

# Implemente un acceso definido por software para redes inalámbricas con DNA

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[SD-Access.](#)

[Arquitectura inalámbrica de acceso SD](#)

[Overview](#)

[Terminología y funciones de SDA](#)

[Redes subyacentes y superpuestas](#)

[Flujos de trabajo básicos](#)

[Incorporación de AP](#)

[Cliente incorporado](#)

[Itinerancia de clientes](#)

[Configurar](#)

[Diagrama de la red](#)

[Detección y provisión de WLC en DNA de Cisco](#)

[Aregar WLC](#)

[Aregar puntos de acceso](#)

[Crear SSID](#)

[Aprovisionar WLC](#)

[Aprovisionamiento de puntos de acceso](#)

[Crear sitio de fabric](#)

[Aregar WLC al fabric](#)

[Incorporación de AP](#)

[Cliente incorporado](#)

[Verificación](#)

[Verifique la configuración del fabric en el WLC y el DNA de Cisco](#)

[Troubleshoot](#)

[El cliente no obtiene la dirección IP](#)

[SSID no se ha transmitido](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo implementar SDA para la tecnología inalámbrica relacionada con el WLC habilitado para el entramado y el LAP de acceso en el DNA de Cisco.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de controladores LAN inalámbricos (WLC) 9800
- Puntos de acceso ligeros (LAP)
- DNA de Cisco

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800-CL WLC Cisco IOS® XE, versión 17.9.3
- Puntos de acceso de Cisco: 9130AX, 3802E, 1832I
- Cisco DNA versión 2.3.3.7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## SD-Access.

El acceso definido por software establece y aplica automáticamente políticas de seguridad en toda la red, con reglas dinámicas y segmentación automatizada, y permite al usuario final controlar y configurar la forma en que los usuarios se conectan a su red. SD-Access establece un nivel inicial de confianza con cada terminal conectado y lo supervisa continuamente para volver a verificar su nivel de confianza. Si un terminal no se comporta con normalidad o se detecta una amenaza, el usuario final puede contenerlo inmediatamente y tomar medidas, antes de que se produzca una brecha, reducir el riesgo empresarial y proteger sus recursos. Solución totalmente integrada y fácil de implementar y configurar tanto en redes nuevas como implementadas.

SD-Access es una tecnología de Cisco que representa una evolución de la red de campus tradicional que ofrece redes basadas en intención (IBN) y control de políticas central con el uso de componentes de redes definidas por software (SDN).

Tres pilares de red de SD-Access:

1. Un fabric de red: Se trata de una abstracción de la propia red que admite superposiciones programables y virtualización. El fabric de red admite el acceso por cable e inalámbrico y permite alojar varias redes lógicas segmentadas entre sí y definidas por objetivos empresariales.

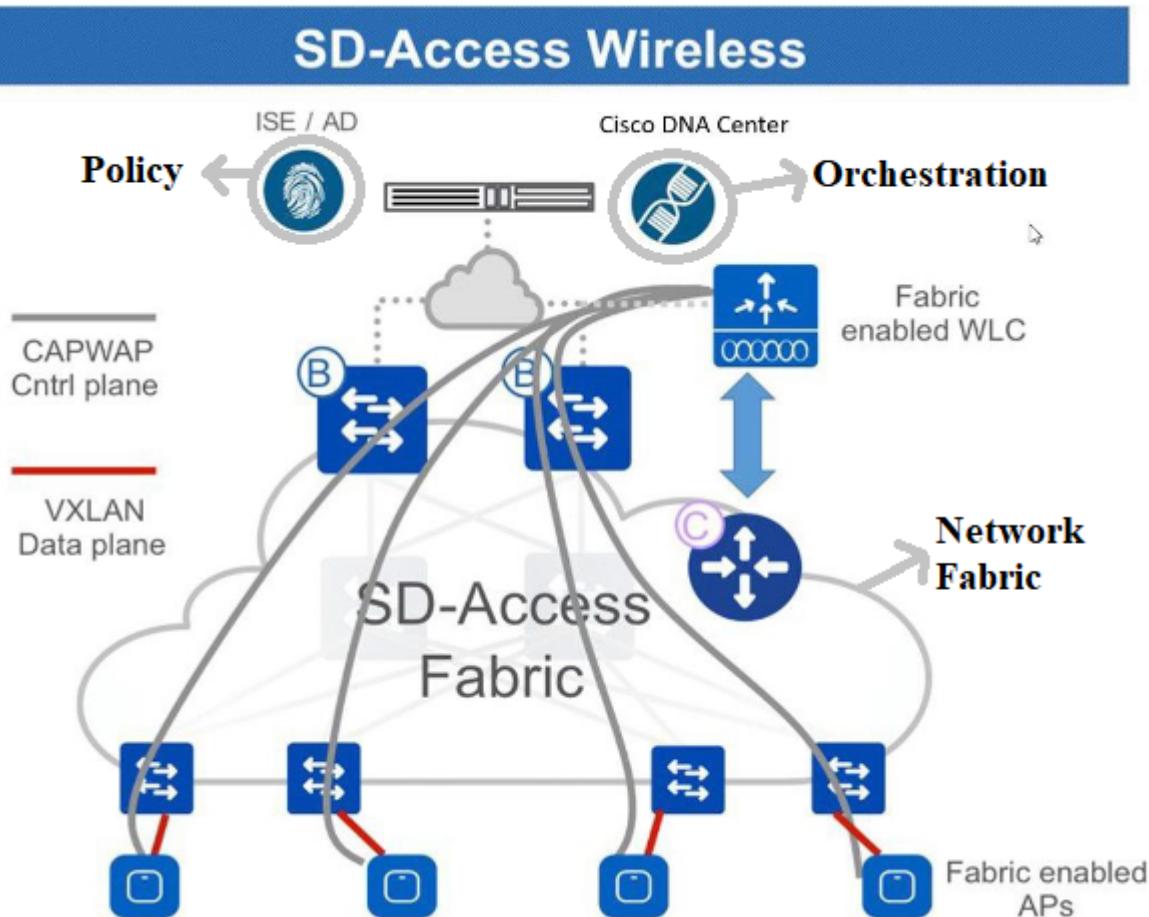
2. Orquestación: Cisco DNA es el motor de orquestación de SDA. Cisco DNA funciona como un controlador SDN. Implementa políticas y cambios de configuración en el fabric. También incorpora una herramienta compatible con el diseño de red y con las operaciones de telemetría de red en tiempo real y los análisis de rendimiento a través de DNA Assurance. La función de Cisco DNA es orquestar el fabric de red para ofrecer cambios en las políticas y las intenciones de la red en cuanto a seguridad, calidad del servicio (QoS) y microsegmentación.
3. Política: Identity Services Engine (ISE) es la herramienta que define la política de red. ISE organiza el modo en que los dispositivos y los nodos se segmentan en redes virtuales. ISE también define etiquetas de grupo escalables (SGT) que utilizan los dispositivos de acceso para segmentar el tráfico de los usuarios a medida que entra en el fabric. Los SGR son responsables de aplicar la política de microsegmentación definida por ISE.

SDA se basa en una orquestación centralizada. Las combinaciones de Cisco DNA como motor de orquestación programable, ISE como motor de políticas y una nueva generación de switches programables lo convierten en un sistema de fabric mucho más flexible y gestionable que cualquier otro que se haya presentado anteriormente.



Nota: Este documento trata específicamente sobre SD-Access Wireless.

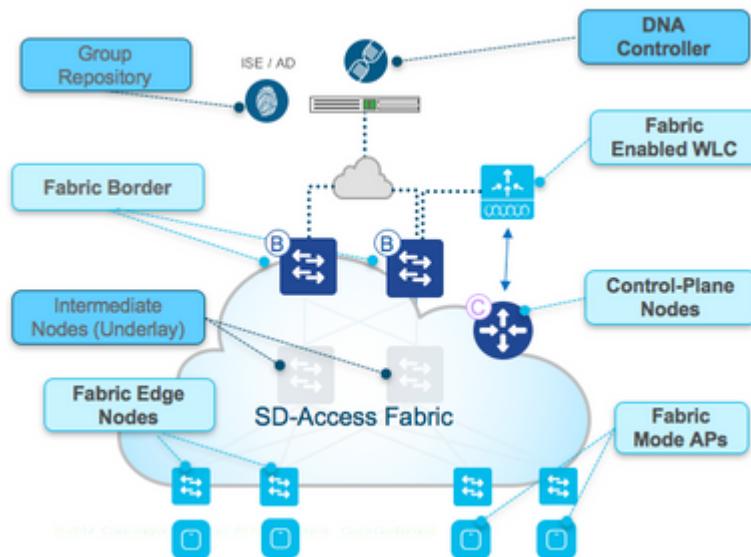
El fabric de red se compone de los siguientes elementos:



La integración inalámbrica en el fabric conlleva varias ventajas para la red inalámbrica, por ejemplo: abordando la simplificación, la movilidad con subredes extendidas a través de ubicaciones físicas; y microsegmentación con una política centralizada que es uniforme en los dominios conectados por cable e inalámbricos. También permite al controlador reducir el plano de datos para reenviar tareas mientras sigue funcionando como el plano de control y servicios centralizados para la red inalámbrica. Por lo tanto, la escalabilidad del controlador inalámbrico se ve aumentada porque ya no es necesario procesar el tráfico del plano de datos, de forma similar al modelo FlexConnect.

## Arquitectura inalámbrica de acceso SD

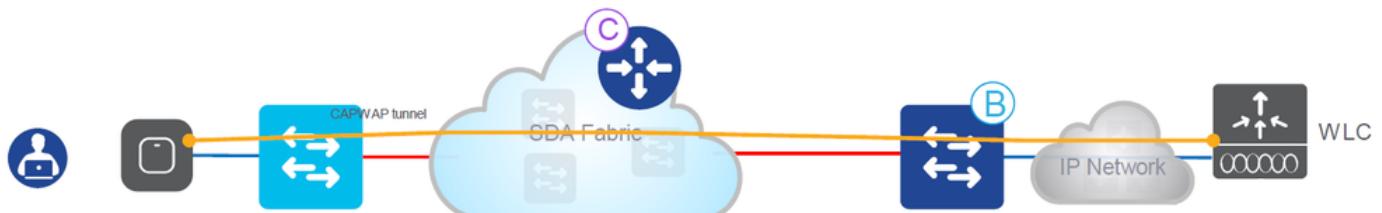
### Overview



Descripción general de SDA

Existen dos modelos de implementación inalámbrica SDA principales compatibles:

Uno es un método de transmisión libre (OTT), una implementación CAPWAP tradicional conectada en la parte superior de una red por cable de fabric. El fabric SDA transporta el control CAPWAP y el tráfico del plano de datos al controlador inalámbrico:

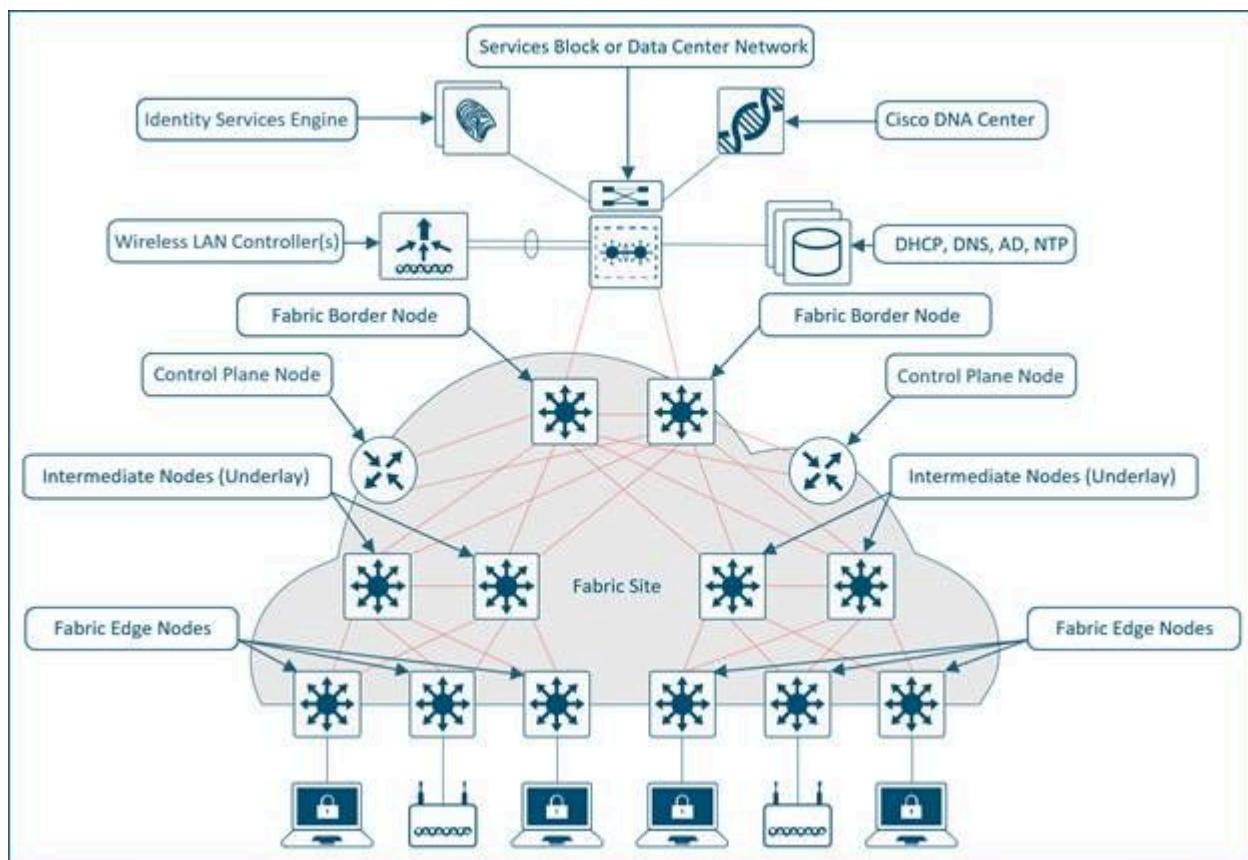


Método Over-The-Top

En este modelo de implementación, el fabric SDA es una red de transporte para el tráfico

inalámbrico (un modelo que se suele implementar en las migraciones). El AP funciona de manera muy similar al modo local clásico: tanto los planos de datos como de control CAPWAP terminan en el controlador, lo que significa que el controlador no participa directamente en el fabric. Este modelo se utiliza a menudo cuando los switches por cable se migran por primera vez al fabric SDA, pero la red inalámbrica todavía no está preparada para la integración completa de la superposición del fabric.

Los otros modelos de implementación utilizan el modelo SDA totalmente integrado. La red inalámbrica está totalmente integrada en el fabric y participa en superposiciones, lo que permite que diferentes WLAN formen parte de diferentes redes virtuales (VPN). El controlador inalámbrico solo administra el plano de control CAPWAP (para administrar los AP), y el plano de datos CAPWAP no llega al controlador:



Modelo SDA completamente integrado

El plano de datos inalámbricos se gestiona de forma similar a los switches por cable: cada punto de acceso encapsula los datos en VXLAN y los envía a un nodo de la frontera del fabric, donde a continuación se envían a través del fabric a otro nodo de la frontera. Los controladores inalámbricos deben configurarse como controladores de fabric, lo que supone una modificación con respecto a su funcionamiento normal.

Los controladores habilitados para fabric se comunican con el plano de control de fabric, registran las direcciones MAC de los clientes de capa 2 y la información del identificador de red virtual (VNI) de capa 2. Los AP son responsables de la comunicación con los terminales inalámbricos y ayudan al plano de datos VXLAN mediante el encapsulamiento y el tráfico de desencapsulamiento.

## Terminología y funciones de SDA

El fabric de red se compone de los siguientes elementos:

- Nodo del plano de control: Se trata del sistema de asignación de ubicaciones (base de datos de host) que forma parte del plano de control del protocolo de separación de ubicaciones (LISP), que gestiona la identidad de terminales (EID) para las relaciones de ubicación (o las relaciones de dispositivos). El plano de control puede ser un router dedicado que proporcionó funciones de plano de control o puede coexistir con otros elementos de la red del fabric.
- Nodos de límite de fabric: Normalmente, un router que funciona en el borde entre las redes externas y el fabric SDA, que proporciona servicios de routing a las redes virtuales del fabric. Conecta las redes externas de capa 3 al fabric SDA.
- Nodos periféricos del fabric: Dispositivo del fabric que conecta dispositivos que no son de fabric, como switches, puntos de acceso y routers al fabric SDA. Estos son los nodos que crean los túneles superpuestos virtuales y las VLAN con la LAN extensible virtual (VXLAN) e imponen las SGT en el tráfico enlazado al fabric. Las redes de ambos lados del extremo del fabric se encuentran dentro de la red SDA. Conectan los terminales con cables al fabric de acceso SD.
- Nodos intermedios: Estos nodos se encuentran dentro del núcleo del fabric SDA y se conectan a nodos de borde o de borde. Los nodos intermedios simplemente reenvían el tráfico SDA como paquetes IP, sin darse cuenta de que hay varias redes virtuales involucradas.
- WLC de fabric: Controlador inalámbrico habilitado para fabric que participa en el plano de control SDA pero que no procesa el plano de datos CAPWAP.
- AP de modo de fabric: Puntos de acceso habilitados para fabric. El tráfico inalámbrico se encapsula en VXLAN en el AP, lo que permite enviarlo al fabric a través de un nodo de borde.
- DNA de Cisco (DNAC): El controlador de SDN empresarial para la red de superposición de fabric de acceso definido por software (SDA) y es responsable de las tareas de automatización y garantía. También se puede utilizar para algunas tareas de automatización y relacionadas con los dispositivos de red que forman la base (que no están relacionados con SDA).
- ISE: Identity Services Engine (ISE) es una plataforma de políticas mejorada que puede prestar servicio a una gran variedad de roles y funciones, entre los que destaca el servidor de autenticación, autorización y contabilidad (AAA). ISE suele interactuar con Active Directory (AD), pero los usuarios se pueden configurar localmente, así como en ISE para implementaciones más pequeñas.



---

Nota: El plano de control es una parte fundamental de la infraestructura de la arquitectura SDA, por lo que se recomienda implementarlo de forma flexible.

---

## Redes subyacentes y superpuestas

La arquitectura SDA utiliza tecnología de fabric que admite redes virtuales programables (redes superpuestas) que se ejecutan en una red física (una red subyacente).

Una tela es una superposición.

Una red superpuesta es una topología lógica utilizada para conectar dispositivos virtualmente, construida sobre una topología subyacente física arbitraria. Utiliza atributos de reenvío alternativos para proporcionar servicios adicionales que no proporciona el subyacente. Se crea sobre la capa subyacente para crear una o más redes virtualizadas y segmentadas. Debido a la naturaleza definida por software de las superposiciones, es posible conectarlas de formas muy flexibles sin las limitaciones de la conectividad física. Se trata de una forma sencilla de aplicar políticas de seguridad, ya que la superposición puede programarse para tener un único punto de salida físico (el nodo de borde del fabric) y se puede utilizar un firewall para proteger las redes detrás de él (independientemente de si se pueden localizar). La superposición encapsula el tráfico con el uso de VXLAN. VXLAN encapsula tramas de capa 2 completas para su transporte a través de la capa subyacente con cada red superpuesta identificada por un identificador de red VXLAN (VNI). Los fabrics superpuestos suelen ser complejos y requieren una cantidad significativa de sobrecarga del administrador en las nuevas redes virtuales implementadas o para implementar políticas de seguridad.

Ejemplos de redes superpuestas:

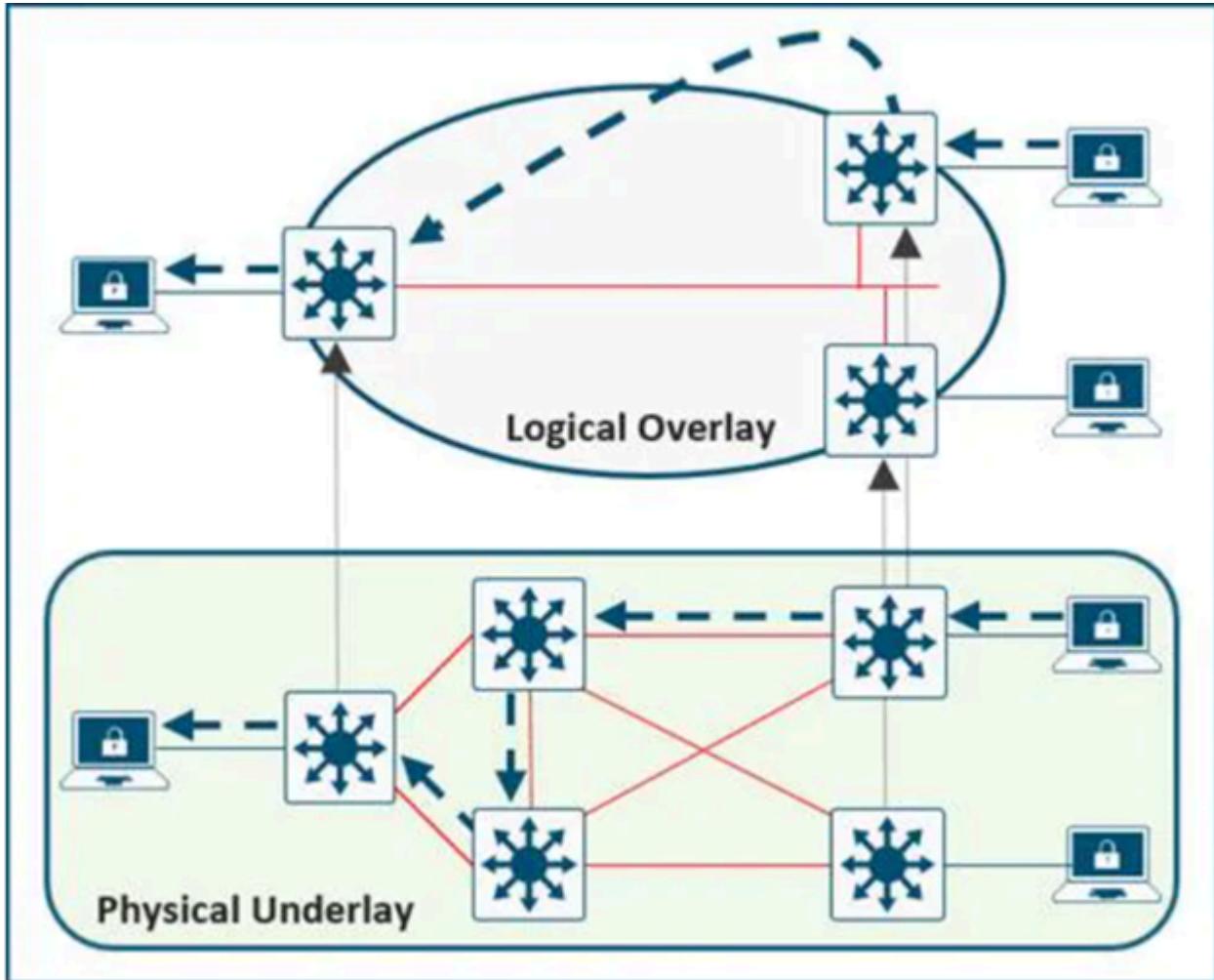
- GRE, mGRE
- MPLS y VPLS
- IPSec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

Una red subyacente está definida por los nodos físicos, como switches, routers y puntos de acceso inalámbricos, que se utilizan para implementar la red SDA. Todos los elementos de red de la capa subyacente deben establecer la conectividad IP mediante el uso de un protocolo de routing. Aunque no es probable que la red subyacente utilice el modelo de núcleo, distribución y acceso tradicional, debe utilizar una base de capa 3 bien diseñada que ofrezca un sólido rendimiento, escalabilidad y alta disponibilidad.



Nota: SDA admite IPv4 en la red subyacente e IPv4 o IPv6 en redes superpuestas.

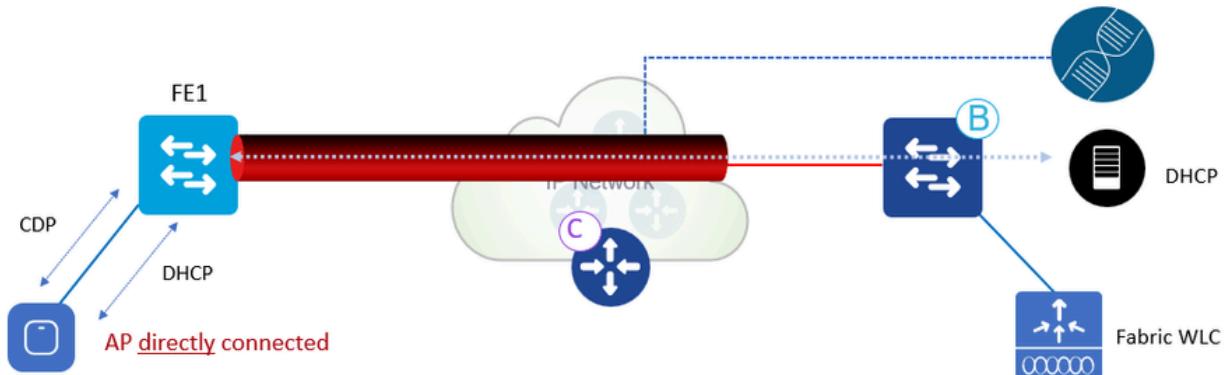
---



Redes subyacentes y superpuestas

## Flujos de trabajo básicos

Incorporación de AP



Flujo de trabajo de unión a PA

Flujo de trabajo de unión a PA:

1. El administrador configura el conjunto de AP en DNAC en INFRA\_VN. Cisco DNA

preaprovisiona una configuración en todos los nodos de frontera del fabric para incorporar automáticamente los puntos de acceso.

2. El AP está conectado y se enciende. Fabric Edge detecta que es un AP a través de CDP y aplica la macro para asignar (o la plantilla de interfaz) el puerto del switch a la VLAN correcta.
3. AP obtiene una dirección IP vía DHCP en la superposición.
4. Fabric Edge registra la dirección IP y MAC (EID) de los AP y actualiza el plano de control (CP).
5. AP aprende WLC IP con métodos tradicionales. El AP de entramado se une como un AP de modo local.
6. El WLC verifica si es apto para el entramado (AP del Wave 2 o del Wave 1).
7. Si el AP se soporta para el entramado, el WLC consulta el CP para saber si el AP está conectado al entramado.
8. El plano de control (CP) responde al WLC con RLOC. Esto significa que el punto de acceso está conectado al fabric y se muestra como "habilitado para fabric".
9. El WLC hace un registro del LISP del L2 para el AP en el CP (que es registro "especial" seguro del cliente del AP). Esto se utiliza para pasar información importante de metadatos del WLC al borde del entramado.
10. En respuesta a este registro de proxy, el plano de control (CP) notifica al borde del entramado y pasa los metadatos recibidos del WLC (indicador que dice que es un AP y la dirección IP del AP).
11. Fabric Edge procesa la información, aprende que es un AP y crea una interfaz de túnel VXLAN a la IP especificada (optimización: el lado del switch está listo para que los clientes se unan).

Los comandos debug/show se pueden utilizar para verificar y validar el flujo de trabajo de unión de AP.

#### Plano de Control

```
debug lisp control-plane all
```

```
show lisp instance-id <L3 instance id> ipv4 server (Debe mostrar la dirección IP del AP registrada por el switch periférico donde está conectado el AP).
```

```
show lisp instance-id <L2 instance id> ethernet server (Debe mostrar la radio AP, así como la dirección mac ethernet, la radio AP registrada por el WLC y la mac ethernet por el switch de borde donde está conectado el AP).
```

#### Switch perimetral

```
debug access-tunnel all
```

```
debug lisp control-plane all
```

```
show access-tunnel summary
```

```
show lisp instance < L2 instance id> ethernet database wlc access-points (Debe mostrar la MAC de radio AP aquí.)
```

WLC

```
show fabric ap summary
```

Depuraciones de WLC LISP

```
set platform software trace wncl chassis active r0 lisp-agent-api debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-db debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-fsm debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-internal debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-lib debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-lispmsg debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-shim debug
```

```
set platform software trace wncl chassis active r0 lisp-agent-transport debug
```

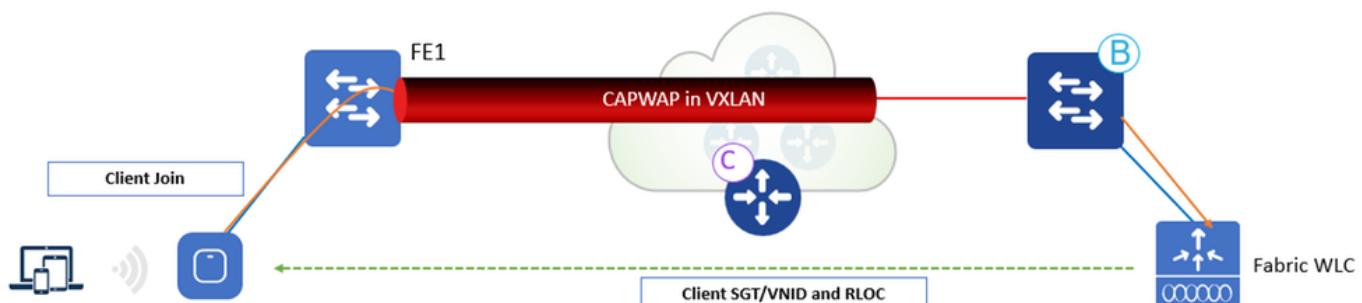
```
set platform software trace wncl chassis active r0 lisp-agent-ha debug
```

```
set platform software trace wncl chassis active r0 ewlc-infra-evq debug
```

Punto de Acceso

```
show ip tunnel fabric
```

Cliente incorporado



Flujo de trabajo integrado del cliente

Flujo de trabajo integrado del cliente:

1. El cliente se autentica en una WLAN habilitada para Fabric. WLC obtiene SGT de ISE, actualiza AP con L2VNID y SGT del cliente junto con IP RLOC. El WLC conoce el RLOC del AP de la base de datos interna.
2. El proxy WLC registra la información del cliente L2 en CP; Este es un mensaje modificado por LISP para pasar información adicional, como la SGT del cliente.
3. El extremo del fabric recibe la notificación del PC y agrega el MAC del cliente en L2 a la tabla de reenvío, y va a buscar la política de ISE en función de la SGT del cliente.
4. El cliente inicia la solicitud DHCP.
5. AP lo encapsula en VXLAN con información de VNI L2.
6. Fabric Edge asigna VNID L2 a la interfaz VLAN y reenvía DHCP en la superposición (igual que para un cliente de fabric cableado).
7. El cliente recibe una dirección IP de DHCP.
8. El snooping DHCP (y/o ARP para estática) activa el registro de EID del cliente por parte del Fabric Edge en el CP.

Los comandos debug/show se pueden utilizar para verificar y validar el flujo de trabajo interno del cliente.

Plano de Control

```
debug lisp control-plane all
```

Switch perimetral

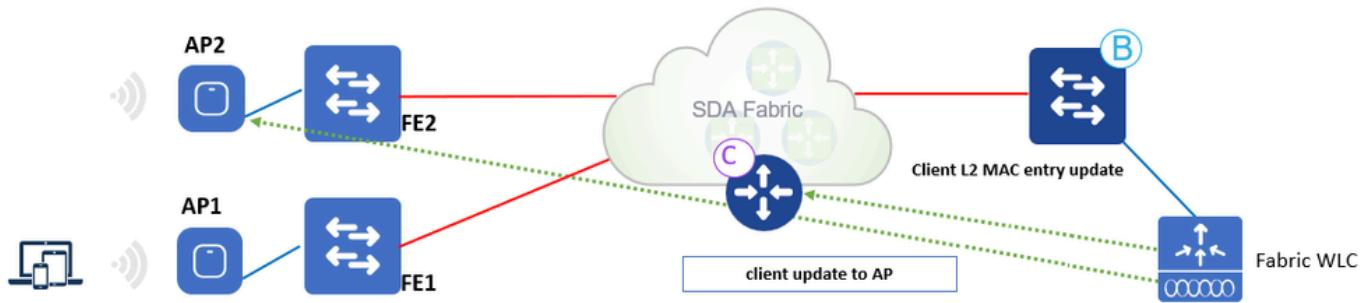
```
debug lisp control-plane all
```

```
debug ip dhcp snooping packet/event
```

WLC

Para la comunicación LISP, los mismos debugs que se unen al AP.

Itinerancia de clientes



Flujo de trabajo de itinerancias del cliente

Flujo de trabajo de itinerancias del cliente:

1. El cliente se traslada a AP2 en FE2 (itinerancia entre switches). El WLC es notificado por el AP.
2. El WLC actualiza la tabla de reenvío en el AP con la información del cliente (SGT, RLOC).
3. El WLC actualiza la entrada L2 MAC en el PC con el nuevo borde 2 de la estructura RLOC.
4. CP notifica a continuación:
  - Fabric Edge FE2 (switch de itinerancia a) para agregar el MAC del cliente a la tabla de reenvío que apunta al túnel VXLAN.
  - Fabric Edge FE1 (switch de itinerancia) para limpiar el cliente inalámbrico.
5. Fabric Edge actualiza la entrada L3 (IP) en la base de datos CP cuando recibe tráfico.
6. La itinerancia es de capa 2, ya que el Fabric Edge 2 tiene la misma interfaz VLAN (Anycast GW).

## Configurar

Diagrama de la red

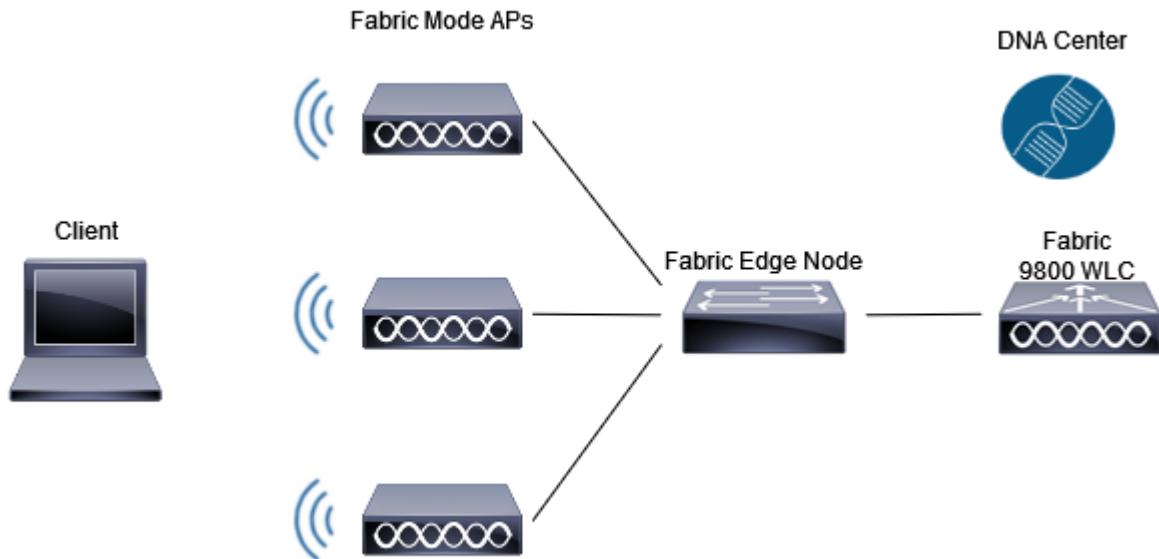


Diagrama de la red

## Detección y provisión de WLC en DNA de Cisco

### Agregar WLC

Paso 1. Navegue hasta la ubicación donde desea agregar el WLC. Puede añadir un nuevo edificio o planta.

Navegue hasta Diseño > Jerarquía de red e ingrese al edificio/planta, o puede crear un nuevo piso, como se muestra en la imagen:

 Cisco DNA Center

The screenshot shows the Ekahau Site Survey application. On the left, there is a search bar labeled "Search Hierarchy" and a "Search Help" button. The main navigation tree on the left includes a "Global" section with many collapsed items and a "Lisbon" section which is expanded, showing "Floor 1" and "MyFloor". On the right, a map of the area around "CABEÇO DE MOURO" is displayed, with several buildings highlighted in green. A context menu is open over one of these buildings, listing options: "Edit Building", "Delete Building", "Add Floor" (which is highlighted with a red box), "Import Ekahau Project", "Import Ekahau Survey", "Sync: DNA Spaces/CMX", "Export Maps", "View Devices", and "View Settings".

## Crear nueva planta

Bosque 3. Agave piña. También puede cargar una imagen de la planta del piña.

y verifique la cadena configurada. Debe agregar la cadena de comunidad SNMP correcta cuando agrega el WLC en el ADN de Cisco, y asegurarse de que netconf-yang esté habilitado en el WLC 9800 con los comandos de estado show netconf-yang. Al final, haga clic en Add:

The screenshot shows the 'Community Strings' tab selected in the top navigation bar. The table below lists two community strings: 'private' (Read/Write) and 'public' (Read Only). The 'Community Name' column contains checkboxes for each entry. The 'Access Mode' column indicates the level of access for each community string.

	Community Name	Access Mode
<input type="checkbox"/>	private	Read/Write
<input type="checkbox"/>	public	Read Only

Below the table are navigation buttons for pages 1 through 10, with the current page set to 1. A message at the bottom right indicates there are 2 items.

#### Configuración de SNMP

Paso 5. Agregue la dirección IP del WLC, las credenciales de CLI (las credenciales que Cisco DNA utiliza para iniciar sesión en el WLC y estas deben configurarse en el WLC antes de agregarlo al Cisco DNA), la cadena SNMP y verifique si el puerto NETCONF está configurado en el puerto 830:

## Add Device

Device Controllability is **Enabled**. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Firepower Management Center devices are not supported. [Learn more](#) | [Disable](#)

Type\* **Network Device**

Device IP / DNS Name\* **10.48.39.186**

Credentials [Validate](#)

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

**CLI\***

Select global credential  Add device specific credential

Username\* **admin**

Enable Password **\*\*\*\*\***

WARNING: Do not use 'admin' as the username for your device CLI credentials, if you are using Cisco ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

**SNMP\***

Select global credential  Add device specific credential

Version\* **V2C**

Credential\* **private | Write**

SNMP RETRIES AND TIMEOUT\*

HTTP(S)

**NETCONF**

Port **830**

Netconf with user privilege 15 is mandatory for enabling Wireless Services on Wireless capable devices such as C9800 Switches/Controllers. The NETCONF credentials are required to connect to eWLC devices. Majority of data collection is done using NETCONF for eWLC.

Cancel **Add**

Agregar WLC

El WLC se muestra como NA porque el ADN de Cisco aún está en proceso de sincronización:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>NA</b>	10.48.39.186	<span>Reachable</span>	Not Available	<span>Managed</span>	N/A	NA	Assign
--------------------------	-------------------------------------	-----------	--------------	------------------------	---------------	----------------------	-----	----	--------

WLC en proceso de sincronización

Cuando termine el proceso de sincronización, puede ver el nombre del WLC, la dirección IP, si es accesible, administrado y la versión de software:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	9800-17-9-RMI-RP-HA.dns-ams.cisco.com	<span>Reachable</span>	Not Available	<span>Managed</span>	N/A	No Health	Assign	17.9.3
--------------------------	-------------------------------------	---------------------------------------	------------------------	---------------	----------------------	-----	-----------	--------	--------

WLC sincronizado

Paso 6. Asigne el WLC a un sitio. En la lista de dispositivos, haga clic en Asignar y elija un sitio:

## Assign Device to Site

Serial Number  
9

Devices  
9800-17-9-RMI-RP-HA.dns-ams.cisco

 Choose a site

Asignar dispositivo al sitio

Puede decidir asignar el sitio ahora o más tarde:

## Assign Device to Site

Now     Later

Generate configuration preview

Creates preview which can be later used to deploy on selected devices. View status in [Work Items](#)

Task Name\*

Assign 1 Device(s) to Site

Asignar dispositivo al sitio ahora o más tarde

## Agregar puntos de acceso

Paso 1.Una vez que el WLC es agregado y alcanzable, navegue a Provisión > Inventario > Global > Dispositivos no asignados y busque los AP que usted ha unido a su WLC:

DEVICES (12)										
FOCUS: Inventory ▾										
	Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	Actions
>	<input checked="" type="checkbox"/> 3800E-I	10.14.19.173	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
>	<input checked="" type="checkbox"/> AP0C75	10.14.19.190	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	7	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input type="checkbox"/>		Unified AP	Unreachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
>	<input checked="" type="checkbox"/> DO_NOT_MOVE_Static_AP1	10.14.19.78	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	6	Assign	1
>	<input type="checkbox"/>		Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
>	<input type="checkbox"/>		Wireless Controller	Reachable	Not Scanned	Managed	Non-Compliant	No Health	Assign	1

Agregar puntos de acceso

Paso 2. Seleccione la opción Asignar. Asigne los APs a un sitio. Marque la casilla Apply to All para realizar la configuración para más de un dispositivo al mismo tiempo.

## Assign Device to Site

Serial Number F	Devices 3800E-I	Choose a floor
		<input checked="" type="checkbox"/> Apply to All <span style="border: 2px solid red; padding: 2px;">(1)</span>
K	DO_NOT_MOVE.Static_AP1	Choose a floor
K	AP0C75	Choose a floor

Asignar puntos de acceso al sitio

Navegue hasta su planta y podrá ver todos los dispositivos asignados a ella - WLC y AP:

DEVICES (4) FOCUS: Inventory <span style="color: blue;">▼</span>										
<span style="font-size: small;">Filter</span>   <span style="color: blue;">Add Device</span> Tag Actions <span style="color: blue;">(1)</span>   Take a Tour		IP Address	Device Family	Reachability <span style="color: blue;">(1)</span>	EoX Status <span style="color: blue;">(1)</span>	Manageability <span style="color: blue;">(1)</span>	Compliance <span style="color: blue;">(1)</span>	Health Score	Site	Image Version
<input type="checkbox"/>	Device Name <span style="color: blue;">▲</span>	10.14.19.173	Unified AP	<span style="color: green;">●</span> Reachable	<span style="color: orange;">▲</span> Not Scanned	<span style="color: green;">●</span> Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
<input type="checkbox"/>	9800-17-9-RMI-RP-HA.dns-ams.cisco.com <span style="color: blue;">▲</span>	10.48.39.186	Wireless Controller	<span style="color: green;">●</span> Reachable	<span style="color: orange;">▲</span> Not Scanned	<span style="color: green;">●</span> Managed	N/A	10	.../Lisbon/Floor 1	17.9.3
<input type="checkbox"/>	AP0C75 <span style="color: blue;">▲</span>	10.14.19.190	Unified AP	<span style="color: green;">●</span> Reachable	<span style="color: orange;">▲</span> Not Scanned	<span style="color: green;">●</span> Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
<input type="checkbox"/>	DO_NOT_MOVE.Static_AP1 <span style="color: blue;">▲</span>	10.14.19.78	Unified AP	<span style="color: green;">●</span> Reachable	<span style="color: orange;">▲</span> Not Scanned	<span style="color: green;">●</span> Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50

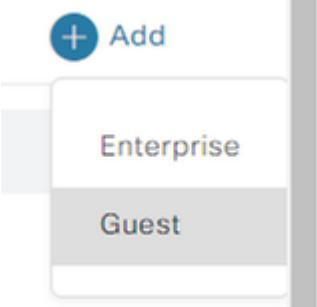
Dispositivos asignados al sitio

## Crear SSID

Paso 1. Navegue hasta Diseño > Configuración de red > Inalámbrico > Global y agregue un SSID:

Crear SSID

Puede crear un Enterprise SSID o un Guest SSID. En esta demostración, se crea un SSID de invitado:



SSID de empresa o invitado

Paso 2. Elija la configuración que desee para el SSID. En este caso, se crea un SSID abierto. El estado del administrador y el SSID de difusión deben estar habilitados:



#### Wireless Option ⓘ

- Multi band operation (2.4GHz, 5GHz, 6GHz)    Multi band operation with Band Select    5GHz only    2.4GHz only    6GHz Only

Primary Traffic Type  
**Best Effort (Silver)** ⓘ

#### SSID STATE

- Admin Status  
 Broadcast SSID

Configuración básica de SSID

# Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

**SSID Name:** Demo (Guest)

Level of Security

L2 SECURITY

Enterprise    Personal    Open Secured    Open

**Least Secure :**

Any user can associate to the network.

L3 SECURITY

Web Policy    Open

**Least Secure :**

Any user can associate to the network.

Authentication, Authorization, and Accounting Configuration



Please associate one or more AAA servers using Configure AAA link to ensure right configuration is pushed for the selected security setting.



[Configure AAA](#)

Mac Filtering

Fast Lane [\(i\)](#)

Deny RCM Clients [\(i\)](#)

Configuración de seguridad SSID



Precaución: No olvide configurar y asociar el servidor AAA para el SSID. La lista de métodos predeterminada se asigna si no se configuran servidores AAA.

Al hacer clic en Next, podrá ver la configuración avanzada del SSID:

## Advanced Settings

Configure the advanced fields to complete SSID setup.

**SSID Name:** Demo (Guest)

Fast Transition (802.11r)

Adaptive    Enable    Disable  
 Over the DS

MFP Client Protection ⓘ

Optional    Required    Disabled

11k

Neighbor List

Session Timeout ⓘ  in (secs)\*

Client Exclusion ⓘ  in (secs)\*

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout  Client User Idle Timeout(Default: 300 secs)\*

Directed Multicast Service

Radius Client Profiling

NAS-ID ⓘ

NAS-ID Opt. 1

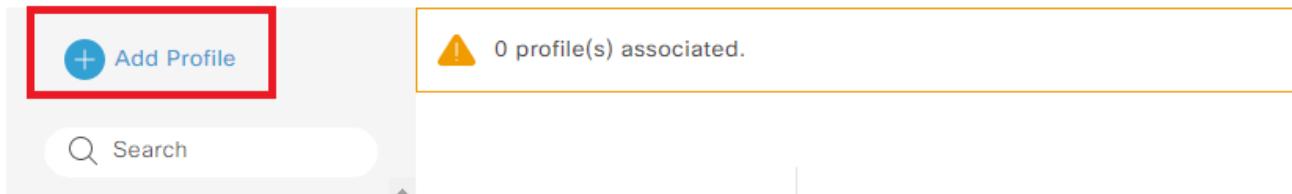
Configuración avanzada de SSID

Paso 3. Después de la creación del SSID, debe asociarlo a un perfil. Haga clic en Agregar perfil:

## Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

**SSID Name:** Demo (Guest)



Agregar perfil

Paso 4. Dé un nombre al perfil, seleccione Fabric y al final haga clic en Associate Profile:

 Associate Profile

Cancel

Profile Name

DemoProfile

Fabric

Yes

No

Asociar perfil

Aparecerá un resumen del SSID y el perfil que ha creado:

# Summary

Review all changes

## Basic Settings [Edit](#)

SSID Name	Demo
Primary Traffic Type	Best Effort (Silver) <a href="#">(i)</a>
Admin Status	Yes
Broadcast SSID	Yes

---

## Security Settings [Edit](#)

L2 Security	open
L3 Security	open
AAA Servers	
Mac Filtering	Yes
Fast Lane	No
Deny RCM Clients	No
Enable Posture	No
ACL Name	

---

## Advanced Settings [Edit](#)

Fast Transition (802.11r)	Disable
Over the DS	No
MFP Client Protection	Optional
Session Timeout	1800
Client Exclusion	180
Radius Client Profiling	No
NAS-ID	

---

## Network Profile Settings [Edit](#)

DemoProfile	Fabric (Associated)
-------------	---------------------

que desee configurar. En esta demostración, se configuraron los parámetros predeterminados. Haga clic en Save (Guardar):

Agregar perfil de RF básico

## Aprovisionamiento de puntos de acceso

Paso 1. Desplácese hasta el edificio o planta. Seleccione APs y Actions > Provisioning > Provisioning Device:

Aprovisionar puntos de acceso

Paso 2. Compruebe si el sitio asignado es correcto y seleccione Aplicar a todo:

Inventory / Provision Devices

- 1 Assign Site
- 2 Configuration
- 3 Summary

Serial Number F	Devices 3800E-I	Global/Lisbon/Lisbon/Floor 1 <span>X</span>
K	AP0C75	Global/Lisbon/Lisbon/Floor 1 <span>X</span>
K	DO_NOT_MOVE.Static_AP1	Global/Lisbon/Lisbon/Floor 1 <span>X</span>

Asignar sitio a AP

### Paso 3. Seleccione un perfil de RF de la lista desplegable y verifique si el SSID es el correcto:

Inventory / Provision Devices

- 1 Assign Site
- 2 Configuration
- 3 Summary

<b>⚠ Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.</b>				
9130AXE Access points with 17.6 version and higher, support advanced configurations to configure Radio Antenna profiles on Antenna slot.				
<b>Advanced Configuration</b>				
Serial Number F	Device Name 3800E-I	AP Zone Name Not Applicable	RF Profile <b>DemoRFProfile</b>	SSIDs <b>Demo</b>
K	AP0C75	Not Applicable	DemoRFProfile	Demo
K	DO_NOT_MOVE.Static_AP1	Not Applicable	DemoRFProfile	Demo

Seleccionar perfil de RF

### Paso 4. Verifique la configuración en los AP. Si todo está correcto, seleccione Deploy:

1 Assign Site    2 Configuration    3 Summary

3800E-I APOC75 DO_NOT_MOVE_Static_API	<p>Device Details</p> <p>Device Name: 3800E-I Serial Number: F Mac Address: 7B Device Location: Global/Lisbon/Lisbon/Floor 1</p> <p>AP Zone Details</p> <p>AP Zone Name: default-zone</p> <p>RF Profile Details</p> <table border="1"> <thead> <tr><th>RF Profile Name:</th><th>DemoRFProfile</th><th>Radio Type:</th><th>2.4GHz</th><th>5GHz</th><th>6GHz</th></tr> </thead> <tbody> <tr><td>Parent Profile</td><td>HIGH</td><td>LOW</td><td>CUSTOM</td></tr> <tr><td>Status</td><td>Enabled</td><td>Enabled</td><td>Enabled</td></tr> <tr><td>DCA Channels</td><td>1, 6, 11</td><td>36, 40, 44, 48, 52, 56, 60, 64</td><td>37, 41, 45, 49, 53, 57, 61, 65</td></tr> <tr><td>Ignored DCA Channels</td><td>N/A</td><td>149,153,157,161</td><td>149,153,157,161</td></tr> <tr><td>Channel Width</td><td>20 MHz</td><td>20 MHz</td><td>Best</td></tr> <tr><td>Supported Data Rates (in Mbps)</td><td>9,12,18,24,36,48,54</td><td>6,9,12,18,24,36,48,54</td><td>6,9,12,18,24,36,48,54</td></tr> <tr><td>Mandatory Data Rates (in Mbps)</td><td>9</td><td>6</td><td>6</td></tr> <tr><td>Tx Power Level (in dBm)</td><td>7/30</td><td>-10/30</td><td>-10/30</td></tr> <tr><td>TPC Power Threshold (in dBm)</td><td>-70</td><td>-60</td><td>-70</td></tr> <tr><td>Rx SOP</td><td>MEDIUM</td><td>LOW</td><td>AUTO</td></tr> <tr><td>Max Client</td><td>200</td><td>200</td><td>200</td></tr> </tbody> </table>	RF Profile Name:	DemoRFProfile	Radio Type:	2.4GHz	5GHz	6GHz	Parent Profile	HIGH	LOW	CUSTOM	Status	Enabled	Enabled	Enabled	DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64	37, 41, 45, 49, 53, 57, 61, 65	Ignored DCA Channels	N/A	149,153,157,161	149,153,157,161	Channel Width	20 MHz	20 MHz	Best	Supported Data Rates (in Mbps)	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	Mandatory Data Rates (in Mbps)	9	6	6	Tx Power Level (in dBm)	7/30	-10/30	-10/30	TPC Power Threshold (in dBm)	-70	-60	-70	Rx SOP	MEDIUM	LOW	AUTO	Max Client	200	200	200
RF Profile Name:	DemoRFProfile	Radio Type:	2.4GHz	5GHz	6GHz																																														
Parent Profile	HIGH	LOW	CUSTOM																																																
Status	Enabled	Enabled	Enabled																																																
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64	37, 41, 45, 49, 53, 57, 61, 65																																																
Ignored DCA Channels	N/A	149,153,157,161	149,153,157,161																																																
Channel Width	20 MHz	20 MHz	Best																																																
Supported Data Rates (in Mbps)	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54																																																
Mandatory Data Rates (in Mbps)	9	6	6																																																
Tx Power Level (in dBm)	7/30	-10/30	-10/30																																																
TPC Power Threshold (in dBm)	-70	-60	-70																																																
Rx SOP	MEDIUM	LOW	AUTO																																																
Max Client	200	200	200																																																

Cancel Deploy

Implementación de aprovisionamiento de puntos de acceso

Paso 5. El aprovisionamiento de dispositivos se puede implementar en este momento o más tarde. Al final, seleccione Apply:

## Provision Device

Now

Later

Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in [Work Items](#)

Task Name\*

Provision Device

Cancel

Apply

Aprovisionar puntos de acceso ahora o más tarde



Precaución: Cuando se aprovisionan los AP, que ya forman parte del suelo configurado para el perfil de RF seleccionado, se procesan y se reinician.

Los AP ahora están aprovisionados.

Paso 6. En el lado del WLC, navegue hasta Configuration > Wireless > Access Points. Verifique que las etiquetas AP se hayan enviado desde el ADN de Cisco:

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 3			Misconfigured APs			Select an Action	
tion	Country Code Misconfigured	LSC Fallback Misconfigured	Policy Tag	Site Tag	RF Tag	Location	Country
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile	default location	PT	
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile	default location	PT	
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile	default location	PT	

Etiquetas en AP

Paso 7. Navegue hasta Configuration > Tags & Profiles > WLANs y verifique que el SSID fue transferido desde Cisco DNA:

Configuration > Tags & Profiles > WLANs

+ Add	X Delete	Clone	Enable WLAN	Disable WLAN	WLAN Wizard
Selected WLANs : 0					
Status	Name	ID	SSID	Security	
<input type="checkbox"/>	Demo_Global_NF_986e8d08	17	Demo	[open],MAC Filtering	
1 - 1 of 1 items					

WLAN

Crear sitio de fabric

Paso 1. Vaya a Aprovisionamiento > Sitios de fabric. Cree un sitio de fabric:

Virtual Networks

Fabric Sites

Transits

 Search Table

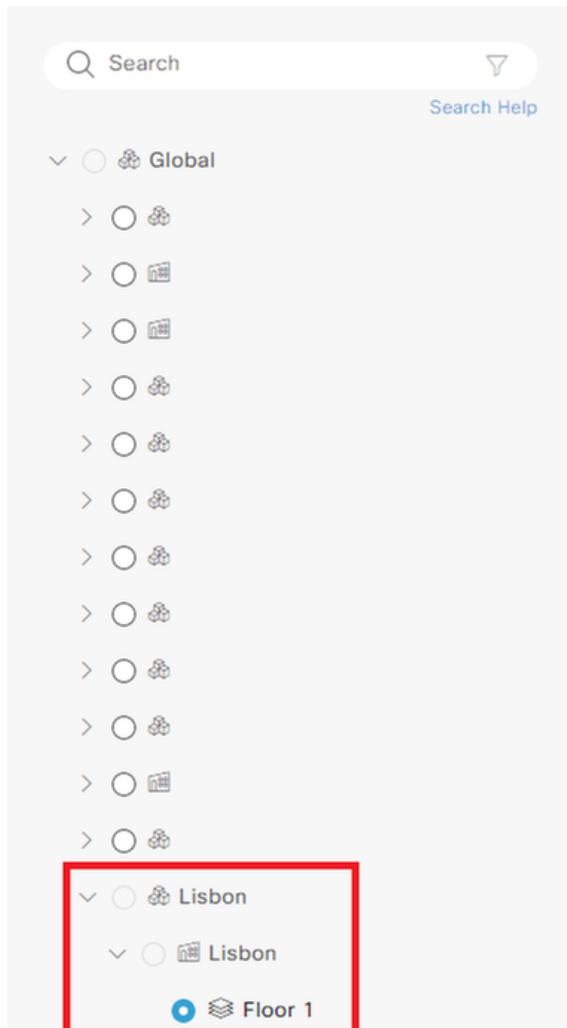
 Create Fabric Sites and Fabric Zones

Crear sitios de fabric

Paso 2. Seleccione el edificio/planta para el sitio de fabric:

## Fabric Site Location

A Fabric Site begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Site.



The screenshot shows a hierarchical tree structure for selecting a Fabric Site location. The root node is 'Global', which has several child nodes represented by icons of buildings and floors. One node under 'Global' is 'Lisbon', which further has a child node 'Floor 1'. A red box highlights the 'Lisbon' node under 'Global', and another red box highlights the 'Floor 1' node under 'Lisbon'.

- Global
  - Lisbon
    - Floor 1

Seleccionar sitio de fabric

Paso 3. Seleccione una plantilla de autenticación. En esta demostración, se aplicó None:

## Authentication Template

Select a Template for the Fabric Site. The Template will apply a port-based network access control configuration to all access ports on Edge Nodes and Extended Nodes.

- Closed Authentication [i](#) [Edit](#)
- Open Authentication [i](#) [Edit](#)
- Low Impact [i](#) [Edit](#)
- None** [i](#)

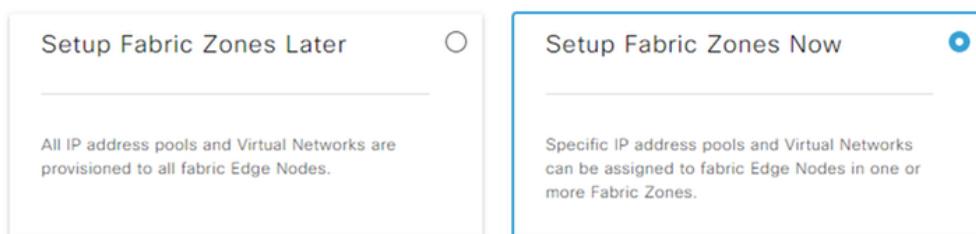
Plantilla de autenticación

Paso 3. Puede elegir si desea configurar la zona de fabric ahora o más tarde:

## Fabric Zones

Fabric Zones are optional. They reside within a Fabric Site and can only contain Edge Nodes and Extended Nodes. If Fabric Zones are used, only select Virtual Networks and Anycast Gateways (IP address pools) are provisioned to the Edge Nodes in each Fabric Zone.

If Fabric Zones are not used, all Virtual Networks and Anycast Gateways are provisioned to all Edge Nodes in the Fabric Site.



Select one or more areas, buildings, or floors to enable as a fabric zone

A Fabric Zone begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Zone.

LEGEND  Fabric Site

The image is a screenshot of a user interface for selecting a fabric zone. At the top, there is a search bar with the placeholder 'Search Hierarchy' and a magnifying glass icon. To the right of the search bar is a small circular icon with a downward arrow. Below the search bar, the text 'Search Help' is visible. Underneath the search bar, there is a list item: 'Floor 1' preceded by a small square checkbox. In the bottom left corner of the interface, there is a circular button with a downward-pointing triangle symbol.

Configuración de zonas de fabric

Paso 4. Compruebe la configuración de la zona de fabric. Si todo está correcto, seleccione Deploy:

Summary

Review the Fabric Site and Fabric Zone settings before deploying.

Fabric Site Location [Edit](#)  
Site Name: Global/Lisbon/Lisbon/Floor\_1

Wired Endpoint Data Collection [Edit](#)  
Monitor wired clients: Enable

Authentication Template [Edit](#)  
Authentication Template: No Authentication

Fabric Zones [Edit](#)  
Enable fabric zones?: No

Changes saved

Review [Back](#) [Deploy](#)

Implementar sitio de fabric

Ha creado un sitio de fabric:

Success! You created a Fabric Site.

Your Fabric Site, Global/Lisbon/Lisbon/Floor\_1, was created successfully.

Creación de sitios de fabric

Agregar WLC al fabric

Navegue hasta Aprovisionamiento > Sitios de fabric y seleccione su sitio de fabric. Haga clic en la parte superior de su WLC y navegue a la pestaña Fabric. Habilite fabric al WLC y seleccione Add:

Fabric Sites

Fabric Site: Global/Lisbon/Lisbon/Floor\_1

Floor 1

Fabric Infrastructure

Host Onboarding

9800-17-9-RMI-RP-HA.dns-ams.cisco.com (10.48.39.186)

Reachable Uptime: 16 days 5 hrs 5 mins

One (1) Warning Alert and One (1) Information Alert on this page

Fabric

Wireless LAN Controller

Add

Agregar WLC al fabric

## Incorporación de AP

Paso 1. Vaya a Diseño > Configuración de red > Pools de direcciones IP. Cree un pool de direcciones IP.

The screenshot shows the 'IP Address Pools' configuration page. On the left, there is a list of existing pools: 'S1-INFRA' (General), 'S2-INFRA' (General), and 'S3-INFRA' (General). A red box highlights the 'Add' button. On the right, a modal window titled 'Add IP Pool' is open. It contains fields for 'Pool Name' (set to 'S1-INFRA'), 'Pool Type' (set to 'General'), 'IP Address Space' (set to 'IPv4'), and 'IP Range' (set to '172.16.0.0/24'). Other fields like 'Gateway IP Address', 'DHCP Server(s)', and 'DNS Server(s)' are also present but empty. A red box highlights the 'IP Range' field.

Conjunto de direcciones IP

Paso 2. Navegue hasta Aprovisionamiento > Sitios de fabric y seleccione su sitio de fabric. Vaya a Host Onboarding > Virtual Networks.

INFRA\_VN se introduce en los puntos de acceso fácilmente incorporados. Los AP se encuentran en la superposición del entramado, pero INFRA\_VN está asignado a la tabla de ruteo global. Solo los AP y los nodos extendidos pueden pertenecer a INFRA\_VN. La extensión de capa 2 se habilita automáticamente y activa el servicio LISP de capa 2.

Seleccione INFRA\_VN > Agregar:

The screenshot shows the 'Edit Virtual Network: INFRA\_VN' configuration page. On the left, a sidebar shows 'Fabric Site / Page 1' and 'Floor 1'. Under 'Fabric Infrastructure', 'Virtual Networks' is selected. A red box highlights the 'Virtual Networks' tab. Below it, a list of VLANs includes 'DEFAULT\_VN' and 'INFRA\_VN', with 'INFRA\_VN' highlighted by a red box. On the right, the main panel shows the 'Edit Virtual Network: INFRA\_VN' interface. A red box highlights the 'Add Components' button at the bottom right of the main panel.

Editar red virtual

Paso 3. Agregue un Pool de Direcciones IP con el Tipo de Pool como AP:

Edit Virtual Network: INFRA\_VN

< Back

The screenshot shows the 'Edit Virtual Network: INFRA\_VN' configuration page. At the top, there are two dropdown menus: 'IP Address Pool' set to 'S1-INFRA (172.16.0.0/24)' and 'Pool Type' set to 'AP'. Below these, there are fields for 'VLAN' (set to '39') and 'VLAN Name' (set to 'VLAN0039'). A blue circular icon with a plus sign is located in the top right corner of the form area. At the bottom right, there is a checkbox for 'Auto generate VLAN name' which is unchecked.

Editar red virtual S1-INFRA

Paso 4. Compruebe si la extensión de capa 2 está habilitada.

Edit Virtual Network: INFRA_VN						
						x
VLAN Name	Delete	Enable/Disable Suplicant-Based Extended Node Onboarding				
VLAN0039			Pool Type	Suplicant-Based Extended Node	IP Address Pool	VLAN Layer-2 Flooding
			AP	Disabled	S1-INFRA 172.16.0.0/24	39 Disabled
						Layer-2 Extension
						Enabled

Editar red virtual

Con Pool Type = AP y Layer-2 extension a ON, Cisco DNA se conecta al WLC y configura la interfaz de Fabric para la asignación VN\_ID para la subred de AP para VN\_IDs L2 y L3.

Paso 5. En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > General. Agregue un nuevo cliente y AP VN\_ID:

The screenshot shows the 'Edit Add Client and AP VNID' dialog box. The 'General' tab is selected in the navigation bar. The dialog contains the following fields:

- Name\*: S2-INFRA
- L2 VNID\*: 8188
- Control Plane Name: default-control-pl ...
- L3 VNID: 4097
- IP Address: 172.16.0.0
- Netmask: 255.255.255.0

On the left, there is a list of clients with 'S2-INFRA' selected at index 1. At the bottom, there are buttons for 'Cancel', 'Update & Apply to Device', and 'Configure Multicast and IC'.

Agregar nuevo cliente y AP VN\_ID

Paso 6. Navegue hasta Configuración > Inalámbrico > Puntos de acceso. Seleccione un AP de la lista. Verifique que el estado del fabric esté habilitado, la dirección IP del plano de control y el nombre del plano de control:

Edit AP			
Configuration	AP Mode	Local	Primary Software Version
All Access Points	Operation Status	Registered	Predownloaded Status
Total APs : 3	Fabric Status	Enabled	Predownloaded Version
AP Name	CleanAir NSI Key		Next Retry Time
AP0C75-BDB	RLOC IP	10.XX.XX.XX	Boot Version
3800E-I	Control Plane Name	default-control-plane	IOS Version
			Mini IOS Version

Verificar el estado del fabric AP

## Cliente incorporado

Paso 1. Agregue el pool a la red virtual y verifique que la opción Layer-2 Extension esté ON para habilitar el LISP de capa 2 y la extensión de subred de capa 2 en el pool/subred del cliente. En Cisco DNA 1.3.x, no se puede inhabilitar.

Layer 2 Only  Layer 3 Only

IP Address Pool  
S1\_CLIENT-IP (10.0.0.0/24)

VLAN  
39

VLAN Name  
VLAN0039  Auto generate VLAN name

Security Group  Traffic   IP-directed broadcast

Layer-2 Flooding  Critical Pool  Wireless Pool

Bridge-Network Virtual Machine

Agregar conjunto de direcciones IP

Paso 2. Verifique si la extensión de capa 2 y el conjunto inalámbrico están habilitados.

## Edit Virtual Network: S1\_Corp\_VN

Filter		Actions								
<input type="checkbox"/>	VLAN Name			VLAN	Traffic Type	Security Group	Layer-2 Flooding	Wireless Pool	Bridge-Network Virtual Machine	Layer-2 Extension
<input type="checkbox"/>	VLAN0039	S1-CLIENT-IP 10.0.0.0/24		39	Data	-	Disabled	Enabled	Disabled	Enabled

Showing 1 of 1

Editar red virtual

Paso 3. En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > General. Agregue un nuevo cliente y AP VN\_ID.

Cuando el conjunto se asigna a la red virtual, la interfaz de fabric correspondiente a la asignación de VNID se envía al controlador. Todos ellos son VNID L2.

Configuration > Wireless > Fabric

General Control Plane Profiles

Fabric Status

ENABLED

Apply

Fabric VNID Mapping

+ Add  X Delete

	Name	L2 VNID	L3 VNID	IP Address	Netmask
<input type="checkbox"/>	S2-INFRA	8188	4097	172.16.0.0	255.255.255.0
<input type="checkbox"/>	10_1_0_0-S2_Corp_VN	8189	0	0.0.0.0	0.0.0.0

Agregar nuevo cliente y AP VN\_ID

Paso 4. Los SSID se asignan al conjunto en las redes virtuales respectivas:

## Floor 1

Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs

Wireless SSID's

SSID Name: Demo Type: Enterprise Security: WPA2 Personal Traffic Type: Voice + Data Address Pool: Choose Pool 10\_1\_0\_0-S2\_Corp\_VN Assign SGT: Assign SGT

Reset Save Find

SSID asignados

Paso 5. Se agrega un perfil de fabric con el VNID de capa 2 al grupo seleccionado y el perfil de política se asigna al perfil de fabric, que se habilita para el fabric.

En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > Profiles.

Configuration > Wireless > Fabric > Profiles

Edit Fabric Profile

⚠️ Modifying the profile may result in loss of connectivity

Profile Name*	s2-demo_Global_F_d3r
Description	s2-demo_Global_F_d3r
L2 VNID	8189
SGT Tag	2-65519

Perfil de fabric

Paso 6. Navegue hasta Configuración > Etiquetas y perfiles > Política. Verifique el perfil de fabric asignado al perfil de política:

Perfil de fabric configurado en la política

## Verificación

Verifique la configuración del fabric en el WLC y el DNA de Cisco

En la CLI del WLC:

```
WLC1# show tech
```

```
WLC1# show tech wireless
```

Configuración del plano de control:

```
router lisp
```

```
locator-table default
```

```
locator-set WLC
```

```
172.16.201.202
```

```
exit-locator-set
```

```
!
```

```
map-server session passive-open WLC
```

```
site_uci
```

```
description map-server configured from Cisco DNA-Center
```

```
authentication-key 7 <Key>
```

```
CB1-S1#sh lisp session
```

Sesiones por defecto de VRF, total: 9, establecido: 5

Estado de par arriba/abajo dentro/fuera

172.16.201.202:4342 Hasta 3d07h 14/14

Configuración de WLC:

tejido inalámbrico

wireless fabric control-plane default-control-plane

ip address 172.16.2.2 key 0 47aa5a

WLC1# show fabric map-server summary

Estado de la conexión MS-IP

---

172.16.1.2 UP

WLC1# show wireless fabric summary

Estado del fabric: Habilitado

Plano de control:

Name IP-address Key Status

---

default-control-plane 172.16.2.2 47aa5a Up

En la GUI del WLC navegue hasta Configuration > Wireless > Fabric y verifique si el estado del fabric está habilitado.

Vaya a Configuration > Wireless > Access Points . Seleccione un AP de la lista. Compruebe que el estado del fabric es Enabled (Activado).

En Cisco DNA, navegue hasta Aprovisionar > Sitios de fabric y verifique si tiene un sitio de fabric. En ese sitio de entramado, navegue hasta Fabric Infrastructure > Fabric y verifique si el WLC está habilitado como entramado.

## Troubleshoot

El cliente no obtiene la dirección IP

Paso 1. Verifique si el SSID es fabric. En la GUI del WLC, navegue hasta Configuration > Tags & Profiles > Policy. Seleccione la política y desplácese hasta Avanzadas. Verifique si el perfil de fabric está habilitado.

Paso 2. Compruebe si el cliente está atascado en el estado de aprendizaje de IP. En la GUI del WLC, navegue hasta Monitoring > Wireless > Clients. Verifique el estado del cliente.

Paso 3. Verifique si la política es DHCP requerido.

Paso 4. Si el tráfico se conmuta localmente entre AP - nodo de borde, recopile los registros de AP (seguimiento del cliente) para la conexión del cliente. Verifique si se reenvía la detección DHCP. Si no llega ninguna oferta de DHCP, hay un problema en el nodo de borde. Si el DHCP no se reenvía, entonces algo está mal en el AP.

Paso 5. Puede recopilar un EPC en el puerto del nodo de borde para ver los paquetes de detección DHCP. Si no ve los paquetes de detección DHCP, el problema está en el AP.

## SSID no se ha transmitido

Paso 1. Verifique si las radios AP están inactivas.

Paso 2. Verifique si la WLAN está en estado encendido y difunda el SSID habilitado.

Paso 3. Verifique la configuración del AP si el AP está habilitado para el entrampado. Navegue hasta Configuration > Wireless > Access Points, seleccione one AP y en la pestaña General puede ver Fabric Status Enabled y la información de RLOC.

Paso 4. Vaya a Configuración > Inalámbrico > Fabric > Plano de control. Verifique si el plano de control está configurado (con la dirección IP).

Paso 5. Navegue hasta Configuración > Etiquetas y perfiles > Política. Seleccione la política y desplácese hasta Avanzadas. Verifique si el perfil de fabric está habilitado.

Paso 6. Navegue hasta Cisco DNA y vuelva a hacer los pasos en [Crear SSID](#) y [Aprovisionar WLC](#). El DNA de Cisco debe empujar el SSID al WLC otra vez.

## Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).