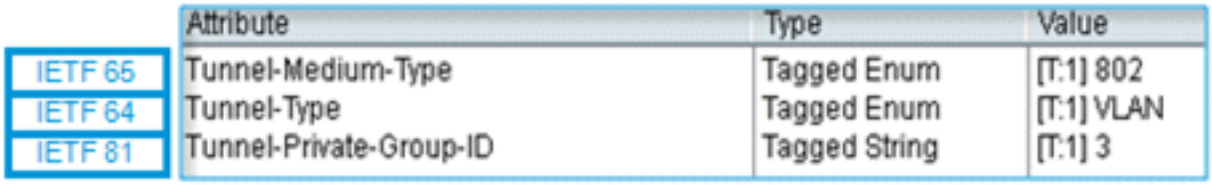
```
interface GigabitEthernet1/0/4
 description AP3500
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

Nota: En esta configuración, vlan 109 se utiliza para el mapping de VLAN WLAN y vlan 3 se utiliza para el reemplazo de AAA.

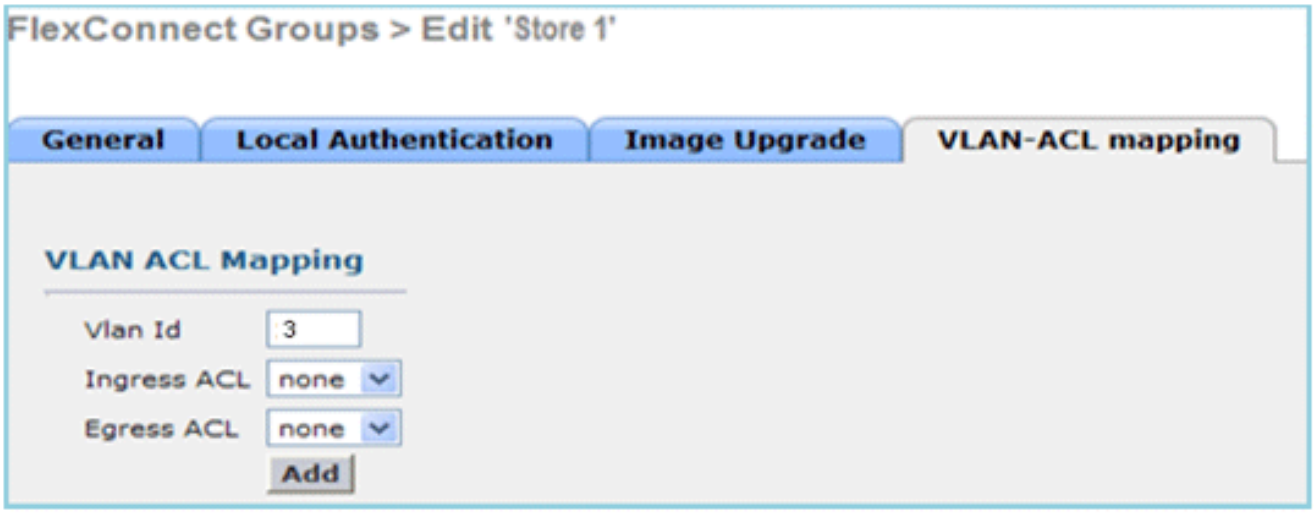
7. Configure el mapeo de WLAN a VLAN para el punto de acceso FlexConnect. Según esta configuración, el AP tendría las interfaces para la VLAN. Cuando el AP recibe la configuración de VLAN, se crean las subinterfaces dot11 y Ethernet correspondientes y se agregan a un grupo de bridges. Asocie un cliente en esta WLAN y cuando el cliente se asocia, se asigna su VLAN (predeterminada, basada en la asignación WLAN-VLAN).Navegue hasta WLAN GUI > **Wireless** > **All APs** > haga clic en la pestaña AP específica > **FlexConnect**, y haga clic en VLAN Mapping.



8. Cree un usuario en el servidor AAA y configure el usuario para que devuelva el ID de VLAN en el atributo IETF Radius.



9. Para tener una asignación de VLAN dinámica, el AP tendría las interfaces para la VLAN dinámica previamente creadas en función de la configuración usando el mapping de WLAN-VLAN existente para el AP FlexConnect individual o usando el mapping de ACL-VLAN en el grupo FlexConnect.Para configurar la VLAN AAA en el AP de FlexConnect, navegue hasta la GUI de WLC > **Inalámbrico** > **Grupo FlexConnect** > haga clic en el grupo específico de FlexConnect > mapeo VLAN-ACL e ingrese VLAN en el campo **ID de VLAN**.



10. Asocie un cliente en esta WLAN y autentique usando el nombre de usuario configurado en el servidor AAA para devolver la VLAN AAA.
11. El cliente debe recibir una dirección IP de la VLAN dinámica devuelta a través del servidor AAA.
12. Para verificar, haga clic en **WLC GUI > Monitor > Cliente >** haga clic en la dirección MAC del cliente específico para verificar los detalles del cliente.

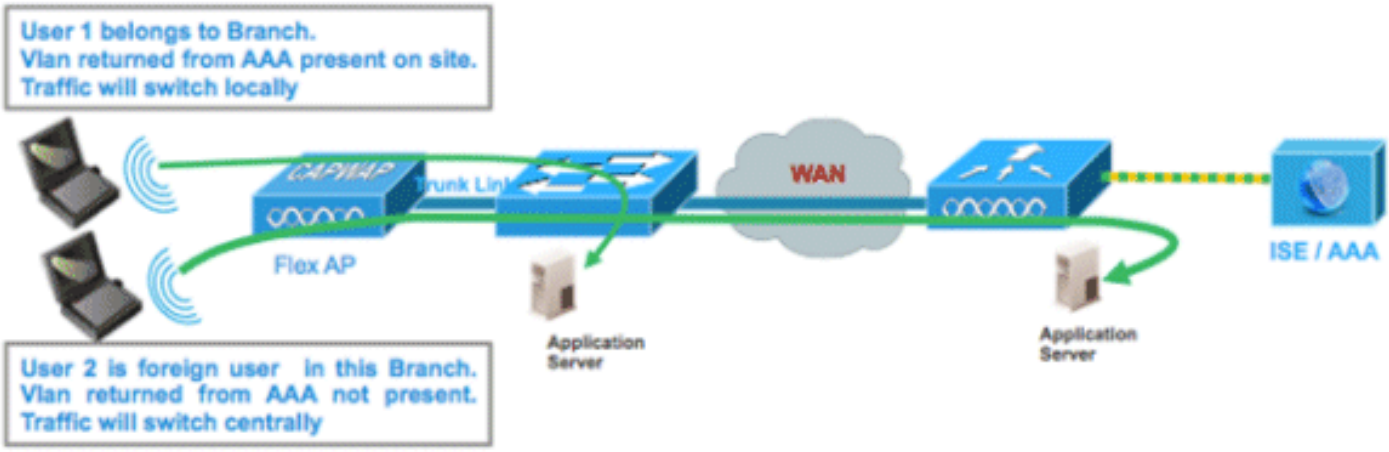
Limitaciones

- No se admitirán los atributos específicos de **Cisco Airespace** y sólo se admitirá el ID de VLAN de atributo IETF.
- Se puede configurar un máximo de 16 VLAN en la configuración por AP, ya sea a través del mapping WLAN-VLAN para el punto de acceso FlexConnect individual o mediante el mapping ACL-VLAN en el grupo FlexConnect.

Switching central basado en VLAN FlexConnect

En las versiones 7.2 del software del controlador, el reemplazo AAA de VLAN (asignación de VLAN dinámica) para las WLANs conmutadas localmente colocará a los clientes inalámbricos en la VLAN proporcionada por el servidor AAA. Si la VLAN proporcionada por el servidor AAA no está presente en el AP, el cliente se coloca en una VLAN asignada a la WLAN en ese AP y el tráfico se conmutará localmente en esa VLAN. Además, antes de la versión 7.3, el tráfico para una WLAN determinada de los AP de FlexConnect se puede conmutar de forma centralizada o local según la configuración de la WLAN.

A partir de la versión 7.3 en adelante, el tráfico de los AP de FlexConnect se puede conmutar de forma centralizada o local según la presencia de una VLAN en un AP de FlexConnect.



Summary

Flujo de tráfico en las WLANs configuradas para el Switching Local cuando los APs Flex están en el Modo Conectado:

- Si la VLAN se devuelve como uno de los atributos AAA y esa VLAN no está presente en la base de datos Flex AP, el tráfico se conmutará centralmente y al cliente se le asignará esta VLAN/interfaz devuelta desde el servidor AAA siempre que la VLAN exista en el WLC.
- Si la VLAN se devuelve como uno de los atributos AAA y esa VLAN no está presente en la base de datos Flex AP, el tráfico se conmutará de forma centralizada. Si esa VLAN tampoco está presente en el WLC, al cliente se le asignará una VLAN/interfaz asignada a una WLAN en el WLC.
- Si la VLAN se devuelve como uno de los atributos AAA y esa VLAN está presente en la base de datos de FlexConnect AP, el tráfico se conmutará localmente.
- Si la VLAN no se devuelve del servidor AAA, al cliente se le asignará una VLAN asignada a la WLAN en ese punto de acceso FlexConnect y el tráfico se conmutará localmente.

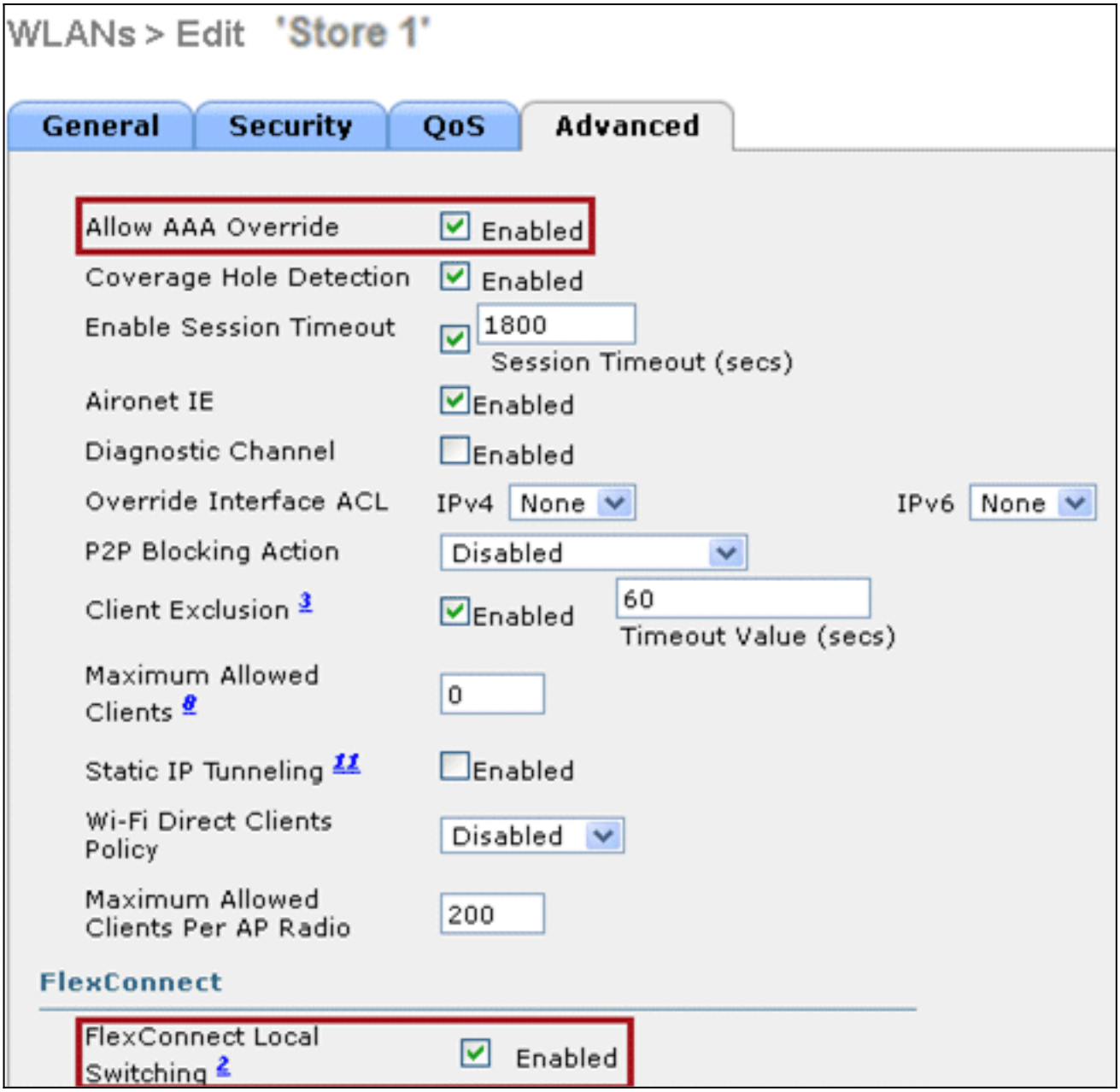
Flujo de tráfico en las WLANs configuradas para el Switching Local cuando los APs Flex están en el Modo Independiente:

- Si la VLAN devuelta por un servidor AAA no está presente en la base de datos Flex AP, el cliente será colocado en la VLAN predeterminada (es decir, una VLAN asignada a WLAN en Flex AP). Cuando el AP se conecta de nuevo, este cliente será desautenticado y conmutará el tráfico de forma centralizada.
- Si la VLAN devuelta por un servidor AAA está presente en la base de datos de Flex AP, el cliente se pondrá en una VLAN devuelta y el tráfico se conmutará localmente.
- Si la VLAN no se devuelve desde un servidor AAA, al cliente se le asignará una VLAN asignada a la WLAN en ese punto de acceso FlexConnect y el tráfico se conmutará localmente.

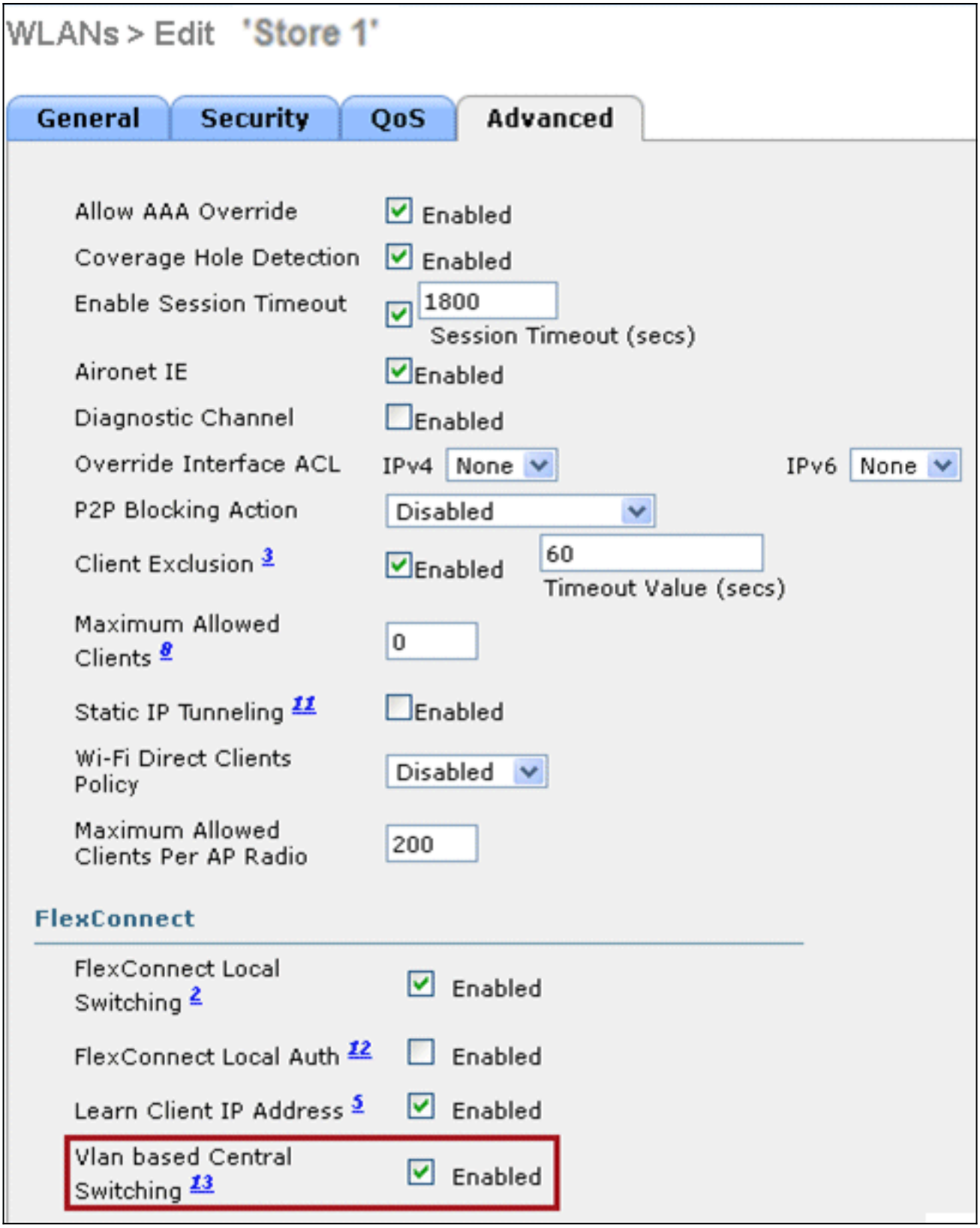
Procedimiento

Complete estos pasos:

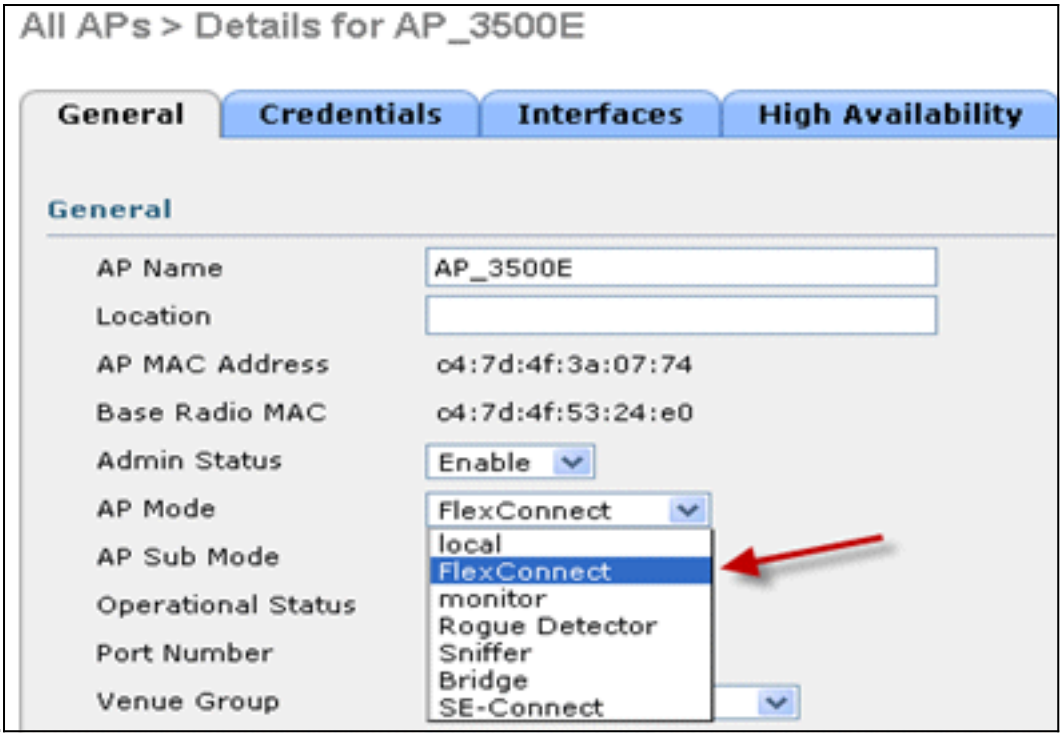
1. Configure una WLAN para Local Switching y habilite el reemplazo AAA.



2. Habilite **Switching Central Basado en Vlan** en la WLAN recién creada.

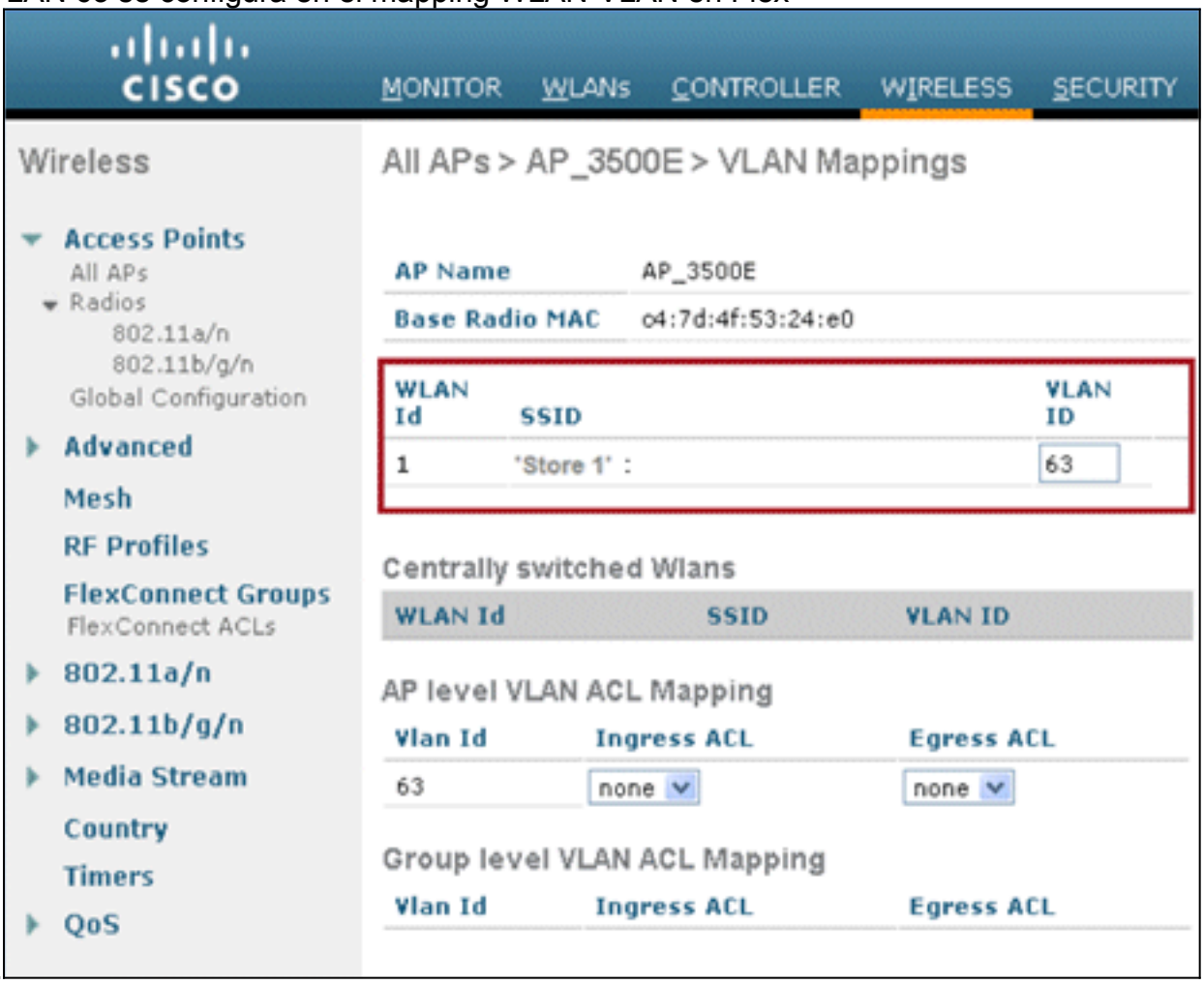


3. Establezca AP Mode en



FlexConnect.

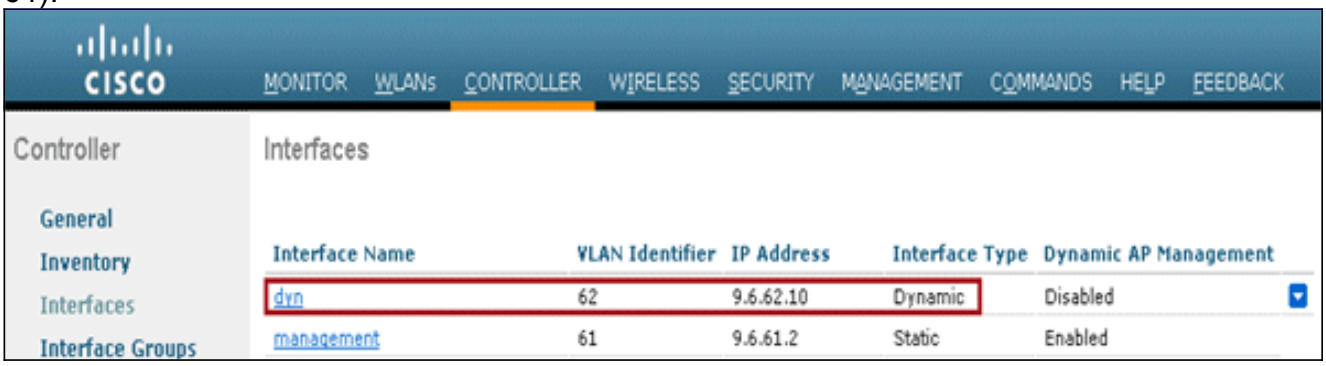
4. Asegúrese de que el punto de acceso FlexConnect tenga alguna subinterfaz presente en su base de datos, ya sea a través del mapping WLAN-VLAN en un punto de acceso flexible determinado o a través de la configuración de VLAN desde un grupo Flex. En este ejemplo, la VLAN 63 se configura en el mapping WLAN-VLAN en Flex



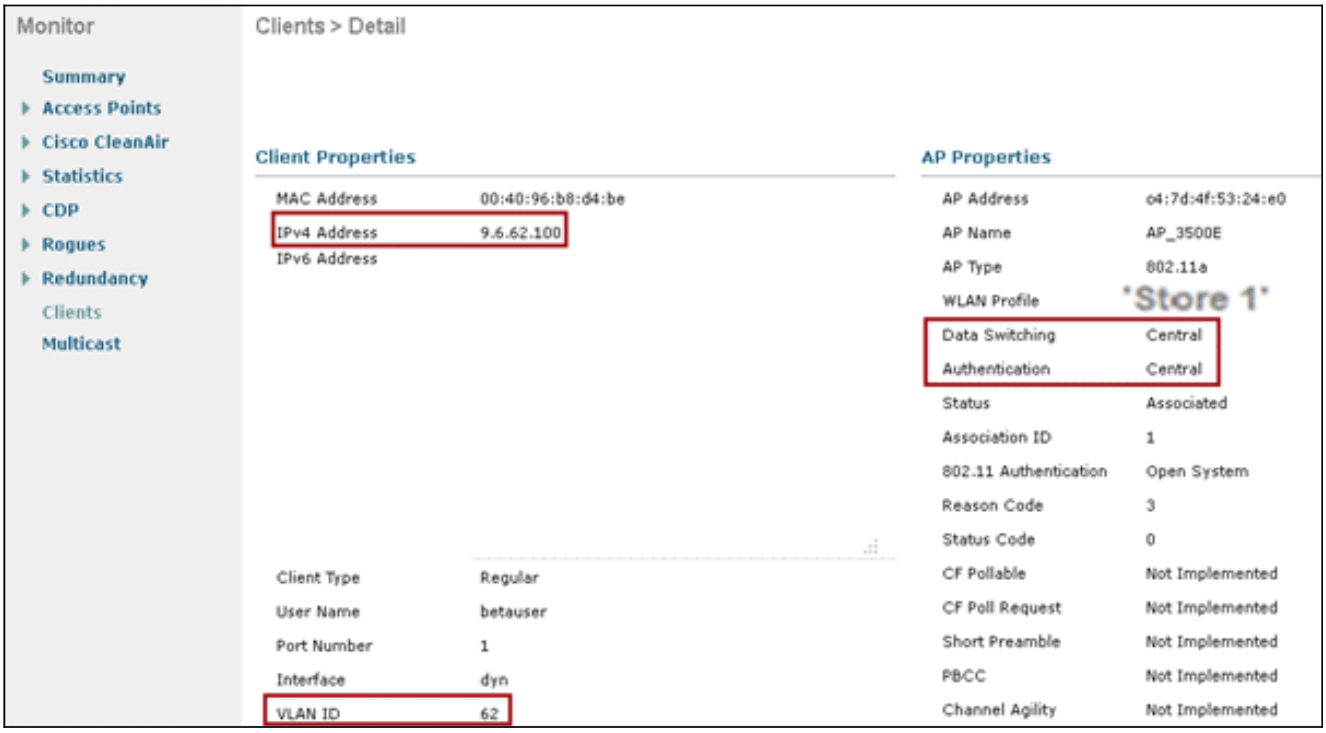
AP.

5. En este ejemplo, la VLAN 62 se configura en el WLC como una de las interfaces dinámicas y no se mapea a la WLAN en el WLC. La WLAN en el WLC se mapea a la VLAN de administración (es decir, VLAN

61).

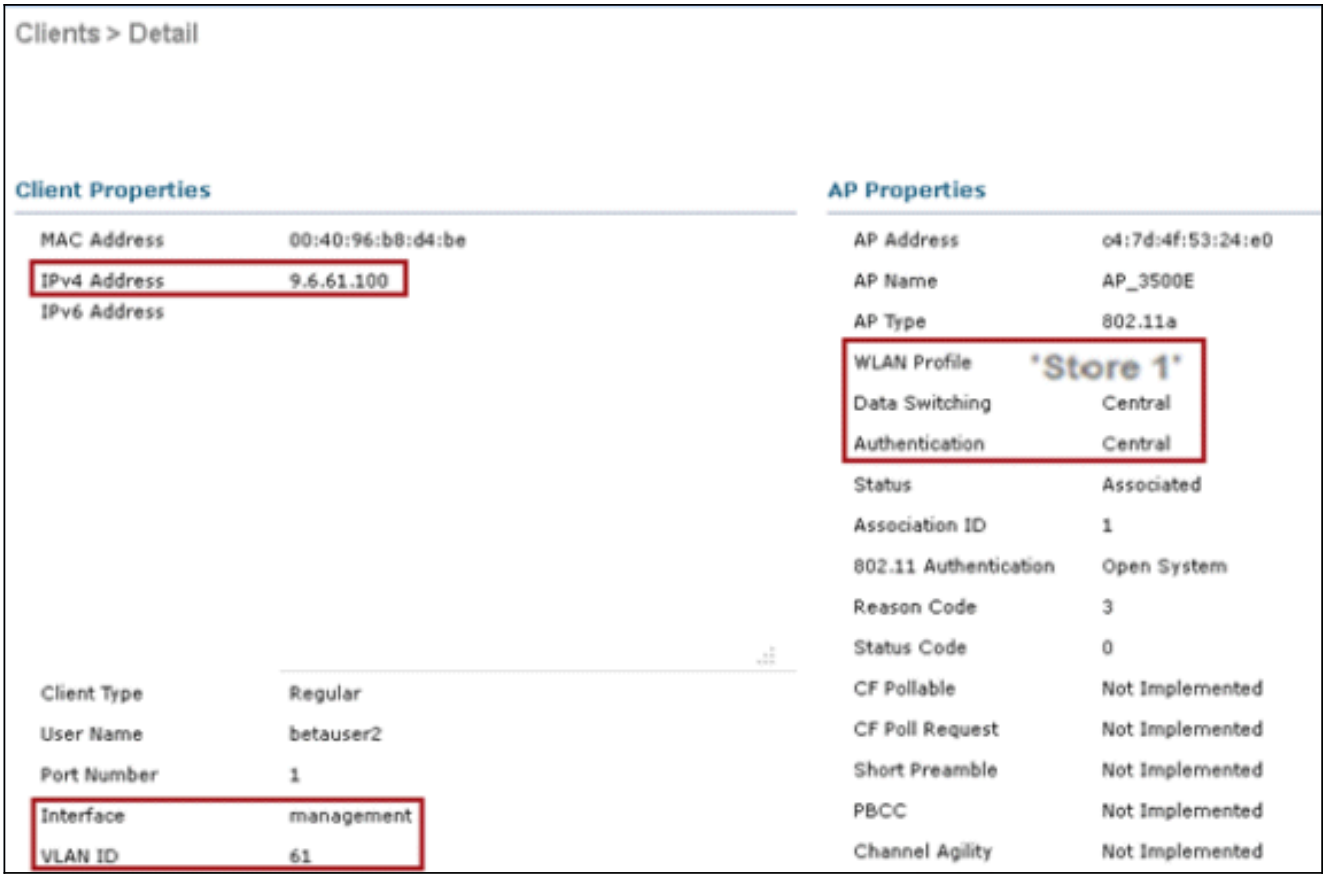


6. Asocie un cliente a la WLAN configurada en el Paso 1 en este Flex AP y devuelva la VLAN 62 del servidor AAA. La VLAN 62 no está presente en este Flex AP, pero está presente en el WLC como una interfaz dinámica, por lo que el tráfico se conmutará de forma centralizada y al cliente se le asignará VLAN 62 en el WLC. En el resultado capturado aquí, al cliente se le ha asignado VLAN 62 y la conmutación y autenticación de datos se configuran en **Central**.



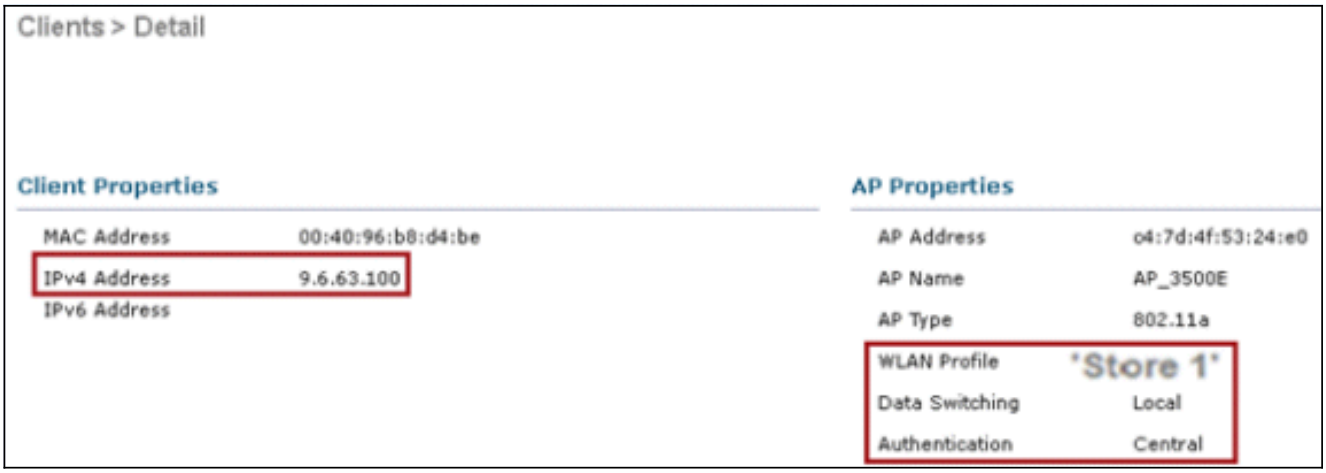
Nota: Observe que aunque la WLAN se configura para Local Switching, el campo Data Switching para este cliente es Central basado en la presencia de una VLAN (es decir, VLAN 62, que se devuelve del servidor AAA, no está presente en la base de datos AP).

7. Si otro usuario se asocia al mismo AP en esta WLAN creada y alguna VLAN se devuelve del servidor AAA que no está presente en el AP así como en el WLC, el tráfico se conmutará centralmente y al cliente se le asignará la interfaz mapeada WLAN en el WLC (es decir, VLAN 61 en esta configuración de ejemplo), porque la WLAN se mapea a la interfaz de administración configurada para VLAN
61



Nota: Observe que aunque la WLAN está configurada para Local Switching, el campo Data Switching para este cliente es Central basado en la presencia de una VLAN. Es decir, la VLAN 61, que se devuelve del servidor AAA, no está presente en la base de datos AP pero tampoco está presente en la base de datos del WLC. Como resultado, al cliente se le asigna una interfaz VLAN/interfaz predeterminada que se asigna a la WLAN. En este ejemplo, la WLAN se mapea a una interfaz de administración (es decir, VLAN 61) y así el cliente ha recibido una dirección IP de la VLAN 61.

8. Si otro usuario se asocia a él en esta WLAN creada y la VLAN 63 se devuelve del servidor AAA (que está presente en este punto de acceso flexible), al cliente se le asignará VLAN 63 y el tráfico se conmutará
localmente.



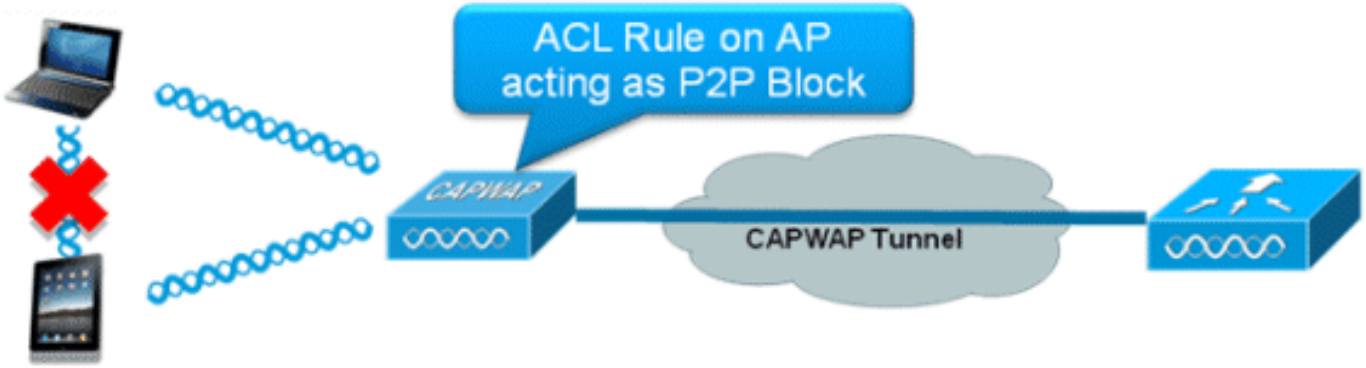
Limitaciones

- El Switching Central Basado en VLAN sólo se soporta en las WLANs configuradas para la Autenticación Central y el Switching Local.

- La subinterfaz AP (es decir, asignación de VLAN) se debe configurar en el punto de acceso FlexConnect.

ACL de FlexConnect

Con la introducción de las ACL en FlexConnect, existe un mecanismo para satisfacer la necesidad de control de acceso en el punto de acceso FlexConnect para la protección e integridad del tráfico de datos conmutados localmente desde el punto de acceso. Las ACL de FlexConnect se crean en el WLC y luego deben configurarse con la VLAN presente en el grupo FlexConnect AP o FlexConnect mediante la asignación de VLAN-ACL que será para las VLAN de invalidación de AAA. Estos se envían luego al AP.



Summary

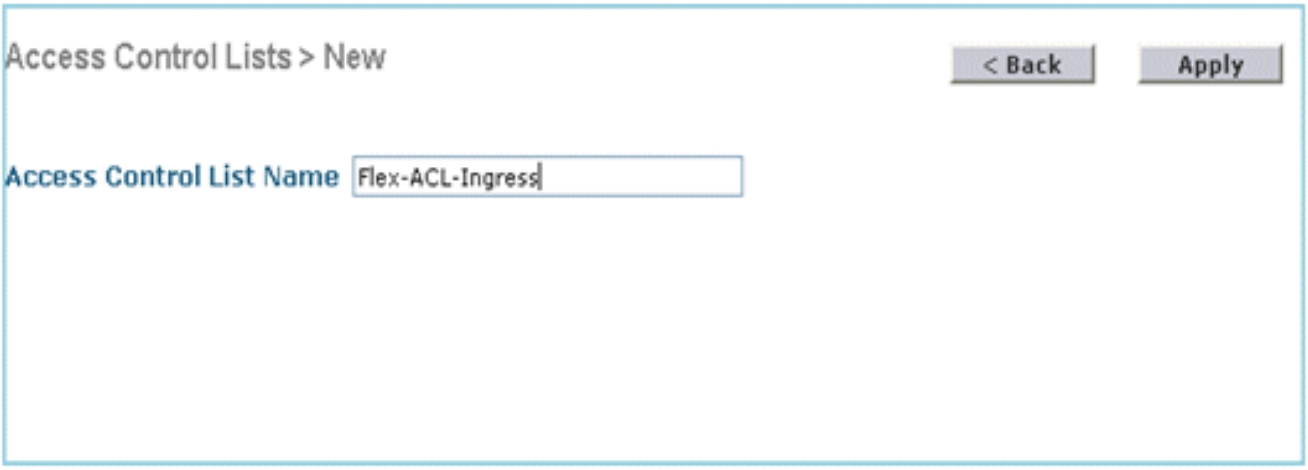
- Cree una ACL de FlexConnect en el controlador.
- Aplique lo mismo en una VLAN presente en FlexConnect AP bajo la asignación de ACL de VLAN de Nivel AP.
- Se puede aplicar en una VLAN presente en el grupo FlexConnect bajo la asignación de VLAN-ACL (generalmente se realiza para las VLAN anuladas por AAA).
- Al aplicar ACL en VLAN, seleccione la dirección a aplicar que será "ingreso", "egreso" o "ingreso y egreso".

Procedimiento

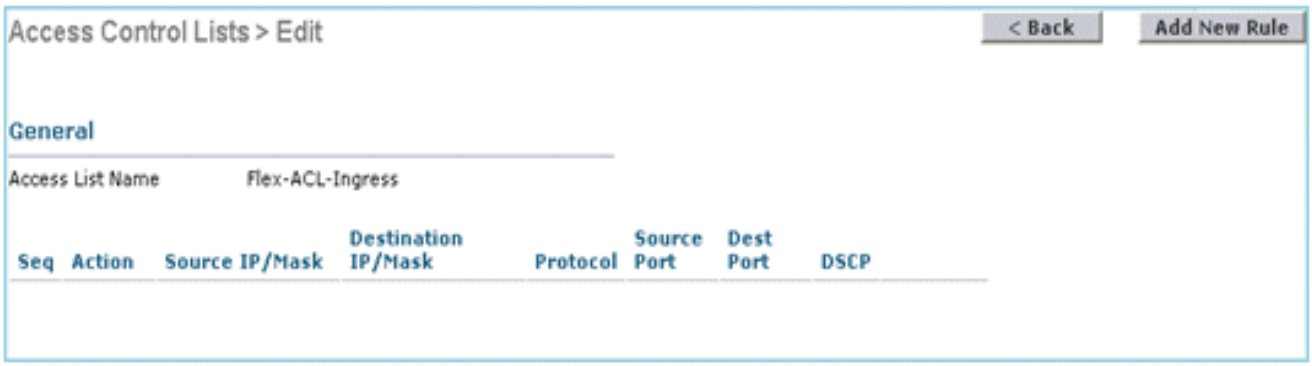
Complete estos pasos:

1. Cree una ACL FlexConnect en el WLC. Navegue hasta **GUI del WLC > Seguridad > Lista de Control de Acceso > ACL de FlexConnect**.

2. Haga clic en **New**.
3. Configure el nombre ACL.



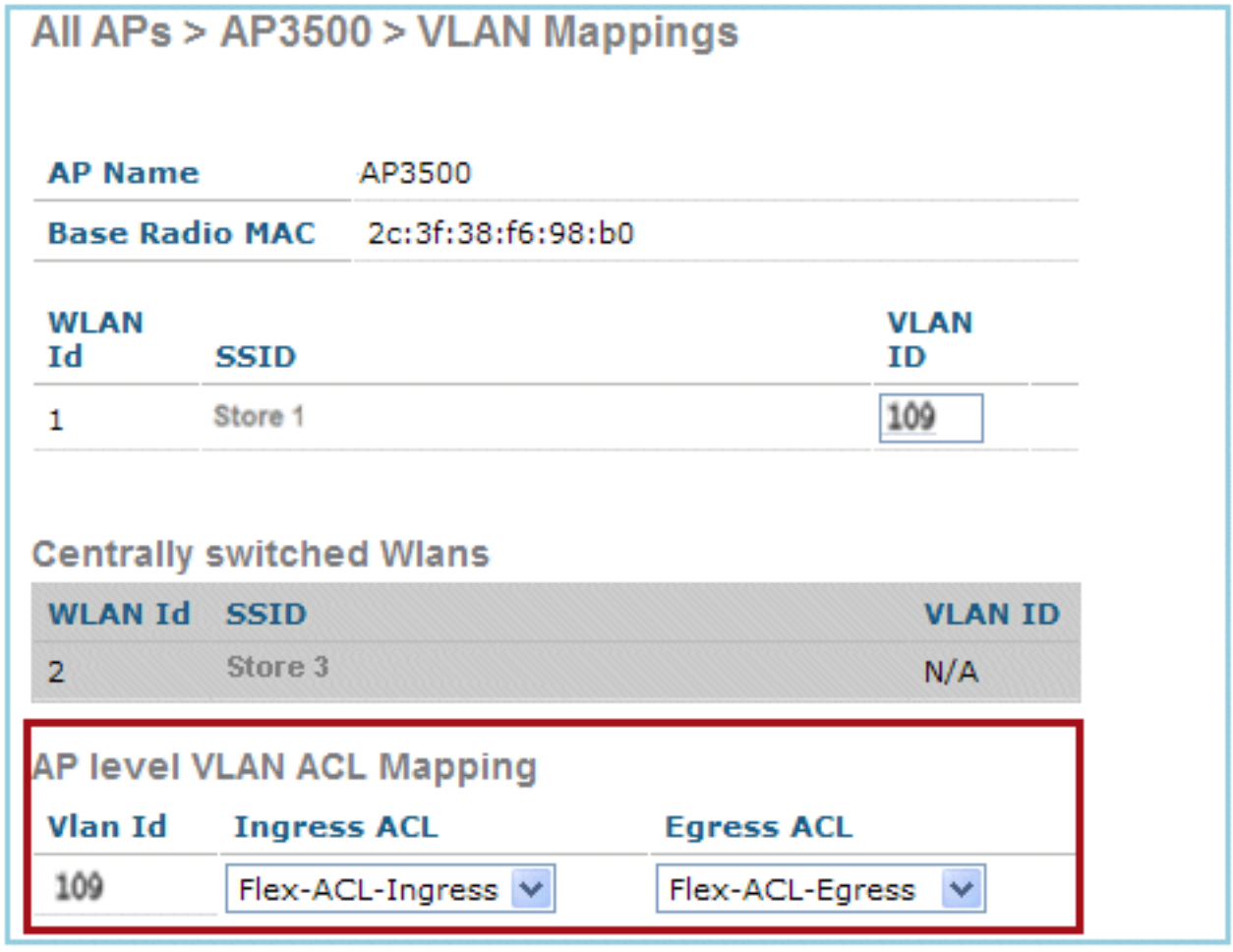
4. Haga clic en Apply (Aplicar).
5. Cree reglas para cada ACL. Para crear reglas, navegue hasta **WLC GUI > Seguridad > Lista de Control de Acceso > ACL de FlexConnect** y haga clic en la ACL creada anteriormente.



6. Haga clic en **Agregar nueva regla**.

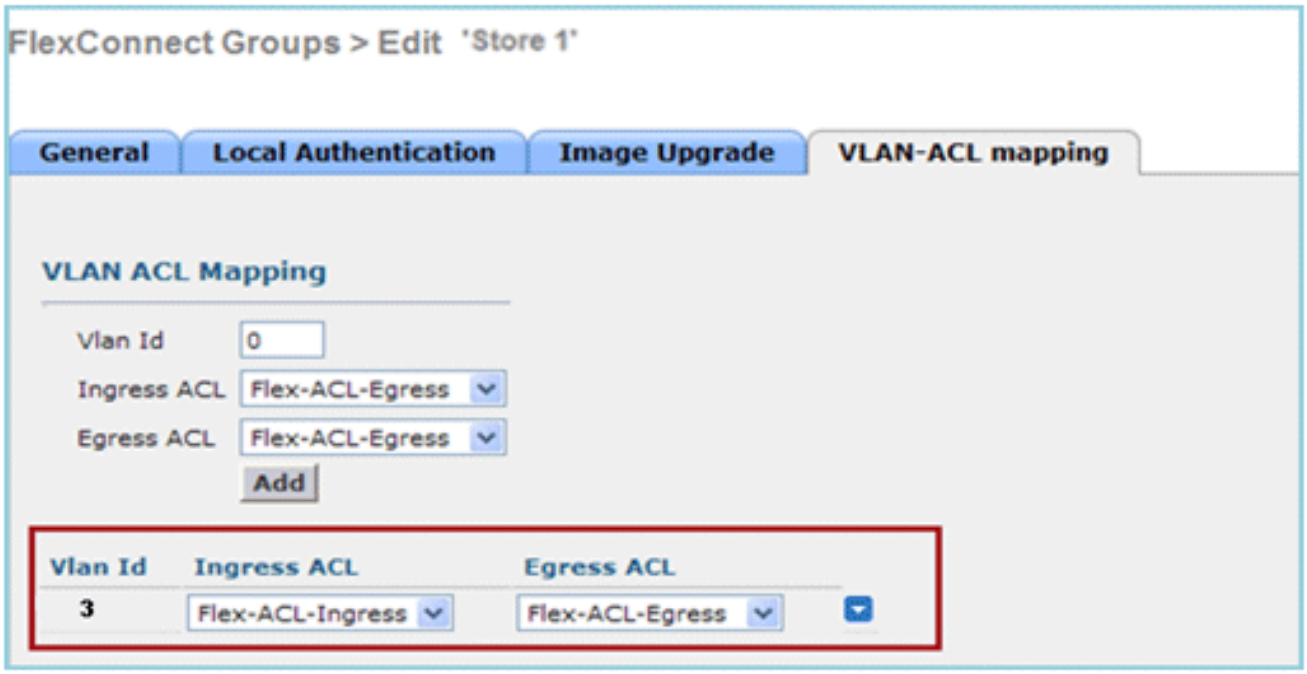
Nota: Configure las reglas según el requisito. Si no se configura la regla permit any any al final, hay una negación implícita que bloqueará todo el tráfico.

7. Una vez creadas las ACL de FlexConnect, se puede asignar para la asignación WLAN-VLAN bajo un punto de acceso FlexConnect individual o se puede aplicar en la asignación VLAN-ACL en el grupo FlexConnect.
8. Asigne la ACL FlexConnect configurada arriba en el nivel AP para las VLAN individuales bajo las asignaciones de VLAN para el punto de acceso FlexConnect individual. Vaya a WLC GUI > **Wireless** > **All AP** > haga clic en el AP específico > la pestaña FlexConnect > **VLAN Mapping**.



9. FlexConnect ACL también se puede aplicar en la asignación de VLAN-ACL en el grupo FlexConnect. Las VLAN creadas bajo la asignación VLAN-ACL en el grupo FlexConnect se

utilizan principalmente para la invalidación de VLAN dinámica.



Limitaciones

- Se puede configurar un máximo de 512 ACL FlexConnect en el WLC.
- Cada ACL individual se puede configurar con 64 reglas.
- Se puede asignar un máximo de 32 ACL por grupo FlexConnect o por punto de acceso FlexConnect.
- En cualquier momento dado, hay un máximo de 16 VLAN y 32 ACL en el punto de acceso FlexConnect.

Tunelización dividida FlexConnect

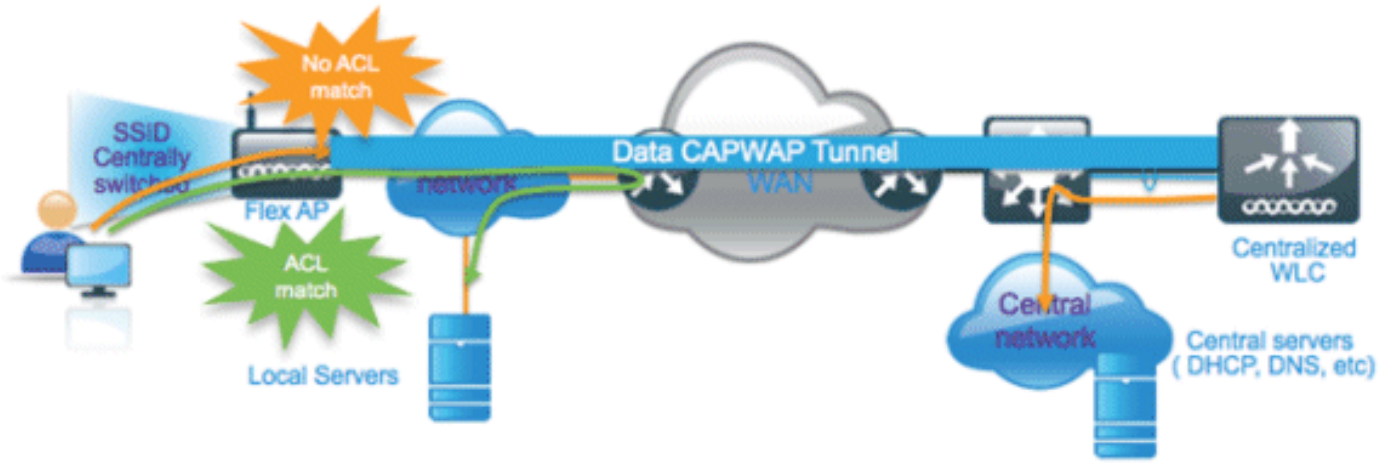
En las versiones del WLC anteriores a la 7.3, si un cliente que se conecta en un punto de acceso FlexConnect asociado con una WLAN conmutada centralmente necesita enviar algo de tráfico a un dispositivo presente en el sitio/red local, necesitan enviar tráfico a través de CAPWAP al WLC y luego obtener el mismo tráfico de vuelta al sitio local a través de CAPWAP o usando alguna conectividad fuera de banda.

A partir de la versión 7.3 en adelante, la **tunelización dividida** introduce un mecanismo por el cual el tráfico enviado por el cliente se clasificará según el contenido del paquete **usando Flex ACL**. Los paquetes coincidentes se conmutan localmente desde Flex AP y el resto de los paquetes se conmutan centralmente a través de CAPWAP.

La funcionalidad de tunelización dividida es una ventaja añadida para la configuración de AP OEAP, en la que los clientes de un SSID corporativo pueden comunicarse con los dispositivos de una red local (impresoras, máquinas cableadas en un puerto LAN remoto o dispositivos inalámbricos en un SSID personal) directamente sin consumir ancho de banda WAN enviando paquetes a través de CAPWAP. La tunelización dividida no se soporta en los AP OEAP 600. Flex ACL se puede crear con reglas para permitir todos los dispositivos presentes en el sitio/red local. Cuando los paquetes de un cliente inalámbrico en el SSID corporativo coinciden con las reglas de Flex ACL configuradas en el AP OEAP, ese tráfico se conmuta localmente y el resto del tráfico (es

decir, tráfico de denegación implícito) se conmutará centralmente sobre CAPWAP.

La solución de tunelización dividida supone que la subred/VLAN asociada a un cliente en el sitio central no está presente en el sitio local (es decir, el tráfico para los clientes que reciben una dirección IP de la subred presente en el sitio central no podrá conmutar localmente). La funcionalidad de tunelización dividida está diseñada para conmutar el tráfico localmente para las subredes que pertenecen al sitio local para evitar el consumo de ancho de banda de la WAN. El tráfico que coincide con las reglas de Flex ACL se conmuta localmente y el funcionamiento de NAT se realiza cambiando la dirección IP de origen del cliente a la dirección IP de la interfaz BVI de Flex AP que se puede enrutar en el sitio/red local.



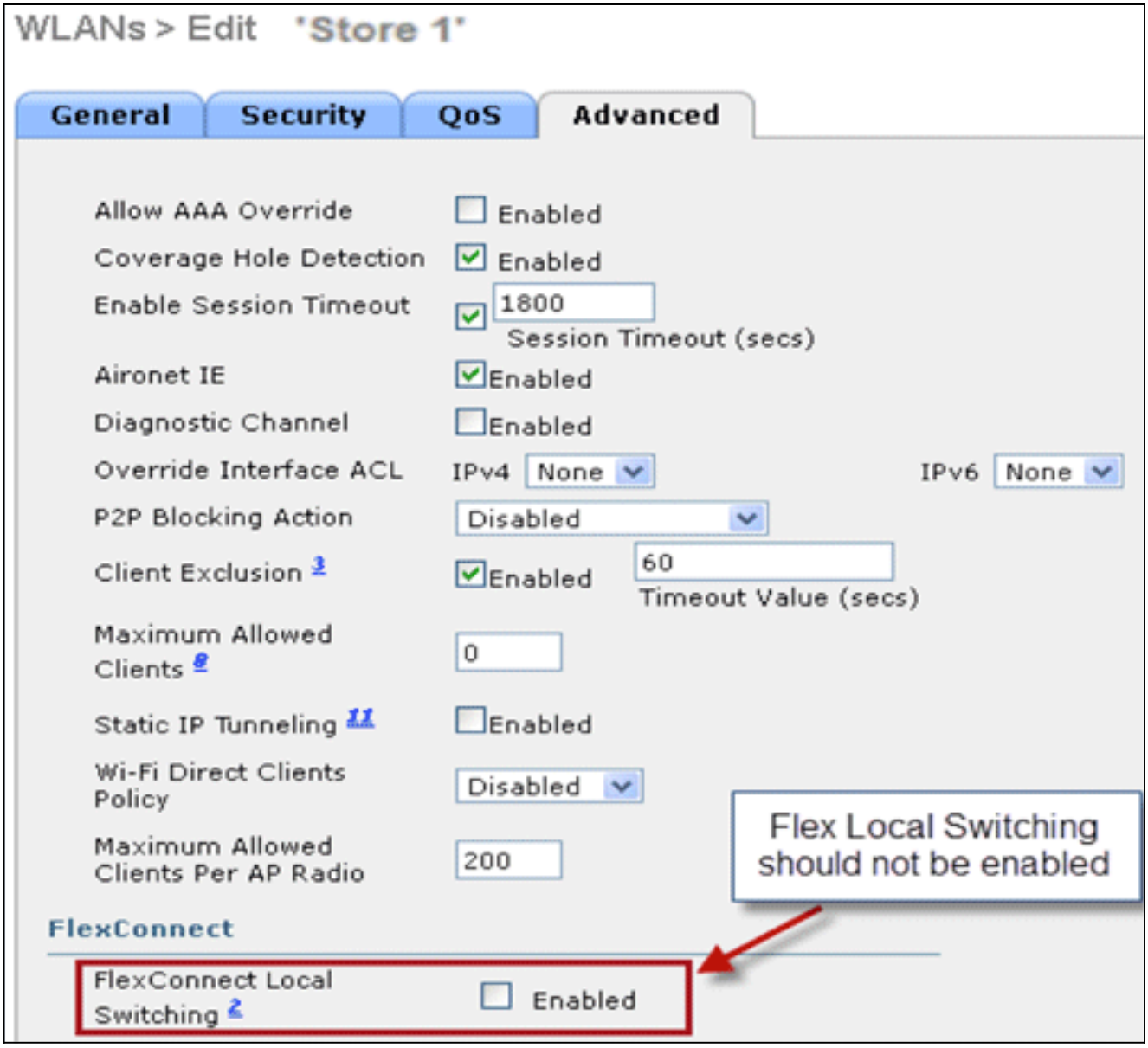
Summary

- La funcionalidad de Tunelización Dividida se soporta en las WLANs configuradas para el Switching Central anunciado solamente por los APs Flex.
- El DHCP requerido debe estar habilitado en las WLAN configuradas para la tunelización dividida.
- La configuración de tunelización dividida se aplica por WLAN configurada para el switching central en cada punto de acceso flexible o para todos los puntos de acceso flexibles en un grupo FlexConnect.

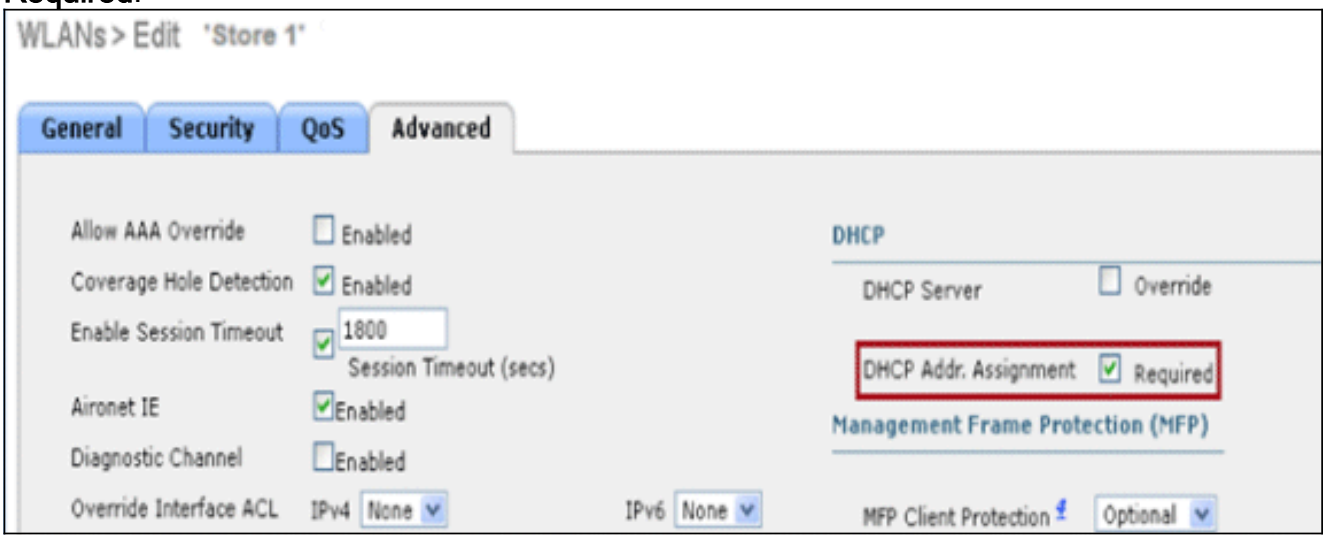
Procedimiento

Complete estos pasos:

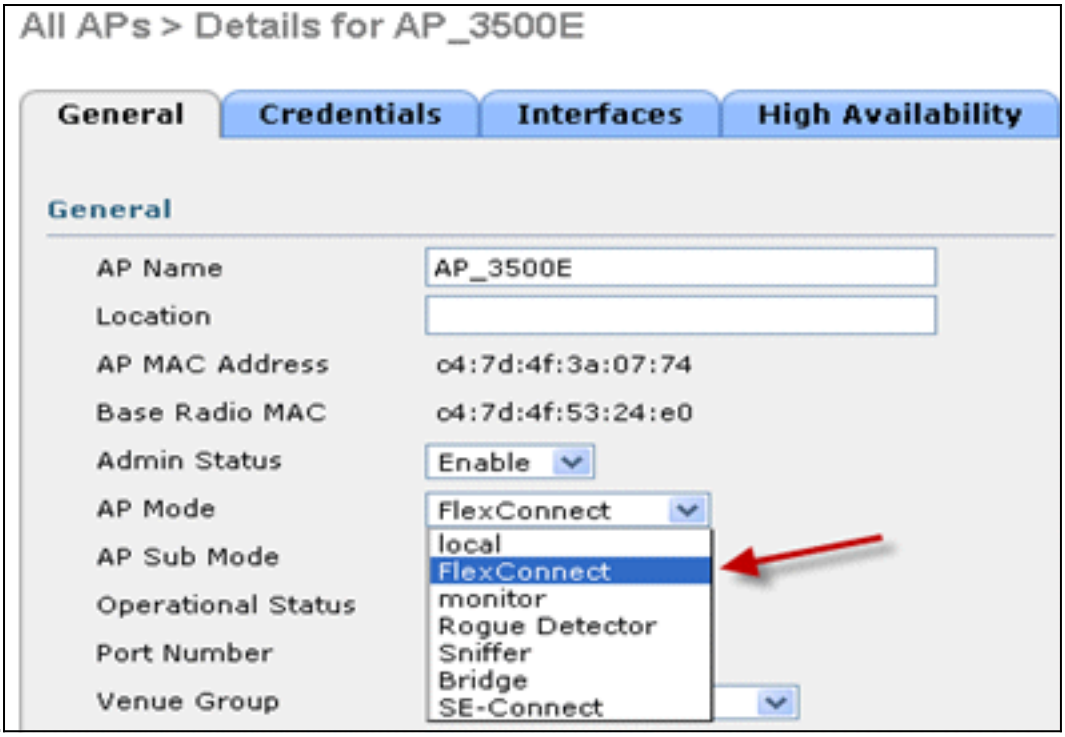
1. Configure una WLAN para Central Switching (es decir, **Flex Local Switching** no debería estar habilitado).



2. Establezca DHCP Address Assignment (Asignación de dirección DHCP) en **Required**.



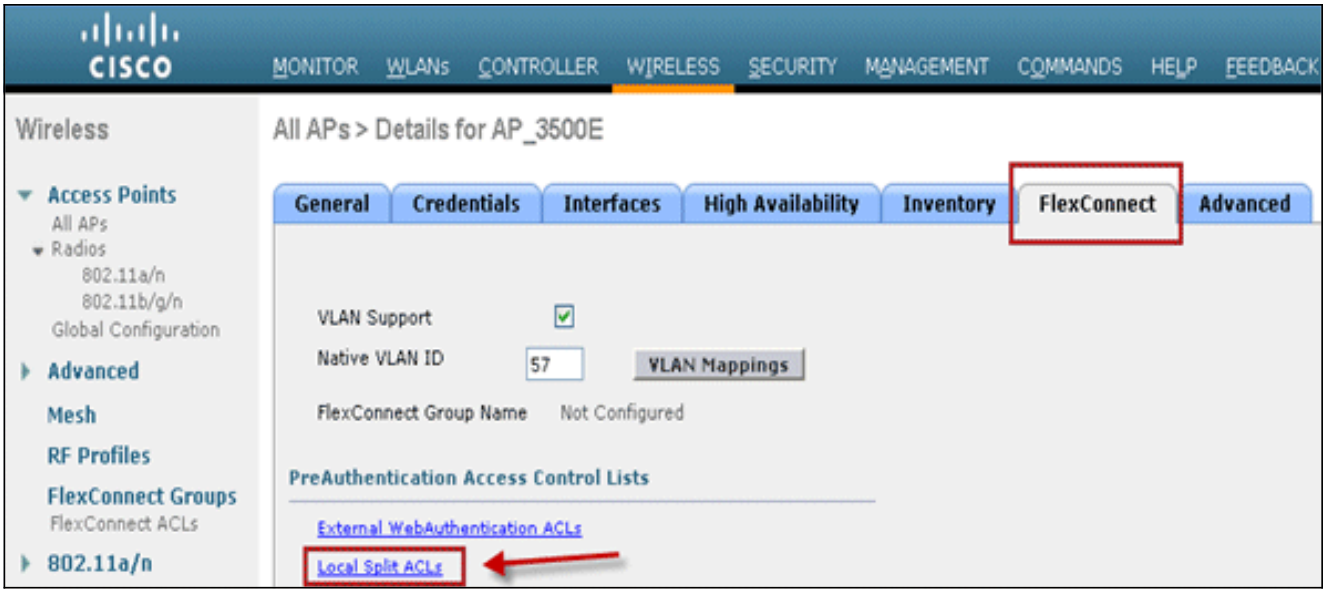
3. Establezca AP Mode en



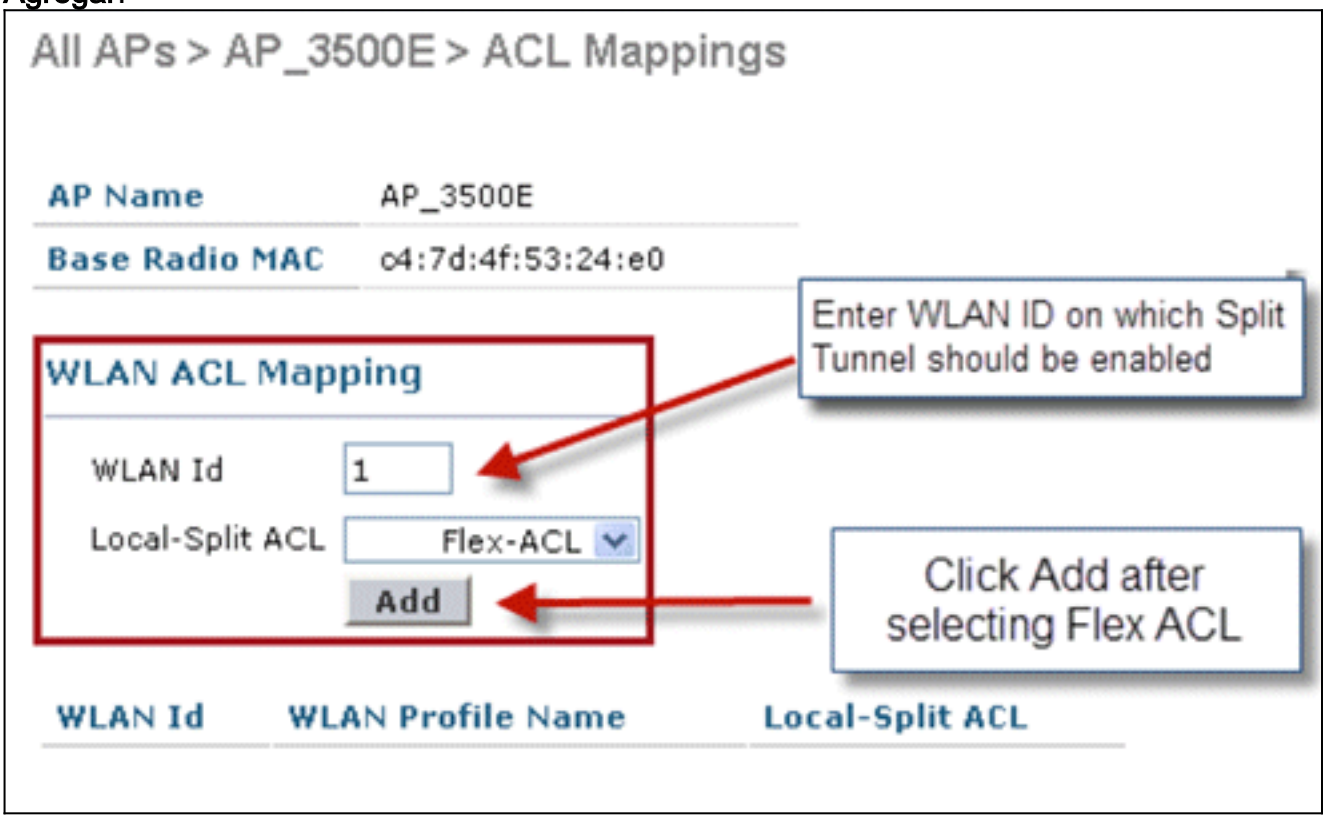
FlexConnect.

4. Configure la ACL de FlexConnect con una regla de permiso para el tráfico que se debe conmutar localmente en la WLAN del switch central. En este ejemplo, se configura la regla de ACL de FlexConnect para que avise al tráfico ICMP de todos los clientes que están en la subred 9.6.61.0 (es decir, que existen en el sitio central) a 9.1.0.150 para que se conmute localmente después de que la operación de NAT se aplique en Flex AP. El resto del tráfico llegará a una regla de denegación implícita y se conmutará centralmente sobre CAPWAP.

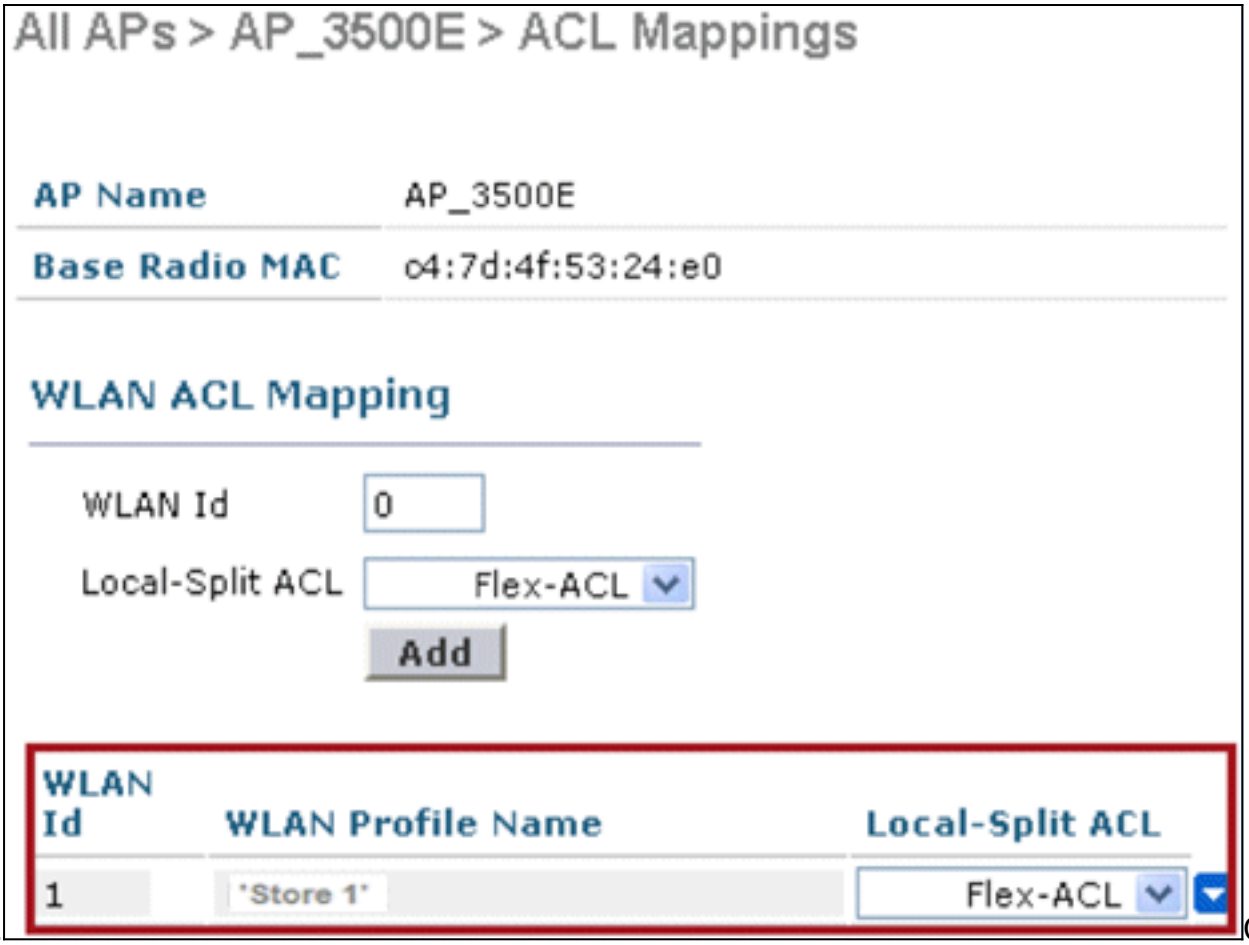
5. Esta ACL FlexConnect creada se puede enviar como una ACL de túnel dividido a un punto de acceso flexible individual o también se puede enviar a todos los puntos de acceso flexibles en un grupo de Flex Connect.Complete estos pasos para presionar Flex ACL como una ACL Dividida Local para un Flex AP individual:Haga clic en **ACL divididas locales**.



Seleccione **WLAN Id** en la función de túnel dividido que se debe habilitar, elija **Flex-ACL** y haga clic en
Agregar.



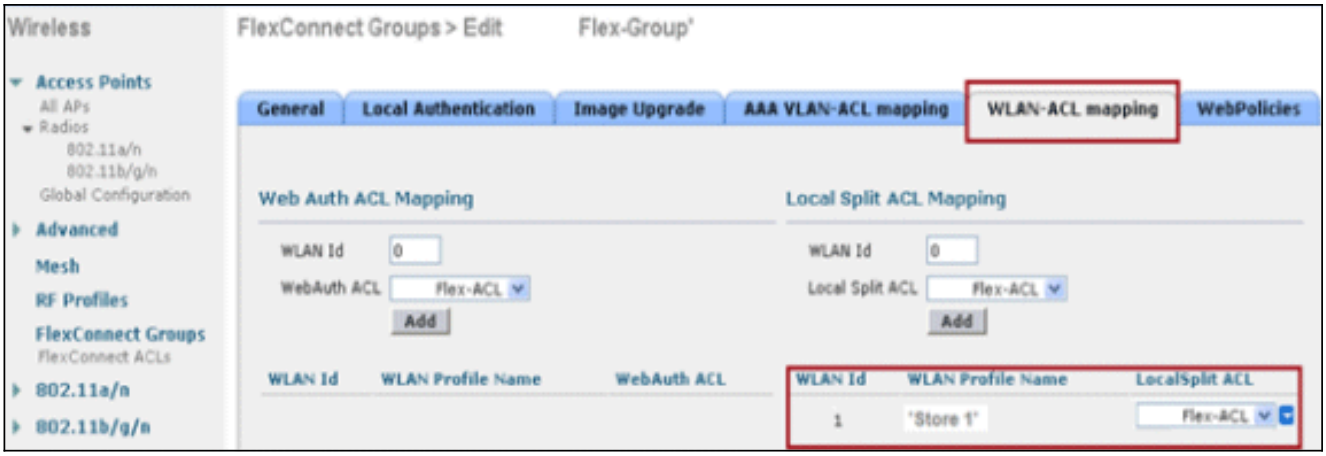
Flex-ACL se envía como ACL dividida local al Flex



AP.C

omplete estos pasos para presionar Flex ACL como ACL Dividida Local a un Grupo FlexConnect:Seleccione el ID de WLAN en el que se debe habilitar la función de tunelización dividida. En la pestaña **mapeo WLAN-ACL**, seleccione FlexConnect ACL del grupo FlexConnect donde se agregan determinados Flex AP y haga clic en **Agregar**.

Flex-ACL se envía como ACL de división local a AP flexibles en ese grupo Flex.



Limitaciones

- Las reglas de ACL flexible no se deben configurar con la instrucción permit/deny con la misma subred que el origen y el destino.
- El tráfico en una WLAN conmutada centralmente configurada para la tunelización dividida se puede conmutar localmente solamente cuando un cliente inalámbrico inicia el tráfico para un host presente en el sitio local. Si el tráfico es iniciado por los clientes/host en un sitio local para los clientes inalámbricos en estas WLAN configuradas, no podrá alcanzar el destino.
- La tunelización dividida no es compatible con el tráfico de multidifusión/difusión. El tráfico de multidifusión/difusión se conmutará de forma centralizada aunque coincida con la ACL flexible.

Tolerancia de fallas

FlexConnect Fault Tolerance permite el acceso inalámbrico y los servicios a los clientes de las sucursales cuando:

- Los puntos de acceso de sucursal FlexConnect pierden conectividad con el controlador Flex 7500 principal.
- Los puntos de acceso de la sucursal FlexConnect están cambiando al controlador secundario Flex 7500.
- Los puntos de acceso de sucursal FlexConnect están restableciendo la conexión con el controlador Flex 7500 principal.

FlexConnect Fault Tolerance, junto con el EAP local descrito anteriormente, proporcionan un tiempo de inactividad de sucursal cero durante una interrupción de la red. Esta función está activada de forma predeterminada y no se puede desactivar. No requiere configuración en el controlador o AP. No obstante, para garantizar que la tolerancia a las fallas funciona sin problemas y es aplicable, deben mantenerse estos criterios:

- Los pedidos y las configuraciones de WLAN deben ser idénticos en los controladores Flex 7500 principales y de respaldo.
- La asignación de VLAN debe ser idéntica en los controladores Flex 7500 principal y de respaldo.
- El nombre de dominio de movilidad debe ser idéntico en los controladores Flex 7500 principales y de respaldo.
- Se recomienda utilizar Flex 7500 como controladores primarios y de respaldo.

Summary

- FlexConnect no desconectará los clientes cuando el AP se conecte nuevamente al mismo controlador siempre que no haya cambios en la configuración en el controlador.
- FlexConnect no desconectará los clientes cuando se conecte al controlador de respaldo siempre que no haya cambios en la configuración y el controlador de respaldo sea idéntico al controlador principal.
- FlexConnect no restablecerá sus radios al conectarse de nuevo al controlador principal siempre que no haya cambios en la configuración del controlador.

Limitaciones

- Solo se admite para FlexConnect con autenticación central/local con conmutación local.
- Los clientes autenticados centralmente requieren una reautenticación completa si el temporizador de sesión del cliente caduca antes de que el punto de acceso FlexConnect pase del modo autónomo al modo conectado.
- Los controladores primarios y de respaldo de Flex 7500 deben estar en el mismo dominio de movilidad.

Límite de cliente por WLAN

Junto con la segmentación del tráfico, surge la necesidad de restringir el acceso total del cliente a los servicios inalámbricos.

Ejemplo: Limitación del total de clientes invitados de la tunelización de la sucursal al Data Center.

Para hacer frente a este desafío, Cisco está introduciendo la función Client Limit per WLAN que puede restringir el total de clientes permitidos por WLAN.

Objetivo principal

- Establecer límites para clientes máximos
- Facilidad operativa

Nota: Esta no es una forma de QoS.

De forma predeterminada, la función está desactivada y no fuerza el límite.

Limitaciones

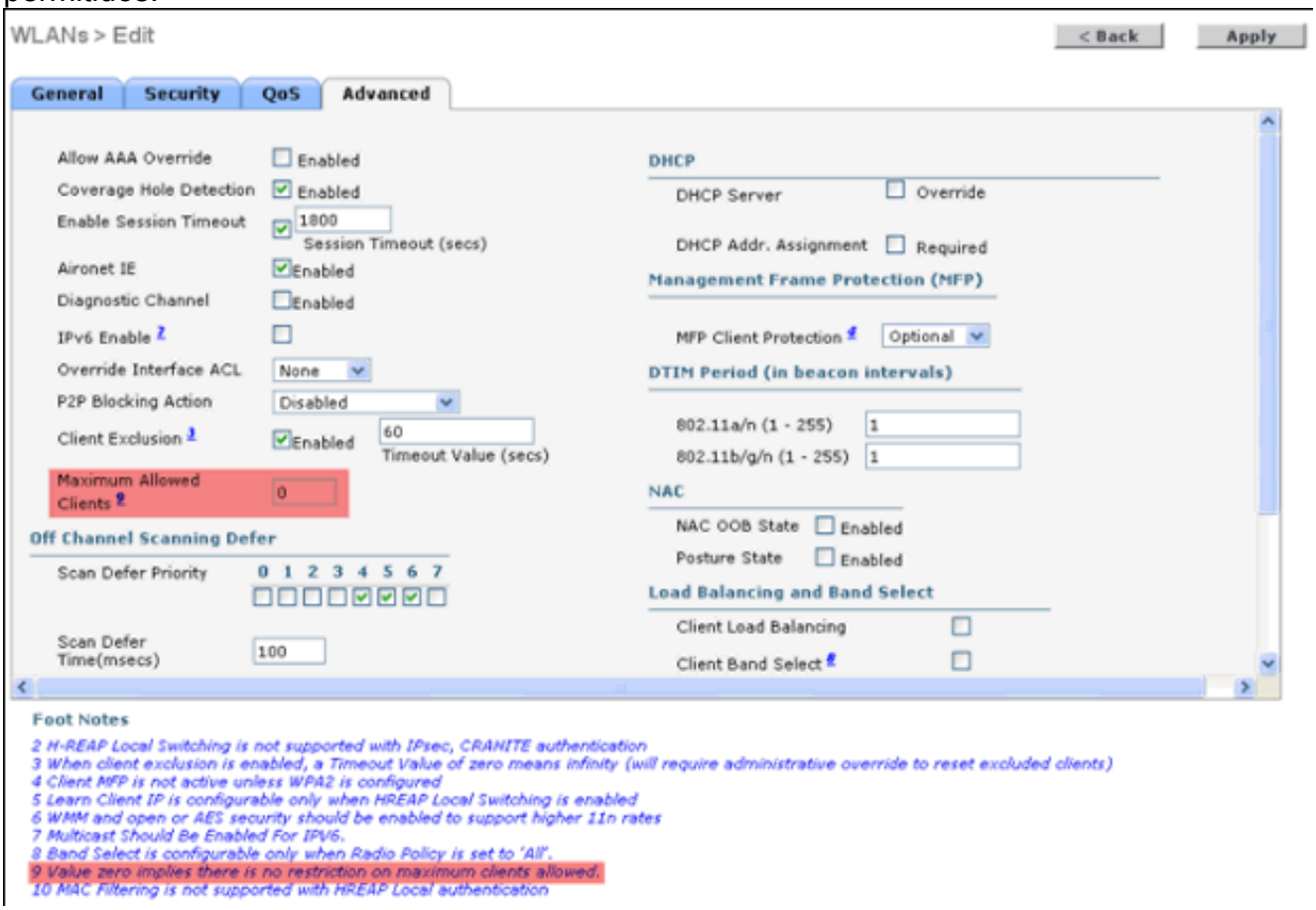
Esta función no impone el límite del cliente cuando FlexConnect está en estado de funcionamiento autónomo.

Configuración de WLC

Complete estos pasos:

1. Seleccione el ID de WLAN 1 conmutado centralmente con SSID **DataCenter**. Esta WLAN fue creada durante la creación del grupo AP. Consulte la Figura 8.

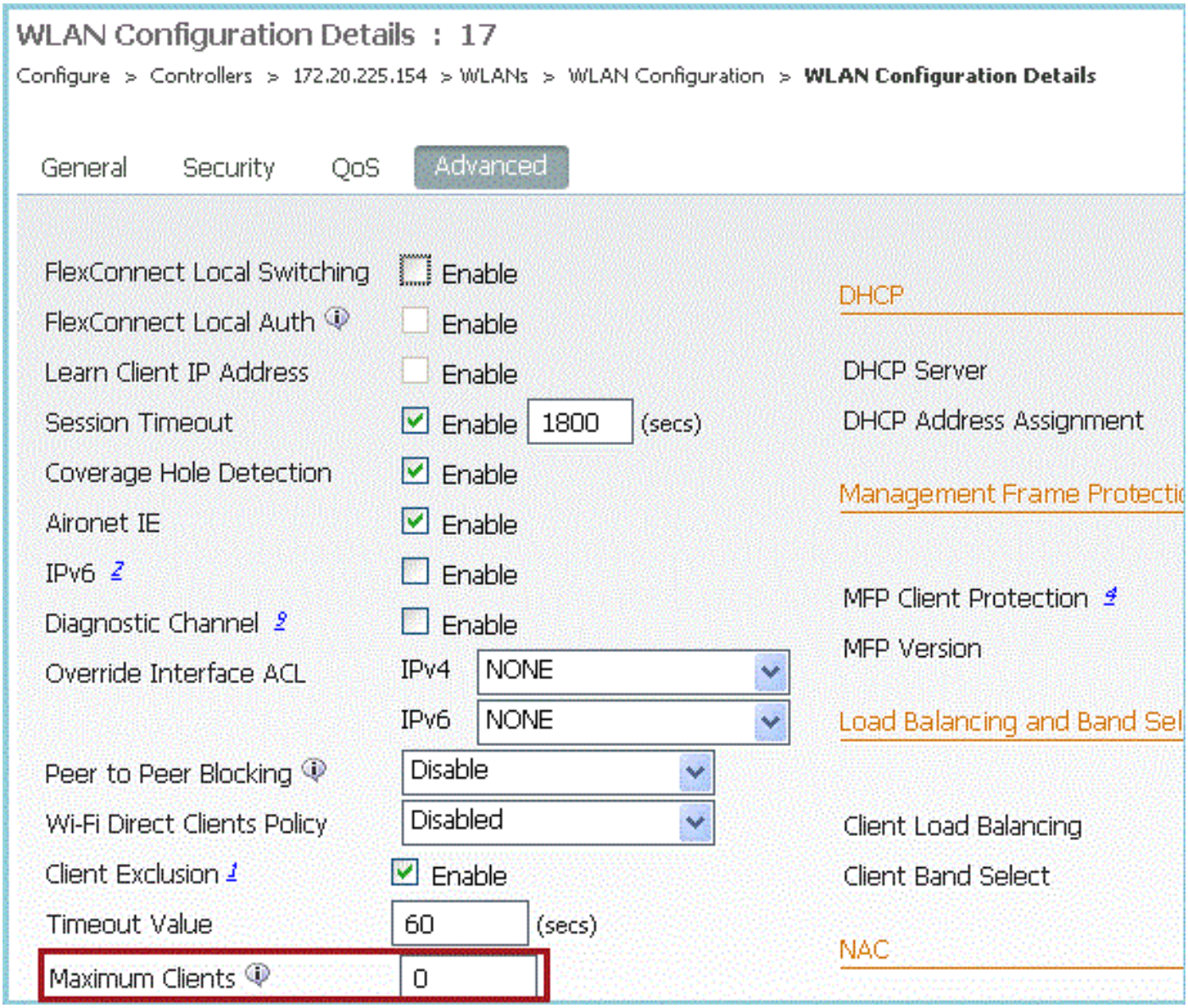
2. Haga clic en la pestaña **Advanced** para el ID de WLAN 1.
3. Establezca el valor límite de cliente para el campo de texto Máximo de clientes permitidos.
4. Haga clic en **Aplicar** después de establecer el campo de texto para el número máximo de clientes
   permitidos.



   El valor predeterminado para el número máximo de clientes permitidos es 0, lo que implica que no hay restricción y que la función está desactivada.

Configuración de NCS

Para habilitar esta función desde el NCS, vaya a Configure > Controllers > Controller IP > **WLANs > WLAN Configuration > WLAN Configuration Details**.

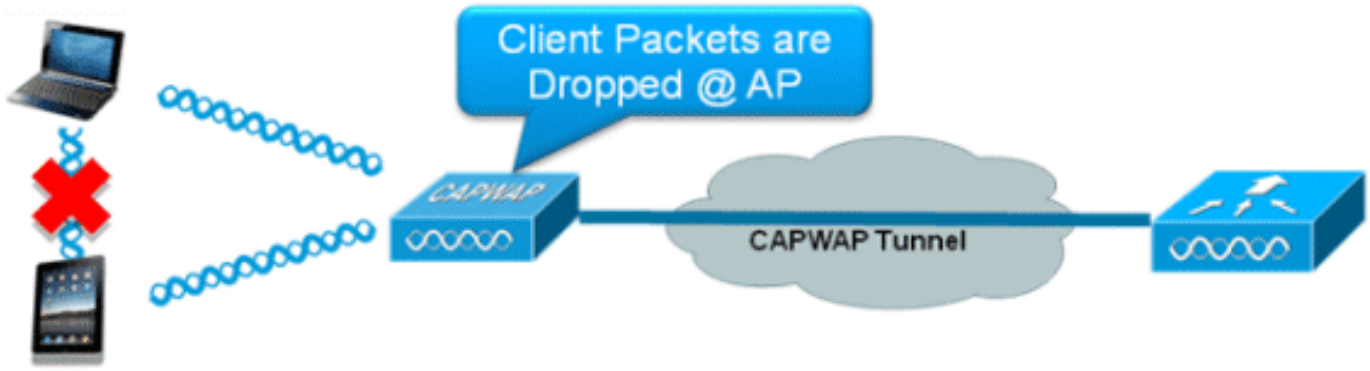


Bloqueo de igual a igual

En las versiones de software del controlador anteriores a la 7.2, el bloqueo de igual a igual (P2P) solo se admitía para las WLAN de switching central. El bloqueo de igual a igual se puede configurar en WLAN con cualquiera de estas tres acciones:

- **Deshabilitado**: inhabilita el bloqueo de peer a peer y el tráfico puenteado localmente dentro del controlador para los clientes en la misma subred. Este es el valor predeterminado.
- **Drop** - Hace que el controlador descarte paquetes para los clientes en la misma subred.
- **Forward Up-Stream** - Hace que el paquete sea reenviado en la VLAN ascendente. Los dispositivos que se encuentran encima del controlador deciden qué acción tomar con respecto al paquete.

Desde la versión 7.2 en adelante, el bloqueo de igual a igual es soportado por los clientes asociados en la WLAN de conmutación local. Por WLAN, la configuración de peer-to-peer se envía por el controlador al punto de acceso FlexConnect.



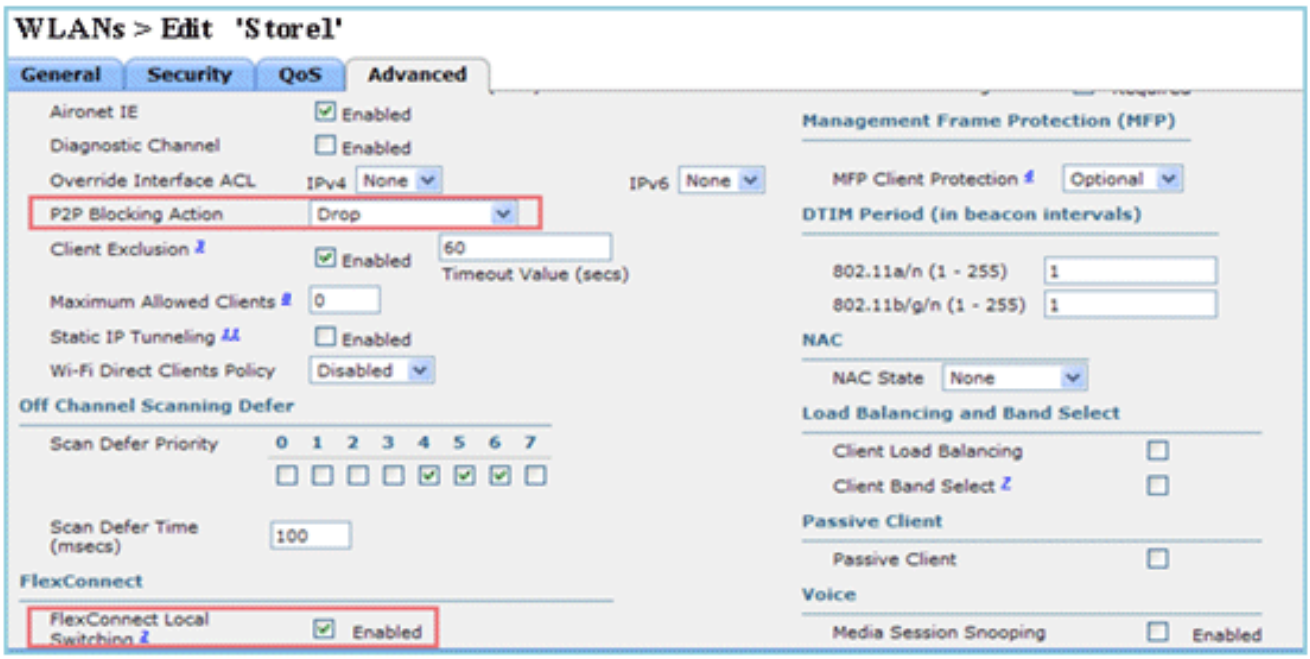
Summary

- El bloqueo de igual a igual se configura por WLAN
- Por WLAN, el WLC envía la configuración de bloqueo de peer a peer a los AP de FlexConnect.
- La acción de bloqueo de igual a igual configurada como drop o upstream-forward en WLAN se trata como bloqueo de igual a igual habilitado en FlexConnect AP.

Procedimiento

Complete estos pasos:

1. Habilite la acción de bloqueo de peer a peer como **Drop** en WLAN configurada para FlexConnect Local
   Switching.



2. Una vez que la acción de bloqueo P2P se configura como **Drop** o **Forward-Upstream** en la WLAN configurada para el switching local, se envía del WLC al AP FlexConnect. Los AP de FlexConnect almacenarán esta información en el archivo de configuración de reap en la memoria flash. Con esto, incluso cuando FlexConnect AP está en modo autónomo, puede aplicar la configuración P2P en las subinterfaces correspondientes.

Limitaciones

- En FlexConnect, la configuración de bloqueo P2P de la solución no se puede aplicar solamente a un punto de acceso o subconjunto de puntos de acceso de FlexConnect determinado. Se aplica a todos los AP de FlexConnect que emiten el SSID.
- La solución unificada para clientes de switching central admite el reenvío ascendente P2P. Sin embargo, esto no se admitirá en la solución FlexConnect. Esto se trata como pérdida P2P y los paquetes de cliente se descartan en lugar de reenviarse al siguiente nodo de red.
- La solución unificada para clientes de switching central admite el bloqueo P2P para clientes asociados a diferentes AP. Sin embargo, esta solución se dirige solamente a los clientes conectados al mismo AP. Las ACL de FlexConnect se pueden utilizar como solución alternativa para esta limitación.

Descarga previa a la imagen de AP

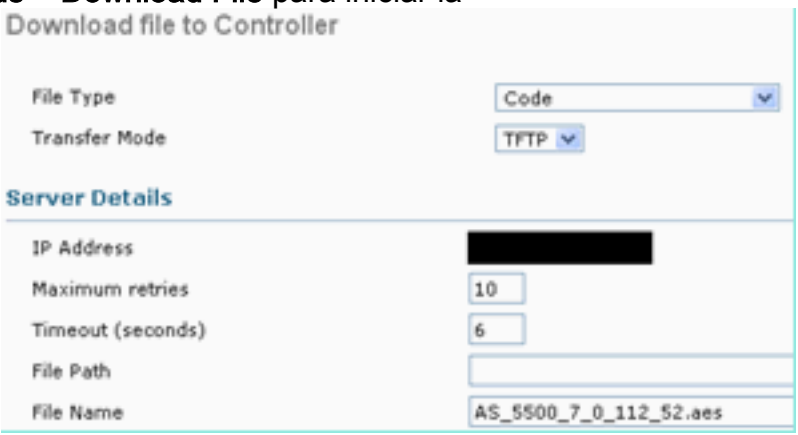
Esta función permite que el AP descargue el código mientras está en funcionamiento. La descarga previa de la imagen AP es extremadamente útil para reducir el tiempo de inactividad de la red durante el mantenimiento o las actualizaciones del software.

Summary

- Facilidad de gestión de software
- Programar actualizaciones por tienda: NCS es necesario para lograr esto
- Reduce el tiempo de inactividad

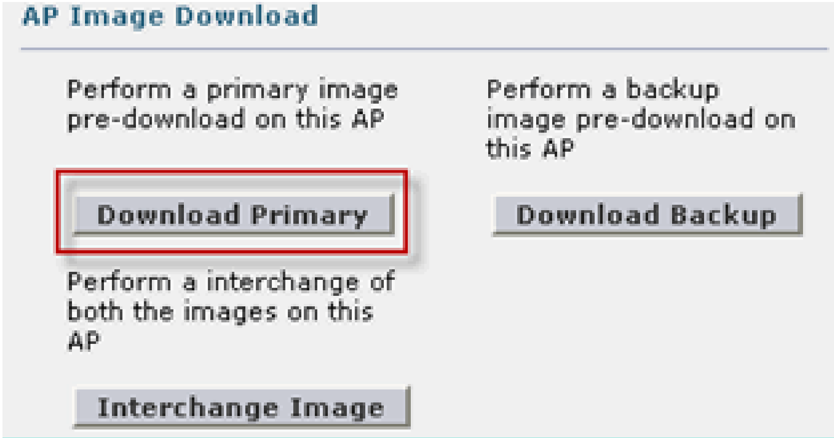
Procedimiento

Complete estos pasos:

1. Actualice la imagen en los controladores primario y de respaldo.Navegue bajo **WLC GUI > Commands > Download File** para iniciar la descarga. 

2. Guarde las configuraciones en los controladores, pero no reinicie el controlador.
3. Ejecute el comando AP pre-image download desde el controlador primario.Navegue hasta **WLC GUI > Wireless > Access Points > All AP** y elija el punto de acceso para iniciar la descarga previa a la imagen.Una vez elegido el punto de acceso, haga clic en la pestaña **Avanzadas**.Haga clic en **Descargar primario** para iniciar la descarga previa de la

imagen.




```
*Sep [redacted].903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [redacted]not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
    Version Suffix: k9w8-.wnbu_j_mr.201009101910
    Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
    Ios Image Size: 5530112
    Total Image Size: 5550592
    Image Feature: WIRELESS LAN|LWAPP
    Image Family: C1250
    Wireless Switch Management Version: [redacted]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre[redacted]..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.
```

4. Reinicie los controladores después de descargar todas las imágenes AP.Los AP ahora vuelven al modo autónomo hasta que los controladores se reinician.**Nota:** En el modo autónomo, la tolerancia a fallos mantendrá a los clientes asociados.Una vez que el controlador vuelve, los APs se reinician automáticamente con la imagen previamente descargada.Después del reinicio, los AP se vuelven a unir al controlador primario y reanudan los servicios del cliente.

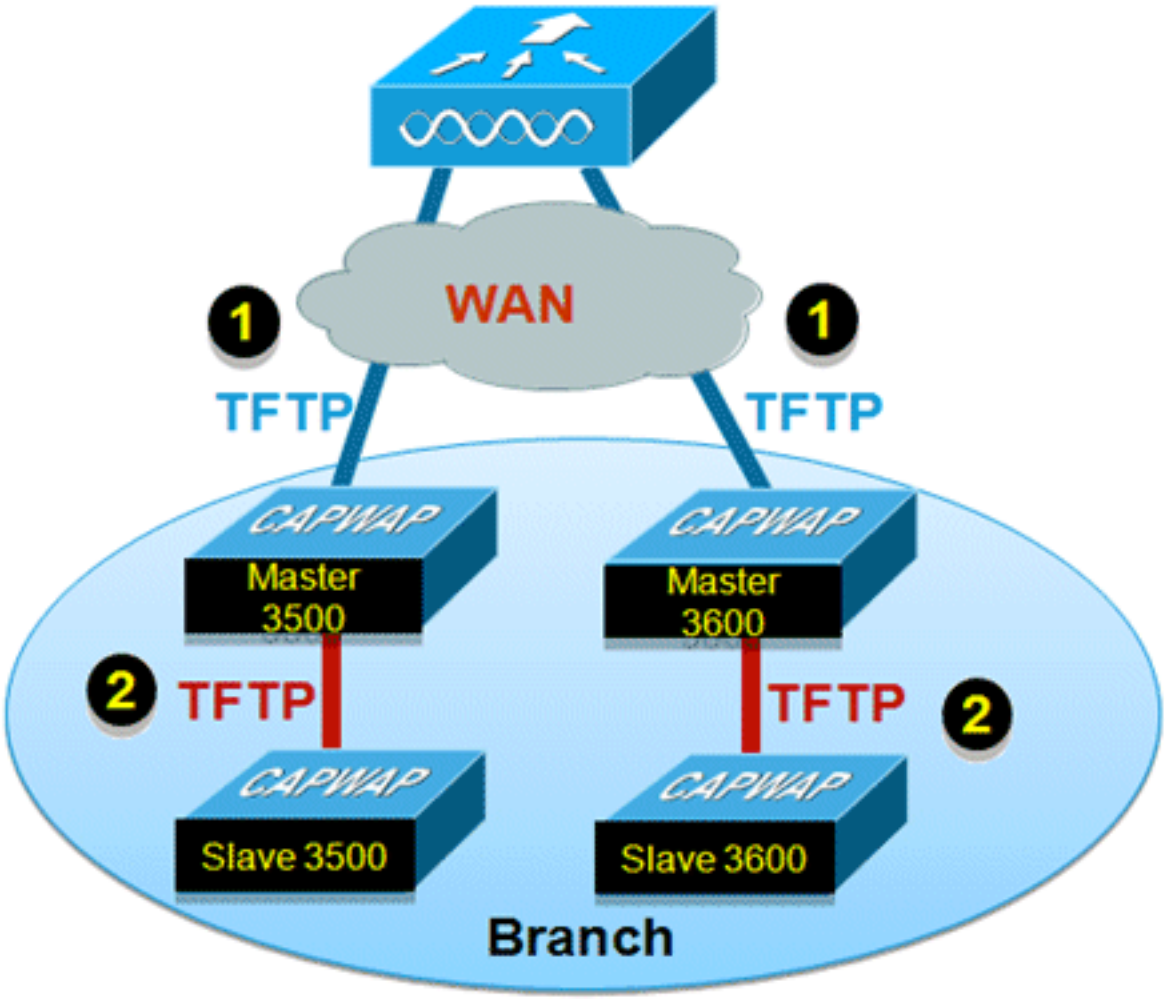
Limitaciones

- Funciona sólo con los AP CAPWAP.

Actualización de imagen FlexConnect Smart AP

La función de descarga previa a la imagen reduce en cierta medida la duración del tiempo de inactividad, pero aún así todos los puntos de acceso FlexConnect tienen que descargar previamente las respectivas imágenes AP a través del enlace WAN con una latencia mayor.

La actualización eficaz de la imagen de punto de acceso reducirá el tiempo de inactividad de cada punto de acceso FlexConnect. La idea básica es que solamente un AP de cada modelo AP descargará la imagen del controlador y actuará como maestro/servidor, y el resto de los AP del mismo modelo funcionará como esclavo/cliente y pre-descargará la imagen AP del maestro. La distribución de la imagen AP del servidor al cliente estará en una red local y no experimentará la latencia del link WAN. Como resultado, el proceso será más rápido.



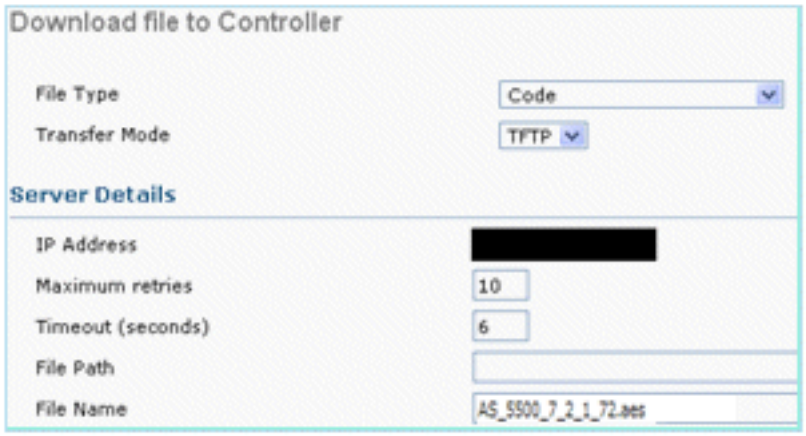
Summary

- Se seleccionan AP maestros y esclavos para cada modelo de AP por grupo de FlexConnect
- Imagen de descarga maestra del WLC
- Imagen de descarga esclava del AP maestro
- Reduce el tiempo de inactividad y ahorra ancho de banda WAN

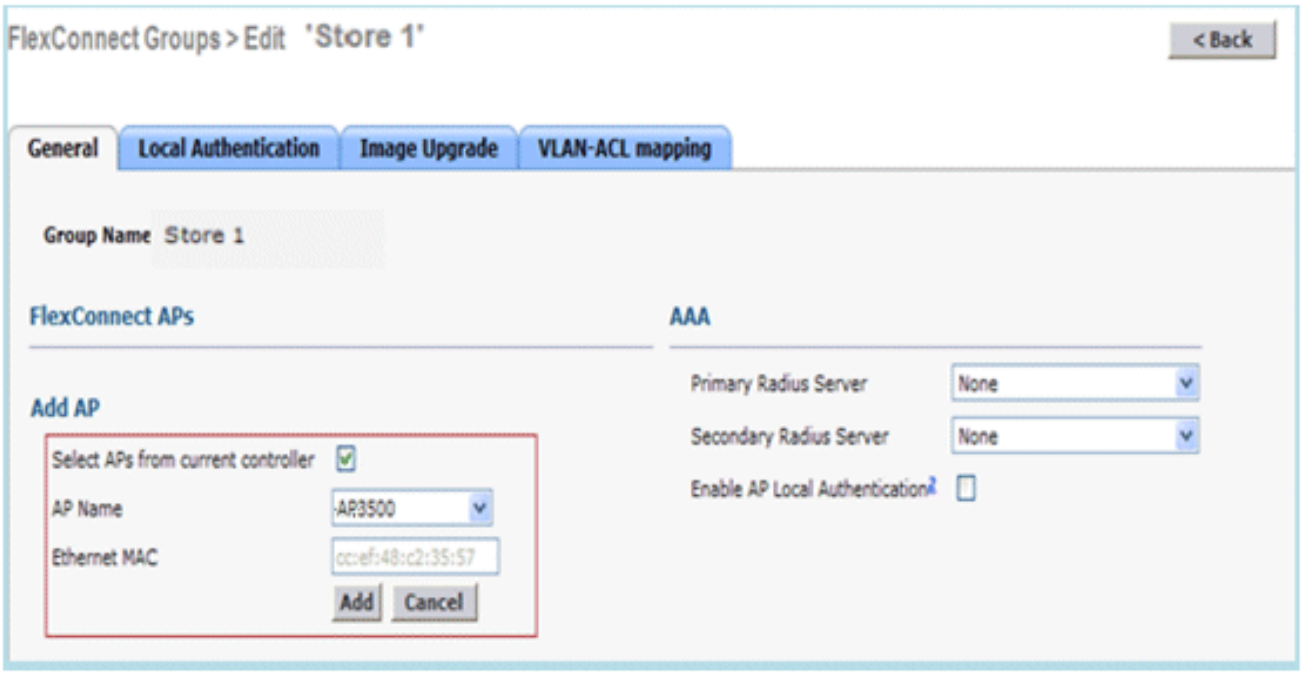
Procedimiento

Complete estos pasos:

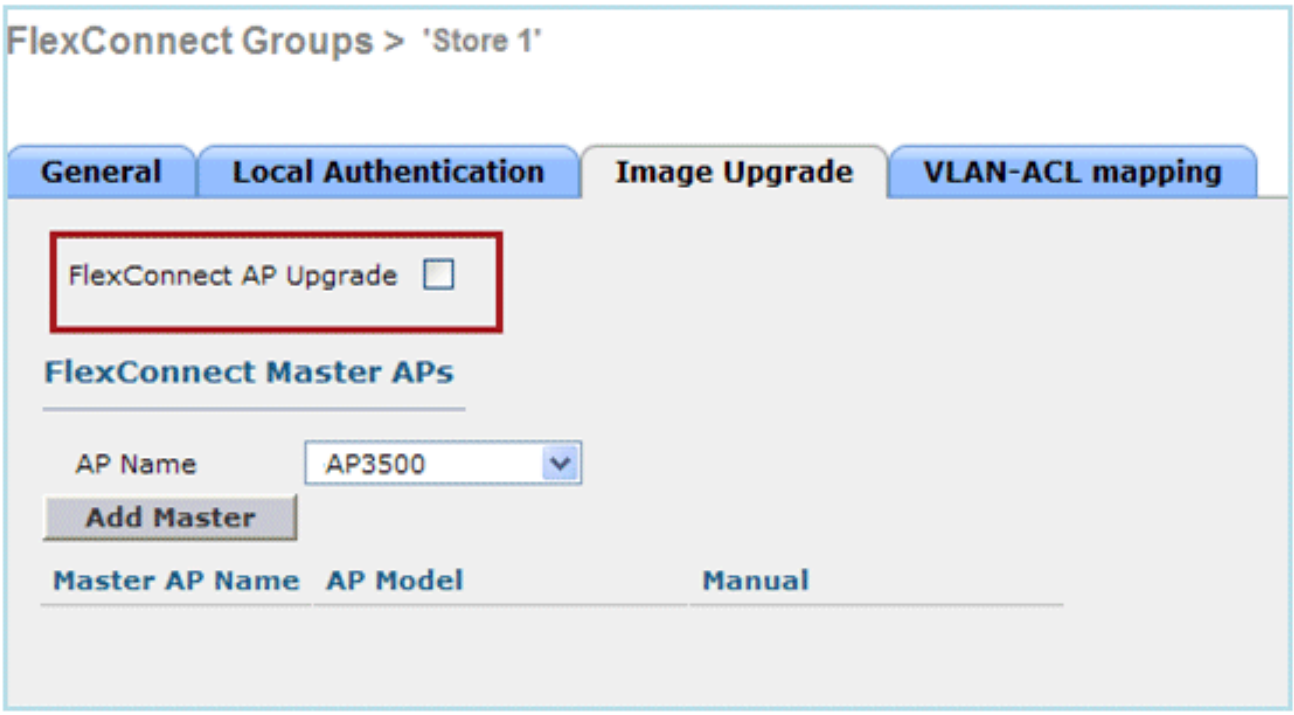
1. Actualice la imagen en el controlador.Navegue hasta **WLC GUI > Comandos > Descargar archivo** para comenzar la descarga.



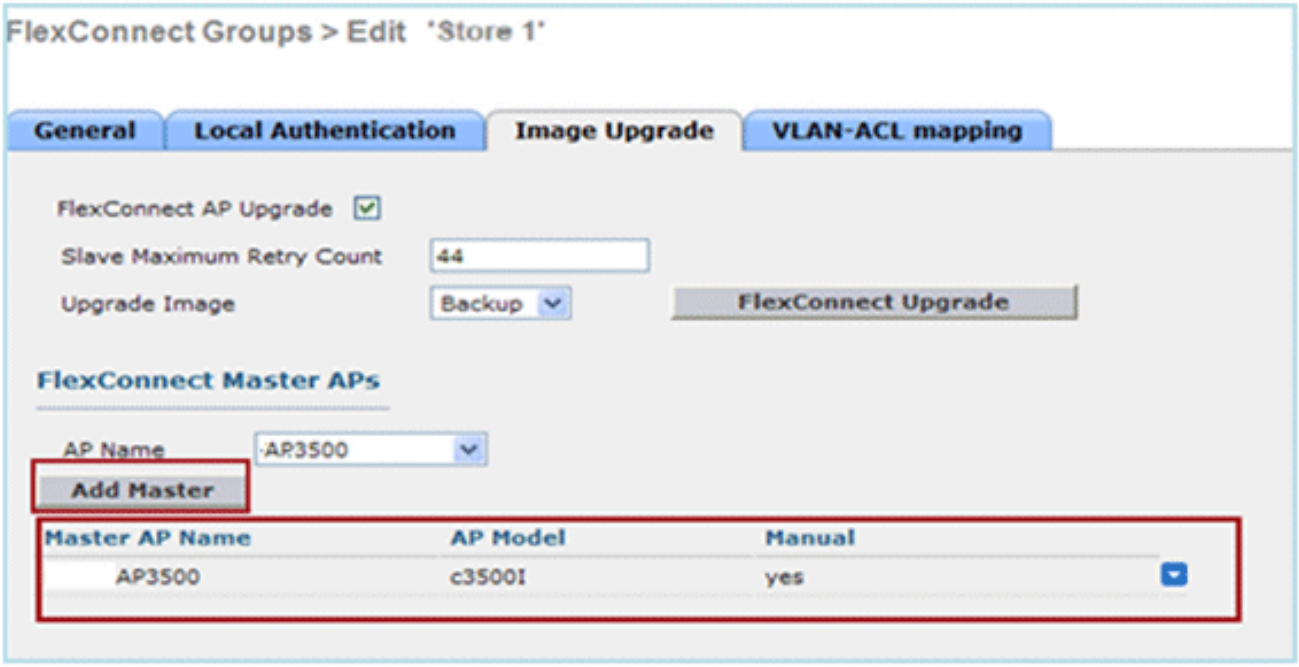
2. Guarde las configuraciones en los controladores, pero no reinicie el controlador.
3. Agregue los puntos de acceso FlexConnect al grupo FlexConnect.Vaya a WLC GUI > Wireless > FlexConnect Groups > seleccione **FlexConnect Group > General** pestaña **> Add AP**.



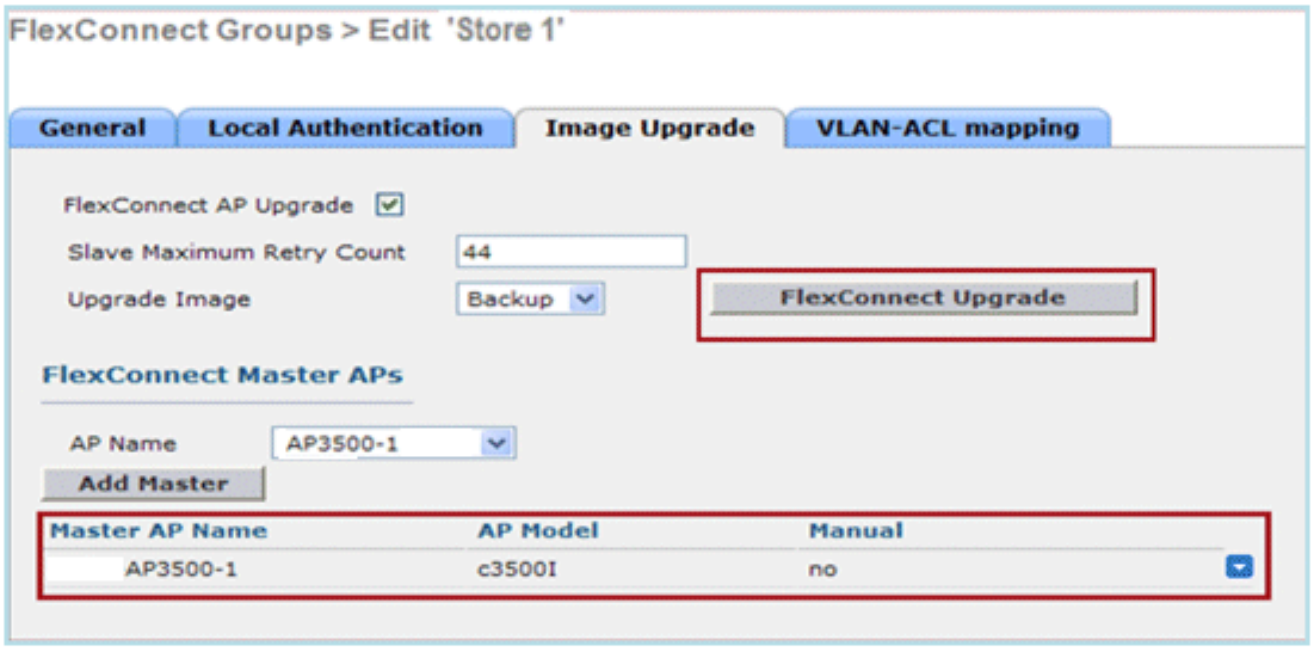
4. Haga clic en la casilla de verificación **FlexConnect AP Upgrade** para lograr una actualización eficiente de la imagen AP.Vaya a WLC GUI > **Wireless > FlexConnect Groups** > seleccione la pestaña **FlexConnect Group** > Image Upgrade.



5. El AP maestro se puede seleccionar manual o automáticamente:Para seleccionar manualmente el AP maestro, navegue a WLC GUI > Wireless > FlexConnect Groups > seleccione FlexConnect Group > Image Upgrade tab > FlexConnect Master APs, seleccione AP en la lista desplegable y haga clic en Add Master.

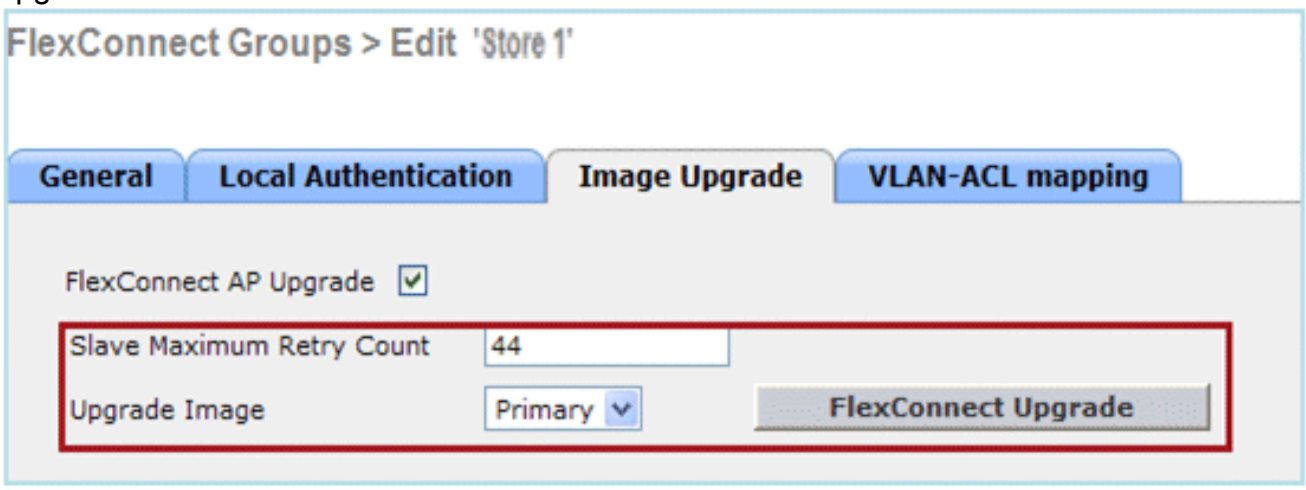


Nota: Sólo se puede configurar un AP por modelo como AP maestro. Si el AP maestro se configura manualmente, el campo Manual se actualizará como **sí**.Para seleccionar automáticamente el AP maestro, navegue a la GUI de WLC > Inalámbrico > Grupos FlexConnect > seleccione **Grupo FlexConnect** > pestaña Actualización de imagen y haga clic en Actualización de FlexConnect.



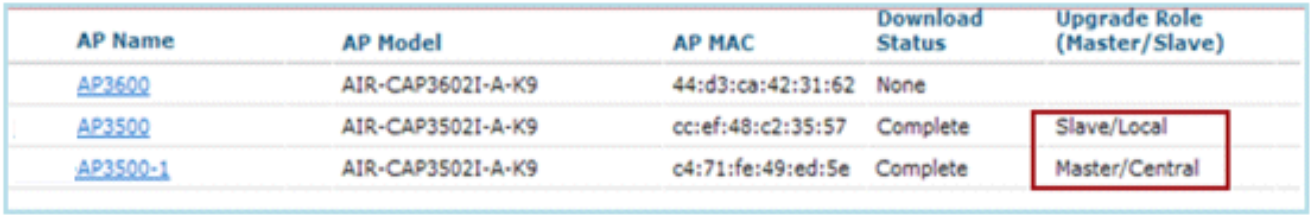
Nota: Si el AP maestro se selecciona automáticamente, el campo Manual se actualizará como **no**.

6. Para iniciar una actualización eficiente de la imagen AP para todos los APs bajo un grupo específico de FlexConnect, haga clic en **Actualización de FlexConnect**.Navegue hasta WLC GUI > Wireless > FlexConnect Groups > seleccione **FlexConnect** group > Image Upgrade y haga clic en FlexConnect
Upgrade.



Nota: El recuento máximo de reintentos esclavos es el número de intentos (44 de forma predeterminada) en los que el AP esclavo hará para descargar una imagen del AP maestro, después de lo cual caerá de nuevo para descargar la imagen del WLC. Hará 20 intentos contra el WLC para descargar una nueva imagen después de lo cual el administrador debe reiniciar el proceso de descarga.

7. Una vez que se inicia la actualización de FlexConnect, sólo el AP maestro descargará la imagen del WLC. En la página All AP, "**Upgrade Role**" se actualizará como **Master/Central**, lo que significa que Master AP ha descargado la imagen del WLC que está en la ubicación central. El punto de acceso esclavo descargará la imagen del punto de acceso maestro que se encuentra en el sitio local y es la razón en la página de todos los puntos de acceso "**rol de actualización**" se actualizará como **esclavo/local**.Para verificar esto, navegue a **WLC GUI > Wireless**.



AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

8. Reinicie los controladores después de descargar todas las imágenes AP. Los AP ahora vuelven al modo autónomo hasta que los controladores se reinician.**Nota:** En el modo autónomo, la tolerancia a fallos mantendrá a los clientes asociados.Una vez que el controlador vuelve, los APs se reinician automáticamente con la imagen previamente descargada.Después del reinicio, los AP se vuelven a unir al controlador primario y reanudan los servicios del cliente.

Limitaciones

- La selección maestra de AP es por grupo FlexConnect y por modelo de AP en cada grupo.
- Solamente 3 AP esclavos del mismo modelo pueden actualizarse simultáneamente desde su AP maestro y el resto de los AP esclavos usarán el temporizador de respaldo aleatorio para reintentar para el AP maestro para descargar la imagen AP.
- En el caso de que el AP esclavo no descargue la imagen del AP maestro por alguna razón, irá al WLC para obtener la nueva imagen.
- Esto sólo funciona con los AP CAPWAP.

Auto Convert APs in FlexConnect Mode

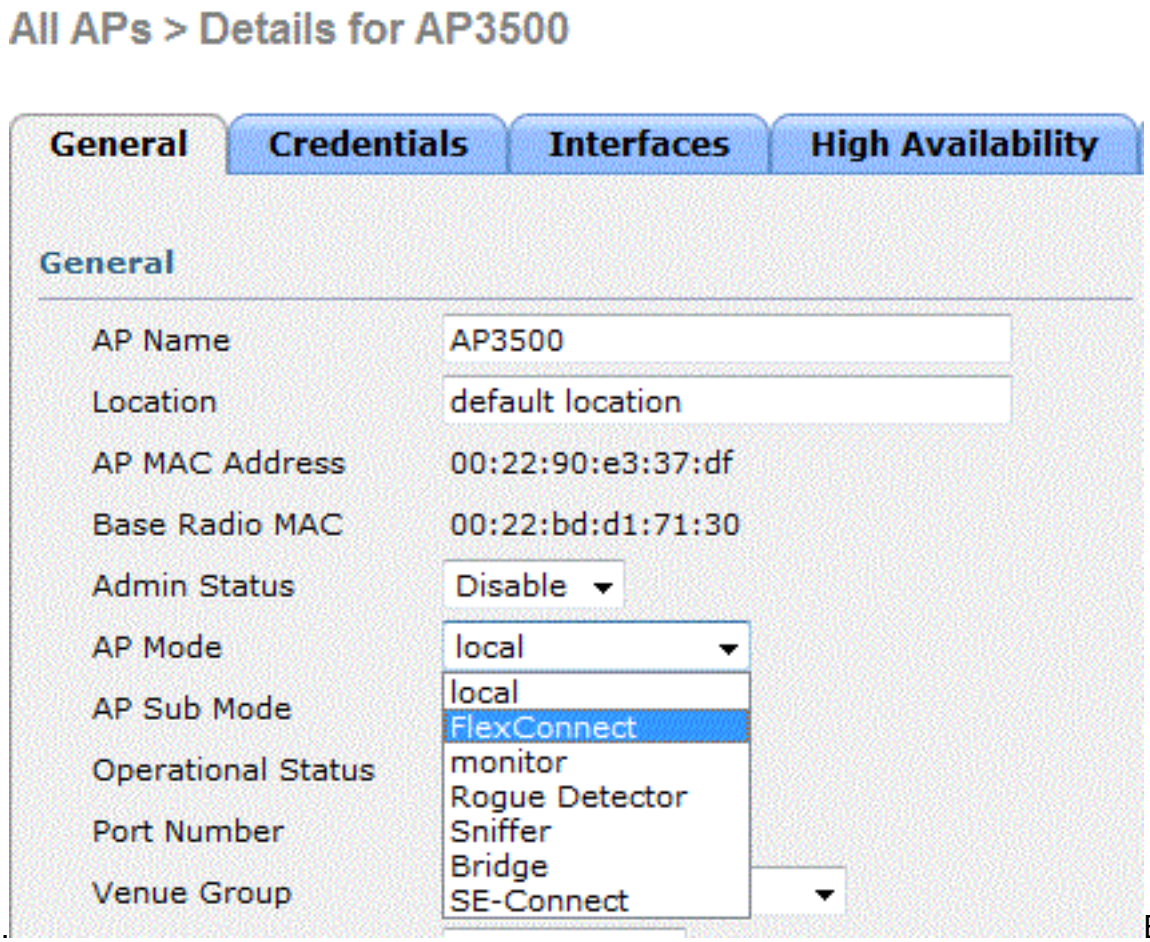
Flex 7500 proporciona estas dos opciones para convertir el modo AP en FlexConnect:

- Modo manual
- Modo de conversión automática

Modo manual

Este modo está disponible en todas las plataformas y permite que el cambio tenga lugar solamente por AP.

1. Navegue hasta **WLC GUI > Wireless > All AP** y elija el AP.
2. Seleccione **FlexConnect** como modo AP y luego haga clic en **Aplicar**.
3. El cambio del modo AP hace que el AP se



reinicie. Esta opción también está disponible en todas las plataformas WLC actuales.

Modo de conversión automática

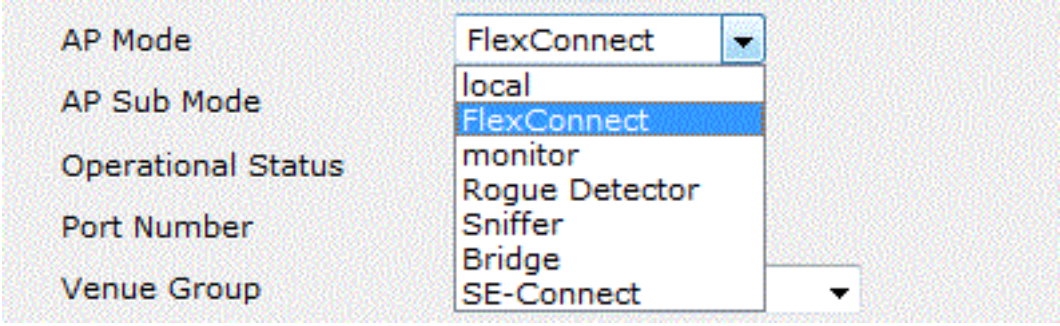
Este modo sólo está disponible para el controlador Flex 7500 y sólo se admite mediante CLI. Este modo activa el cambio en todos los AP conectados. Se recomienda que Flex 7500 se implemente en un dominio de movilidad diferente al de los controladores de campus WLC existentes antes de habilitar esta CLI:

```
(Cisco Controller) >config ap autoconvert ?

disable         Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect     Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins

(Cisco Controller) >
```

1. La función de conversión automática se inhabilita de forma predeterminada, la cual se puede verificar usando este comando **show**:

   ```
   (Cisco Controller) >show ap autoconvert

   AP Autoconvert ..............................  Disabled
   ```

   Modos AP no soportados = Modo local, Sniffer, Detector no autorizado y



Puente. Esta opción sólo está disponible actualmente a través de CLI.Estas CLI están disponibles solamente en el WLC 7500.

2. La **CLI de autoconversión de config ap flexconnect** convierte todos los AP en la red con el modo AP no soportado al modo FlexConnect. Los AP que ya están en FlexConnect o en el Modo Monitor no se ven afectados.

```
(Cisco Controller) >config ap autoconvert flexconnect


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ FlexConnect

(Cisco Controller) >
```

3. Al realizar la CLI **config ap autoConvert monitor**, todos los AP de la red con el modo AP no soportado se convierten al modo Monitor. Los AP que ya están en modo FlexConnect o Monitor no se ven afectados.

```
(Cisco Controller >config ap autoconvert monitor


(Cisco Controller) >show ap autoconvert

AP Autoconvert ................................ Monitor
```

No existe la opción de realizar **config ap autoconvertflexconnect** y **config ap autoConvert monitor** al mismo tiempo.

Soporte de FlexConnect WGB/uWGB para WLANs de Switching Local

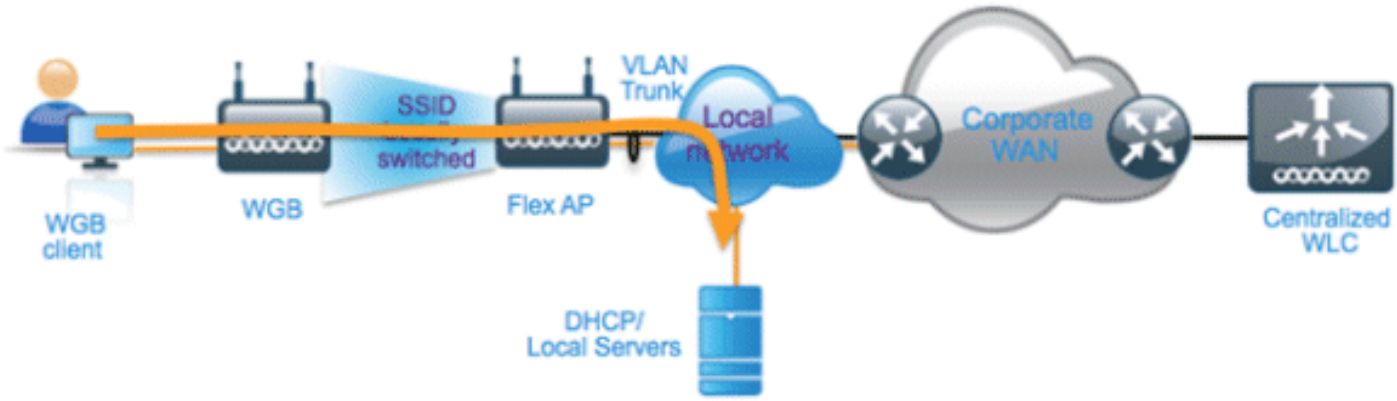
Desde la versión 7.3 en adelante, se admiten WGB/uWGB y clientes por cable/inalámbricos detrás de WGB, que funcionarán como clientes normales en WLANs configuradas para conmutación local.

Después de la asociación, WGB envía los mensajes IAPP para cada uno de sus clientes por cable/inalámbricos, y Flex AP se comportará de la siguiente manera:

- Cuando Flex AP está en modo conectado, reenvía todos los mensajes IAPP al controlador y el controlador procesará los mensajes IAPP de la misma manera que el AP de modo local. El tráfico para los clientes por cable/inalámbricos se conmutará localmente desde los puntos de acceso flexibles.
- Cuando AP está en modo autónomo, procesa los mensajes IAPP, los clientes por cable/inalámbricos en el WGB deben poder registrarse y anular el registro. Al pasar al modo conectado, Flex AP enviará la información de los clientes cableados de nuevo al controlador. WGB enviará mensajes de registro tres veces cuando Flex AP pase del modo autónomo al

modo conectado.

Los clientes por cable/inalámbricos heredarán la configuración de WGB, lo que significa que no se requiere una configuración independiente como la autenticación AAA, la anulación de AAA y la ACL FlexConnect para los clientes detrás de WGB.



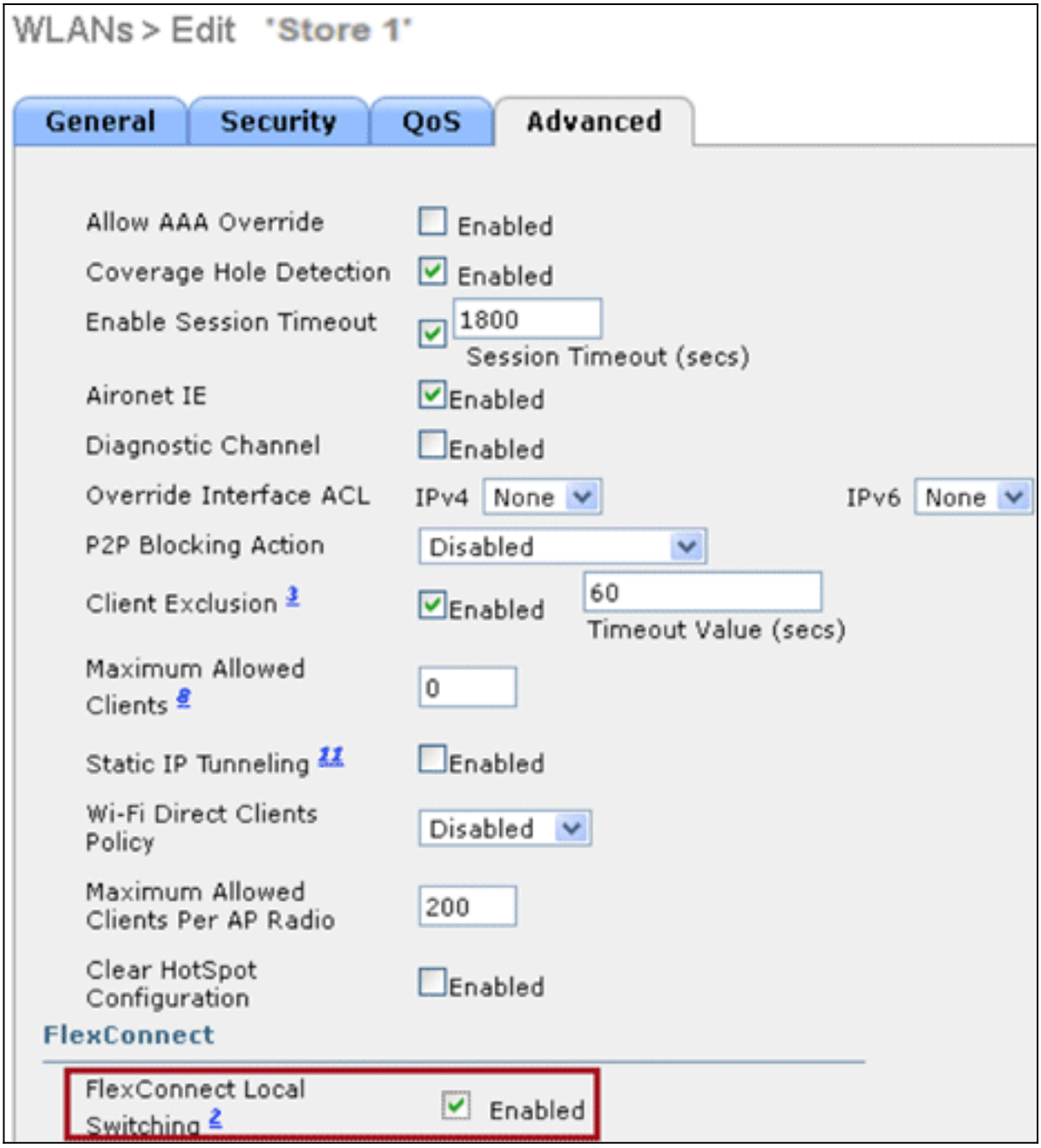
Summary

- No se requiere una configuración especial en el WLC para soportar el WGB en el Flex AP.
- La tolerancia de fallas es compatible con WGB y los clientes detrás de WGB.
- WGB es soportado en un IOS AP: 1240, 1130, 1140, 1260 y 1250.

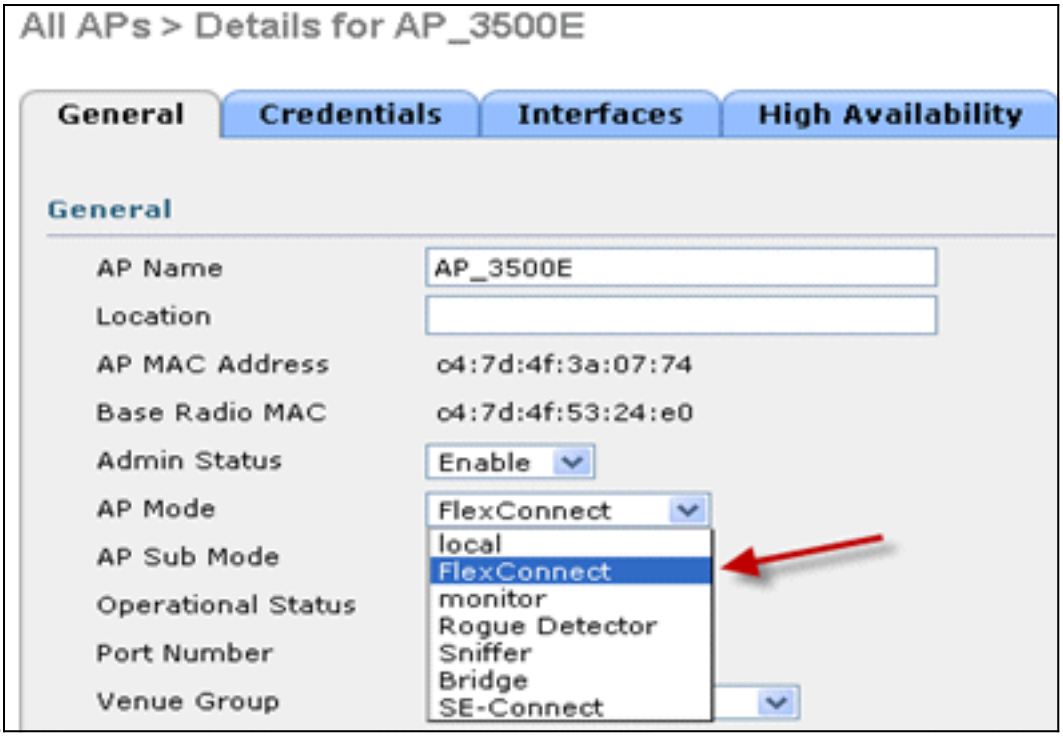
Procedimiento

Complete estos pasos:

1. No se necesita una configuración especial para habilitar el soporte WGB/uWGB en los AP FlexConnect para WLANs configurados para conmutación local como WGB. Además, los clientes detrás de WGB son tratados como clientes normales en WLAN configuradas de conmutación local por los APs Flex. Habilite **FlexConnect Local Switching** en una WLAN.



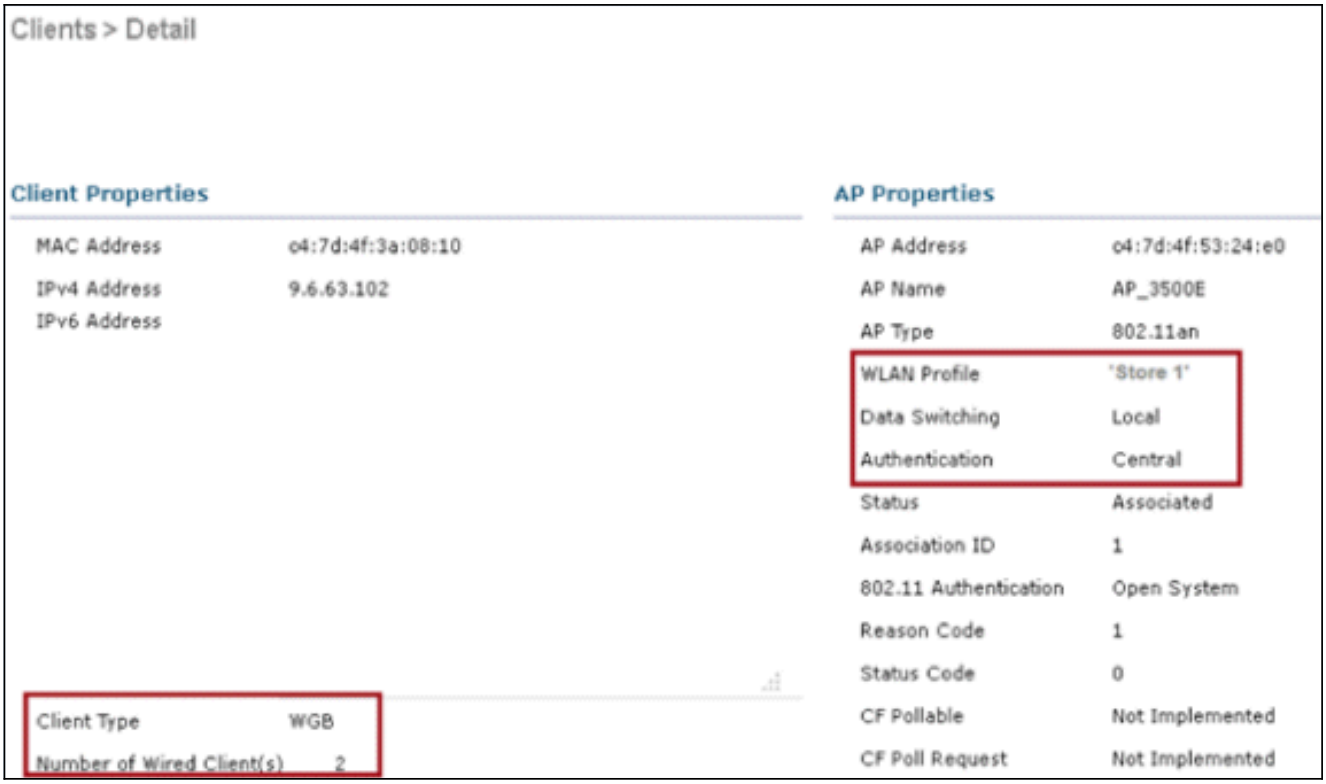
2. Establezca AP Mode en



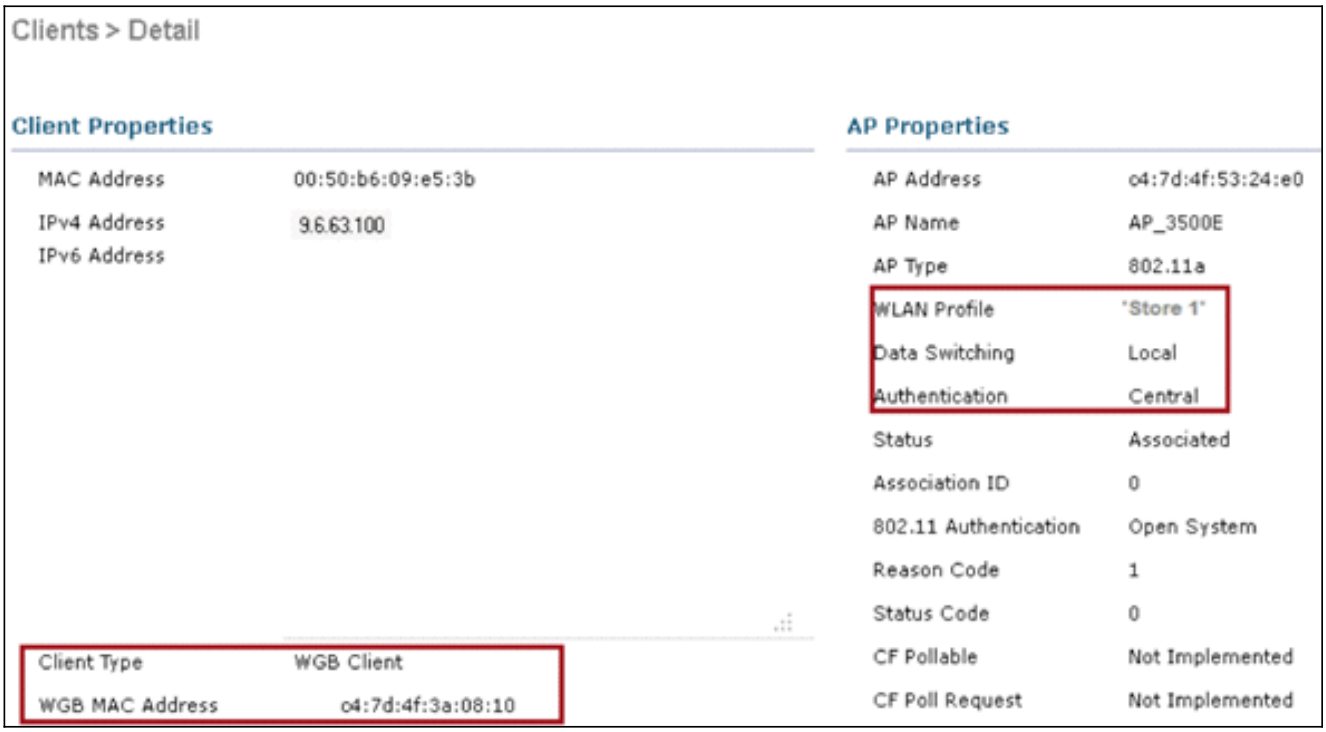
FlexConnect.

3. Asocie WGB a clientes con cables detrás de esta WLAN configurada.

4. Para verificar los detalles de WGB, vaya a **Monitor > Clients**, y seleccione **WGB** de la lista de clientes.



5. Para verificar los detalles de los clientes por cable/inalámbricos detrás de WGB, vaya a **Monitor > Clients**, y seleccione el cliente.



Limitaciones

- Los clientes cableados detrás de WGB siempre estarán en la misma VLAN que el propio WGN. El soporte de VLAN múltiple para los clientes detrás de WGB no es soportado en Flex AP para WLANs configurado para el Switching Local.
- Se admiten un máximo de 20 clientes (por cable/inalámbricos) detrás de WGB cuando se asocian a Flex AP en WLAN configurado para conmutación local. Este número es el mismo que el que tenemos hoy para el soporte WGB en el modo local AP.

- Web Auth no es soportado por los clientes detrás de WGB asociados en WLANs configurados para conmutación local.

Compatibilidad con un mayor número de servidores Radius

Antes de la versión 7.4, la configuración de los servidores RADIUS en el grupo FlexConnect se realizaba desde una lista global de servidores RADIUS en el controlador. El número máximo de servidores RADIUS, que se pueden configurar en esta lista global, es 17. Con un número cada vez mayor de sucursales, es necesario poder configurar un servidor RADIUS por sucursal. En la versión 7.4 en adelante, será posible configurar los servidores RADIUS primario y de respaldo por grupo FlexConnect que pueden o no formar parte de la lista global de 17 servidores de autenticación RADIUS configurados en el controlador.

También se soportará una configuración específica AP para los servidores RADIUS. La configuración específica de AP tendrá mayor prioridad que la configuración del grupo FlexConnect.

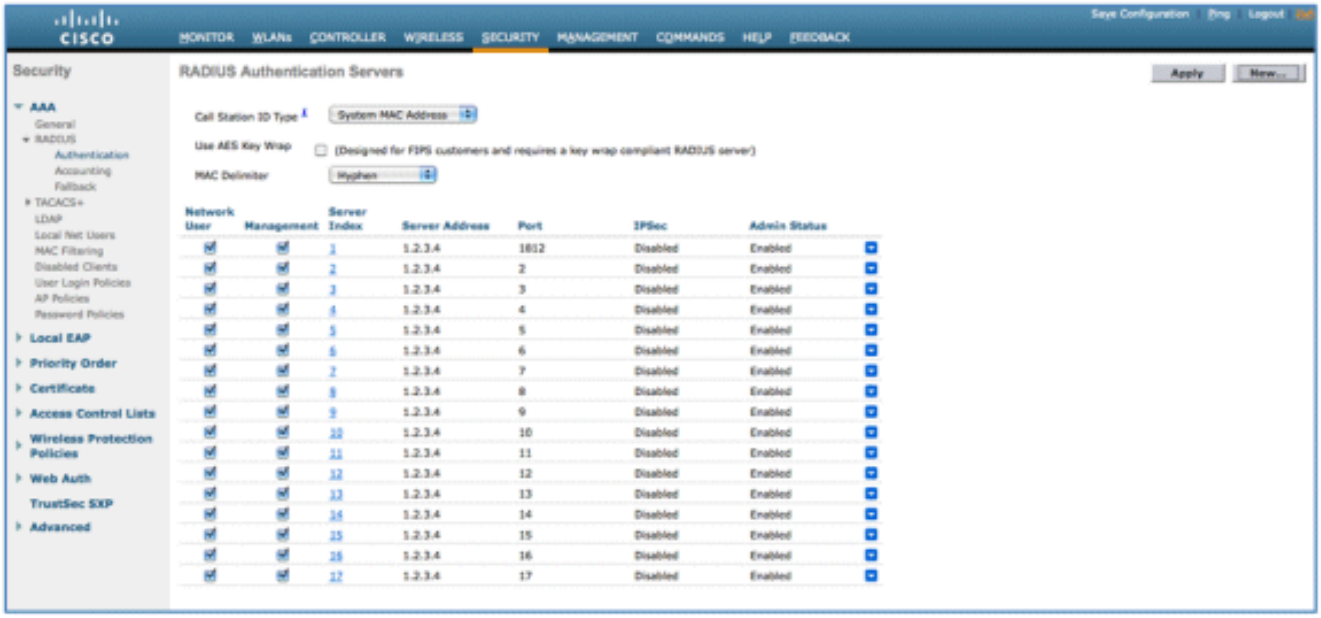
El comando de configuración existente en el grupo FlexConnect, que necesita el índice del servidor RADIUS en la lista global de servidores RADIUS en el controlador, quedará obsoleto y será reemplazado por un comando de configuración, que configura un servidor RADIUS en el grupo Flexconnect usando la dirección IP del servidor y el secreto compartido.

Summary

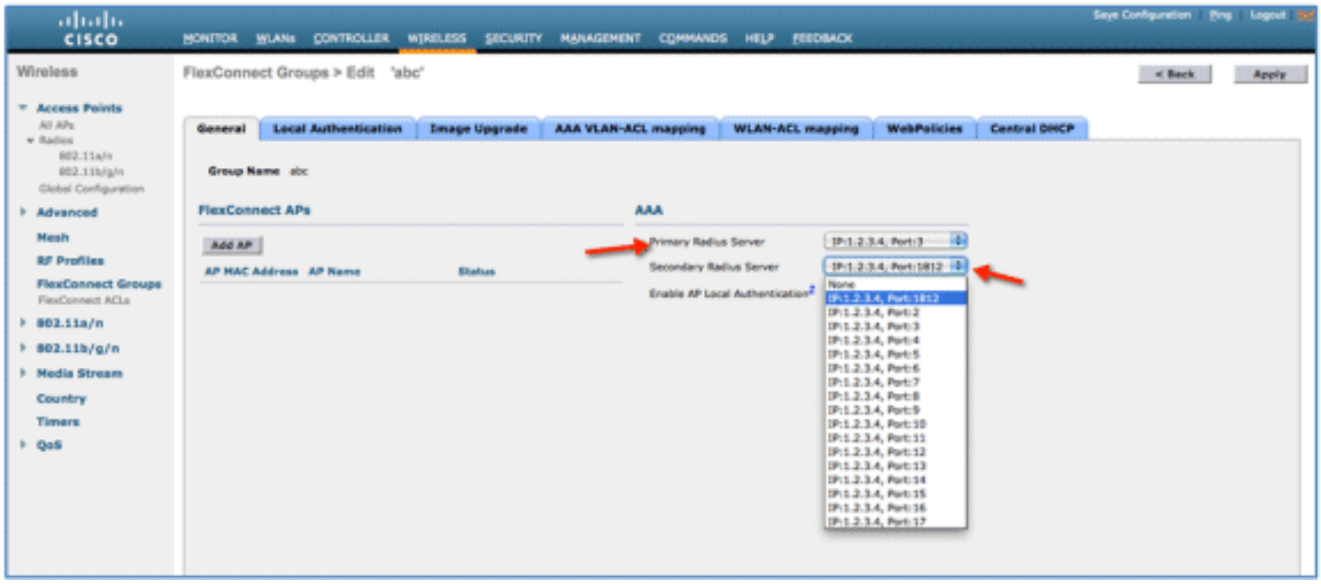
- Compatibilidad con la configuración de servidores RADIUS primario y de respaldo por grupo FlexConnect, que pueden o no estar presentes en la lista global de servidores de autenticación RADIUS.
- El número máximo de servidores RADIUS únicos que se pueden agregar en un WLC es el número de grupos FlexConnect que se pueden configurar en una plataforma determinada por dos veces. Un ejemplo es un servidor RADIUS primario y un servidor RADIUS secundario por grupo FlexConnect.
- La actualización de software de una versión anterior a la versión 7.4 no causará ninguna pérdida de configuración RADIUS.
- Se permite la eliminación del servidor RADIUS primario sin tener que eliminar el servidor RADIUS secundario. Esto es coherente con la configuración actual del grupo FlexConnect para el servidor RADIUS.

Procedimiento

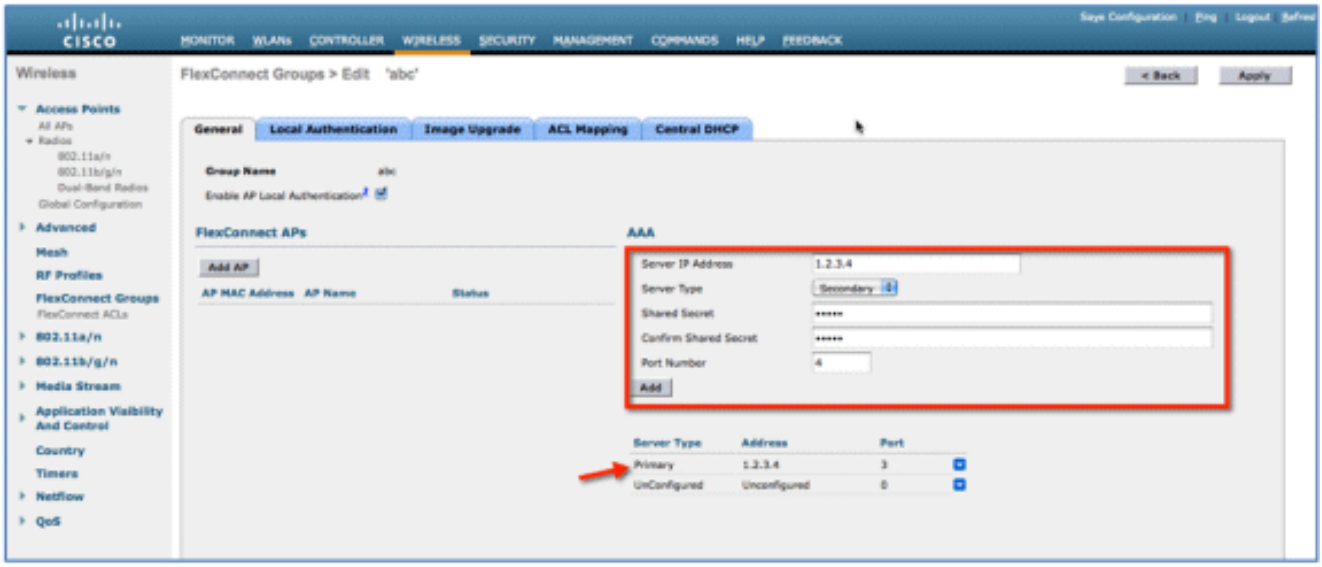
1. Modo de configuración anterior a la versión 7.4.Se puede configurar un máximo de 17 servidores RADIUS bajo la configuración de autenticación AAA.



2. Los servidores RADIUS primario y secundario se pueden asociar a un grupo FlexConnect mediante una lista desplegable que incluye los servidores RADIUS configurados en la página de autenticación
AAA.



3. Modo de configuración en FlexConnect Group en la versión 7.4.Los servidores RADIUS primario y secundario se pueden configurar en el grupo FlexConnect mediante una dirección IP, un número de puerto y un secreto
compartido.



Limitaciones

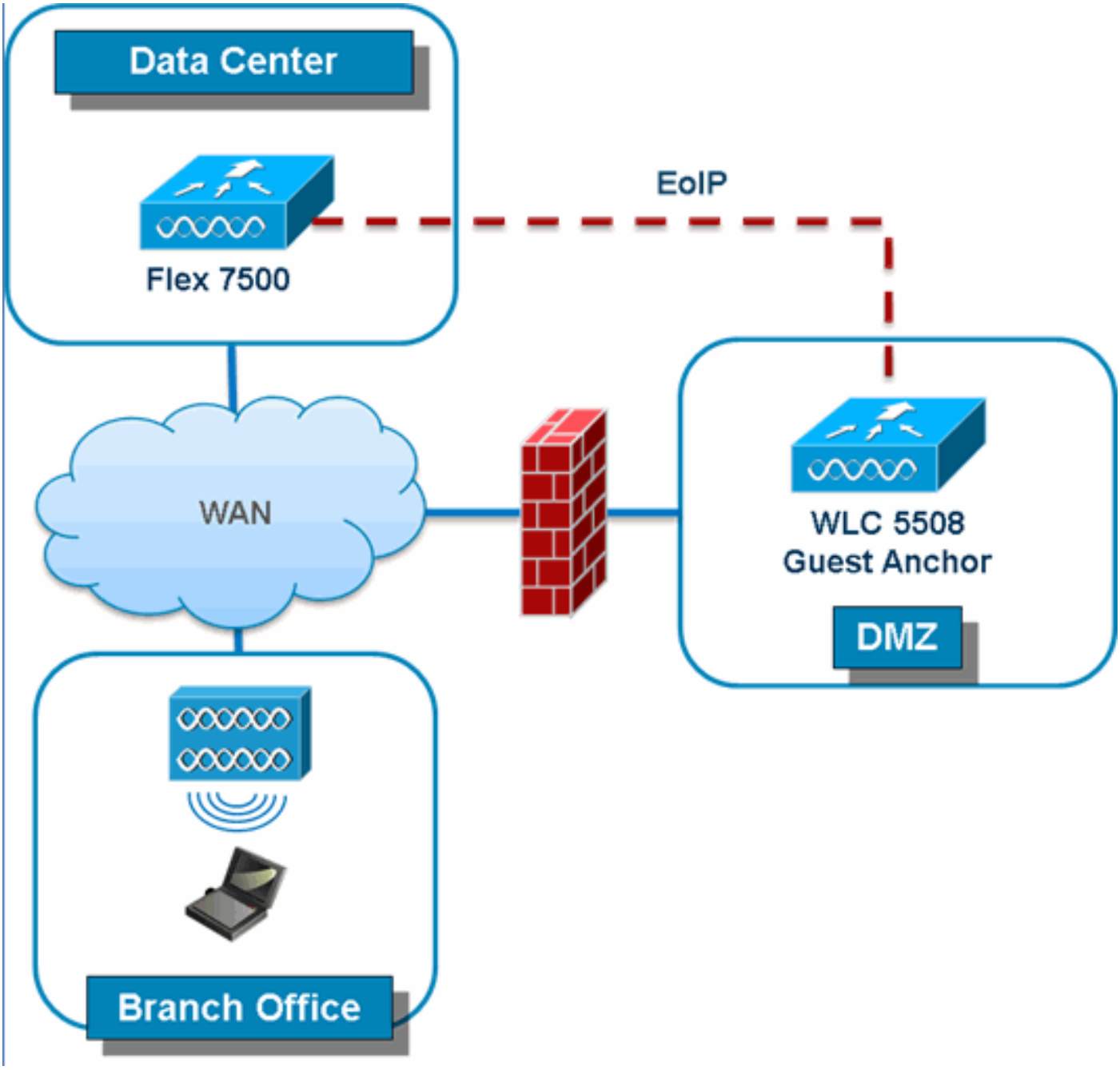
- La actualización de software de la versión 7.4 a una versión anterior conservará la configuración, pero con algunas limitaciones.
- La configuración de un servidor RADIUS primario/secundario cuando se configura uno anterior hará que la entrada anterior sea reemplazada por la nueva.

Modo local mejorado (ELM)

La solución FlexConnect admite ELM. Consulte la guía de prácticas recomendadas en el ELM para obtener más información.

Soporte de acceso de invitado en Flex 7500

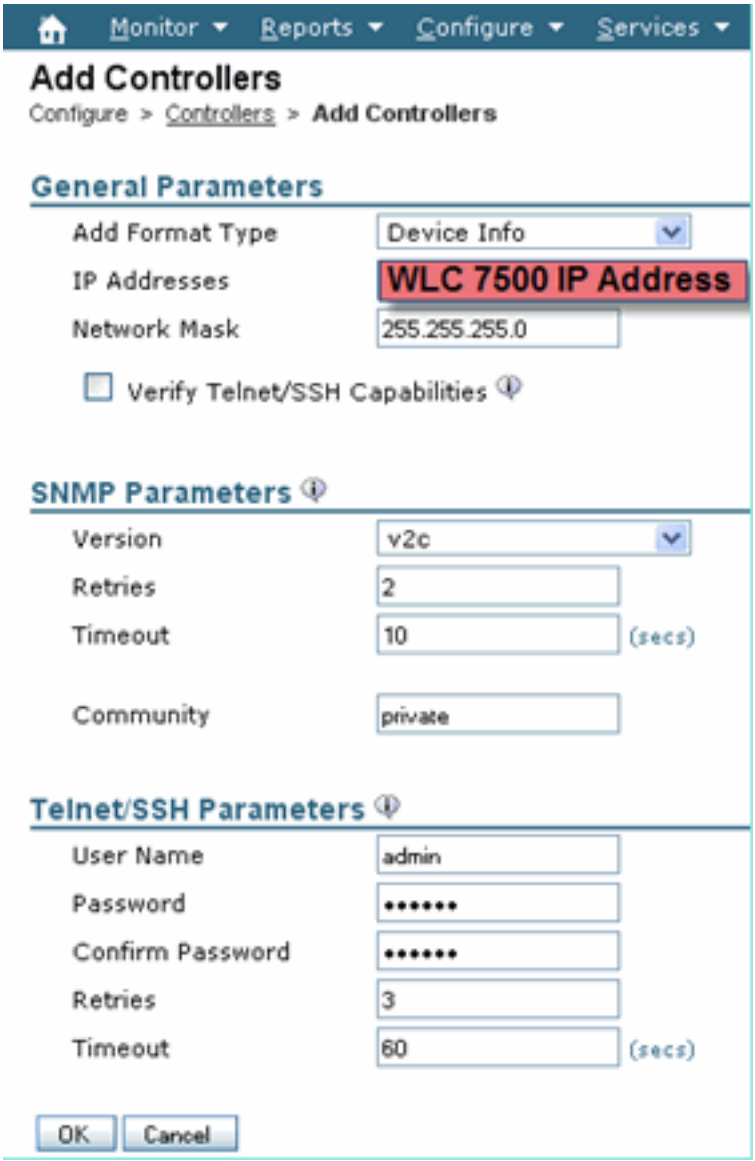
Figura 13: Soporte de acceso de invitado en Flex 7500



Flex 7500 permitirá y continuará admitiendo la creación de un túnel EoIP para su controlador de anclaje invitado en DMZ. Para conocer las prácticas recomendadas en la solución de acceso inalámbrico para invitados, consulte la Guía de implementación para invitados.

Administración del WLC 7500 desde NCS

La administración del WLC 7500 desde el NCS es idéntica a los WLC existentes de Cisco.



Para obtener más información sobre la administración del WLC y el descubrimiento de plantillas, refiérase a la Guía de Configuración del Sistema de Control Inalámbrico de Cisco, Versión 7.0.172.0.

Preguntas frecuentes

P. Si configuro los LAPs en una ubicación remota como FlexConnect, ¿puedo dar a esos LAPs un controlador primario y secundario?

Ejemplo: Un controlador primario está ubicado en el sitio A y un controlador secundario en el sitio B. Si el controlador en el sitio A falla, el LAP conmuta por error al controlador en el sitio B. Si ambos controladores no están disponibles, ¿el LAP cae en el modo independiente de FlexConnect?

A. Yes. Primero, el LAP conmuta por error al controlador secundario. Todas las WLAN que se

conmutan localmente no tienen ningún cambio y todas las que se conmutan centralmente desvían el tráfico hacia el nuevo controlador. Y, si el controlador secundario falla, todas las WLANs marcadas para la conmutación local (y la autentificación de clave previamente compartida/abierta y el autenticador de AP) permanecen activadas.

P. ¿Cómo tratan los puntos de acceso configurados en el modo local con las WLAN configuradas con FlexConnect Local Switching?

A. Los puntos de acceso del modo local tratan estas WLAN como WLANs normales. La autentificación y el tráfico de datos se tunelizan de nuevo hacia WLC. Durante una falla del link de la WAN, esta WLAN está totalmente inactiva y no hay ningún cliente activo en ella hasta que se restaura la conexión al WLC.

P. ¿Es posible realizar la autentificación web con conmutación local?

A. Sí, puede tener un SSID con la autentificación web habilitada y descartar el tráfico localmente después de la autentificación web. La autentificación web con conmutación local funciona correctamente.

P. ¿Puedo utilizar mi Portal de invitado en el controlador para un SSID, que es manejado localmente por el H REAP? En caso afirmativo, ¿qué sucede si pierdo la conectividad con el controlador? ¿Los clientes actuales se descartan inmediatamente?

A. Yes. Puesto que esta WLAN está localmente conmutada, la WLAN está disponible pero no se pueden autentificar clientes nuevos ya que la página web no está disponible. Pero los clientes existentes no se descartan.

P. ¿Puede FlexConnect certificar la conformidad con PCI?

A. Yes. La solución FlexConnect es compatible con la detección no autorizada para cumplir con PCI.

Información Relacionada

- Guía de diseño e implementación de HREAP
- Controladores LAN inalámbricos Cisco de la serie 4400
- Controladores LAN inalámbricos Cisco de la serie 2000
- Cisco Wireless Control System
- Motor de servicios de movilidad de la serie 3300 de Cisco
- Cisco Aironet 3500 Series
- Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems