Ejemplo de Configuración de Red de Malla del Controlador de LAN Inalámbrica

Contenido

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.

Por favor consulte Ejemplo de Configuración de Red de Malla del Controlador de LAN Inalámbrica para las Versiones 5.2 y posteriores para la Versión 5.2 del WLC y versiones posteriores

Prerequisites

- El WLC se configura para el funcionamiento básico.
- El WLC se configura en el modo de Capa 3.
- El switch para el WLC está configurado.

Requirements

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).
- Información de la configuración de un servidor DHCP externo o del servidor de nombre de dominio (DNS)
- Información básica de configuración de switches de Cisco

Componentes Utilizados

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

- WLC de la serie 4402 de Cisco que ejecuta firmware 3.2.150.6
- Dos (2) LAPs Cisco Aironet serie 1510
- Switch de capa 2 de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Antecedentes

Punto de acceso ligero de malla exterior Cisco Aironet serie 1510

Cisco Aironet 1510 Series Lightweight Outdoor Mesh AP es un dispositivo inalámbrico diseñado para acceso inalámbrico de cliente y puentes punto a punto, puentes punto a multipunto y conectividad inalámbrica de malla punto a multipunto. El punto de acceso exterior es una unidad autónoma que se puede montar en una pared o sobre el techo, en un poste de techo o en un poste de luz de la calle.

El AP1510 funciona con controladores para proporcionar gestión centralizada y escalable, alta seguridad y movilidad. Diseñado para admitir implementaciones de configuración cero, el AP1510 se une de forma fácil y segura a la red de malla y está disponible para administrar y monitorear la red a través de la GUI o CLI del controlador.

El AP1510 está equipado con dos radios de funcionamiento simultáneo: una radio de 2,4 GHz utilizada para el acceso del cliente y una radio de 5 GHz utilizada para la red de retorno de datos a otros AP1510. El tráfico del cliente de LAN inalámbrica pasa a través de la radio de retorno del AP o se retransmite a través de otros AP1510 hasta que alcanza la conexión Ethernet del controlador.

Punto de acceso de techo (RAP)

Los RAP tienen una conexión cableada a un WLC de Cisco. Utilizan la interfaz inalámbrica de red de retorno para comunicarse con los PAP vecinos. Los RAP son el nodo principal a cualquier red de conexión en puente o de malla y conectan un puente o una red de malla a la red con cables. Por lo tanto, puede solamente haber un RAP para cualquier segmento interligado o de la red de interconexión.

Nota: Cuando utiliza la solución de interconexión de redes para el bridging de LAN a LAN, no conecte un RAP directamente a un Cisco WLC. Se requiere un switch o router entre el WLC de Cisco y el RAP porque los WLC de Cisco no reenvían el tráfico Ethernet que viene de un puerto habilitado para LWAPP. Los RAP pueden funcionar en el modo LWAPP de Capa 2 o Capa 3.

Punto de acceso de poste (PAP)

Las PAP no tienen conexión por cable a un WLC de Cisco. Pueden ser completamente inalámbricos y admitir clientes que se comunican con otras PAP o RAP, o pueden utilizarse para conectarse a dispositivos periféricos o a una red con cables. El acceso de Ethernet está invalidado por abandono por las razones de seguridad, pero debe habilitarlo para los PAP.

Nota: Los LAPs Cisco Aironet 1030 Remote Edge admiten implementaciones de un solo salto mientras que los AP para exteriores ligeros Cisco Aironet serie 1500 admiten implementaciones de uno y varios saltos. Por lo tanto, los AP para exteriores ligeros Cisco Aironet serie 1500 se pueden utilizar como AP de techo y como PAP para uno o más saltos del WLC de Cisco.

Funciones no admitidas en redes de malla

Estas funciones del controlador no se soportan en las redes de malla:

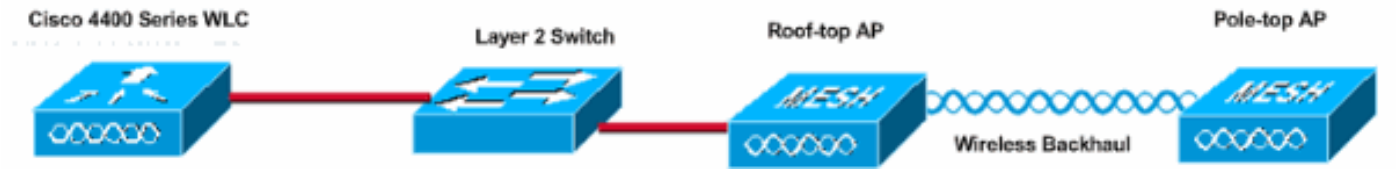
- Compatibilidad con varios países
- CAC basado en la carga (las redes de malla solo admiten CAC estática o basada en el ancho de banda).
- Alta disponibilidad (latido rápido y temporizador de incorporación de detección principal)
- Autenticación EAP-FASTv1 y 802.1X
- Autenticación EAP-FASTv1 y 802.1X
- Certificado de importancia local
- Servicios basados en la ubicación

Secuencia de inicio del punto de acceso

Esta lista describe lo que sucede cuando el RAP y el PAP comienzan:

- Todo el tráfico viaja a través del RAP y del WLC de Cisco antes de que se envíe a la LAN.
- Cuando aparece el RAP, las PAP se conectan automáticamente a él.
- El enlace conectado utiliza un secreto compartido para generar una clave que se utiliza para proporcionar el estándar de cifrado avanzado (AES) para el enlace.
- Una vez que el PAP remoto se conecta con el RAP, los AP de malla pueden pasar el tráfico de datos.
- Los usuarios pueden cambiar el secreto compartido o configurar los AP de malla mediante la interfaz de línea de comandos (CLI) de Cisco, la interfaz de usuario web de Cisco del controlador o Cisco Wireless Control System (Cisco WCS). Cisco recomienda que modifique

el secreto compartido.



Configurar

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

1. Habilite la configuración sin interacción en el WLC.
2. Agregue el MIC a la lista de autorización de AP.
3. Configure los parámetros de conexión en puente para los AP.
4. Verifique la Configuración.

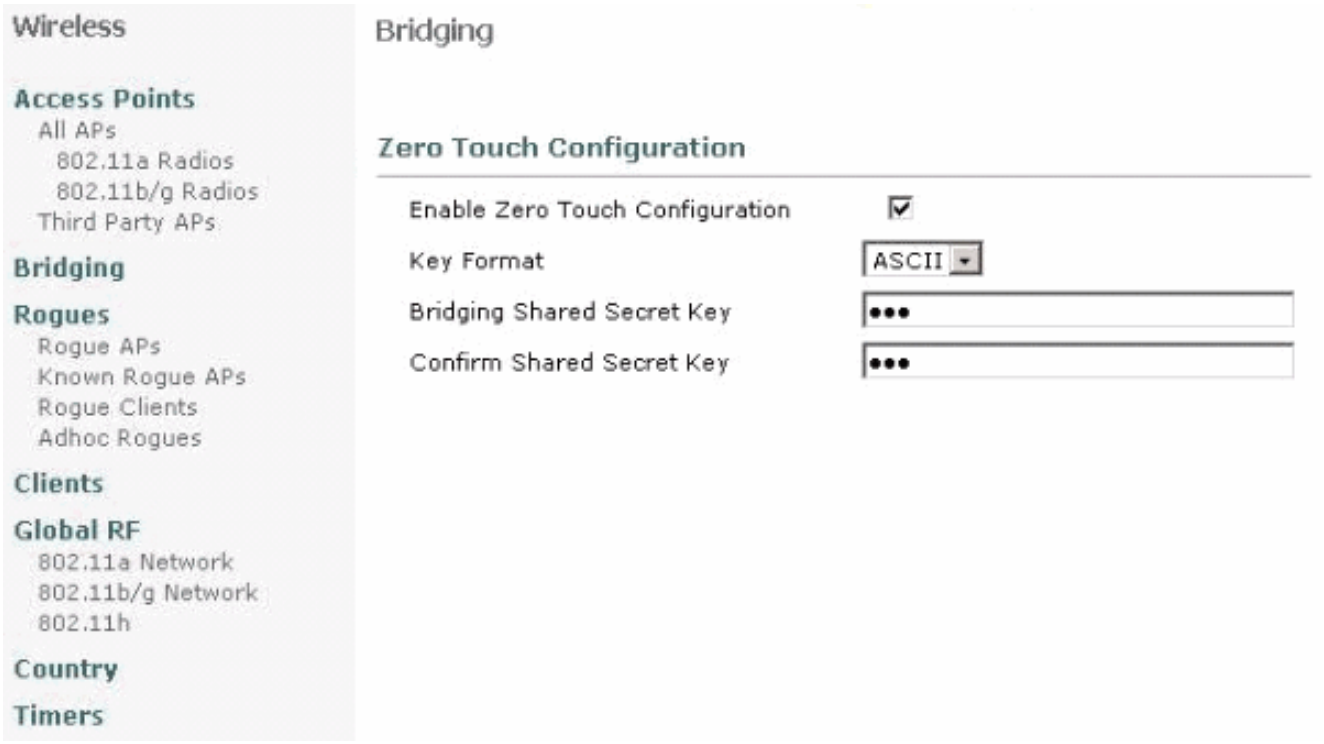
Activar configuración sin intervención (activada de forma predeterminada)

Configuración de la interfaz gráfica para el usuario

Enable Zero Touch Configuration habilita a los APs para obtener la clave secreta compartida del controlador cuando se registra con el WLC. Si desmarca esta casilla, el controlador no proporciona la clave secreta compartida y los AP utilizan una clave previamente compartida predeterminada para una comunicación segura. El valor predeterminado está activado (o activado). Complete estos pasos desde la GUI del WLC:

Nota: No hay ninguna disposición para la configuración de Zero-Touch en la versión 4.1 y posteriores del WLC.

1. Elija **Wireless > Bridging** y haga clic en **Enable Zero Touch Configuration**.
2. Seleccione el formato de clave.
3. Introduzca la clave secreta compartida en puente.
4. Vuelva a introducir la clave secreta compartida en puente en Confirmar clave secreta compartida.



Configuración de CLI

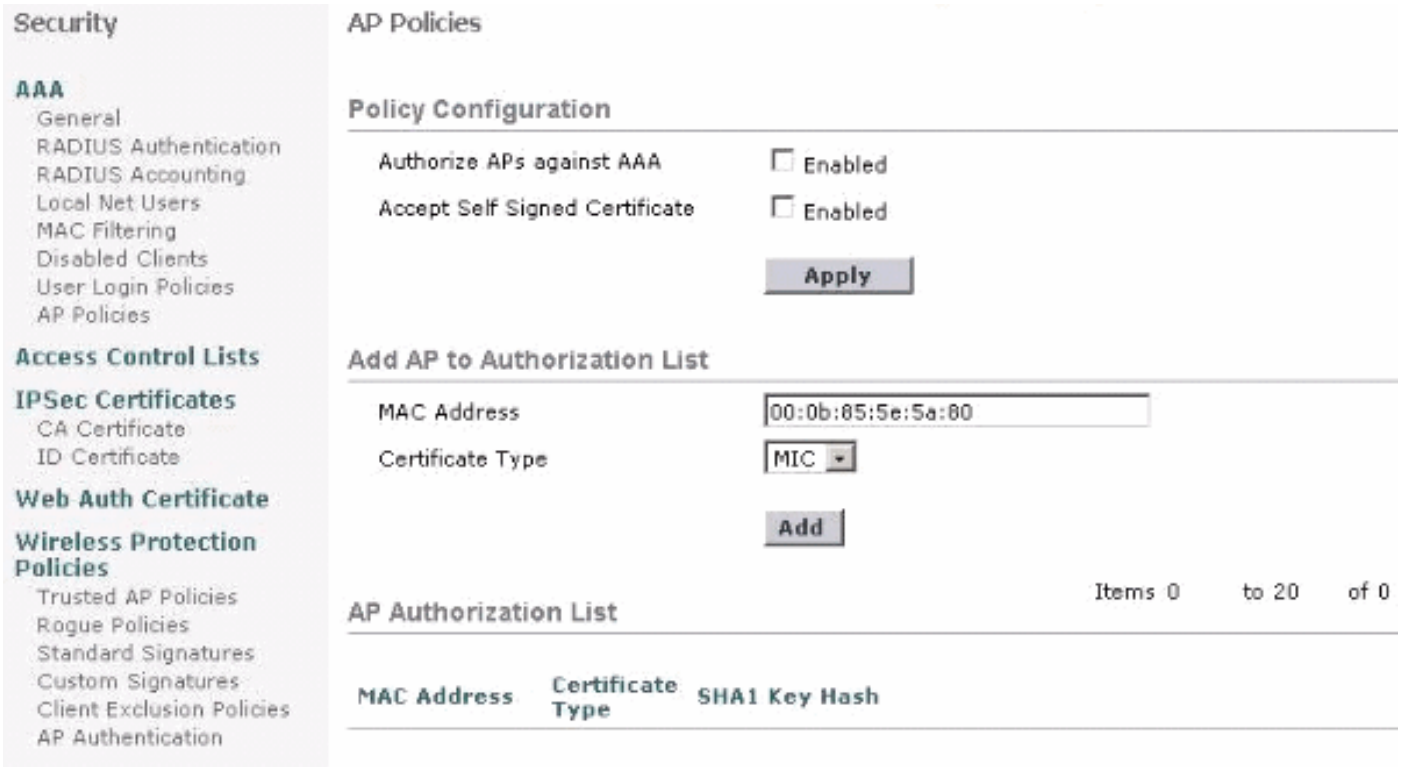
Complete estos pasos desde la CLI:

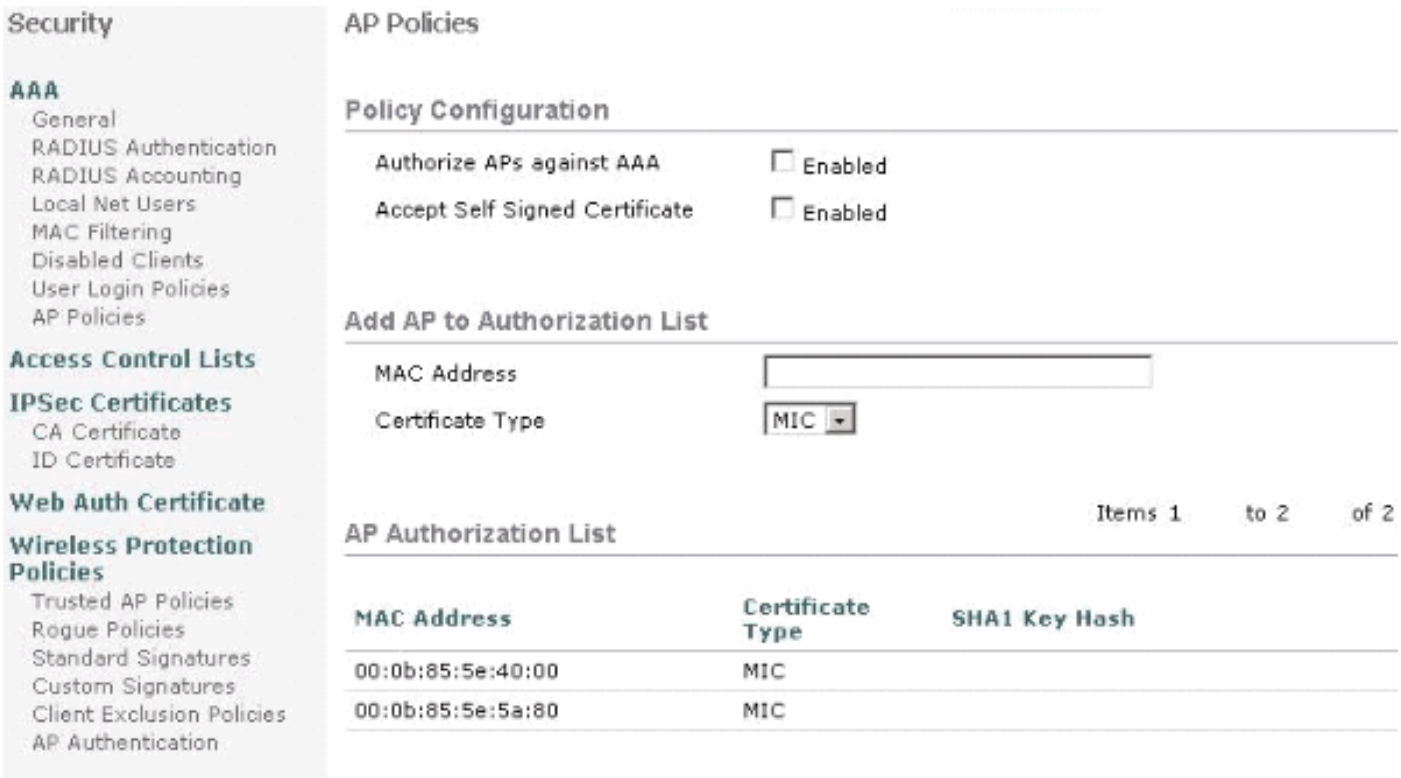
1. Ejecute el comando **config network zero-config enable** para habilitar la configuración sin intervención.
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. Ejecute el comando **config network bridging-shared-secret <string>** para agregar la clave secreta compartida de puente.
   ```
   (Cisco Controller) >config network bridging-shared-secret Cisco
   ```

Agregue el MIC a la lista de autorización de AP

El siguiente paso es agregar el AP a la lista de autorización en el WLC. Para hacer esto, elija **Security > AP Policies**, ingrese la dirección MAC AP bajo Add AP to Authorization List y haga clic en **Add**.





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

Configuración de CLI

Ejecute el comando **config auth-list add mic <AP mac>** para agregar el MIC a la lista de 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:

Cisco WLC 4402

```
(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
           STP   Admin   Physical   Physical   Link
Link    Mcast
Pr  Type   Stat   Mode     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
```

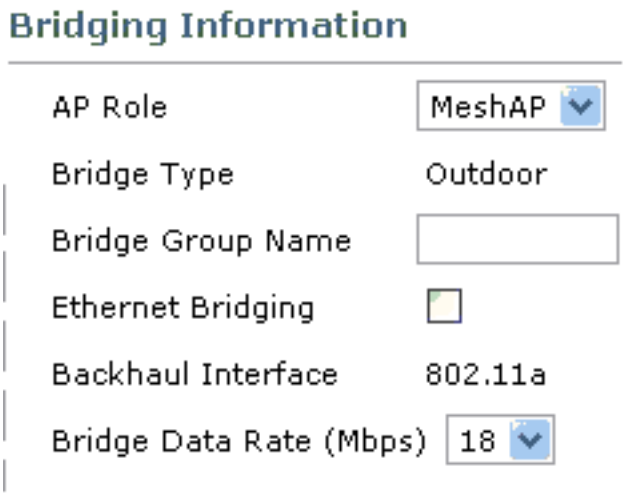
Configuración de los Parámetros de Bridging para los AP

Esta sección proporciona instrucciones sobre cómo configurar el rol del AP en la red de malla y los parámetros de bridging relacionados. Puede configurar estos parámetros mediante la GUI o la CLI.

1. Haga clic en **Wireless** y luego **All AP** bajo Access Points. Aparece la página Todos los AP.
2. Haga clic en el enlace **Detail** para su AP1510 para acceder a la página All APs > Details

En esta página, el modo AP en General se configura automáticamente en Bridge para los AP que tienen funcionalidad de bridge, como el AP1510. Esta página también muestra esta información en Bridging Information . En Bridging Information , elija una de estas opciones para especificar el rol de este AP en la red de interconexión:

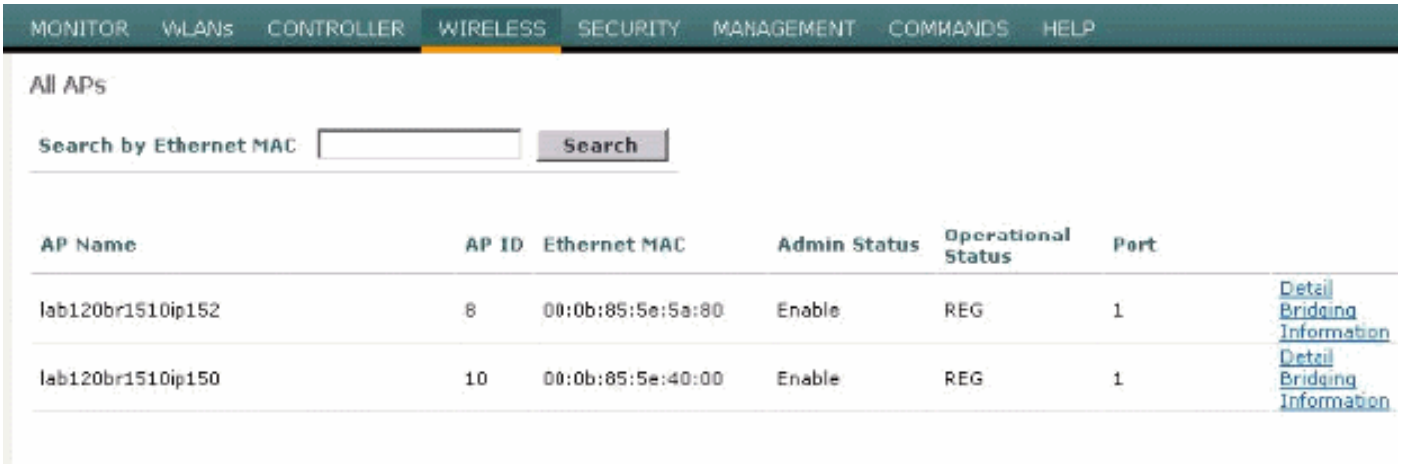
- **MeshAP**: Elija esta opción si el AP1510 tiene una conexión inalámbrica al controlador.
- **RootAP**: Elija esta opción si el AP1510 tiene una conexión cableada al controlador.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

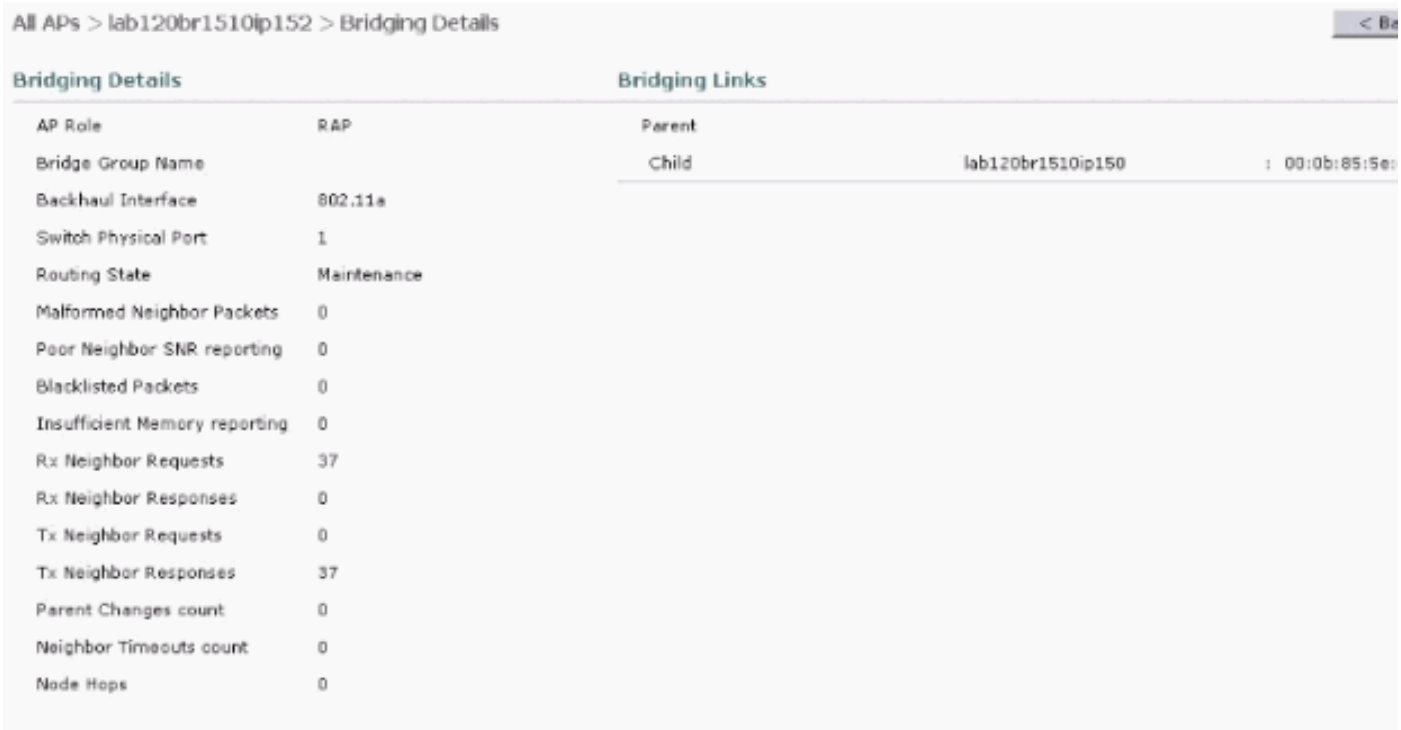
Después de que los AP se registran con el WLC, puede verlos en la pestaña Wireless en la parte superior de la GUI del WLC:



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 en **Detalles de Bridging** en la GUI para verificar el rol del AP:



En la CLI, puede utilizar los comandos **show mesh path <Cisco AP>** y **show mesh neigh <Cisco AP>** 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) >
```

Troubleshoot

`Los AP de malla no se asocian al WLC` es uno de los problemas más comunes vistos en la implementación de malla. Complete estas comprobaciones:

1. Verifique que la dirección MAC del punto de acceso se agrega en la lista de filtros Mac en el WLC. Esto se puede ver en **Seguridad > Filtrado de Mac**.
2. Verifique el secreto compartido entre el RAP y el MAP. Puede ver este mensaje en el WLC cuando hay una discordancia en la clave.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, hash de clave de BRIDGE no válido AP 00:0b:85:68:c1:d0"` **Nota:** Intente siempre utilizar la opción **Activar configuración sin intervención** si está disponible para una versión. Esto configura automáticamente la clave para los AP de malla y evita errores de configuración.
3. Los RAP no reenvían ningún mensaje de difusión en su interfaz de radio. Configure el servidor DHCP para enviar direcciones IP a través de unicast de modo que MAP pueda obtener sus direcciones IP reenviadas por RAP. De lo contrario, utilice una IP estática para el MAP.
4. Deje el Bridge Group Name en los valores predeterminados o asegúrese de que los Bridge Group Names estén configurados exactamente igual en los MAP y el RAP correspondiente.

Estos son problemas específicos de los puntos de acceso de malla. Para los problemas de conectividad que son comunes entre el WLC y un punto de acceso, refiérase a Troubleshooting de un Punto de Acceso Ligero que No se Une a un Controlador de LAN Inalámbrico.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos

debug.

Puede utilizar estos comandos debug para resolver problemas del WLC:

- **debug pem state enable** —Se utiliza para configurar las opciones de depuración del administrador de políticas de acceso.
- **debug pem events enable** —Se utiliza para configurar las opciones de depuración del administrador de políticas de acceso.
- **debug dhcp message enable** —Muestra la depuración de mensajes DHCP que se intercambian hacia y desde el servidor DHCP.
- **debug dhcp packet enable** —Muestra la depuración de los detalles del paquete DHCP que se envían hacia y desde el servidor DHCP.

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

- **debug lwapp errors enable**—Muestra la depuración de errores LWAPP.
- **debug pm pki enable**—Muestra el debug de los mensajes de certificado que se pasan entre el AP y el WLC.

Esta salida del comando **debug lwapp events enable** WLC muestra que el LAP se registra en el WLC:

```
(Cisco Controller) >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, gtw 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 implementación de la solución Cisco Mesh Networking
- Guía de inicio rápido: Puntos de acceso de malla exteriores ligeros Cisco Aironet serie 1500
- 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