

# Ejemplo de configuración de la red de interconexión del regulador del Wireless LAN

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Malla al aire libre ligera AP de las 1510 Series del Cisco Aironet](#)

[Punto de acceso del tejado \(RAP\)](#)

[Punto de acceso del Poste-top \(PAP\)](#)

[Características no soportadas en las redes de interconexión](#)

[Secuencia de inicio del Punto de acceso](#)

[Configurar](#)

[Permiso cero configuración del tacto \(habilitada por abandono\)](#)

[Agregue el MIC a la lista de la autorización AP](#)

[Configure los parámetros del bridging para los AP](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento proporciona un ejemplo de configuración básica para establecer un Bridged Link de punto a punto usando la solución Mesh Network. Este ejemplo utiliza dos Lightweight Access Points (LAP). Un LAP actúa como punto de acceso del tejado (RAP), el otro LAP actúa como punto de acceso del Poste-top (PAP), y están conectados a un Cisco Wireless LAN (WLAN) Controller (WLC). El RAP está conectado con el WLC a través de un switch Cisco Catalyst.

Refiera por favor al [ejemplo de configuración de la red de interconexión del regulador del Wireless LAN para las versiones 5.2 y posterior](#) para las versiones de la versión 5.2 del WLC y posterior

## [prerrequisitos](#)

- El WLC se configura para la operación básica.
- El WLC se configura en el modo de la capa 3.
- El Switch para el WLC se configura.

## Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimientos básicos de la configuración de LAPs y WLCs de Cisco
- Conocimiento básico del protocolo ligero AP (LWAPP).
- Conocimiento de la configuración de un servidor DHCP externo y/o del Domain Name Server (DNS)
- Conocimiento de la configuración básica de los switches Cisco

## Componentes Utilizados

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

- WLC de las Cisco 4402 Series que funciona con el firmware 3.2.150.6
- Dos (2) revestimientos de las 1510 Series del Cisco Aironet
- Layer 2 Switch de Cisco

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

## Antecedentes

### Malla al aire libre ligera AP de las 1510 Series del Cisco Aironet

La malla al aire libre ligera AP de las 1510 Series del Cisco Aironet es un dispositivo de red inalámbrica diseñado para el acceso de cliente de red inalámbrica y el bridging del Punto a punto, el bridging de la punta a de múltiples puntos, y la conectividad de red inalámbrica de la malla de la punta a de múltiples puntos. El Punto de acceso al aire libre es una unidad autónoma que se puede montar en una pared o una proyección, en un polo del tejado, o en un polo ligero de calle.

El AP1510 actúa con los reguladores para proporcionar la Administración centralizada y scalable, la gran seguridad, y la movilidad. Diseñó soportar las implementaciones de la cero-configuración, el AP1510 fácilmente y se une a con seguridad la red de interconexión y está disponible manejar y monitorear la red a través del regulador GUI o CLI.

El AP1510 se equipa de dos radios simultáneamente de funcionamiento: un 2.4-GHz radia utilizado para el acceso al cliente y un 5-GHz radia utilizado para el regreso de los datos al otro AP1510s. El tráfico del cliente del Wireless LAN pasa a través de la radio del regreso del AP o se retransmite con el otro AP1510s hasta que alcance la conexión de Ethernet del regulador.

### Punto de acceso del tejado (RAP)

Los rap tienen una conexión alámbrica a un WLC de Cisco. Utilizan la interfaz inalámbrica del regreso para comunicar con los PAP vecinos. Los rap son el nodo primario a cualquier bridging o red de interconexión y conectan un Bridge o una red de interconexión con la red alámbrica. Por lo tanto, puede solamente haber un RAP para cualquier segmento interligado o de la red de interconexión.

**Note:** Cuando usted utiliza la solución de interconexión de redes de la malla para el LAN a LAN que interliga, no conecte un RAP directamente con un WLC de Cisco. Requieren un Switch o a un router entre el WLC de Cisco y el RAP porque el WLCs de Cisco no remite el tráfico de Ethernet que viene de un puerto Lwapp-habilitado. Los rap pueden trabajar en el modo LWAPP de la capa 2 o de la capa 3.

## Punto de acceso del Poste-top (PAP)

Los PAP no tienen ninguna conexión alámbrica a un WLC de Cisco. Pueden ser totalmente inalámbricos, y apoyan a los clientes que comunican con otros PAP o rap, o pueden ser utilizados para conectar con los dispositivos periféricos o una red alámbrica. El acceso de Ethernet está invalidado por abandono por las razones de seguridad, pero debe habilitarlo para los PAP.

**Note:** El Cisco Aironet 1030 revestimientos del borde del telecontrol soporta las implementaciones del salto único mientras que el Cisco Aironet de la serie 1500 AP al aire libre ligeros soporta las implementaciones solas y del multi-salto. Como tal, el Cisco Aironet de la serie 1500 AP al aire libre ligeros se puede utilizar como tejado AP y como PAP para uno o más saltos del WLC de Cisco.

## Características no soportadas en las redes de interconexión

Estas características del regulador no se soportan en las redes de interconexión:

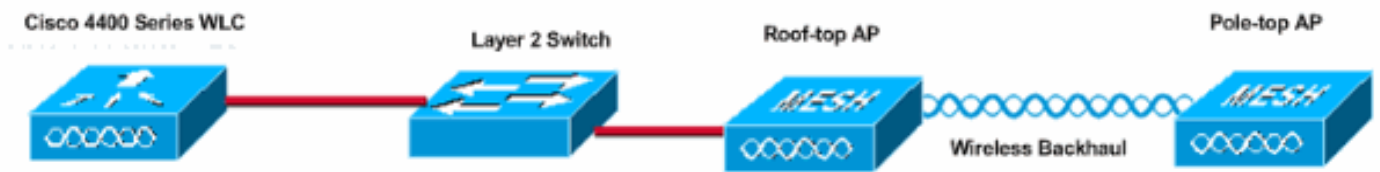
- Soporte plurinacional
- CAC Carga-basado (soporte de las redes de interconexión solamente basado en el ancho de banda, o estático, CAC.)
- Alta disponibilidad (el latido del corazón rápido y la detección primaria se unen al temporizador)
- Autenticación EAP-FASTv1 y del 802.1x
- Autenticación EAP-FASTv1 y del 802.1x
- Localmente - certificado significativo
- Servicios location basados

## Secuencia de inicio del Punto de acceso

Esta lista describe qué sucede cuando el RAP y el PAP empiezan para arriba:

- Todo el tráfico viaja con el RAP y el WLC de Cisco antes de que se envíe al LAN.
- Cuando sube el RAP, los PAP conectan automáticamente con él.
- El link conectado utiliza un secreto compartido para generar una clave que se utilice para proporcionar el Advanced Encryption Standard (AES) para el link.
- Una vez que el telecontrol PAP conecta con el RAP, la malla AP puede pasar el tráfico de datos.
- Los usuarios pueden cambiar el secreto compartido o configurar la malla AP usando la

interfaz de línea del comando cisco (CLI), la interfaz del Web User de Cisco del regulador, o el Cisco Wireless Control System (Cisco WCS). Cisco recomienda que usted modifica el secreto compartido.



## Configurar

Complete estos pasos para configurar el WLC y los AP para el bridging de punto a punto.

1. [Habilite la configuración cero del tacto en el WLC.](#)
2. [Agregue el MIC a la lista de la autorización AP.](#)
3. [Configure los parámetros del bridging para los AP.](#)
4. [Verifique la configuración.](#)

## Habilite la configuración cero del tacto (habilitada por abandono)

### Configuración de la interfaz gráfica para el usuario

El permiso cero configuración del tacto permite a los AP para conseguir la clave secreta compartida del regulador cuando se registra con el WLC. Si usted desmarca el este cuadro, el regulador no proporciona la clave secreta compartida, y los AP utilizan una clave previamente compartida predeterminada para la comunicación segura. Se habilita el valor predeterminado (o marcado). Complete estos pasos del WLC GUI:

**Note:** No hay disposición para la configuración del Cero-tacto en la versión 4.1 y posterior del WLC.

1. Elija la **Tecnología inalámbrica > el bridging** y haga clic el **permiso cero configuración del tacto**.
2. Seleccione el formato dominante.
3. Ingrese la clave secreta compartida bridging.
4. Ingrese la clave secreta compartida bridging otra vez en la clave secreta compartida confirmar.

The image shows a network configuration interface. On the left is a sidebar menu with categories: Wireless, Access Points (All APs, 802.11a Radios, 802.11b/g Radios, Third Party APs), Bridging, Rogues (Rogue APs, Known Rogue APs, Rogue Clients, Adhoc Rogues), Clients, Global RF (802.11a Network, 802.11b/g Network, 802.11h), Country, and Timers. The main content area is titled 'Bridging' and features a 'Zero Touch Configuration' section. This section includes: 'Enable Zero Touch Configuration' with a checked checkbox; 'Key Format' with a dropdown menu set to 'ASCII'; 'Bridging Shared Secret Key' with a text input field containing three dots; and 'Confirm Shared Secret Key' with another text input field containing three dots.

## Configuración de CLI

Complete estos pasos del CLI:

1. Publique el **comando enable de los cero-config de la red de los config** para habilitar la configuración cero del tacto.  
(Cisco Controller) >`config network zero-config enable`
2. Publique el comando del **<string> del bridging-compartir-secreto de la red de los config** para agregar la clave secreta compartida del bridging.  
(Cisco Controller) >`config network bridging-shared-secret Cisco`

## [Agregue el MIC a la lista de la autorización AP](#)

El siguiente paso es agregar el AP a la lista de la autorización en el WLC. Para hacer esto, elija la **Seguridad > las directivas AP**, ingrese el MAC address AP debajo agregan el AP a la lista y al haga click en Add de la autorización

**Security**

**AAA**

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

**Access Control Lists**

**IPSec Certificates**

- CA Certificate
- ID Certificate

**Web Auth Certificate**

**Wireless Protection Policies**

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

**AP Policies**

**Policy Configuration**

Authorize APs against AAA  Enabled

Accept Self Signed Certificate  Enabled

**Apply**

**Add AP to Authorization List**

MAC Address

Certificate Type

**Add**

**AP Authorization List** Items 0 to 20 of 0

MAC Address	Certificate Type	SHA1 Key Hash
-------------	------------------	---------------

**Security**

**AAA**

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

**Access Control Lists**

**IPSec Certificates**

- CA Certificate
- ID Certificate

**Web Auth Certificate**

**Wireless Protection Policies**

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

**AP Policies**

**Policy Configuration**

Authorize APs against AAA  Enabled

Accept Self Signed Certificate  Enabled

**Add AP to Authorization List**

MAC Address

Certificate Type

**AP Authorization List** Items 1 to 2 of 2

MAC Address	Certificate Type	SHA1 Key Hash
00:0b:85:5e:40:00	MIC	
00:0b:85:5e:5a:80	MIC	

En este ejemplo, ambos AP (el RAP y el PAP) se agregan a la lista de la autorización AP en el regulador.

## Configuración de CLI

Publique la auténtico-lista de los config agregan el comando del `mac> mic <AP` para agregar el MIC a la lista de la autorización.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

## Configuración

Este documento usa esta configuración:

### WLC 4402 de Cisco

```
(Cisco Controller) >show run-config
```

```
Press Enter to continue...
```

```
System Inventory
Switch Description..... Cisco
Controller
Machine Model.....
WLC4402-12
Serial Number.....
FLS0943H005
Burned-in MAC Address.....
00:0B:85:40:CF:A0
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2.....
Present, OK
```

```
Press Enter to continue Or <Ctl Z> to abort
```

```
System Information
Manufacturer's Name..... Cisco
Systems, Inc
Product Name..... Cisco
Controller
Product Version.....
3.2.150.6
RTOS Version.....
3.2.150.6
Bootloader Version.....
3.2.150.6
Build Type..... DATA +
WPS

System Name.....
lab120wlc4402ip100
System Location.....
System Contact.....
System ObjectID.....
1.3.6.1.4.1.14179.1.1.4.3
IP Address.....
192.168.120.100
System Up Time..... 0 days
1 hrs 4 mins 6 secs

Configured Country..... United
States
Operating Environment.....
Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to
65 C
Internal Temperature..... +42 C
```

State of 802.11b Network.....  
Disabled  
State of 802.11a Network.....  
Disabled  
Number of WLANs..... 1  
3rd Party Access Point Support.....  
Disabled  
Number of Active Clients..... 0

Press Enter to continue Or <Ctl Z> to abort

Switch Configuration

802.3x Flow Control Mode.....  
Disable  
Current LWAPP Transport Mode..... Layer  
3  
LWAPP Transport Mode after next switch reboot.... Layer  
3  
FIPS prerequisite features.....  
Disabled

Press Enter to continue Or <Ctl Z> to abort

Network Information

RF-Network Name..... airespacerf  
Web Mode..... Enable  
Secure Web Mode..... Enable  
Secure Shell (ssh)..... Enable  
Telnet..... Enable  
Ethernet Multicast Mode..... Disable  
Mode: Ucast  
User Idle Timeout..... 300 seconds  
ARP Idle Timeout..... 300 seconds  
ARP Unicast Mode..... Disabled  
Cisco AP Default Master..... Disable  
Mgmt Via Wireless Interface..... Enable  
Bridge AP Zero Config..... Enable  
Bridge Shared Secret.....  
youshouldsetme  
Allow Old Bridging Aps To Authenticate..... Disable  
Over The Air Provisioning of AP's..... Disable  
Mobile Peer to Peer Blocking..... Disable  
Apple Talk ..... Disable  
AP Fallback ..... Enable  
Web Auth Redirect Ports ..... 80  
Fast SSID Change ..... Disabled

Press Enter to continue Or <Ctl Z> to abort

Port Summary

Link	STP	Admin	Physical	Physical	Link
Pr	Type	Stat	Mode	Status	Status
Trap	Appliance	POE			
1	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		
2	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		

Mobility Configuration

Mobility Protocol Port..... 16666  
Mobility Security Mode.....



```

Disabled
Default Mobility Domain.....
airespacerf
Mobility Group members configured..... 3

Switches configured in the Mobility Group
MAC Address          IP Address          Group Name
00:0b:85:33:a8:40    192.168.5.70       <local>
00:0b:85:40:cf:a0    192.168.120.100    <local>
00:0b:85:43:8c:80    192.168.5.40       airespacerf

Interface Configuration
Interface Name..... ap-
manager
IP Address.....
192.168.120.101
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... Yes

Interface Name.....
management
MAC Address.....
00:0b:85:40:cf:a0
IP Address.....
192.168.120.100
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... No

Interface Name.....
service-port
MAC Address.....
00:0b:85:40:cf:a1
IP Address.....
192.168.250.100

```

```

IP Netmask.....
255.255.255.0
DHCP Protocol.....
Disabled
AP Manager..... No

Interface Name.....
virtual
IP Address.....
1.1.1.1
Virtual DNS Host Name.....
Disabled
AP Manager..... No

WLAN Configuration

WLAN Identifier..... 1
Network Name (SSID).....
lab120wlc4402ip100
Status.....
Enabled
MAC Filtering.....
Enabled
Broadcast SSID.....
Enabled
AAA Policy Override.....
Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60
seconds
Session Timeout..... 1800
seconds
Interface.....
management
WLAN ACL.....
unconfigured
DHCP Server.....
Default
Quality of Service..... Silver
(best effort)
WMM.....
Disabled
802.11e.....
Disabled
Dot11-Phone Mode (7920).....
Disabled
Wired Protocol..... None
IPv6 Support.....
Disabled
Radio Policy..... All
Radius Servers
  Authentication.....
192.168.1.20 1812
Security

  802.11 Authentication:..... Open
System
  Static WEP Keys.....
Enabled
    Key Index:.....
1
    Encryption:.....
104-bit WEP
802.1X.....

```

```

Disabled
  Wi-Fi Protected Access (WPA1).....
Disabled
  Wi-Fi Protected Access v2 (WPA2).....
Disabled
  IP Security.....
Disabled
  IP Security Passthru.....
Disabled
  L2TP.....
Disabled
  Web Based Authentication.....
Disabled
  Web-Passthrough.....
Disabled
  Auto Anchor.....
Disabled
  Cranite Passthru.....
Disabled
  Fortress Passthru.....
Disabled

RADIUS Configuration
Vendor Id Backward Compatibility.....
Disabled
Credentials Caching.....
Disabled
Call Station Id Type..... IP
Address
Administrative Authentication via RADIUS.....
Enabled
Keywrap.....
Disabled

Load Balancing Info
Aggressive Load Balancing.....
Enabled
Aggressive Load Balancing Window..... 0
clients

Signature Policy
  Signature Processing.....
Enabled

Spanning Tree Switch Configuration

STP Specification..... IEEE 802.1D
STP Base MAC Address.....
00:0B:85:40:CF:A0
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15

Spanning Tree Port Configuration

STP Port ID..... 8001
STP Port State..... Forwarding
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 4
STP Port Path Cost Mode..... Auto

```

STP Port ID.....	8002
STP Port State.....	Forwarding
STP Port Administrative Mode.....	802.1D
STP Port Priority.....	128
STP Port Path Cost.....	4
STP Port Path Cost Mode.....	Auto

## [Parámetros del bridging de la configuración para los AP](#)

Esta sección proporciona las instrucciones en cómo configurar el papel del AP en la red de interconexión y los parámetros relacionados del bridging. Usted puede configurar estos parámetros usando el GUI o el CLI.

1. Haga clic la **Tecnología inalámbrica** y entonces **todos los AP** bajo los Puntos de acceso. Toda la página AP aparece.
2. Haga clic el link del **detalle** para su AP1510 para acceder el todo el página AP > de los detalles

En esta página, modo AP bajo fijan al general automáticamente para interligar para los AP que tienen funciones del Bridge, tales como el AP1510. Esta página también muestra esta información conforme a la información del bridging. Conforme a la información del bridging, elija una de estas opciones para especificar el papel de este AP en la red de interconexión:

- **MeshAP** — Elija esta opción si el AP1510 tiene una conexión de red inalámbrica al regulador.
- **RootAP** — Elija esta opción si el AP1510 tiene una conexión alámbrica al regulador.

### Bridging Information

AP Role	MeshAP <input type="button" value="v"/>
Bridge Type	Outdoor
Bridge Group Name	<input type="text"/>
Ethernet Bridging	<input type="checkbox"/>
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	18 <input type="button" value="v"/>

## [Verificación](#)

Use esta sección para confirmar que su configuración funciona correctamente.

Después de que los AP se registren con el WLC, usted puede verlos bajo lengüeta inalámbrica en la cima del GUI del WLC:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

All APs

Search by Ethernet MAC

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
lab120br1510ip152	8	00:0b:85:5e:5a:80	Enable	REG	1	<a href="#">Detail Bridging Information</a>
lab120br1510ip150	10	00:0b:85:5e:40:00	Enable	REG	1	<a href="#">Detail Bridging Information</a>

En el CLI, puede usar el comando **show ap summary** para verificar que los APs se registraron con el WLC:

(Cisco Controller) >**show ap summary**

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
lab120br1510ip152	2	OAP1500	00:0b:85:5e:5a:80	default_location	1
lab120br1510ip150	2	OAP1500	00:0b:85:5e:40:00	default_location	1

(Cisco Controller) >

Haga clic los **detalles del bridging** en el GUI para verificar el papel del AP:

All APs > lab120br1510ip152 > Bridging Details

Bridging Details		Bridging Links	
AP Role	RAP	Parent	
Bridge Group Name		Child	lab120br1510ip150 : 00:0b:85:5e:40:00
Backhaul Interface	802.11a		
Switch Physical Port	1		
Routing State	Maintenance		
Malformed Neighbor Packets	0		
Poor Neighbor SNR reporting	0		
Blacklisted Packets	0		
Insufficient Memory reporting	0		
Rx Neighbor Requests	37		
Rx Neighbor Responses	0		
Tx Neighbor Requests	0		
Tx Neighbor Responses	37		
Parent Changes count	0		
Neighbor Timeouts count	0		
Node Hops	0		

En el CLI, usted puede utilizar el <Cisco AP> de la trayectoria de la malla de la demostración y **mostrar los comandos del <Cisco AP> del relincho de la malla** para verificar que los AP se

registraron con el WLC:

```
(Cisco Controller) >show mesh path lab120br1510ip152  
00:0B:85:5E:5A:80 is RAP
```

```
(Cisco Controller) >show mesh neigh lab120br1510ip152
```

```
AP MAC : 00:0B:85:5E:40:00
```

```
FLAGS : 160 CHILD
```

```
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
```

```
Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0
```

```
adjustedEase 0, unadjustedEase 0
```

```
txParent 0, rxParent 0
```

```
poorSnr 0
```

```
lastUpdate 1150103792 (Mon Jun 12 09:16:32 2006)
```

```
parentChange 0
```

```
Per antenna smoothed snr values: 0 0 0 0
```

```
Vector through 00:0B:85:5E:40:00
```

```
(Cisco Controller) >
```

## Troubleshooting

La malla AP no se asocia al WLC es uno de la mayoría de los problemas frecuentes considerados en el despliegue de la malla. Complete estos controles:

1. Marque que la dirección MAC del Punto de acceso está agregada en la lista de filtros del mac en el WLC. Esto se puede ver bajo la **Seguridad > filtración del mac**.
2. Marque el secreto compartido entre el RAP y el MAPA. Usted puede ver este mensaje en el WLC cuando hay una discordancia en la clave. "Unir a-petición AUTH\_STRING\_PAYLOAD del LWAPP, hash inválido AP el 00:0b:85:68:c1:d0" de la clave del BRIDGE **Note:** Intente siempre utilizar el **permiso cero opción de configuración del tacto** si está disponible para una versión. Esto configura automáticamente la clave para la malla AP y evita el misconfigurations.
3. Los rap no remiten ninguna mensajes de broadcast en su interfaz radio. Configure tan al servidor DHCP para enviar los IP Addresses con el unicast de modo que el MAPA pueda conseguir sus IP Addresses remitidos por el RAP. Si no utilice a IP estático para el MAPA.
4. Deje el nombre de Grupo de Bridge en los valores predeterminados o asegurese que los nombres de Grupo de Bridge están configurados exactamente lo mismo en los mapas y el RAP correspondiente.

Éstos son los problemas que son específicos enredar los Puntos de acceso. Por problemas de conectividad que sean comunes entre el WLC y un Punto de acceso, refiera al [Troubleshooting al Lightweight Access Point que no se une a un regulador del Wireless LAN](#).

## Comandos para resolución de problemas

**Note:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

Usted puede utilizar estos comandos debug de resolver problemas el WLC:

- [permiso del estado PEM del debug](#) — Utilizado para configurar las opciones del debug del administrador de la política de acceso.
- [permiso de los eventos PEM del debug](#) — Utilizado para configurar las opciones del debug del administrador de la política de acceso.
- [permiso del mensaje DHCP del debug](#) — Muestra el debug de los mensajes DHCP que se intercambian a y desde el servidor DHCP.
- [permiso del paquete DHCP del debug](#) — Muestra el debug de los detalles del paquete DHCP que se envían a y desde el servidor DHCP.

Algunos comandos debug adicionales que usted puede utilizar para resolver problemas son:

- [permiso de los errores del lwapp del debug](#) — Muestra el debug de los errores del LWAPP.
- [permiso del pki del debug P.M.](#) — Muestra el debug de los mensajes del certificado que se pasan entre el AP y el WLC.

Esta salida de comando del WLC del [permiso de los lwapp eventos del debug](#) muestra que el REVESTIMIENTO consigue registrado al WLC:

```
(Cisco Controllor) >debug lwapp events enable
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST  
from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1'
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce  
00:0B:85:40:CF:A0 rxNonce 00:0B:85:5E:40:00
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from  
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for  
AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223,  
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop  
MAC: 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of  
LWAPP Join-Reply to AP 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 1
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE REQUEST  
from AP 00:0b:85:5e:40:00 to 00:0b:85:40:cf:a3
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00  
-- static 1, 192.168.120.150/255.255.255.0, gw 192.168.120.1
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring  
-A regDfromCb -A
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring
```

-A regDfromCb -A

Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Config-Message to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated. Last AP failure was due to Link Failure, reason: STATISTICS\_INFO\_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE\_STATE\_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 0!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE\_STATE\_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 1!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

## [Información Relacionada](#)

- [Guía de despliegue de la solución de interconexión de redes de la malla de Cisco](#)
- [Guía de inicio rápido: Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point](#)
- [Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)