

# Ejemplo de Configuración de Ethernet Bridging en Point Wireless Mesh Network

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Asignar dirección IP a los AP](#)

[Agregue la dirección MAC de los AP a la lista de filtrado de MAC del WLC](#)

[Registre el AP con el WLC](#)

[Configuración de la Función AP y Otros Parámetros de Bridging](#)

[Habilitación del Bridging Ethernet en los AP](#)

[Activar configuración sin intervención en el WLC](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento proporciona un ejemplo de configuración simple para la configuración de Ethernet Bridging en una red de interconexión inalámbrica al aire libre. Este documento explica el Ethernet Bridging punto a punto entre los puntos de acceso (AP) de interconexión inalámbrica al aire libre.

## [prerrequisitos](#)

- El controlador de LAN inalámbrica (WLC) está configurado para el funcionamiento básico.
- El WLC se configura en el modo de Capa 3.
- El switch para el WLC está configurado.

## [Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los puntos de acceso ligeros (LAP) y los WLC de Cisco
- Conocimientos básicos sobre la solución de red de malla inalámbrica
- Información básica sobre el protocolo de punto de acceso ligero (LWAPP)
- 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 las Cisco 2000 Series que ejecuta firmware 4.0.217.0
- Dos (2) LAPs Cisco Aironet serie 1510
- Switch de capa 2 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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

La solución de red de malla, que forma parte de la solución de red inalámbrica unificada de Cisco, permite que dos o más puntos de acceso de malla ligeros Cisco Aironet (en lo sucesivo denominados puntos de acceso de malla) se comuniquen entre sí a través de uno o más saltos inalámbricos para unirse a varias LAN o ampliar la cobertura inalámbrica 802.11b. Los puntos de acceso de malla de Cisco están configurados, supervisados y operados desde y a través de cualquier controlador de LAN inalámbrica de Cisco que se implemente en la solución de red de malla.

Las implementaciones de soluciones de red de malla admitidas son de uno de los tres tipos generales:

- Implementación punto a punto
- Implementación punto a multipunto
- Implementación de malla

Este documento se centra en cómo configurar la implementación de malla punto a punto y el bridging Ethernet en el mismo. En la implementación de malla punto a punto, los puntos de acceso de malla proporcionan acceso inalámbrico y red de retorno a los clientes inalámbricos, y pueden soportar simultáneamente el bridging entre una LAN y una terminación a un dispositivo Ethernet remoto u otra LAN Ethernet.

Consulte [Implementaciones de soluciones de redes de malla](#) para obtener información detallada sobre cada uno de estos tipos de implementación.

El punto de acceso de malla exterior ligero Cisco Aironet serie 1510 es un dispositivo inalámbrico diseñado para el acceso inalámbrico del cliente y el puente punto a punto, el puente punto a multipunto y la 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.

Puede utilizar los puntos de acceso ligeros de borde remoto Cisco Aironet 1510 y los puntos de acceso exteriores ligeros Cisco Aironet serie 1500 en una de estas funciones:

- Punto de acceso de techo (RAP)
- Punto de acceso de malla (MAP), también denominado punto de acceso superior del poste (PAP)

Los RAP tienen una conexión por cable a un controlador de LAN inalámbrica de Cisco. Utilizan la interfaz inalámbrica de red de retorno para comunicarse con los MAP cercanos. Los RAP son el nodo primario a cualquier red de conexión en puente o de malla y conectan un puente o una red de malla a la red cableada, por lo que sólo puede haber un RAP para cualquier segmento de red puenteado o de malla.

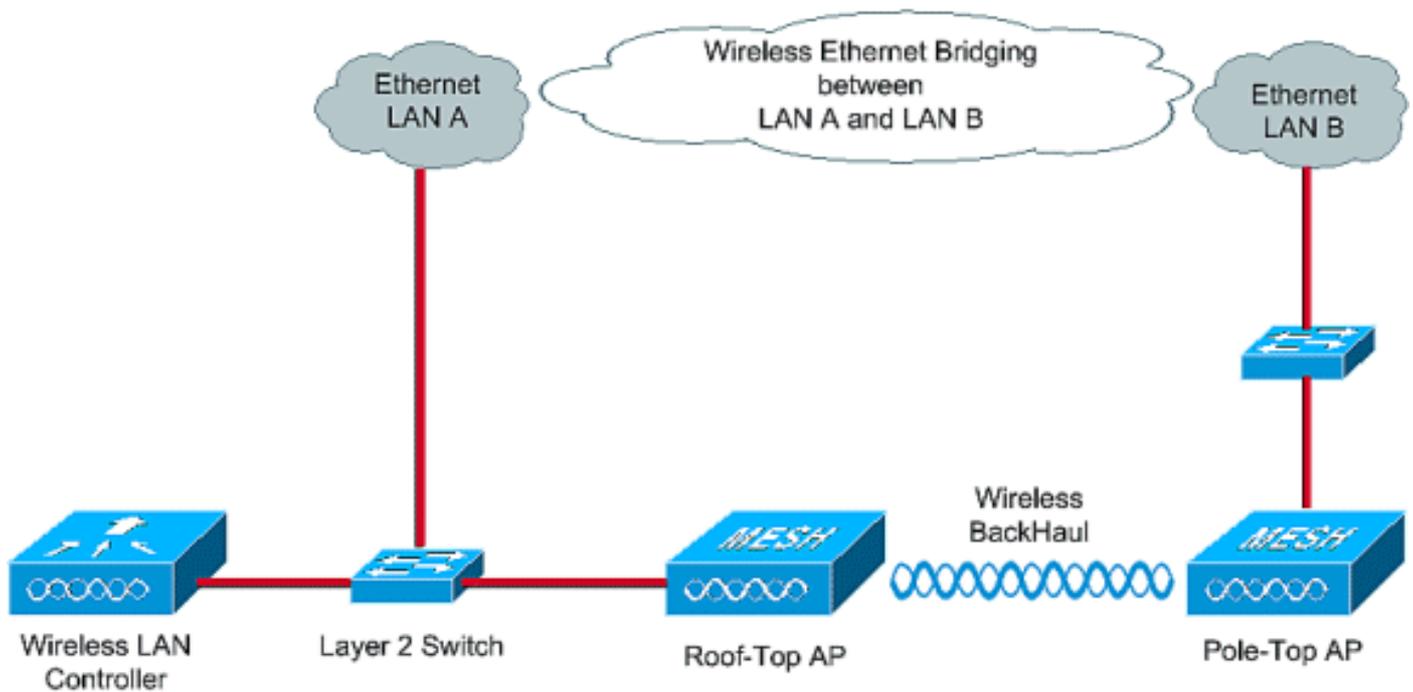
Los MAP no tienen conexión por cable a un controlador de LAN inalámbrica de Cisco. Pueden ser totalmente inalámbricos y admitir clientes que se comunican con otros MAP o RAP, o pueden utilizarse para conectarse a dispositivos periféricos o a una red con cables. El puerto Ethernet está inhabilitado de forma predeterminada por razones de seguridad, pero puede habilitarlo para PAP.

## [Configurar](#)

Este ejemplo de configuración explica cómo configurar la conexión en puente Ethernet entre dos AP de malla exterior ligeros serie 1510 con un AP que actúa como un RAP y el otro AP que actúa como un MAP.

En esta configuración, el AP con dirección MAC 00:0B:85:7F:47:00 se configura como un RAP, y el AP con dirección MAC 00:0B:85:71:1B:00 se configura como un MAP. Una LAN A Ethernet local se conecta en el extremo RAP y la LAN B Ethernet se conecta en el MAP.

## [Diagrama de la red](#)



Para configurar los AP de malla 1510 listos para usar para el bridging Ethernet, realice estos pasos:

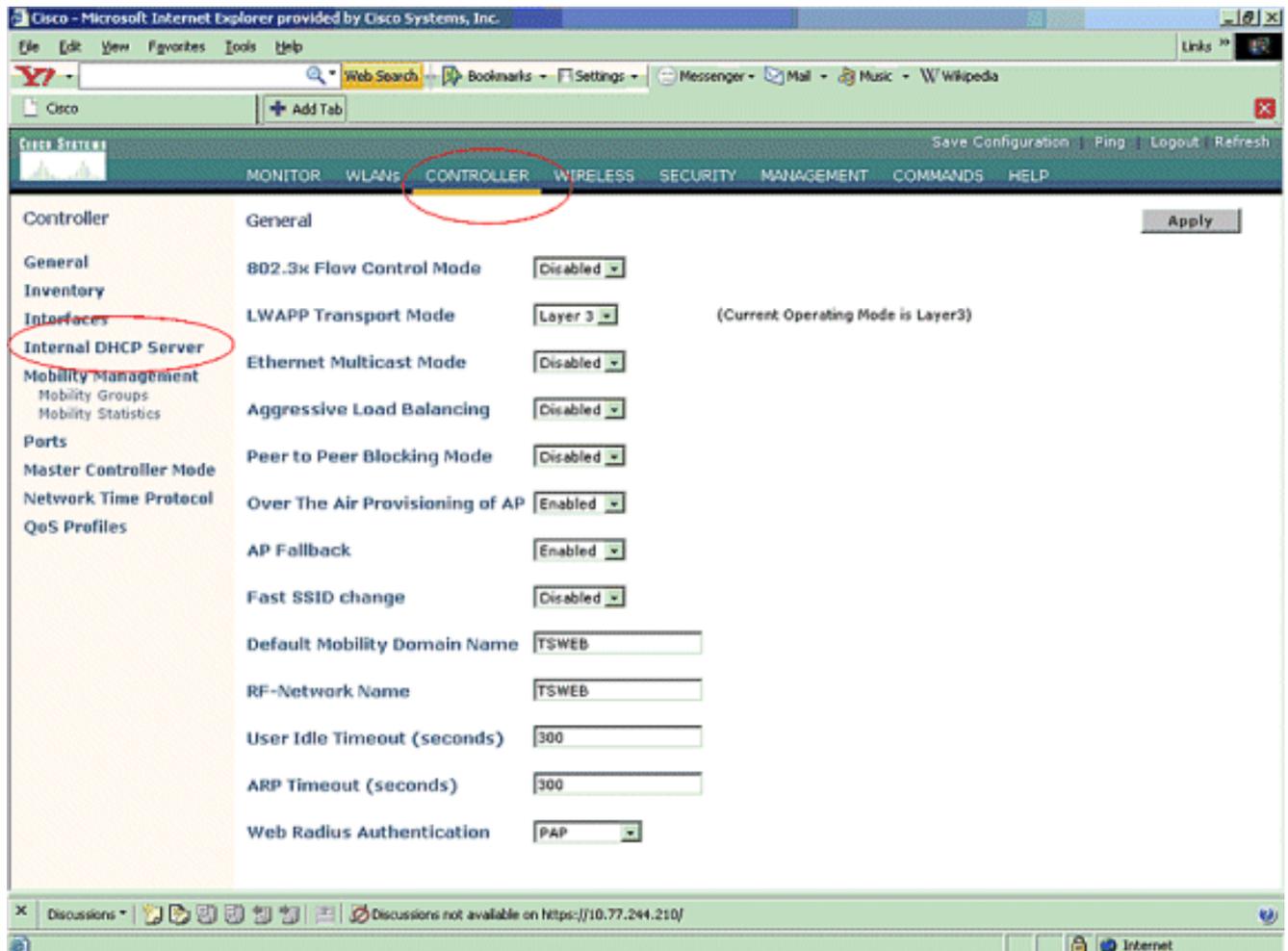
1. [Asignar dirección IP a los AP](#)
2. [Agregue la dirección MAC de los AP a la lista de filtrado de MAC del WLC](#)
3. [Registre los AP con el WLC](#)
4. [Configuración del rol AP y otros parámetros de puente](#)
5. [Habilitación del Bridging Ethernet en los AP](#)
6. [Activar configuración sin intervención en el WLC](#)

## [Asignar dirección IP a los AP](#)

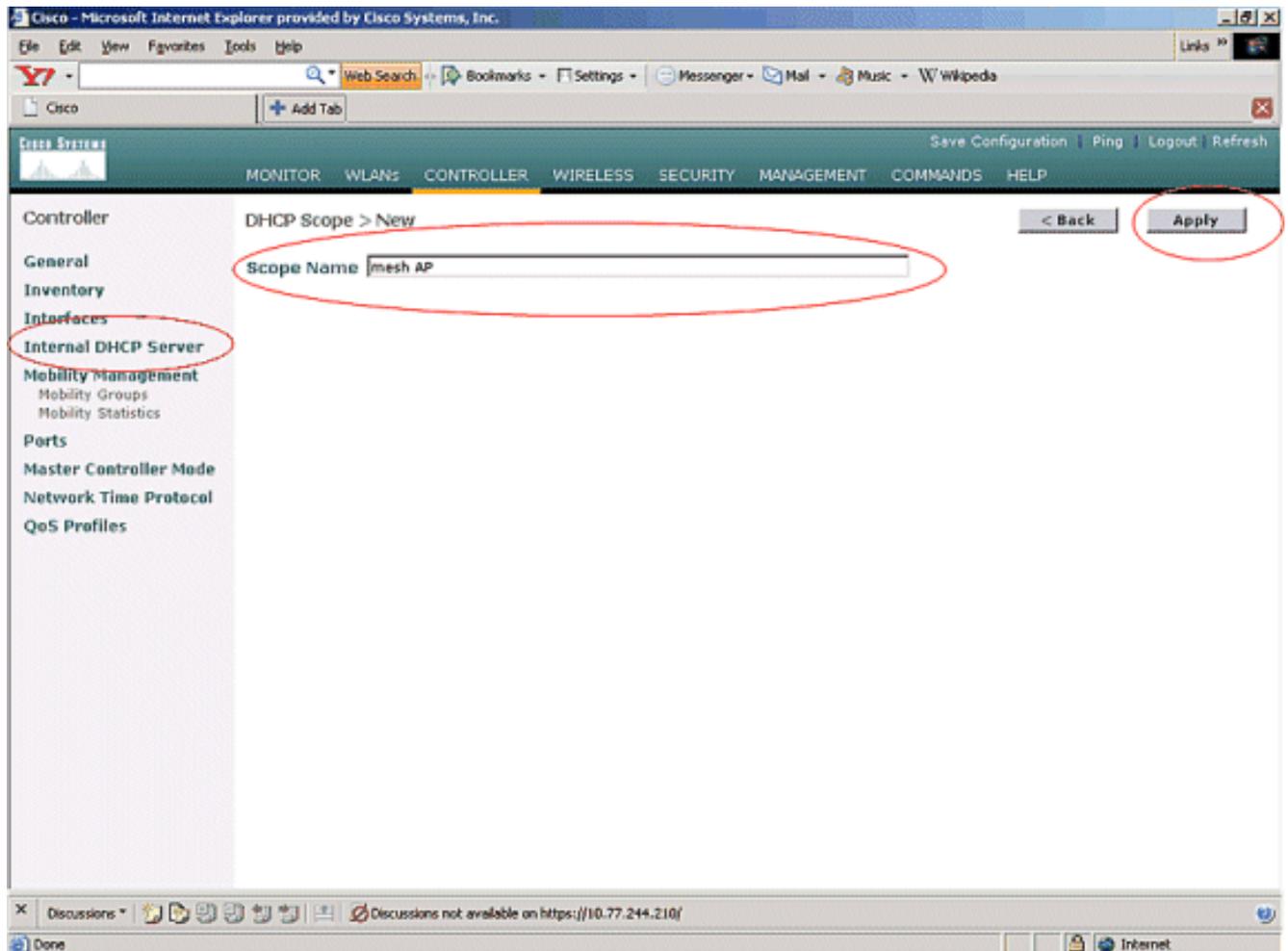
Cuando se inicia un AP, primero busca una dirección IP. Esta dirección IP se puede asignar dinámicamente con un DHCP interno externo como el servidor DHCP de Microsoft Windows<sup>®</sup>. La última versión del WLC (4.0 y posterior) puede asignar la dirección IP a los AP con el servidor DHCP interno en el propio controlador. Este ejemplo utiliza el servidor DHCP interno en el controlador para asignar la dirección IP a los AP.

Complete estos pasos para asignar una dirección IP a los AP a través del servidor DHCP interno en el WLC.

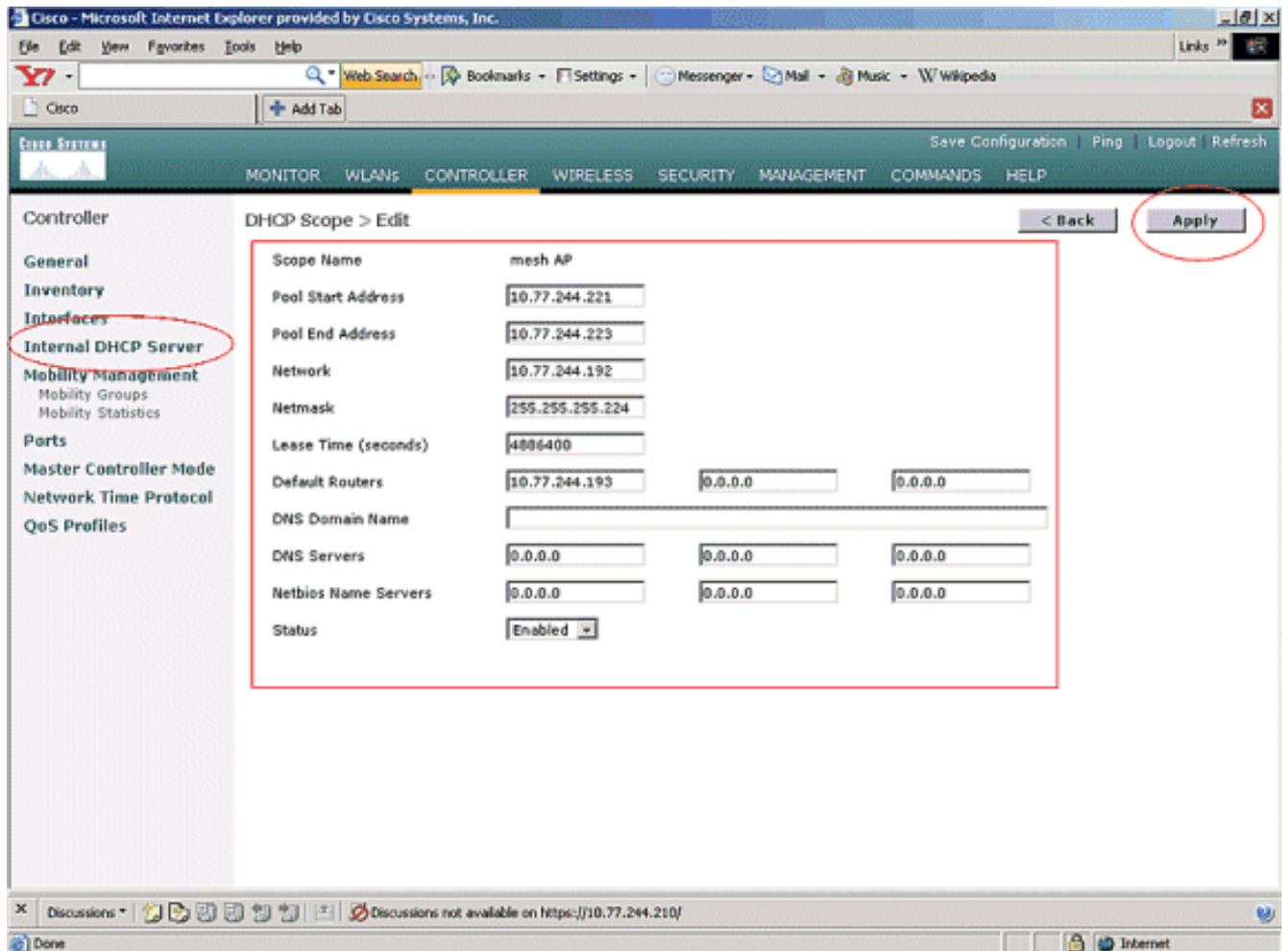
1. Haga clic en **CONTROLLER** en el menú principal de la GUI del WLC. Elija **Servidor DHCP interno** en la esquina izquierda de la página Principal del Controlador.



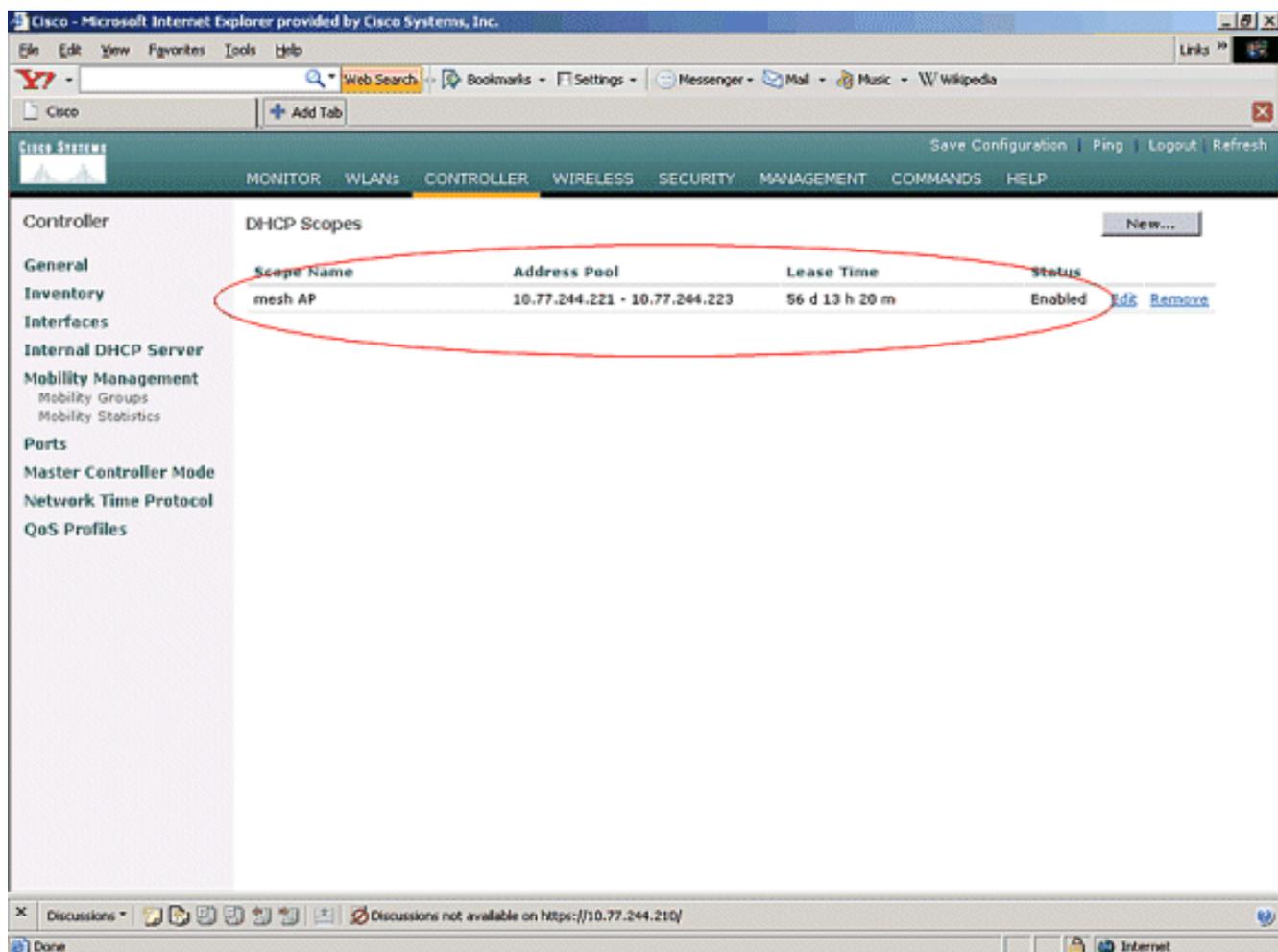
2. En la página **Servidor DHCP interno**, haga clic en **Nuevo** para crear un nuevo ámbito DHCP. Este ejemplo asigna el nombre del ámbito como **AP de malla**. Haga clic en **Apply** (Aplicar). Esto lo lleva a la página de edición del alcance DHCP de la malla AP.



3. En la página **Alcance DHCP > Editar**, configure la dirección inicial del grupo, la dirección final del grupo, la red y la máscara de red, los routers predeterminados y todos los demás parámetros necesarios como se indica en este ejemplo. Elija el estado del servidor DHCP como **Habilitado** en el cuadro desplegable **Estado**. Haga clic en Apply (Aplicar).



4. Ahora, el servidor DHCP interno se configura para asignar direcciones IP a los AP de malla.



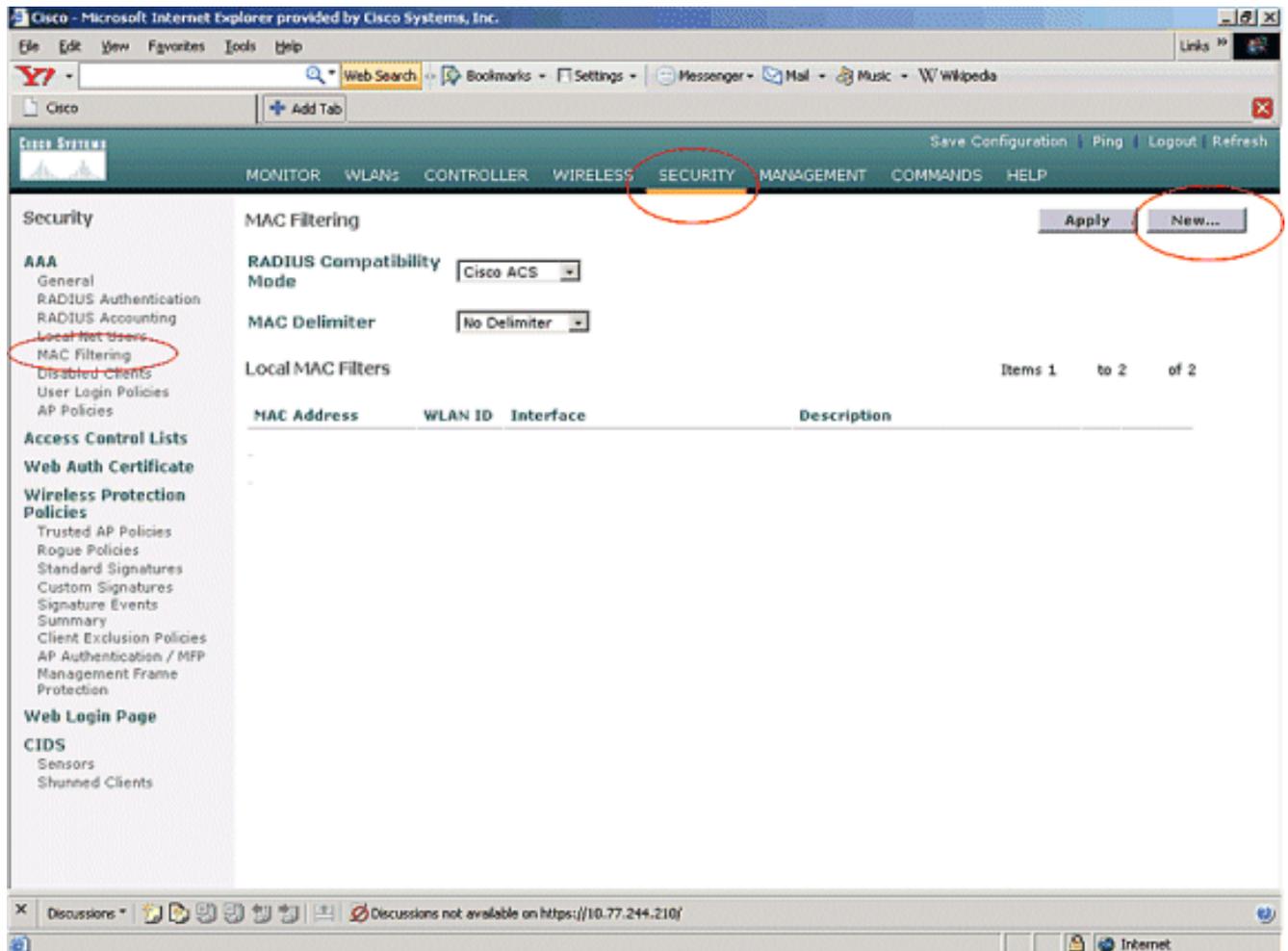
5. Una vez que los AP se registran con el controlador, asigne la dirección IP estática a los AP a través de la GUI del controlador. Si asigna direcciones IP estáticas a AP de malla, proporciona una convergencia más rápida de los AP la próxima vez que se registren con el controlador.

### [Agregue la dirección MAC de los AP a la lista de filtrado de MAC del WLC](#)

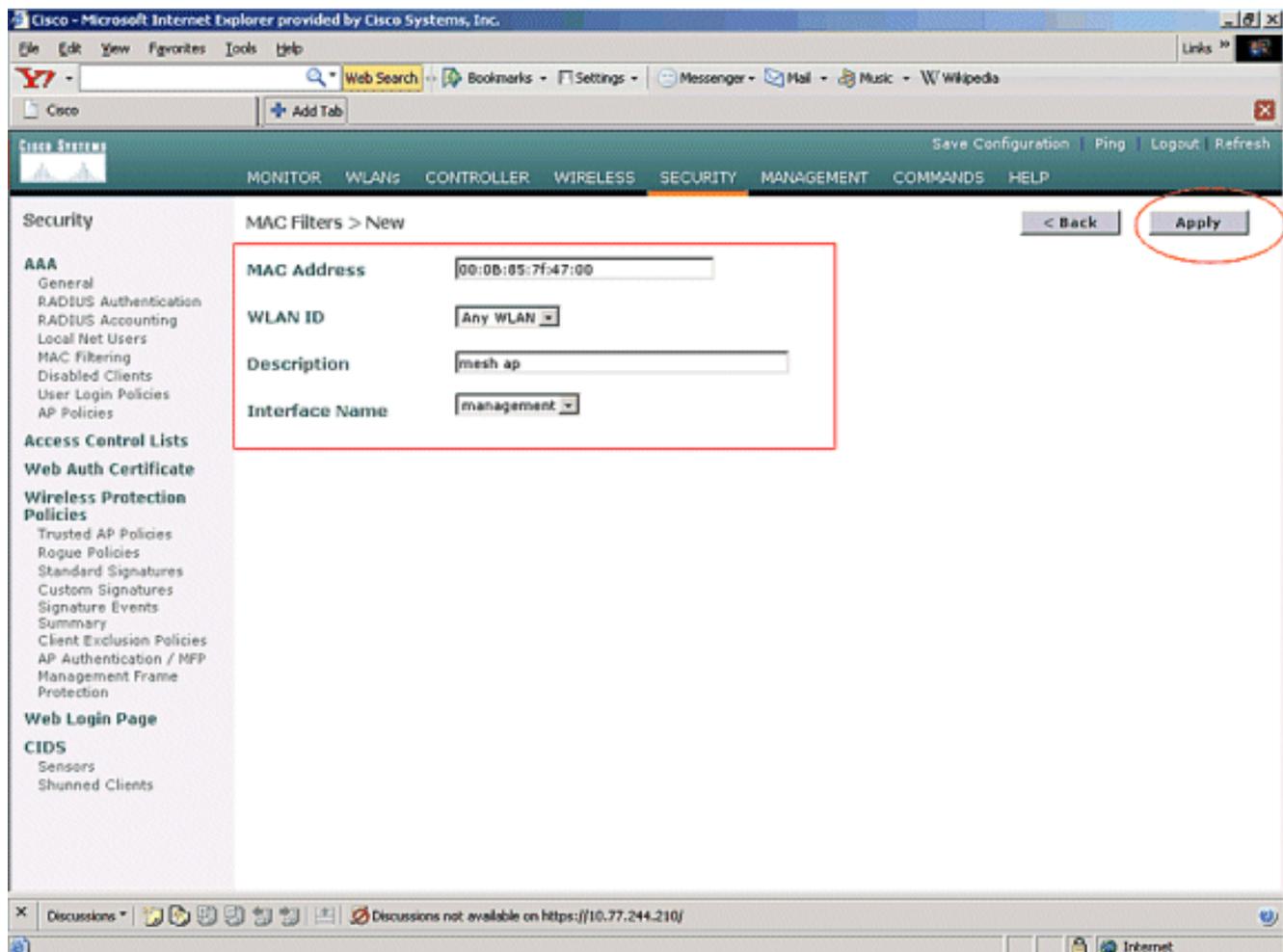
Para registrar los AP de malla con el WLC, primero debe agregar la dirección MAC de los AP a la lista de filtrado MAC del WLC. Puede encontrar la dirección MAC etiquetada en el lado superior del AP de malla.

Complete estos pasos para agregar el AP a la lista de filtrado MAC del WLC.

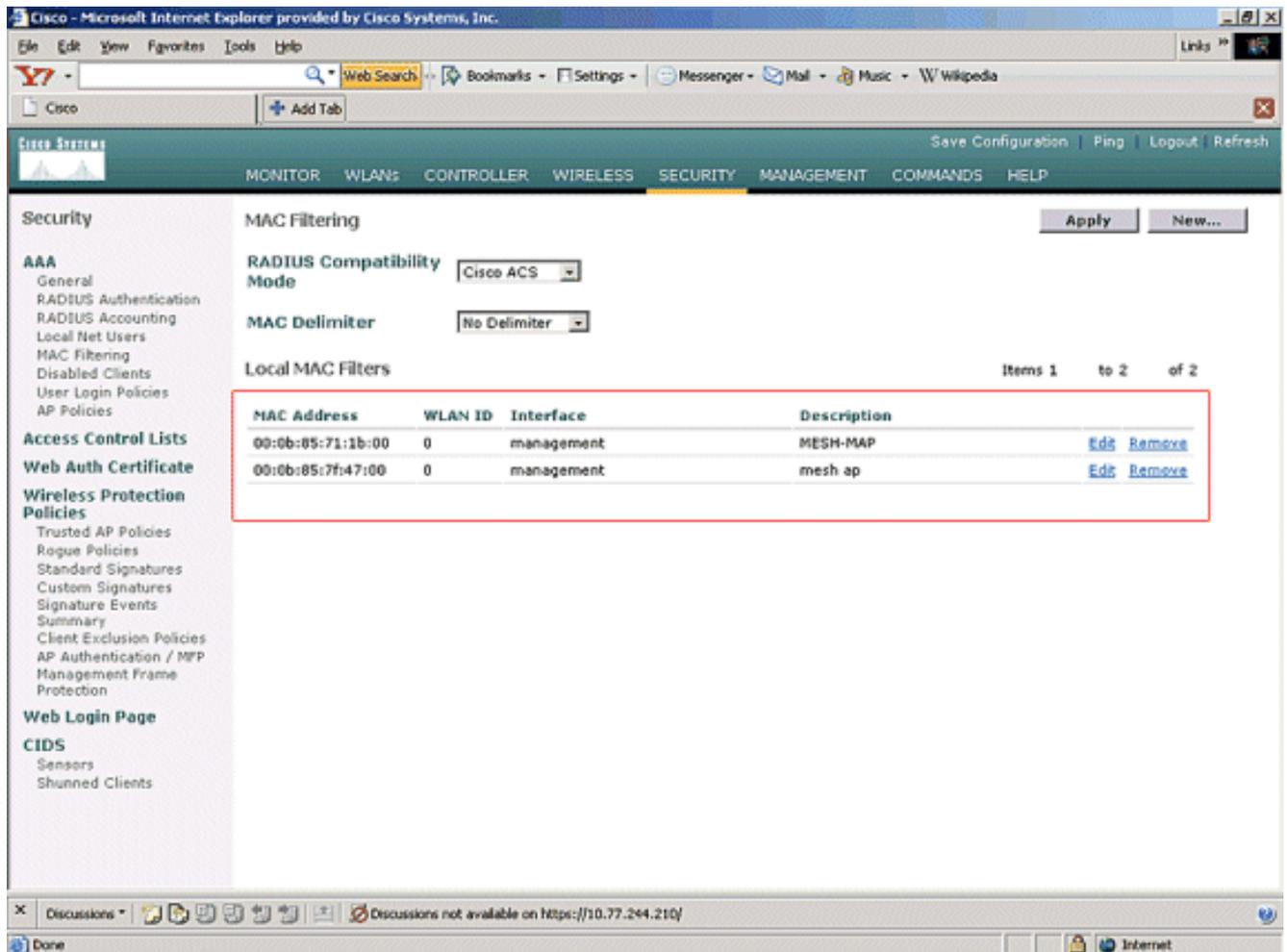
1. Haga clic en **SECURITY** en el menú principal Controller. En la página Seguridad, elija **filtrado MAC** en la **sección AAA**. Esto lo lleva a la página MAC Filtering (Filtrado de MAC). Haga clic en **Nuevo** para crear filtros MAC para los AP de malla.



2. Ingrese la **dirección MAC** del AP y su **descripción** en los cuadros de texto apropiados como se muestra en este ejemplo. Además, elija una **WLAN** y una **interfaz dinámica** en los menús desplegables ID de WLAN y Nombre de la Interfaz, respectivamente. Haga clic en Apply (Aplicar).



- 
- 
3. Repita los pasos 1 y 2 para todos los AP involucrados en esta red de malla, de modo que el filtrado de MAC esté configurado para permitir que los AP de malla se registren con el controlador.



## [Registre el AP con el WLC](#)

El siguiente paso es registrar los AP de malla con el WLC. Hay varios métodos que un AP puede registrar con el WLC. Refiérase a [Registro de AP Ligerero con WLC](#) para obtener detalles sobre cómo un AP se registra con el WLC.

La primera vez que utilice los AP de malla, registre todos los AP directamente conectados con el WLC.

Si no pudo agregar el AP a la lista de filtrado MAC del controlador, los AP no pueden unirse al WLC en el momento del registro con el WLC. La razón es la falla de autorización del resultado del comando **debug lwapp events enable** en el controlador. Este es el ejemplo de salida que indica una falla de autorización.

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

```
.Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to 00:0b:85:33:52:80 on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to ff:ff:ff:ff:ff:ff on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 Received LWAPP JOIN REQUEST from AP
00:0b:85:71:1b:00 to 00:0b:85:33:52:81 on port '2'
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 AP ap:71:1b:00: txNonce 00:0B:85:33
```

```

:52:80 rxNonce 00:0b:85:71:1b:00
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 LWAPP Join-Request MTU path from AP
00:0b:85:71:1b:00 is 1500, remote debug mode is 0
Fri Oct 26 15:52:40 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:71:1b:00

```

En este resultado, puede ver que la solicitud de unión del AP no es aceptada por el controlador debido a la falla de autorización AP.

**Nota:** En implementaciones de red de malla normales que utilizan principalmente AP de malla serie 1500, se recomienda inhabilitar la **configuración Permitir AP de puente antiguo para autenticar** en el controlador. Esto se puede hacer desde el modo CLI del controlador con el comando

**Nota:** (Cisco Controller) > **config network allow-old-bridge-aps disable**

**Nota:** El comando se ha eliminado en 4.1 y posteriores, por lo que esto no es un problema con el WLC 4.1 y posteriores.

En la CLI, puede utilizar el comando **show ap summary** para verificar que los AP están registrados con el WLC:

(Controlador de Cisco) >**show ap summary**

AP Name Port	Slots	AP Model	Ethernet MAC	Location
----- ---	-----	-----	-----	-----
ap:5b:fb:d0 ion 2	2	AP1010	00:0b:85:5b:fb:d0	default_locat
ap:7f:47:00 ion 2	2	<b>LAP1510</b>	00:0b:85:7f:47:00	default_locat
ap:71:1b:00 ion 2	2	<b>LAP1510</b>	00:0b:85:71:1b:00	default_locat

Puede verificarlo desde la GUI bajo la página Wireless **All APs** .

Wireless

Access Points

All APs

Search by Ethernet MAC  Search

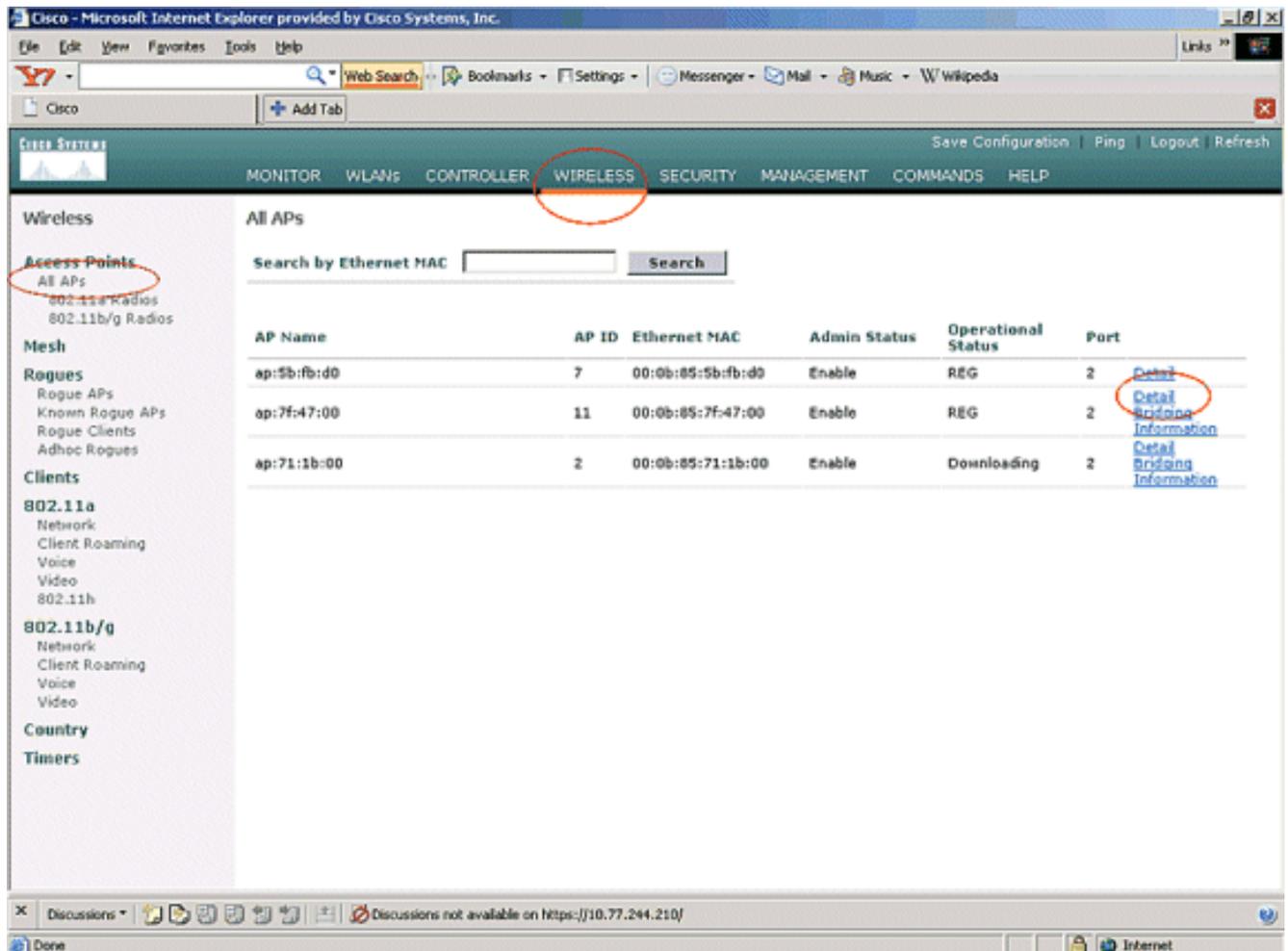
AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:5b:fb:d0	7	00:0b:85:5b:fb:d0	Enable	REG	2
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2

## [Configuración de la Función AP y Otros Parámetros de Bridging](#)

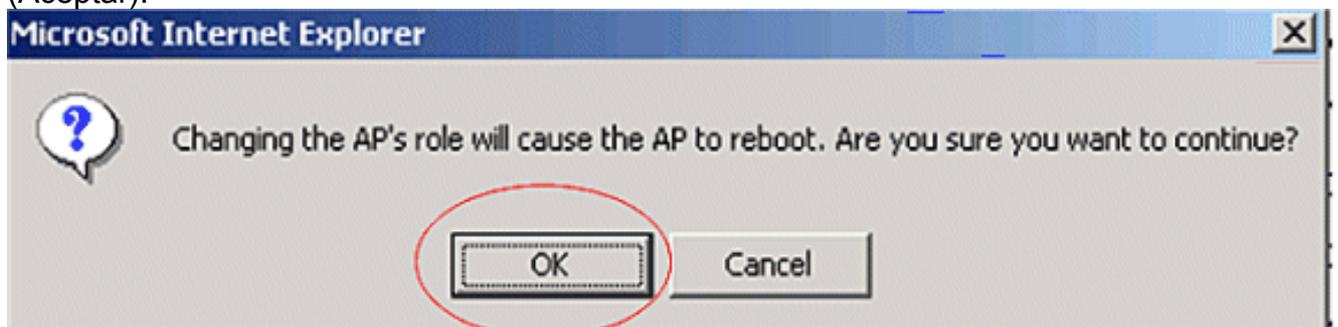
Una vez que los AP se registran en el WLC, debe configurar el rol AP y otros parámetros de bridging. Debe configurar los AP como RAP y MAP, según sea necesario.

Complete estos pasos para configurar esos parámetros AP:

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



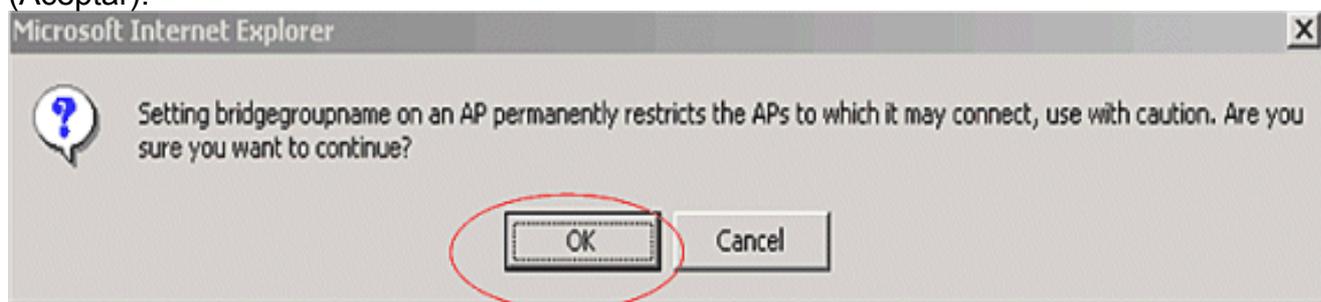
3. En la página **Detalles** de su AP 1510, el **Modo AP** bajo **General** se configura automáticamente en **Bridge** para los AP que tienen funcionalidad de bridge, como el AP1510. Esta página también muestra esta información en Bridging Information. En **Bridging Information**, elija una de estas opciones para especificar el rol de este AP en la red de interconexión: MeshAP (MAP) RootAP (RAP) Los AP configurados como RootAPs deben tener conexión cableada al WLC en el momento de la implementación de la configuración en su entorno de producción. El AP configurado como punto de acceso de malla se conecta de forma inalámbrica al WLC a través de su punto de acceso primario (RAP). Los AP 1510, de forma predeterminada, asumen el rol de los MAP cuando aparecen y se registran con el WLC. Mientras configura la función de puente, un cuadro de alerta muestra este mensaje: **AP se reiniciará**. Para continuar, haga clic en OK (Aceptar).



Puede configurar la función AP con la CLI del controlador con el comando **config ap role role**.

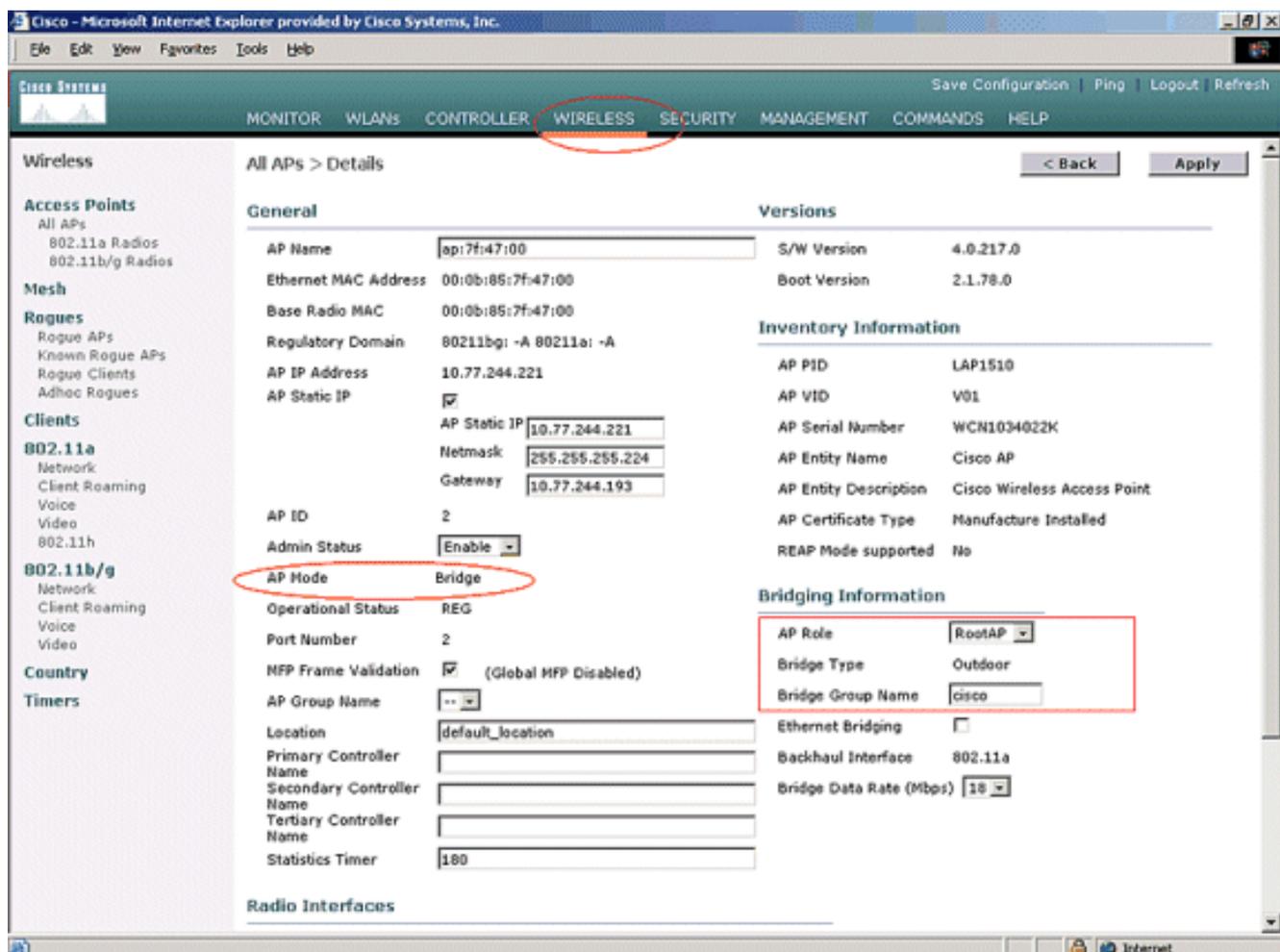
4. Configure el parámetro **Bridge Group Name**. Esta es una cadena de un máximo de 10 caracteres. Utilice nombres de grupos de puentes para agrupar lógicamente los puntos de acceso de malla para evitar que dos redes del mismo canal se comuniquen entre sí. **Para**

que los puntos de acceso de malla se comuniquen, deben tener el mismo nombre de grupo de bridges. En la etapa de fabricación se asigna un nombre de grupo de puentes de punto de acceso de malla predeterminado. No es visible para usted. El campo Bridge Group Name (Nombre de grupo de puentes) aparece en blanco en la GUI hasta que lo cambia. El AP se registra con el WLC por primera vez con este nombre de grupo de bridges predeterminado. Este ejemplo utiliza el nombre del grupo de puentes **cisco** en todos los AP involucrados en esta red de malla. Mientras configura el nombre del grupo de bridges, un cuadro de alerta muestra lo siguiente: **Establecer el nombre del grupo de puentes restringe permanentemente el AP al que puede conectarse**". Para continuar, haga clic en OK (Aceptar).



Puede configurar el nombre del grupo de puentes con la CLI del controlador con el comando **config ap bridgegroupname set cisco**. **Nota:** Si desea cambiar el nombre del grupo de puentes de los AP después de que el RAP se implemente en su sitio remoto, configure el parámetro Bridge Group Name primero en el MAP y luego en el RAP. Si el RAP se configura primero, causa graves problemas de conectividad ya que el MAP pasa al modo predeterminado porque su primario (RAP) se configura con un nombre de grupo de puente diferente. **Nota:** Para las configuraciones con varios RAP, asegúrese de que todos los RAP tengan el mismo nombre de grupo de puente para permitir la conmutación por fallas de un RAP a otro. Por el contrario, en el caso de las configuraciones en las que se requieren sectores separados, asegúrese de que cada RAP y las PAP asociadas tengan nombres de grupo de puente independientes.

5. La **velocidad de datos del puente** es la velocidad a la que se comparten los datos entre los puntos de acceso de malla. Esto se corrige para toda una red. **La velocidad de datos predeterminada es de 18 Mbps, que debe utilizar para la red de retorno.** Las velocidades de datos válidas para 802.11a son 6, 9, 12, 18, 24, 36, 48 y 54.
6. Si configura el AP como un RAP, el parámetro **Backhaul Interface** muestra un menú desplegable, pero si hace clic en el botón desplegable verá solamente la opción 802.11a. **En el MAP no hay disponible el menú desplegable correspondiente.** Haga clic en Apply (Aplicar). Esta es la captura de pantalla que explica los pasos 3 a 6.



Aquí se muestra la configuración de RootAP (RAP).

## Habilitación del Bridging Ethernet en los AP

El siguiente paso es habilitar el puente Ethernet en el RAP y todos los MAP cuyo puerto Ethernet está conectado con un dispositivo Ethernet. Una de las características clave de los AP de malla es el uso de un puerto Ethernet en el MAP para conectar los dispositivos externos y proporcionar un puente Ethernet entre todos los puertos Ethernet de los AP involucrados en la red de malla.

La malla WLAN puede transportar simultáneamente dos tipos de tráfico diferentes, tráfico de cliente WLAN y tráfico de puente MAP. El tráfico del cliente WLAN termina en el Controlador WLAN y el tráfico del bridge termina en los puertos Ethernet de los AP de malla 1500. El tráfico del puente no llega al WLC. Si un nodo de malla funciona como un MAP, el puerto Ethernet en el MAP se bloquea. Esto se ha hecho por razones de seguridad. Si alguien desea utilizar un puerto Ethernet para implementar redes de puente multipunto a punto (P2P) o de puente multipunto (P2MP) o para conectar dispositivos externos, uno debe activarlo en el controlador para cada MAP.

Complete estos pasos para configurar la conexión en puente Ethernet en el RAP y los AP de malla:

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

Wireless

Access Points  
All APs  
802.11a Radios  
802.11b/g Radios

Mesh

Rogues  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

Clients

802.11a  
Network  
Client Roaming  
Voice  
Video  
802.11h

802.11b/g  
Network  
Client Roaming  
Voice  
Video

Country

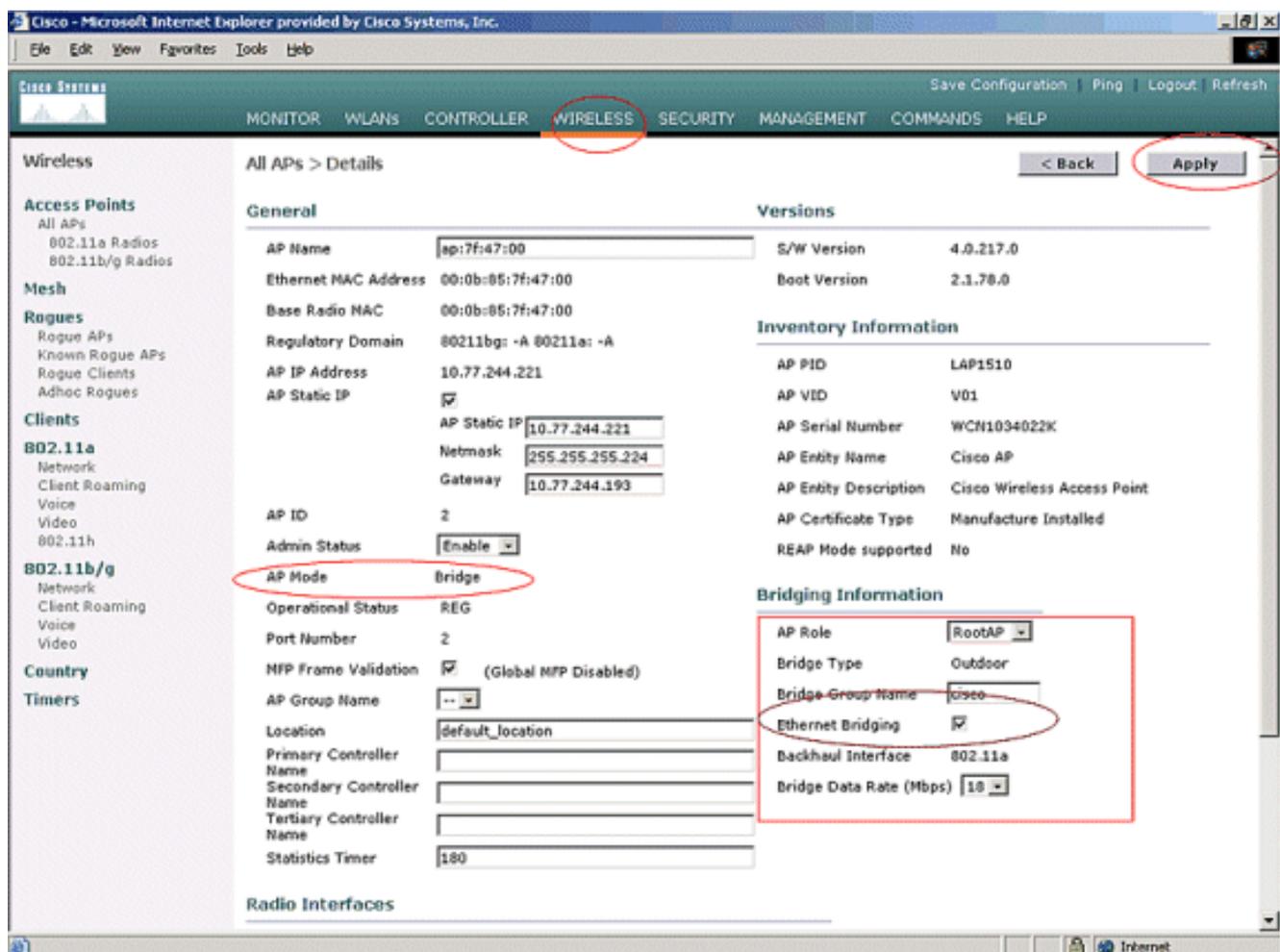
Timers

All APs

Search by Ethernet MAC

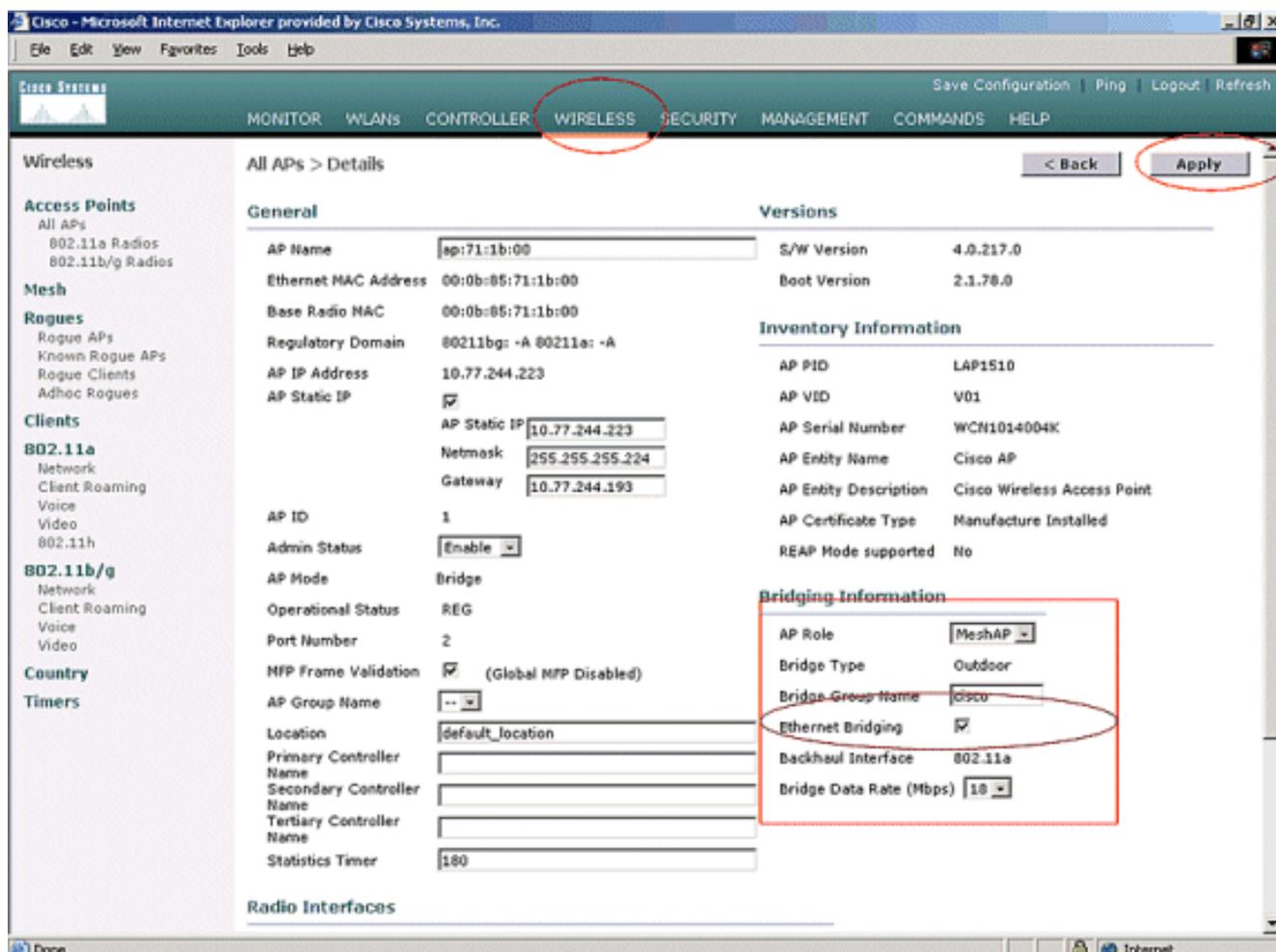
AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:5b:fb:d0	7	00:0b:85:5b:fb:d0	Enable	REG	2	<a href="#">Detailed Bridging Information</a>
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2	<a href="#">Detailed Bridging Information</a>
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2	<a href="#">Detailed Bridging Information</a>

3. En **Bridging Information**, marque la casilla junto a **Ethernet Bridging**. Esto habilita el bridging Ethernet en el AP.



Si utiliza un punto para la red de malla multipunto, habilite el puente Ethernet en los RAP y sólo en los MAP a los que se conectan los dispositivos Ethernet. No es necesario habilitar la conexión en puente Ethernet en todos los MAP en una red de interconexión. Si ha activado la conexión en puente Ethernet para utilizar la red para la conexión en puente (P2P o P2MP), debe habilitar la conexión en puente Ethernet en todos los nodos (MAP y RAP). En el escenario de conexión en puente, un RAP que actúa como puente raíz conecta varios MAP como puentes no raíz con sus LANs cableadas asociadas. Puede habilitar el puente Ethernet en los APs desde la CLI del controlador con este comando: **config ap bridging Enable**. **Nota:** Cualquier switch conectado a los puertos Ethernet de sus MAP NO debe HACER VLAN Trunking Protocol (VTP). VTP puede reconfigurar la VLAN troncal a través de su malla y posiblemente causar una pérdida en la conexión de su RAP a su WLC principal. Si se configura incorrectamente, puede eliminar la implementación de malla.

4. Habilite la conexión en puente Ethernet y todos los parámetros de conexión en puente explicados en la sección anterior en MAP, también.



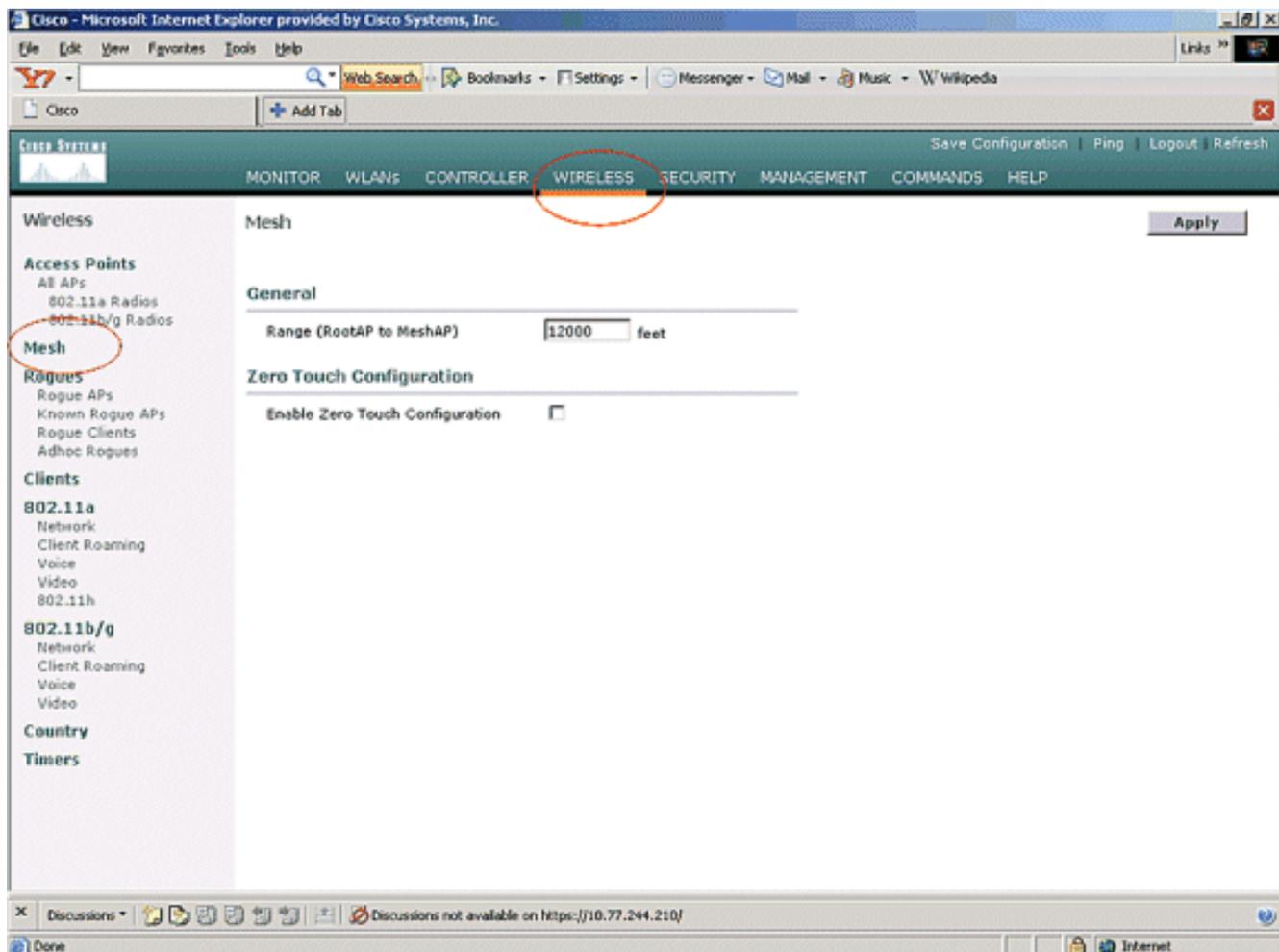
Una vez que haya terminado las configuraciones de los parámetros de puente y los parámetros de puente Ethernet en cada AP, haga clic en **Aplicar** para guardar las configuraciones. Esto hace que el AP cancele el registro del WLC, reinicie y vuelva a registrarse con el WLC.

## [Activar configuración sin intervención en el WLC](#)

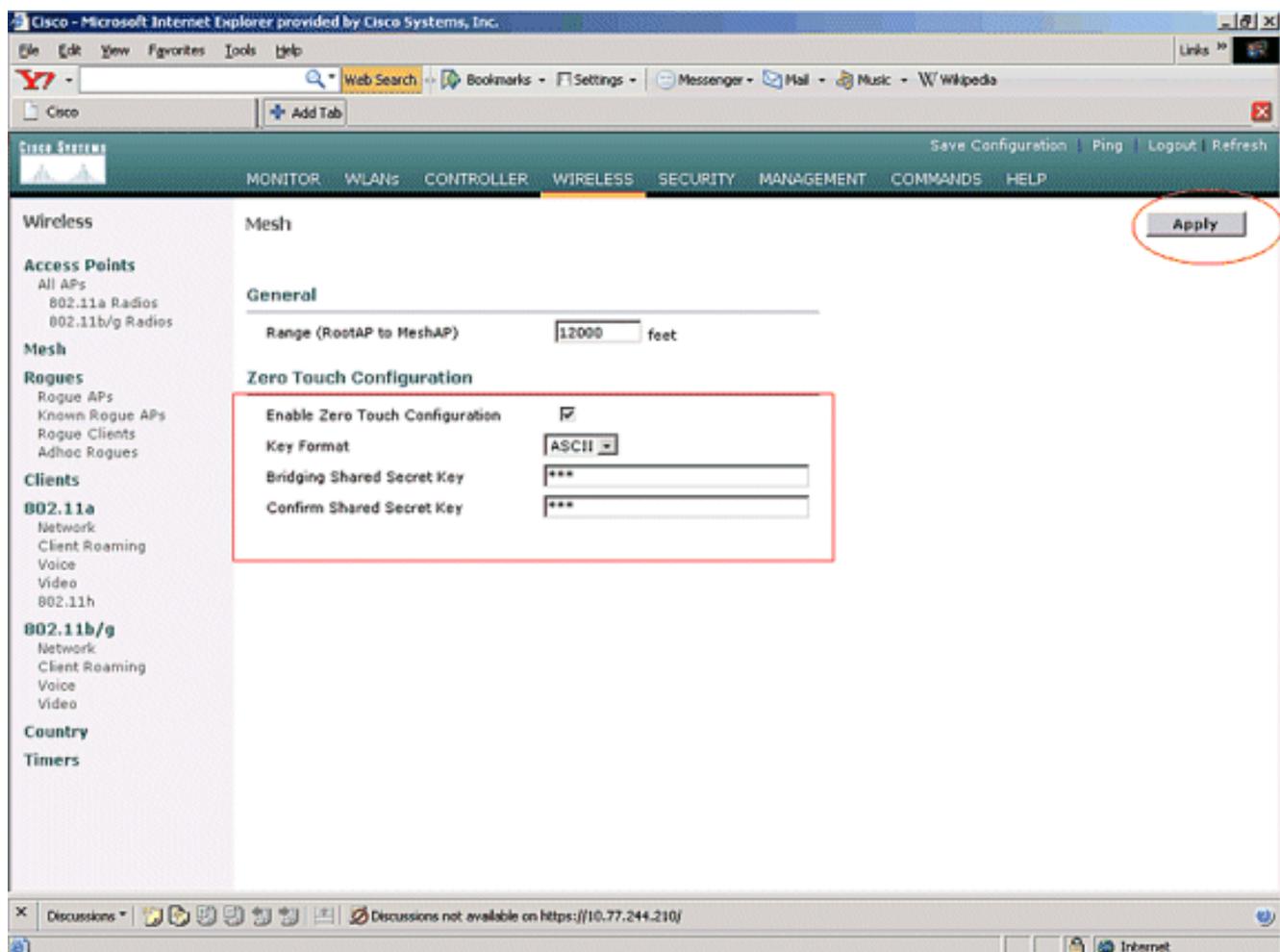
Ahora ha configurado sus AP como RAP y MAP, según sea necesario, así como sus parámetros de conexión en puente. Habilite la **configuración sin interacción en el WLC** de modo que, una vez que el MAP se quita de su conexión cableada con el WLC y se lleva a la red de producción (al otro extremo de la red de interconexión punto a punto), el MAP pueda establecer una conexión LWAPP segura con el WLC sin ninguna conexión cableada con el WLC. El valor predeterminado para la configuración sin intervención del WLC está habilitado (o activado).

Complete estos pasos para configurar la configuración sin intervención en el WLC.

1. Desde la GUI del controlador, elija **Wireless > Mesh** y haga clic en **Enable Zero Touch Configuration**.



2. Elija el formato de clave (ASCII o Hex).
3. Introduzca la clave secreta compartida en puente. Este campo solo se habilita si la opción de configuración sin intervención está activada. Esta es la clave que se proporciona a los puntos de acceso de malla (MAP) para que establezcan una conexión LWAPP segura con el controlador de LAN inalámbrica de Cisco mientras el MAP se conecta de forma inalámbrica desde el otro extremo de la red de malla . La clave debe tener al menos 32 caracteres en formato hexadecimal o ASCII. Una clave secreta compartida predeterminada se asigna en la etapa de fabricación. No es visible para usted. Este ejemplo utiliza la clave secreta compartida de puente **cisco**. Cuando cambia la clave secreta compartida, el controlador de LAN inalámbrica de Cisco envía automáticamente el cambio a todos los RAP, lo que hace que los PAP pierdan la conectividad hasta que puedan obtener la nueva clave secreta compartida del controlador de LAN inalámbrica de Cisco.
4. Vuelva a introducir la clave secreta compartida en puente en el campo **Confirmar clave secreta compartida**.
5. Haga clic en Apply (Aplicar). Esta captura de pantalla explica los pasos 3 a 5.



Si se habilita la configuración sin intervención del usuario en el controlador de LAN inalámbrica de Cisco y el MAP se mueve al otro extremo de la red de interconexión, el RAP y los MAP hacen esto para lograr una configuración segura sin intervención del usuario:

1. Si es un RAP, ya tiene una conexión LWAPP segura al controlador de LAN inalámbrica de Cisco y utiliza la interfaz de red de retorno RAP configurada (Predeterminado: 802.11a).
2. Si es un MAP, escanea las interfaces y canales de retorno para los puntos de acceso de malla vecinos. Cuando encuentra un punto de acceso de malla de vecino con el mismo **nombre de grupo de puente** (configurado como parte de los parámetros de conexión en puente) y una trayectoria de regreso al controlador de LAN inalámbrica de Cisco, hace que ese punto de acceso de malla sea su principal. Si el MAP encuentra más de un punto de acceso de malla de vecino, utiliza un algoritmo de menor costo para determinar qué padre tiene la mejor trayectoria de regreso al controlador de LAN inalámbrica de Cisco. Para configurar una conexión LWAPP segura con el controlador de LAN inalámbrica de Cisco, el MAP envía su clave secreta compartida predeterminada, que ya está disponible en la etapa de fabricación del AP, y la dirección MAC para configurar una conexión segura temporal. El controlador de LAN inalámbrica de Cisco valida la dirección MAC contra la lista de filtrado de MAC y, si se encuentra, envía la clave secreta compartida, que se configura como parte de la configuración de configuración sin intervención al MAP y se desconecta. El MAP almacena la clave secreta compartida y la utiliza para configurar una conexión LWAPP segura. Si un MAP pierde la conexión con el controlador de LAN inalámbrica de Cisco, busca vecinos válidos que utilicen el nombre del grupo de puente de punto de acceso de malla y escanea las interfaces y canales de red de retorno. Cuando encuentra un punto de acceso de malla de vecino, hace que ese punto de acceso de malla sea su principal. Si ya tiene una clave secreta compartida, utiliza esa clave e intenta configurar una conexión LWAPP segura

al controlador de LAN inalámbrica de Cisco. Si la clave secreta compartida no funciona, utiliza la clave secreta predeterminada compartida e intenta obtener una nueva clave secreta compartida.

## Verificación

- Después de todas las configuraciones, desconecte el MAP de la red cableada conectada al WLC y muévelo al otro extremo de la malla. Encienda la malla. Con todas las configuraciones adecuadas, el MAP puede localizar el RAP como su principal y registrarse en el controlador de forma inalámbrica.
- En el WLC CLI, puede utilizar los comandos **show mesh path Cisco AP** y **show mesh neigh Cisco AP** para verificar que los APs se registraron con el WLC:El comando **show mesh path AP name** se utiliza para verificar la trayectoria desde el controlador para alcanzar el AP especificado. Aquí tiene un ejemplo:

```
(Cisco Controller) >show mesh path ap:71:1b:00

00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON
(86B), snrUp 10, snrDown 9, linkSnr 8
00:0B:85:7F:47:00 is RAP
```

Esta salida dice que para alcanzar el AP **ap:71:1b:00(MAP)**, el controlador tiene el AP con la dirección MAC **00:0B:85:7F:47:00** en su trayectoria, y este AP es un **RAP**.

```
(Cisco Controller) >show mesh path ap:7f:47:00
```

```
00:0B:85:7F:47:00 is RAP
```

Esta salida dice que el AP **ap:7f:47:00** está conectado directamente al controlador pues este AP es un **RAP**.El comando **show mesh neigh AP name** muestra la información del vecino del **AP especificado**. Aquí tiene un ejemplo:

```
(Cisco Controller) >show mesh neigh ap:7f:47:00
```

```
AP MAC : 00:0B:85:71:1B:00
```

```
FLAGS : 160 CHILD
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
Numroutes 0, snr 0, snrUp 0, snrDown 10, linkSnr 0
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr 0
lastUpdate 1193504822 (Sat Oct 27 17:07:02 2007)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:0B:85:71:1B:00
```

Esta salida dice que el vecino del AP **ap:7f:47:00** es **MAP 00:0B:85:71:1B:00**, y el MAP es un **CHILD** a este AP dado que este AP es un **RAP**.

```
(Cisco Controller) >show mesh neigh ap:71:1b:00
```

```
AP MAC : 00:0B:85:7F:47:00
```

```
FLAGS : 86A NEIGH PARENT BEACON
worstDv 0, Ant 0, channel 161, biters 0, ppiters 10
Numroutes 1, snr 0, snrUp 10, snrDown 10, linkSnr 8
adjustedEase 213, unadjustedEase 256
```

```
txParent 106, rxParent 5
poorSnr 5
lastUpdate 1193504822 (Sat Oct 27 17:07:02 2007)
parentChange 1009152029 (Mon Dec 24 00:00:29 2001)
Per antenna smoothed snr values: 8 0 0 0
Vector through 00:0B:85:7F:47:00
Vector ease 1 -1, FWD: 00:0B:85:7F:47:00
```

Esta salida dice que el vecino de AP **ap:71:1b:00** es **RAP 00:0B:85:7F:47:00**, y el RAP es un **PARENT** a este AP.

- El comando **show mesh summary Ap name** muestra los detalles de la malla del AP especificado. Aquí tiene un ejemplo:

```
(Cisco Controller) >show mesh summary ap:71:1b:00
```

```
00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON (86B),
snrUp 10, snrDown 10, linkSnr 8
```

```
(Cisco Controller) >show mesh summary ap:7f:47:00
```

```
00:0B:85:71:1B:00 state CHILD (160), snrUp 0, snrDown 10, linkSnr 0
```

- Lo mismo se puede verificar desde la GUI del controlador con estos pasos: Desde la GUI del WLC, haga clic en **Wireless > All APs**. Haga clic en el link **Bridging Information** para su AP1510 para acceder a la página **Bridging Information** del AP.

The screenshot shows the Cisco WLC GUI. The 'Wireless' tab is selected and circled in red. In the left sidebar, 'Access Points' and 'All APs' are also circled. The main content area shows a table of APs with the following columns: AP Name, AP ID, Ethernet MAC, Admin Status, Operational Status, and Port. The table contains three rows of data:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:5b:fb:d0	7	00:0b:85:5b:fb:d0	Enable	REG	2
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2

The 'Bridging Information' link for the AP with MAC 00:0b:85:7f:47:00 is circled in red.

La página **Detalles de Bridging AP** enumera todos los detalles de bridging de este AP, como la información de rol AP y tipo de malla.

Cisco - Microsoft Internet Explorer provided by Cisco Systems, Inc.

MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP

Wireless All APs > ap:71:1b:00 > Bridging Details [Back](#)

**Access Points**  
All APs  
802.11a Radios  
802.11b/g Radios

**Mesh**

**Rogues**  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

**Clients**

**802.11a**  
Network  
Client Roaming  
Voice  
Video  
802.11h

**802.11b/g**  
Network  
Client Roaming  
Voice  
Video

**Country**

**Timers**

**Bridging Details**

AP Role	MeshAP
Bridge Group Name	cisco
Backhaul Interface	802.11a
Switch Physical Port	2
Routing State	Unknown
Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	5
Blacklisted Packets	0
Insufficient Memory reporting	0
Rx Neighbor Requests	0
Rx Neighbor Responses	105
Tx Neighbor Requests	109
Tx Neighbor Responses	0
Parent Changes count	1
Neighbor Timeouts count	0

**Bridging Links**

Mesh Type	AP Name/Radio Mac
Parent	ap:7f:47:00

\* Link is out of date. This can be because the AP has been replaced or

Cisco - Microsoft Internet Explorer provided by Cisco Systems, Inc.

MONITOR WLANs CONTROLLER **WIRELESS** SECURITY MANAGEMENT COMMANDS HELP

Wireless All APs > ap:7f:47:00 > Bridging Details [Back](#)

**Access Points**  
All APs  
802.11a Radios  
802.11b/g Radios

**Mesh**

**Rogues**  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

**Clients**

**802.11a**  
Network  
Client Roaming  
Voice  
Video  
802.11h

**802.11b/g**  
Network  
Client Roaming  
Voice  
Video

**Country**

**Timers**

**Bridging Details**

AP Role	RootAP
Bridge Group Name	cisco
Backhaul Interface	802.11a
Switch Physical Port	2
Routing State	Unknown
Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	0
Blacklisted Packets	0
Insufficient Memory reporting	0
Rx Neighbor Requests	1188
Rx Neighbor Responses	0
Tx Neighbor Requests	0
Tx Neighbor Responses	1188
Parent Changes count	0
Neighbor Timeouts count	0

**Bridging Links**

Mesh Type	AP Name/Radio Mac
Child	ap:71:1b:00

\* Link is out of date. This can be because the AP has been replaced or

En el WLC CLI, puede utilizar los comandos `show mesh path Cisco AP` y `show mesh neigh Cisco`

AP para verificar que los APs estén registrados con el WLC:

Para verificar si su conexión en puente Ethernet funciona correctamente, realice estos pasos:

1. Conecte una red Ethernet (LAN Ethernet B como se indica en el diagrama de red) al puerto Ethernet del MAP a través de un switch. Asegúrese de que el switch esté configurado correctamente según sea necesario.
2. Verifique la conectividad entre la LAN Ethernet B en el MAP y la red cableada (LAN Ethernet A como se indica en el diagrama de red) conectada en el RAP detrás del WLC con el **comando ping**. Si **ping** es exitoso, indica que el puente Ethernet funciona bien.

## Troubleshoot

Estos comandos de resolución de problemas pueden ser útiles:

### Comandos para resolución de problemas

- **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. Este comando muestra claramente si un AP no puede unirse al WLC debido a la discordancia del período de validez de la certificación. A continuación se muestra la salida del comando **debug pm pki enable en el controlador**:

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc()
    for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
    L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
    MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer> O=Cisco Systems,
    CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
    00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco
    Systems.
.....
.....
.....
.....
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verified using
    >ciscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
    2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
    validity interval: make sure the controller
    time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

En esta salida, observe la información resaltada. Esta información muestra claramente que el tiempo del controlador está fuera del intervalo de validez del certificado del AP, por lo que el AP no puede registrarse con el controlador. Los certificados instalados en el AP tienen un intervalo de validez predefinido. El tiempo del controlador debe configurarse de tal manera que esté dentro del intervalo de validez del certificado del AP. Refiérase al documento

[Consejos para Resolver Problemas de las Herramientas de Actualización de LWAPP](#) para obtener más información sobre posibles problemas en un LAP que se registra con el controlador. Refiérase a [Troubleshooting de una Red de Malla](#) para obtener más información sobre la resolución de problemas de una red de malla.

- Estos son comandos debug adicionales que pueden ser útiles: **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.

## [Información Relacionada](#)

- [Guía de implementación de la solución Cisco Mesh Networking](#)
- [Instalación y configuración del punto de acceso de malla](#)
- [Ejemplo de Configuración de Red de Malla del Controlador de LAN Inalámbrica](#)
- [Guía de inicio rápido: Puntos de acceso de malla exteriores ligeros Cisco Aironet serie 1500](#)
- [Guía de instalación de hardware del punto de acceso de malla exterior Cisco Aironet serie 1500](#)
- [Instrucciones de instalación del inyector de alimentación del punto de acceso Cisco Aironet serie 1500](#)
- [Preguntas y respuestas sobre Cisco Aironet 1500 Series](#)
- [Registro de AP Ligero \(LAP\) a un Controlador de LAN Inalámbrica \(WLC\)](#)
- [Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)