

Ethernet Bridging en el ejemplo de la configuración de red de la Malla inalámbrica de la Punta-punta

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Asigne la dirección IP a los AP](#)

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

[Registre el AP con el WLC](#)

[Configure el papel AP y otros parámetros del bridging](#)

[Habilite el Ethernet Bridging en los AP](#)

[Habilite la configuración del Cero-tacto en el WLC](#)

[Verificación](#)

[Troubleshooting](#)

[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 regulador del Wireless LAN (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:

- Conocimiento básico de la configuración de los Puntos de acceso ligeros (revestimientos) y del WLCs de Cisco
- Conocimiento básico en la solución de interconexión de redes de la Malla inalámbrica
- Conocimiento básico del protocolo ligero AP (LWAPP)
- 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 2000 Series que funciona con el firmware 4.0.217.0
- 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 Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Antecedentes

La solución de interconexión de redes de la malla, que es parte de la solución de red del Cisco Unified Wireless, permite a dos o más Puntos de acceso ligeros de la malla del Cisco Aironet (en lo sucesivo llamados los Puntos de acceso de la malla) para comunicar con uno a sobre uno o más saltos de la Tecnología inalámbrica para unirse a los LAN múltiples o para ampliar la cobertura de red inalámbrica del 802.11b. Los Puntos de acceso de la malla de Cisco se configuran, se monitorean, y se actúan desde y a través de cualquier controlador LAN de la tecnología inalámbrica de Cisco que se despliegue en la solución de interconexión de redes de la malla.

Las implementaciones soportadas de la solución de interconexión de redes de la malla están de uno de tres tipos generales:

- Despliegue de punto a punto
- Despliegue de la punta a de múltiples puntos
- Despliegue de la malla

Este documento se centra en cómo configurar el despliegue de punto a punto y el Ethernet Bridging de la malla en lo mismo. En el despliegue de punto a punto de la malla, los Puntos de acceso de la malla proporcionan el acceso de red inalámbrica y el regreso a los clientes de red inalámbrica, y pueden soportar simultáneamente el bridging entre un LAN y una terminación a un dispositivo de los Ethernet remota u otro LAN Ethernet.

Refiera a las [implementaciones de la solución de interconexión de redes de la malla](#) para información detallada sobre cada uno de estos tipos del despliegue.

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.

Usted puede actuar el Cisco Aironet 1510 Puntos de acceso ligeros remotos del borde y los Puntos de acceso al aire libre ligeros del Cisco Aironet de la serie 1500 en uno de estos papeles:

- Punto de acceso del tejado (RAP)
- Punto de acceso de la malla (MAPA), también llamado Punto de acceso del Poste-top (PAP)

Los rap tienen una conexión alámbrica a un controlador LAN de la tecnología inalámbrica de Cisco. Utilizan la interfaz inalámbrica del regreso para comunicar con los mapas próximos. Los rap son el nodo primario a cualquier bridging o red de interconexión y conectan un Bridge o la red de interconexión a la red alámbrica, tan allí puede ser solamente un RAP para cualquier segmento interligado o de la red de interconexión.

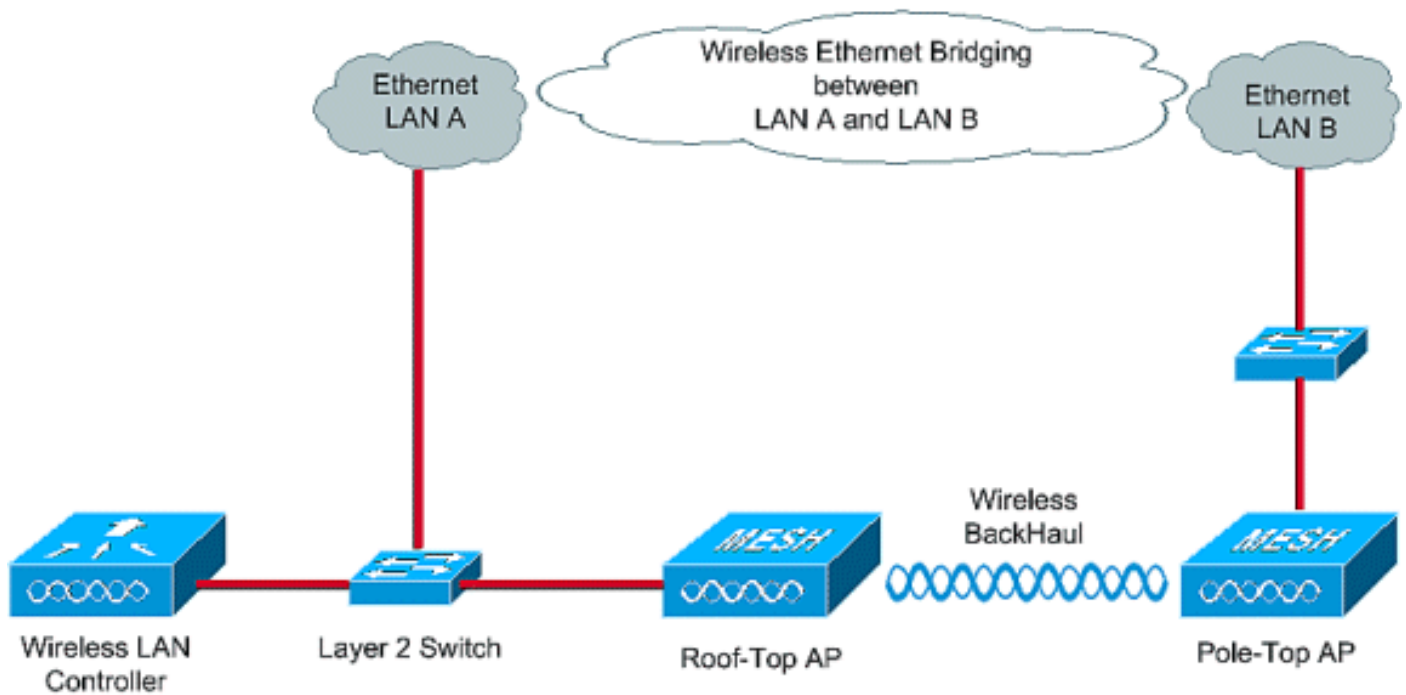
Los mapas no tienen ninguna conexión alámbrica a un controlador LAN de la tecnología inalámbrica de Cisco. Pueden ser los clientes totalmente inalámbricos y soporte que comunican con otros mapas o rap, o pueden ser utilizados para conectar con los dispositivos periféricos o una red alámbrica. El acceso de Ethernet se inhabilita por abandono por razones de seguridad, pero usted puede habilitarlo para los PAP.

[Configurar](#)

Este ejemplo de configuración explica cómo configurar el Ethernet Bridging entre dos 1510 Series de la malla al aire libre ligera AP con un AP que actúe como el RAP y el otro AP que actúa como MAPA.

En esta configuración, el AP con la dirección MAC 00:0B:85:7F:47:00 se configura como RAP, y el AP con la dirección MAC 00:0B:85:71:1B:00 se configura como MAPA. Un Ethernet local LAN A está conectado en el extremo del RAP, y el LAN Ethernet B está conectado en el MAPA.

[Diagrama de la red](#)



Para configurar la malla AP del hacia fuera-de-cuadro 1510 para el Ethernet Bridging, realice estos pasos:

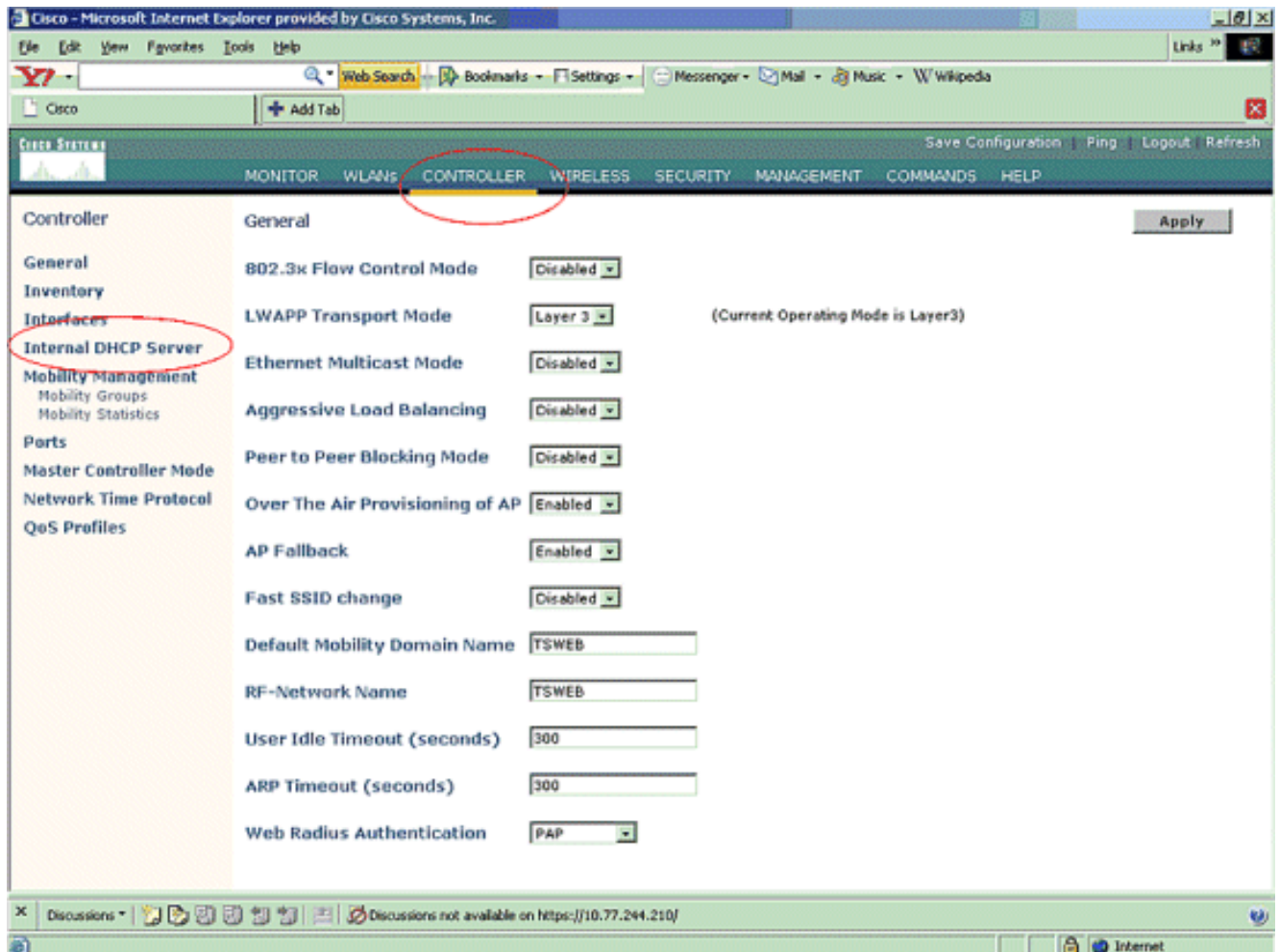
1. [Asigne la dirección IP a los AP](#)
2. [Agregue la dirección MAC de los AP a la lista de filtración MAC del WLC](#)
3. [Registre los AP con el WLC](#)
4. [Configure el papel AP y otros parámetros del bridging](#)
5. [Habilite el Ethernet Bridging en los AP](#)
6. [Habilite la configuración del Cero-tacto en el WLC](#)

[Asigne la dirección IP a los AP](#)

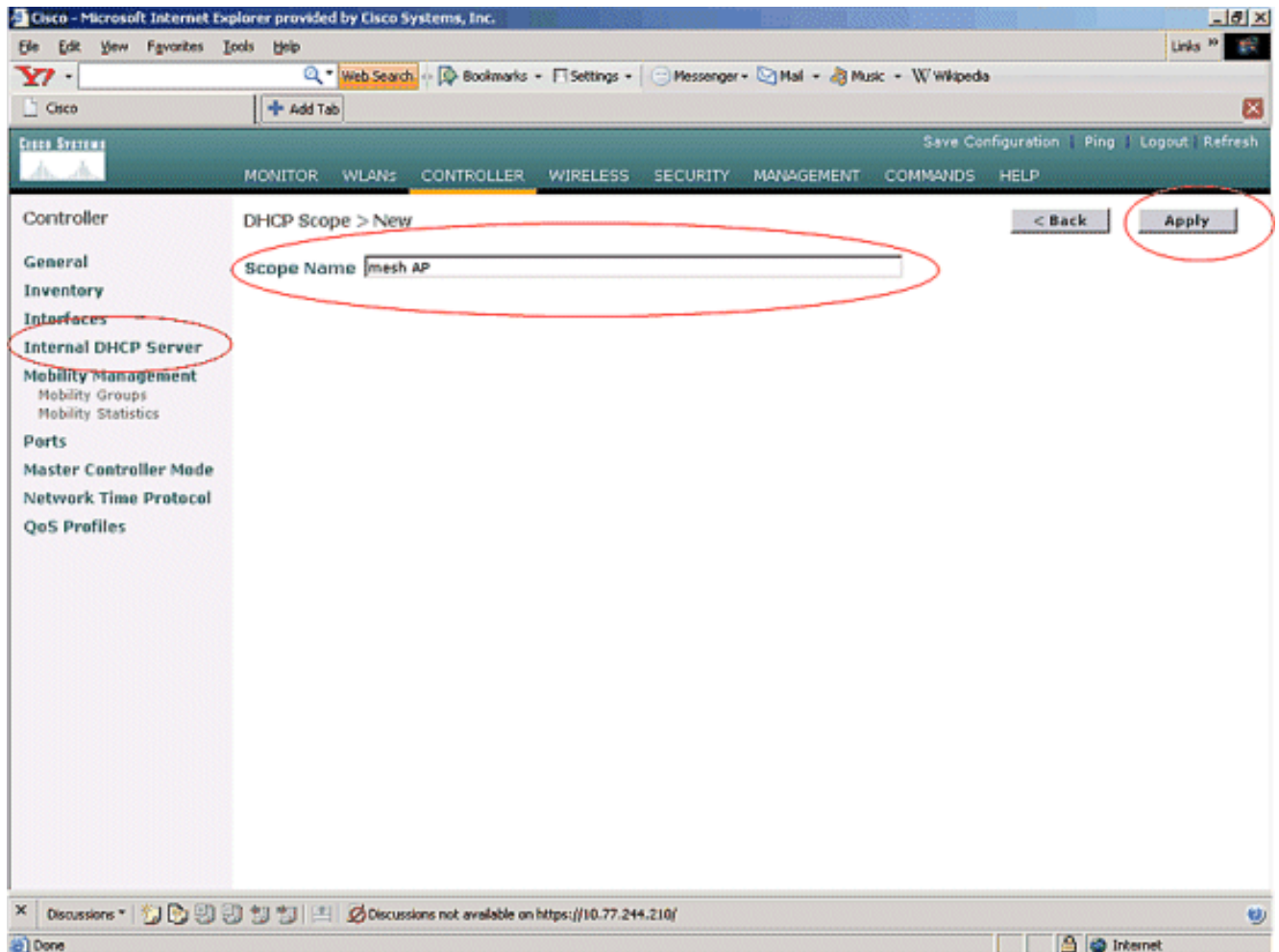
Cuando cualquier AP arranca, primero busca una dirección IP. Esta dirección IP se puede asignar dinámicamente con un DHCP interno externo como el servidor DHCP del [®]de Microsoft Windows. La última versión del WLC (4.0 y posterior) puede asignar la dirección IP a los AP con el servidor DHCP interno en el regulador sí mismo. Este ejemplo utiliza al servidor DHCP interno en el regulador 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.

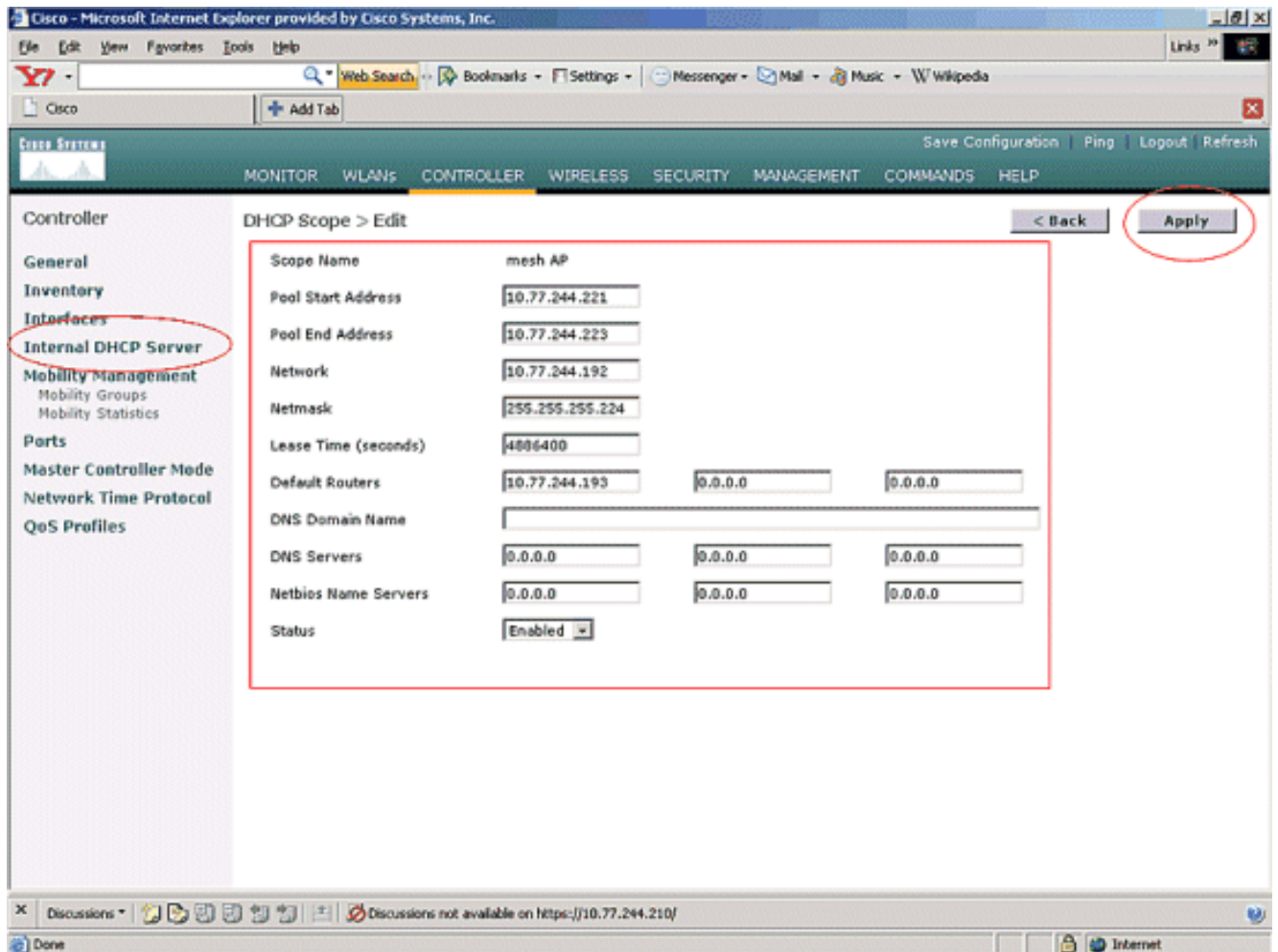
1. Haga clic el **REGULADOR** del menú principal del WLC GUI. Elija al **servidor DHCP interno de la** esquina del lado izquierdo de la página principal del regulador.



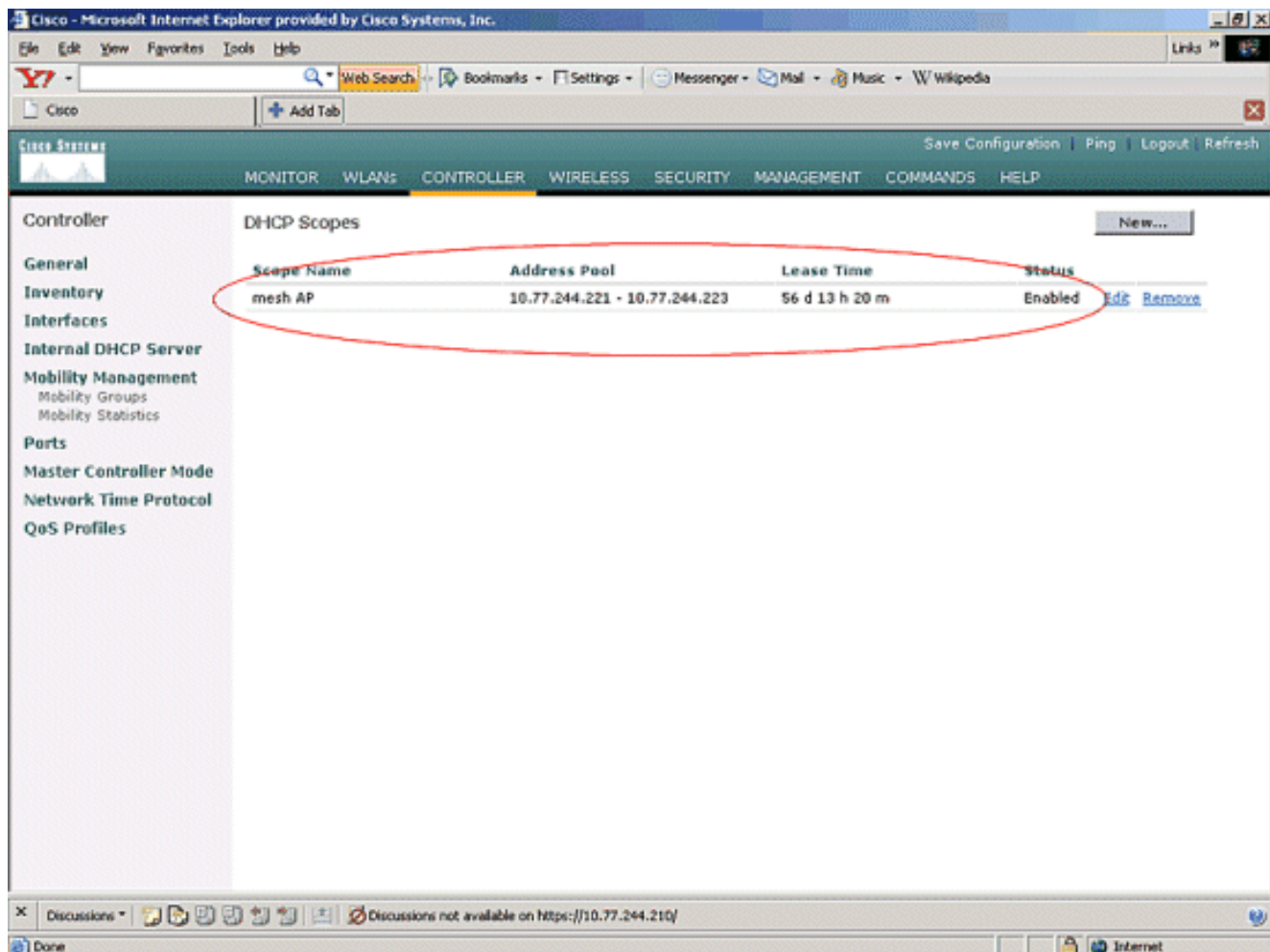
2. En la página **interna del servidor DHCP**, clickNew para crear un nuevo alcance de DHCP. Este ejemplo asigna el nombre del alcance como **mallA AP**. Haga clic en Apply (Aplicar). Esto le lleva al alcance de DHCP de la mallA AP edita la página.



3. En el **alcance de DHCP > edite la página**, configure la Dirección de inicio del pool, reúna el direccionamiento del final, red y netmask, los routers predeterminados, y el resto de parámetros necesarios según lo dado en este ejemplo. Elija el estatus del servidor DHCP según lo **habilitado de la casilla desplegable del estatus**. Haga clic en Apply (Aplicar).



4. Ahora, configuran al servidor DHCP interno para asignar los IP Addresses a la malla AP.



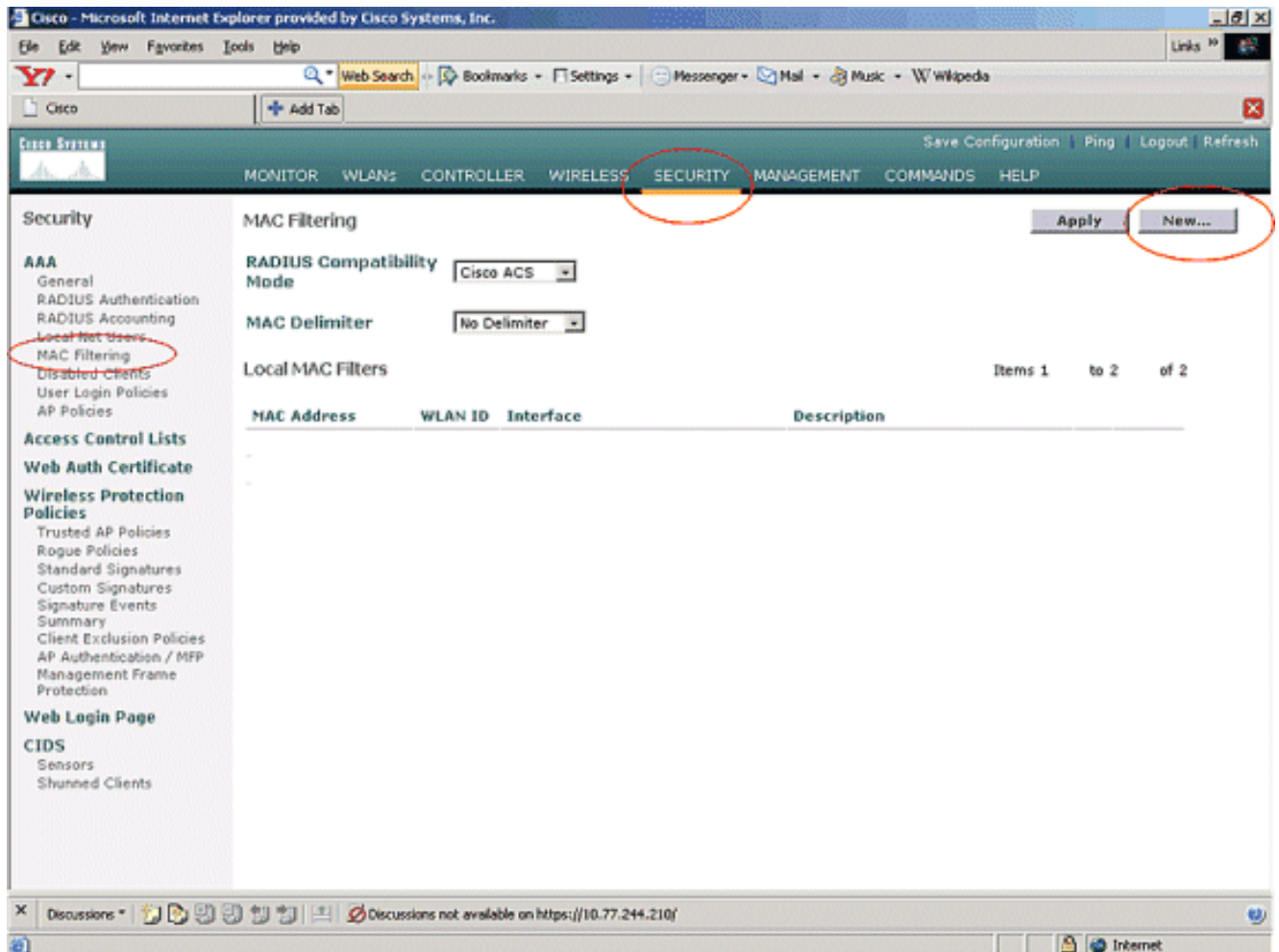
5. Una vez que los AP se registran con el regulador, asigne el IP Address estático a los AP a través del regulador GUI. Si usted asigna los IP Address estáticos para enredar los AP, proporciona una convergencia más rápida de los AP la próxima vez que se registran con el regulador.

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

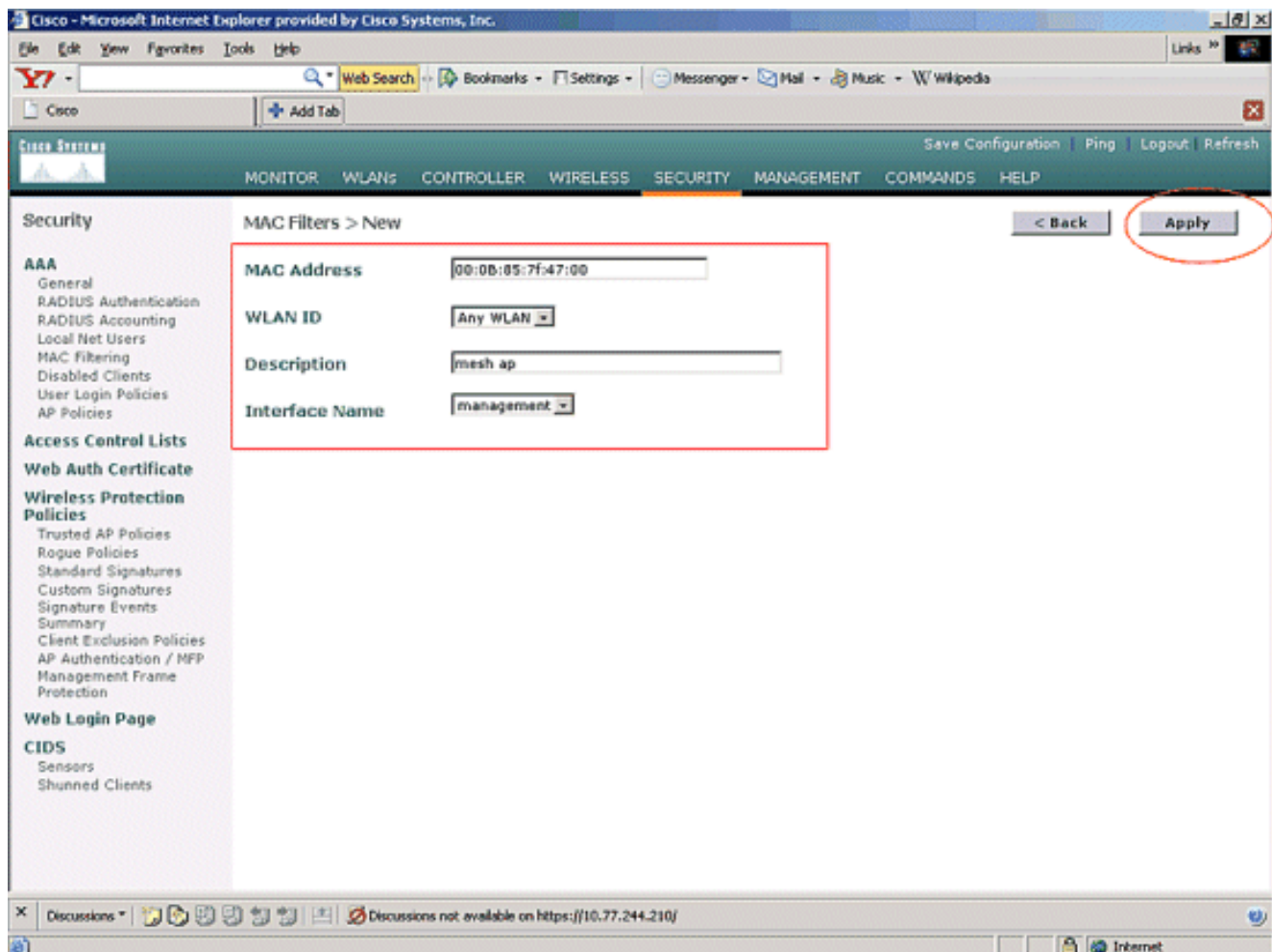
Para registrar la malla AP con el WLC, usted necesita primero agregar la dirección MAC de los AP a la lista de filtración MAC del WLC. Usted puede encontrar la dirección MAC etiquetada en el lado superior de la malla AP.

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

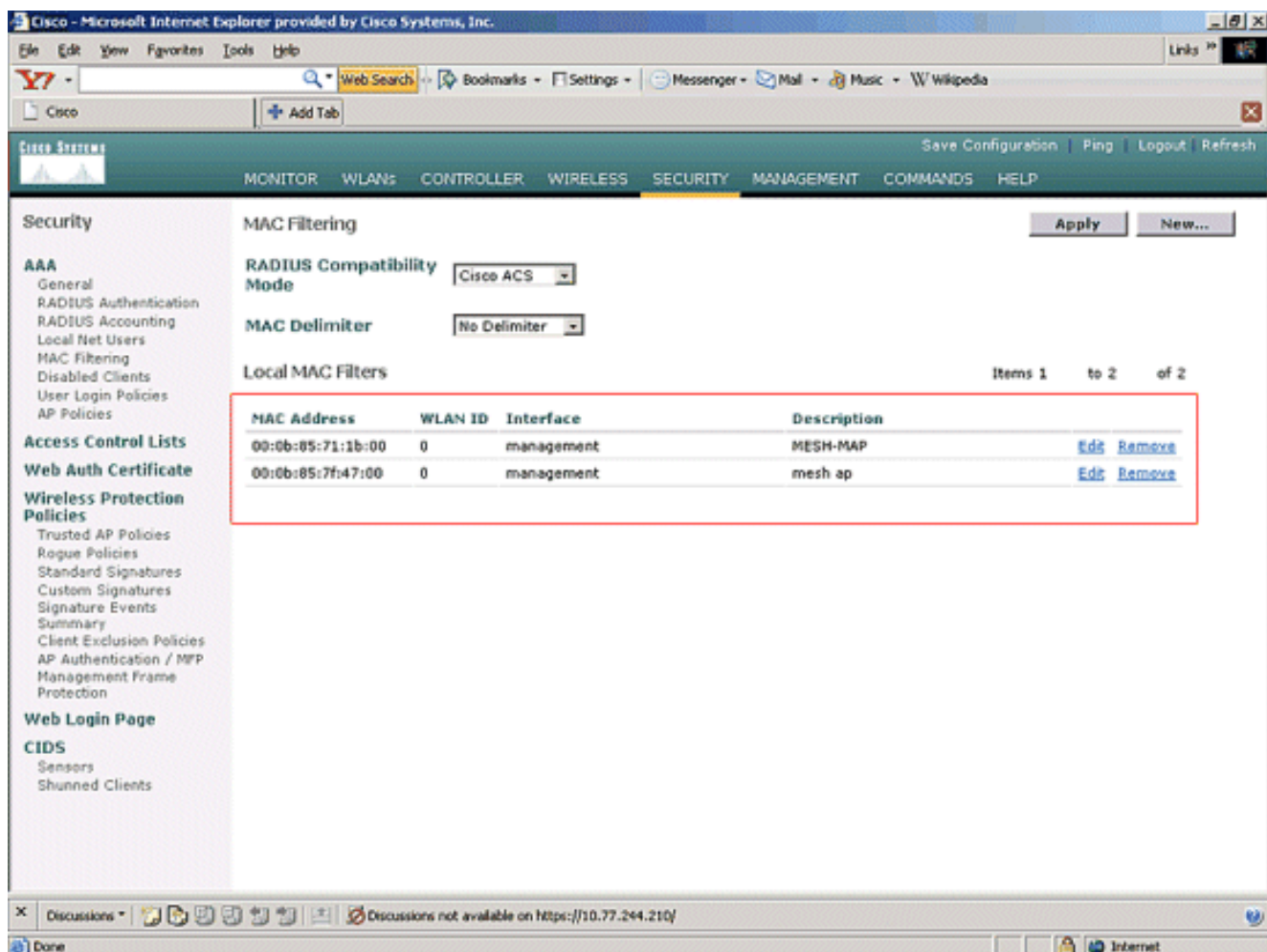
1. Haga clic la **SEGURIDAD** del menú principal del regulador. En la página Seguridad, elija el **MAC que filtra** bajo sección **AAA**. Esto le lleva a la página de filtración MAC. Haga clic **nuevo** para crear los filtros MAC para la malla AP.



2. Ingrese el **MAC address** del AP y de su **descripción** en los cuadros de texto apropiados según lo dado en este ejemplo. También, elija una **red inalámbrica (WLAN)** y una **interfaz dinámica** del ID DE WLAN e interconecte los menús desplegables del nombre, respectivamente. Haga clic en Apply (Aplicar).



3. Relance los pasos 1 y 2 para todos los AP implicados en esta red de interconexión, así que la filtración MAC se configura para permitir que la malla AP se registre con el regulador.



[Registre el AP con el WLC](#)

El siguiente paso es registrar la malla AP con el WLC. Hay varios métodos que un AP puede registrar con el WLC. Refiera al [registro ligero AP con el WLC](#) para los detalles en cómo un AP se registra con el WLC.

La primera vez que usted utiliza la malla AP, registre todos los AP conectados directamente con el WLC.

Si usted no ha podido agregar el AP a la lista de filtración MAC del regulador, los AP no pueden unirse al WLC a la hora del registro con el WLC. La razón es averiada falla de autorización de la salida del comando **debug lwapp events enable** en el regulador. Aquí está la salida de ejemplo que indica la 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 esta salida, usted puede ver que la petición del unido del AP no es validada por el regulador debido a la falla de autorización AP.

Nota: En las implementaciones de red de interconexión normales que utilizan sobre todo la malla AP de las 1500 Series, se recomienda para inhabilitar la **permit AP que interligan viejos de autenticar la configuración** en el regulador. Esto se puede hacer del modo CLI del regulador con el comando

Nota: (Regulador de Cisco) > **neutralización permitir-viejo-Bridge-aps de la red de los config**

Nota: El comando se ha quitado en 4.1 y posterior, así que esto no es un problema con el WLC 4.1 y posterior.

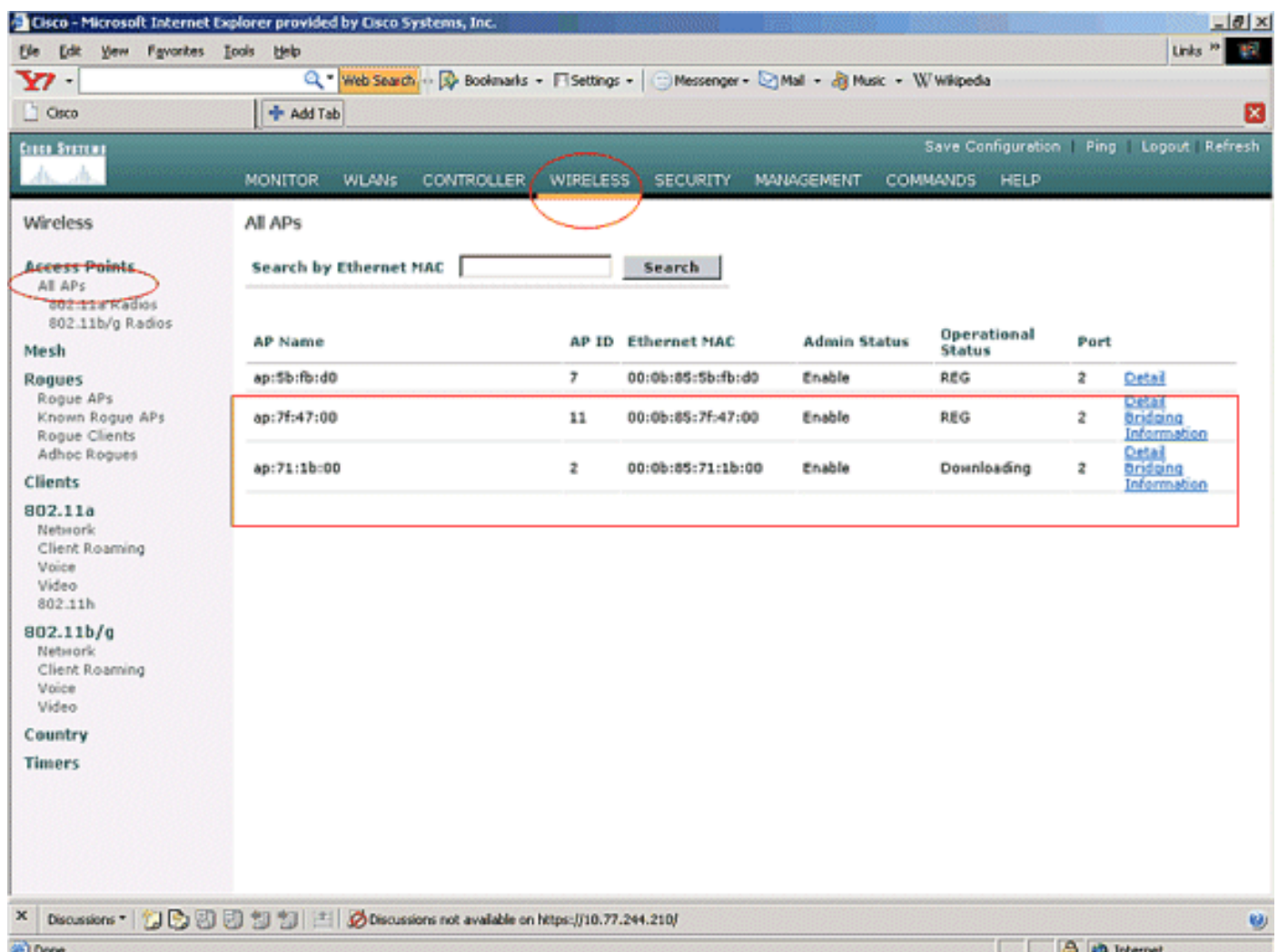
En el CLI, usted puede utilizar el **comando show ap summary** para verificar que los AP están registrados con el WLC:

(Resumen ap del >show del regulador de Cisco)

```

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

Usted puede verificarlo del GUI bajo la Tecnología inalámbrica **toda la página AP**.

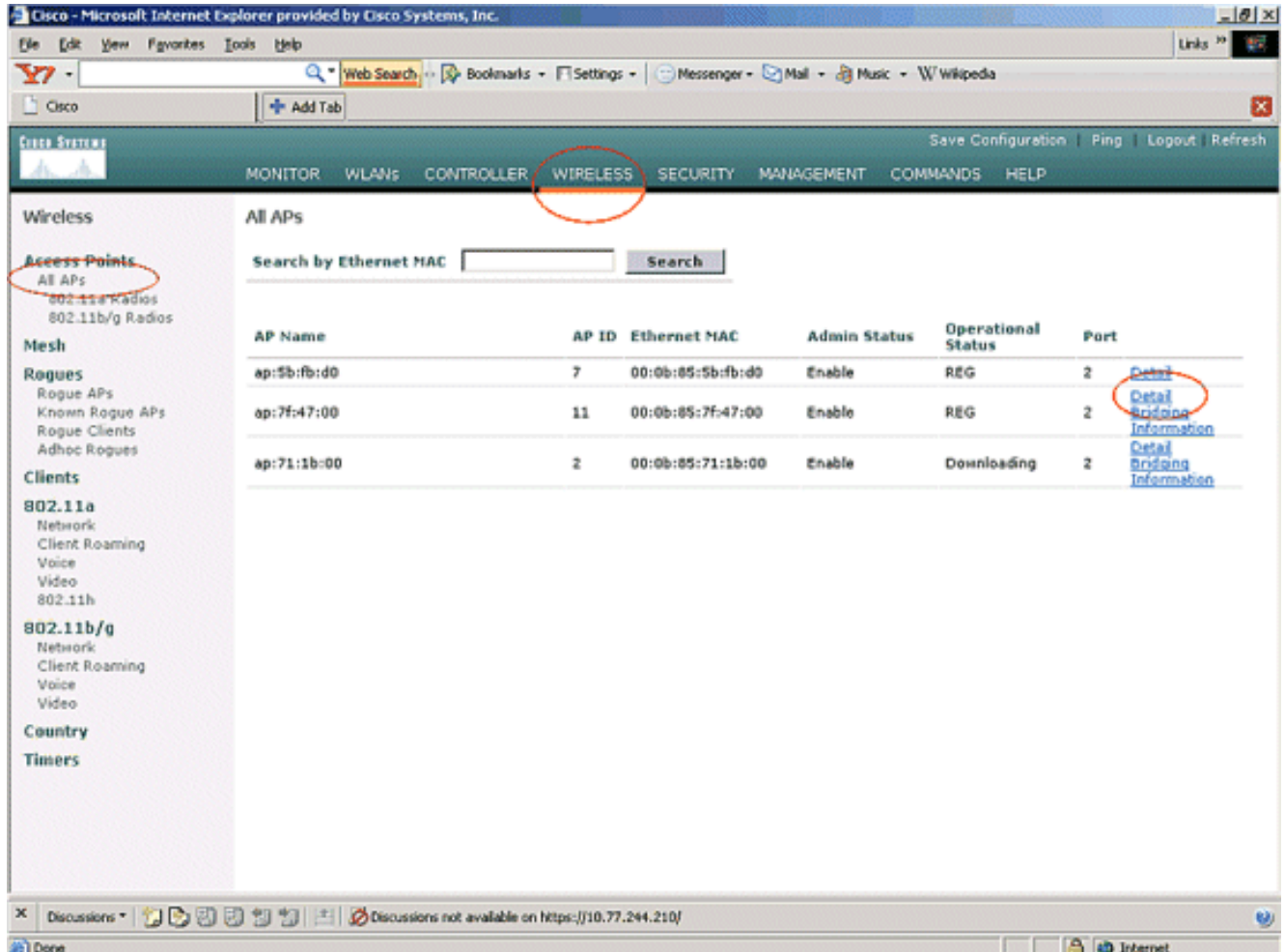


[Configure el papel AP y otros parámetros del bridging](#)

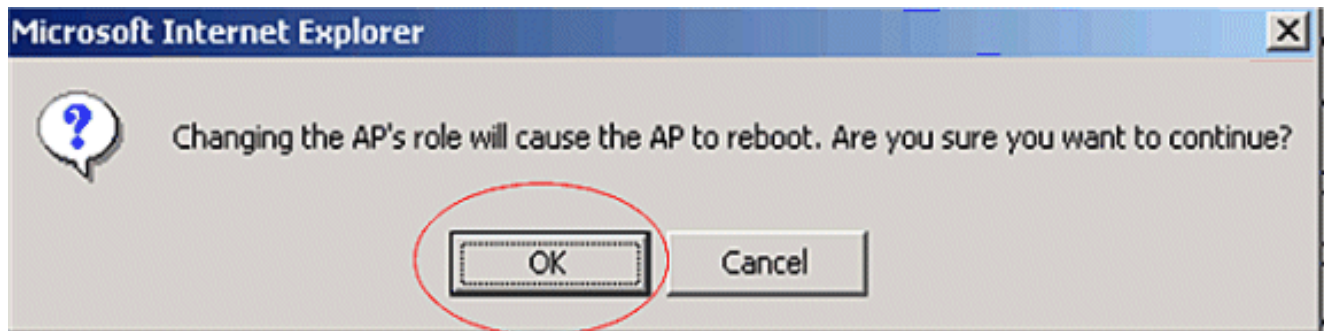
Una vez que los AP se registran al WLC, usted necesita configurar el papel AP y otros parámetros del bridging. Usted necesita configurar los AP como los rap y mapas, como sea necesario.

Complete estos pasos para configurar esos parámetros AP:

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 la página de los **detalles**.

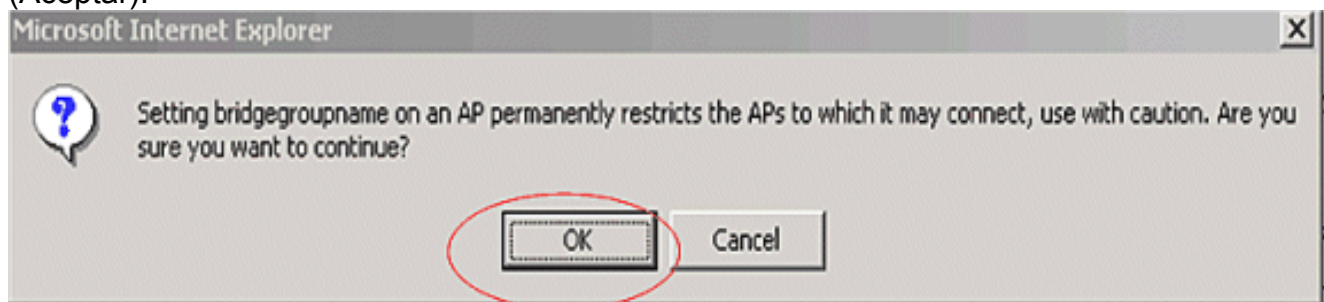


3. En la página de los **detalles** de sus 1510 AP, **modo AP** bajo fijan al **general** automáticamente **para interligar** para los AP que tienen funciones del Bridge, tales como el AP1510. Esta página también muestra esta información conforme a la información del bridging. Conforme a la **información del bridging**, elija una de estas opciones para especificar el papel de este AP en la red de interconexión: MeshAP (MAPA) RootAP (RAP) Los AP configurados como RootAPs deben tener conexión alámbrica al WLC a la hora de la implementación de la configuración en su entorno de producción. El AP configurado como malla AP está conectado sin hilos con el WLC a través de su padre AP (RAP). Los 1510 AP, por abandono, asumen el papel de los mapas cuando suben y se registran con el WLC. Mientras que usted configura el papel del Bridge, un cuadro alerta visualiza este mensaje: **El AP reiniciará**. Para continuar, haga clic en OK (Aceptar).



Usted puede configurar el papel AP con el regulador CLI con el *papel del papel ap del* comando config.

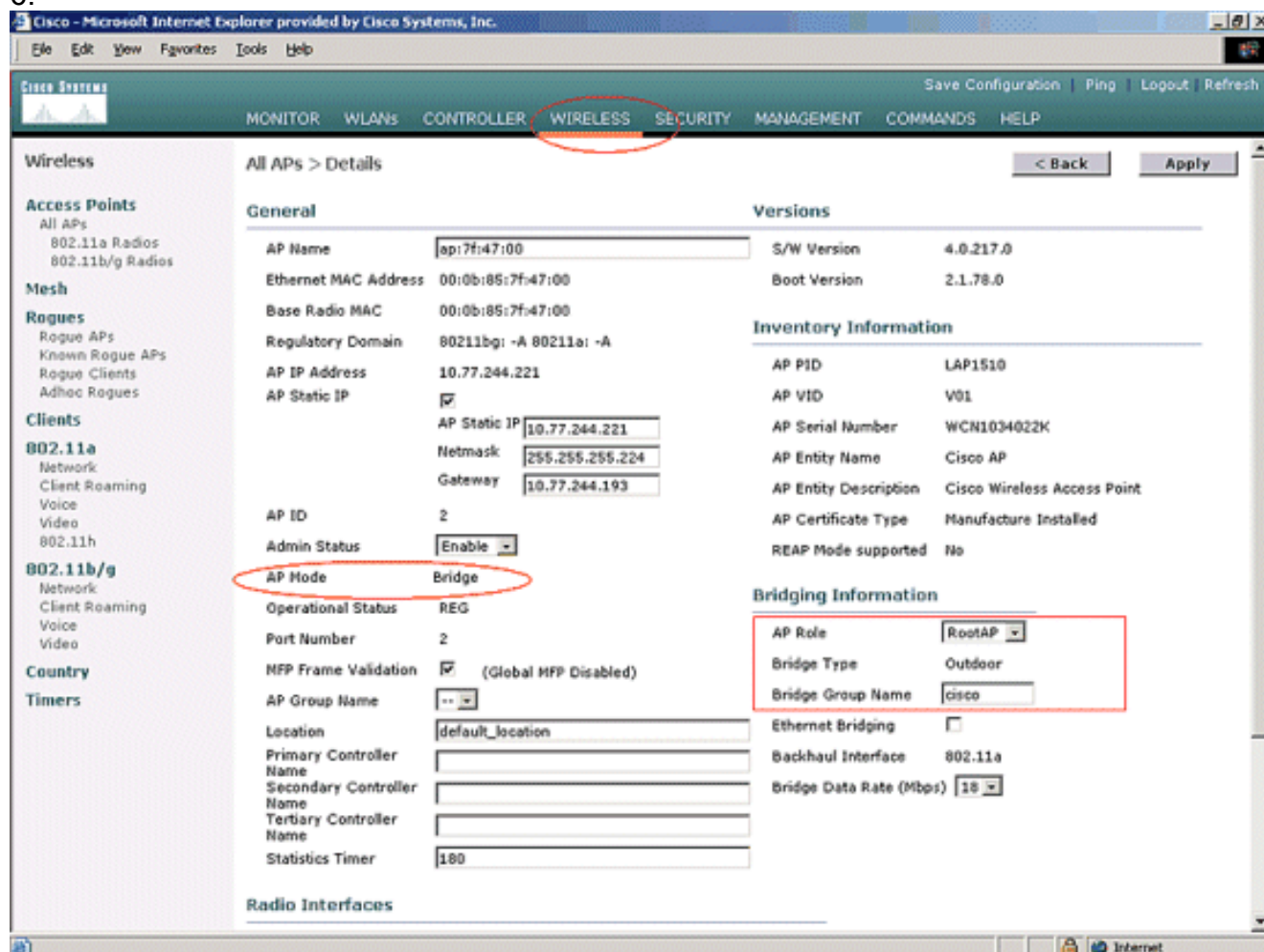
4. Configure el parámetro del **nombre de Grupo de Bridge**. Esto es una cadena de un máximo de 10 caracteres. Utilice los nombres de Grupo de Bridge para agrupar lógicamente los Puntos de acceso de la malla para evitar dos redes en el mismo canal de la comunicación con uno a. **Para que los Puntos de acceso de la malla comuniquen, deben tener el mismo nombre de Grupo de Bridge**. Un nombre de Grupo de Bridge predeterminado del Punto de acceso de la malla se asigna en la etapa de la fabricación. No es visible a usted. El campo de nombre del Grupo de Bridge aparece en blanco en el GUI hasta que usted lo cambie. El AP se registra con el WLC por primera vez con este nombre del grupo del Bridge predeterminado. Este ejemplo utiliza el nombre de Grupo de Bridge **Cisco** en todos los AP implicados en esta red de interconexión. Mientras que usted configura el nombre de Grupo de Bridge, un cuadro alerta visualiza esto: **La determinación del nombre de Grupo de Bridge restringe permanentemente el AP con el cual puede conectar.** Para continuar, haga clic en OK (Aceptar).



Usted puede configurar el nombre de Grupo de Bridge con el regulador CLI con el **bridgegroupname Cisco determinado ap del** comando config. **Nota:** Si usted quiere cambiar el nombre de Grupo de Bridge de los AP después de que el RAP se despliegue en su sitio remoto, configure el parámetro del nombre de Grupo de Bridge primero en el MAPA y entonces en el RAP. Si el RAP se configura primero, causa los problemas de conectividad serios puesto que el MAPA va al modo predeterminado porque su padre (RAP) se configura con un diverso nombre de Grupo de Bridge. **Nota:** Para las configuraciones con los rap múltiples, asegúrese que todos los rap tienen el mismo nombre de Grupo de Bridge para permitir la Conmutación por falla a partir de un RAP a otro. Inversamente, para las configuraciones donde se requieren los sectores separados, asegúrese que cada RAP y PAP asociados tienen nombres de grupo de Bridges diferente.

5. **La velocidad de datos del Bridge** es la tarifa en la cual los datos se comparten entre los Puntos de acceso de la malla. Esto se repara para una red completa. **La velocidad de datos predeterminada es el 18 Mbps, que usted debe utilizar para el regreso.** Las tarifas de datos válidos para el 802.11a son 6,9, 12, 18, 24, 36, 48, y 54.
6. Si usted configura el AP como RAP, el parámetro de la **interfaz del regreso** muestra un menú desplegable, pero si usted hace clic el botón del descenso-abajo usted considera solamente

la opción del 802.11a. En el MAPA no hay tal menú desplegable disponible. Haga clic en Apply (Aplicar). Aquí está el tiro de pantalla que explica los pasos 3 a 6.



La configuración de RootAP (RAP) se muestra aquí.

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

El siguiente paso es habilitar el Ethernet Bridging en el RAP y todos los mapas cuyo acceso de Ethernet está conectado con un dispositivo Ethernet. Una de las características fundamentales de la malla AP es el uso de un acceso de Ethernet en el MAPA para conectar los dispositivos externos y para proporcionar el Ethernet Bridging entre todos los accesos de Ethernet de los AP implicados en la red de interconexión.

La malla de la red inalámbrica (WLAN) puede simultáneamente llevar tráfico dos diversos tipos de tráfico, tráfico del cliente WLAN y Bridges del MAPA. El tráfico del cliente WLAN termina en el controlador de WLAN, y el tráfico del Bridge termina en los accesos de Ethernet 1500 de la malla AP. El tráfico del Bridge no alcanza el WLC. Si un nodo de la malla está trabajando como MAPA, después el acceso de Ethernet en el MAPA consigue bloqueado. Esto se ha hecho por los motivos de seguridad. Si alguien quiere utilizar el acceso de Ethernet para desplegar de punto a punto y la punta (P2P) a las redes de múltiples puntos del bridging (P2MP) o conectar los dispositivos externos, uno debe habilitarla en el regulador para cada MAPA.

Complete estos pasos para configurar el Ethernet Bridging en el RAP y la malla AP:

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 la página de los **detalles AP**.

The screenshot shows the Cisco WLC web interface. The 'WIRELESS' menu item is circled in red. In the left sidebar, 'Access Points' and 'All APs' are also circled in red. The main table lists three APs with their details, and the 'Detail Bridging Information' link for the first AP is circled in red.

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	Detail Bridging Information
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2	Detail Bridging Information
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2	Detail Bridging Information

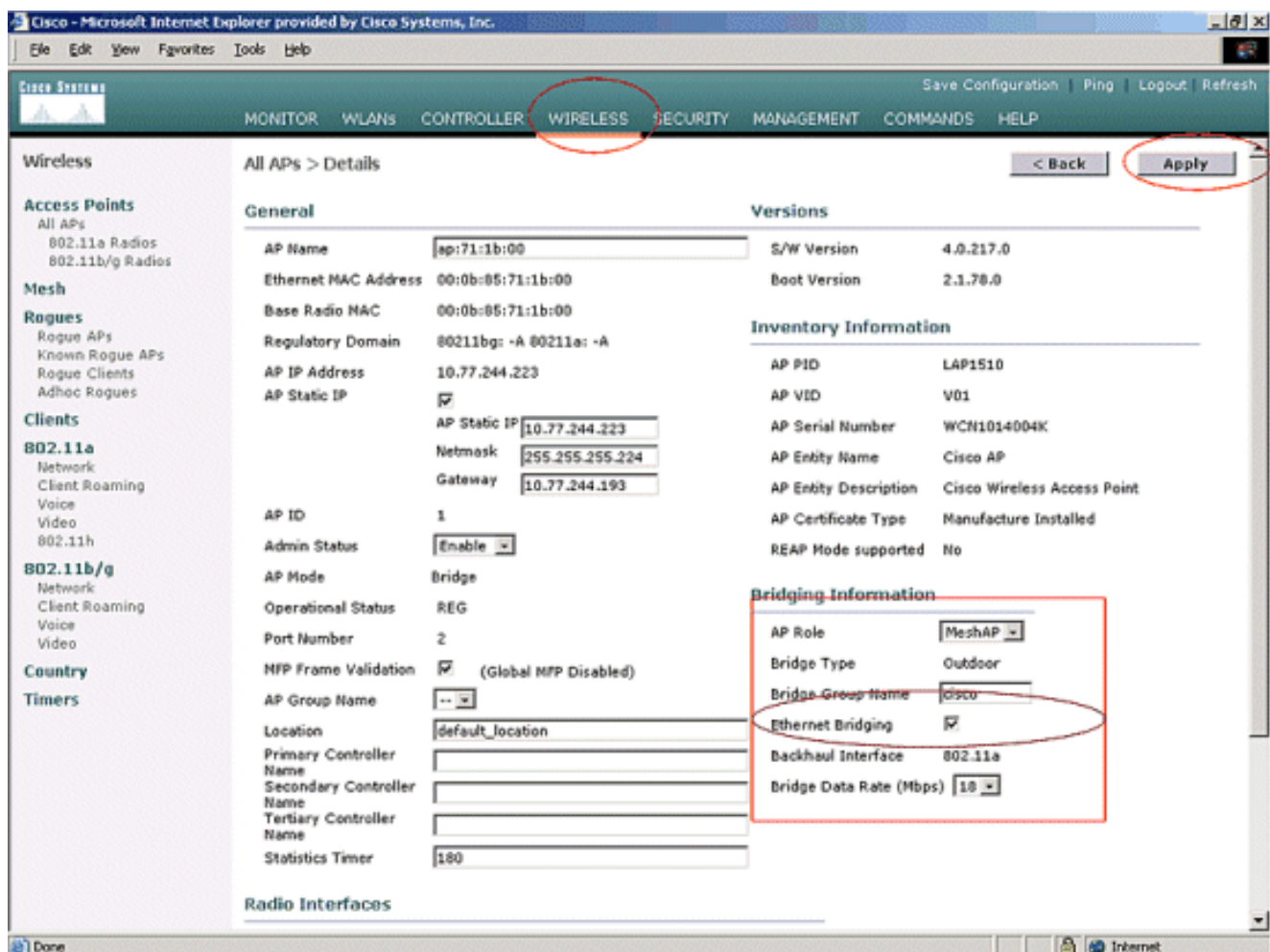
3. Conforme a la **información del bridging**, marque el cuadro al lado del **Ethernet Bridging**. Esto habilita el Ethernet Bridging en el AP.

The screenshot shows the Cisco WLC configuration interface. The 'Wireless' menu is selected. The 'All APs > Details' page is displayed. The 'AP Mode' is set to 'Bridge'. The 'Bridging Information' section is highlighted with a red box, showing the following configuration:

Field	Value
AP Role	RootAP
Bridge Type	Outdoor
Bridge Group Name	Cisco
Ethernet Bridging	<input checked="" type="checkbox"/>
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	18

Si usted utiliza una punta a la red de interconexión de múltiples puntos, habilite el Ethernet Bridging en los rap y solamente en los mapas con los cuales los dispositivos Ethernet están conectados. No es necesario habilitar el Ethernet Bridging en todos los mapas en una red de interconexión. Si usted ha habilitado el Ethernet Bridging para utilizar la red para interligar (P2P o P2MP), usted debe habilitar el Ethernet Bridging en todos los Nodos (los mapas y los rap). En el escenario del bridging, un RAP que actúa como Root Bridge conecta los mapas múltiples como Non-Root Bridge con sus LAN cableados asociados. Usted puede habilitar el Ethernet Bridging en los AP del regulador CLI con este comando: **permiso del bridging ap de los config.** Nota: Ninguna switches conectados a los accesos de Ethernet de sus mapas no deben HACER el VLAN Trunking Protocol (VTP). El VTP puede configurar de nuevo el VLAN N trunked a través de su malla y causar posiblemente una pérdida en la conexión para su RAP a su WLC primario. Si está configurado incorrectamente, puede tomar abajo su despliegue de la malla.

4. Habilite el Ethernet Bridging y todos los parámetros del bridging explicados en la sección anterior en el MAPA, también.



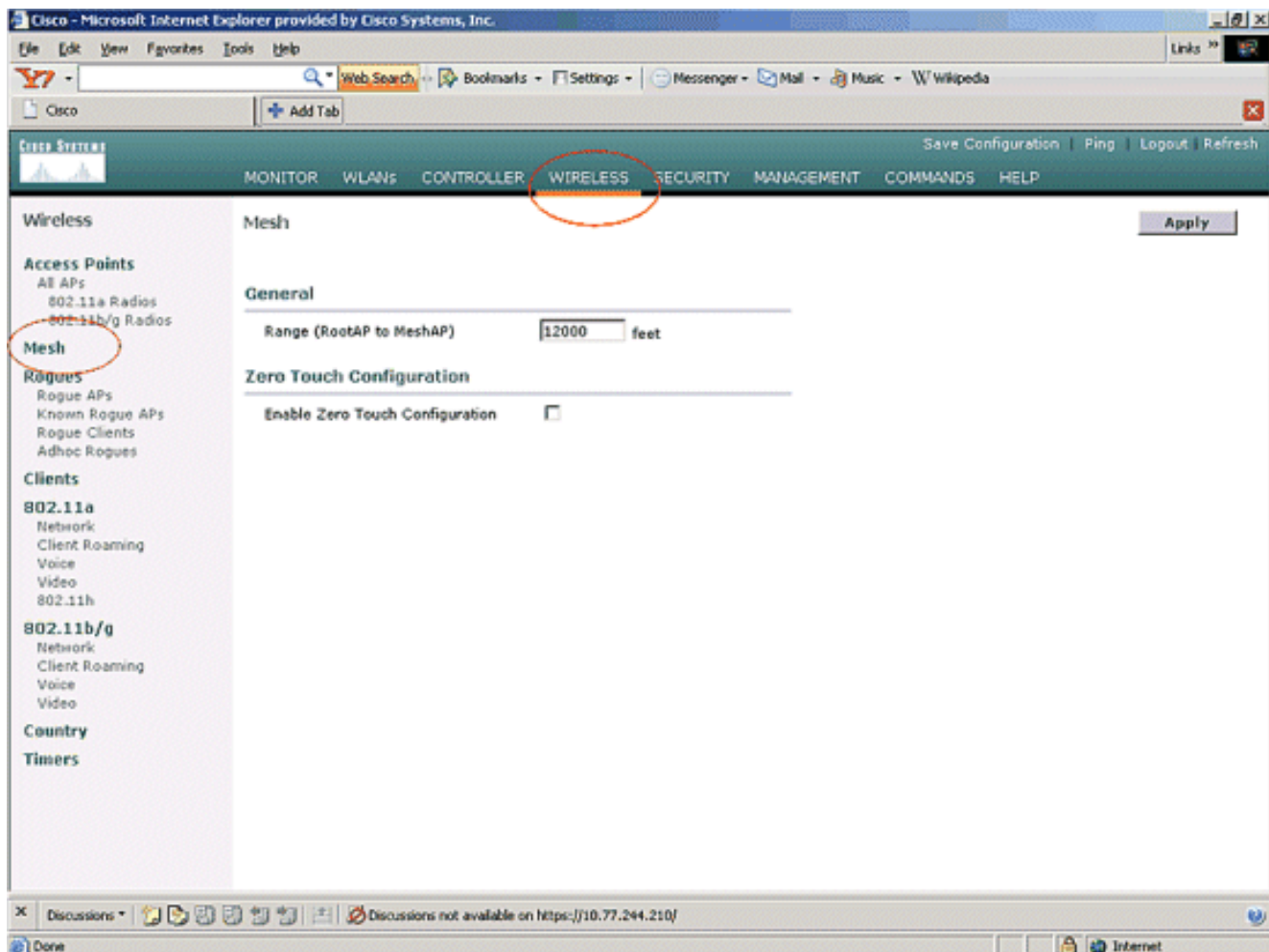
Una vez que usted acaba las configuraciones de los parámetros del Bridge y de los parámetros bridging de los Ethernetes en cada AP, el tecléo **se aplica** para salvar las configuraciones. Esto hace el AP para desregistrar del WLC, para reiniciar, y para reregistrar con el WLC.

[Configuración del Cero-tacto del permiso en el WLC](#)

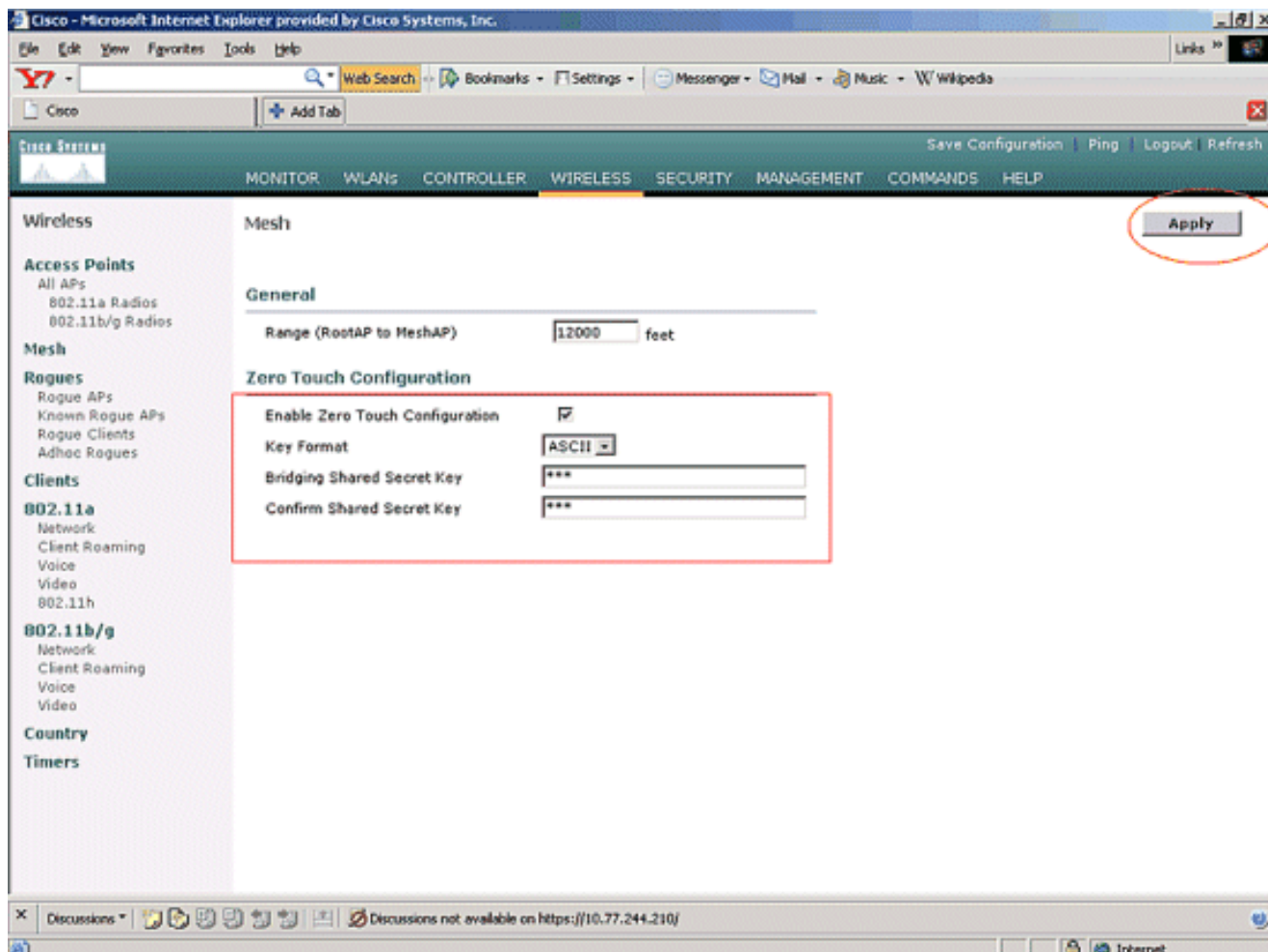
Ahora usted ha configurado sus AP como los rap y mapas, según las necesidades, así como ha configurado sus parámetros del bridging. Habilite la **configuración del Cero-tacto en el WLC** para, quitar una vez el MAPA de su conexión alámbrica con el WLC y llevado la red de producción (al otro extremo de la red de interconexión de punto a punto), el MAPA puede establecer una conexión asegurada del LWAPP con el WLC sin ninguna conexión alámbrica al WLC. El valor predeterminado para la configuración del cero-tacto en el WLC se habilita (o marcado).

Complete estos pasos para configurar la configuración del cero-tacto en el WLC.

1. Del regulador GUI, elija la **Tecnología inalámbrica > la malla** y haga clic el **permiso cero configuración del tacto**.



2. Elija el formato dominante (ASCII o hex.).
3. Ingrese la clave secreta compartida bridging. Se habilita este campo solamente si se habilita la opción de configuración del cero-tacto. Ésta es la clave que se proporciona a los Puntos de acceso de la malla (mapas) para que establezcan una conexión segura del LWAPP con el controlador LAN de la tecnología inalámbrica de Cisco mientras que el MAPA conecta sin hilos del otro extremo de la red de interconexión. La clave debe ser por lo menos 32 caracteres de largo en el hex. o el formato ASCII. Una clave secreta compartida predeterminada se asigna en la etapa de la fabricación. No es visible a usted. Este ejemplo utiliza la clave secreta compartida **Cisco del bridging**. Cuando usted cambia la clave secreta compartida, el controlador LAN de la tecnología inalámbrica de Cisco envía automáticamente el cambio a todos los rap, que hace los PAP perder la Conectividad hasta que puedan obtener la nueva clave secreta compartida del controlador LAN de la tecnología inalámbrica de Cisco.
4. Ingrese la clave secreta compartida bridging otra vez en el campo de **clave secreta compartido confirmar**.
5. Haga clic en Apply (Aplicar). Este tiro de pantalla explica los pasos 3 a 5.



Si la configuración del cero-tacto se habilita en el controlador LAN de la tecnología inalámbrica de Cisco y el MAPA se mueve al otro extremo de la red de interconexión, el RAP y los mapas hacen esto para lograr una configuración segura del cero-tacto:

1. Si es un RAP, tiene una conexión segura del LWAPP al controlador LAN de la tecnología inalámbrica de Cisco y utiliza ya la interfaz configurada del regreso del RAP (valor por defecto: 802.11a).
2. Si es un MAPA, analiza las interfaces y los canales del regreso para los Puntos de acceso vecinos de la malla. Cuando encuentra un Punto de acceso vecino de la malla con el mismo **nombre de Grupo de Bridge** (configurado como parte de los parámetros del bridging) y una trayectoria de nuevo al controlador LAN de la tecnología inalámbrica de Cisco, hace ese Punto de acceso de la malla a su padre. Si el MAP encuentra más de un Punto de acceso vecino de la malla, utiliza un algoritmo de menor coste para determinar qué padre tiene el mejor trayecto de nuevo al controlador LAN de la tecnología inalámbrica de Cisco. Para configurar una conexión segura del LWAPP con el controlador LAN de la tecnología inalámbrica de Cisco, el MAPA envía su clave secreta compartida predeterminada, que está ya disponible en la etapa de la fabricación AP, y la dirección MAC para configurar una conexión asegurada temporal. El controlador LAN de la tecnología inalámbrica de Cisco valida la dirección MAC contra el lista de filtración MAC y, si está encontrado, envía la clave secreta compartida, que se configura como parte del ajuste de la configuración del Cero-tacto al MAPA y desconecta. El MAPA salva la clave secreta compartida y la utiliza para configurar una conexión segura del LWAPP. Si un MAPA pierde la conexión al controlador LAN de la tecnología inalámbrica de Cisco, busca para los vecinos válidos que utilizan el nombre de Grupo de Bridge del Punto de acceso de la malla y analiza las interfaces y los canales del regreso. Cuando encuentra un Punto de acceso vecino de la malla, hace ese

Punto de acceso de la malla a su padre. Si tiene ya una clave secreta compartida, utiliza esa clave e intenta configurar una conexión segura del LWAPP al controlador LAN de la tecnología inalámbrica de Cisco. Si la clave secreta compartida no trabaja, utiliza la clave secreta predeterminada compartida e intenta conseguir una nueva clave secreta compartida.

Verificación

- Después de todas las configuraciones, desconectan el MAPA de la red alámbrica asociada al WLC y lo mueven al otro extremo de la malla. Poder en la malla. Con todas las configuraciones adecuadas, el MAPA puede localizar el RAP como su padre y registro con el regulador sin hilos.
- En el WLC CLI, usted puede utilizar la **trayectoria Cisco AP de la malla de la demostración y mostrar los comandos de Cisco AP del relincho de la malla** para verificar que los AP se registraron con el WLC: **El nombre de la trayectoria AP de la malla del comando show** se utiliza para verificar la trayectoria del regulador 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 eso para alcanzar el AP **ap:71:1b:00(MAP)**, el regulador 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 el AP **ap:7f:47:00** está conectada directamente con el regulador puesto que este AP es un **RAP**. **El nombre del relincho AP de la malla del comando show** visualiza la información de 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 al vecino del AP **ap:7f:47:00** es el **MAPA 00:0B:85:71:1B:00**, y el MAPA es un **NIÑO** a este AP puesto 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` Esta salida dice al vecino de AP **ap:71:1b:00** es el **RAP 00:0B:85:7F:47:00**, y el RAP es un **PADRE** a este AP.
- **El nombre sumario Ap de la malla del comando show** visualiza 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 pueden verificar del regulador GUI con estos pasos: Del WLC GUI, **Tecnología inalámbrica del teclado > todos los AP**. Haga clic el link de **información del bridging** para su AP1510 para acceder la **página de información del bridging del AP**.

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 Detail
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2 Detail Bridging Information
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2 Detail Bridging Information

Discussions not available on https://10.77.244.210/

Done Internet

Los detalles del bridging AP pagan las listas todos los detalles del bridging de este AP, tales como la información de tipo del papel y de la malla AP.

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, usted puede utilizar la trayectoria *Cisco AP de la malla de la demostración* y

mostrar los comandos de *Cisco AP del relincho de la malla* para verificar que los AP están registrados con el WLC:

Para verificar si su Ethernet Bridging trabaja correctamente, realice estos pasos:

1. Conecte una red Ethernet (LAN Ethernet B según lo dado en el diagrama de la red) con el acceso de Ethernet del MAPA a través de un Switch. Asegúrese de que el Switch esté configurado correctamente según las necesidades.
2. Verifique la Conectividad entre el LAN Ethernet B en el MAPA y la red alámbrica (LAN Ethernet A según lo dado en el diagrama de la red) conectados en el RAP detrás del WLC con el **comando ping**. Si el **ping** es acertado, indica que el Ethernet Bridging trabaja muy bien.

Troubleshooting

Estos comandos de Troubleshooting pueden ser útiles:

Comandos para resolución de problemas

- **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. 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
    >cscscoDefaultMfgCaCert<
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 regulador está fuera del intervalo de la validez del certificado del AP, así que el AP no puede registrarse con el regulador. Los certificados instalados en el AP tienen un intervalo de validez predefinido. El tiempo del regulador debe ser fijado de una manera tal que esté dentro del intervalo de la validez del

certificado del AP. Refiera al documento de las [extremidades del Troubleshooting de las herramientas de actualización del LWAPP](#) para más información sobre los posibles problemas en un REVESTIMIENTO que se registre con el regulador. Refiera a [resolver problemas una red de interconexión](#) para más información sobre resolver problemas una red de interconexión.

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

[Información Relacionada](#)

- [Guía de despliegue de la solución de interconexión de redes de la malla de Cisco](#)
- [Instalación y configuración del Punto de acceso de la malla](#)
- [Ejemplo de configuración de la red de interconexión del regulador del Wireless LAN](#)
- [Guía de inicio rápido: Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point](#)
- [Guía de instalación del hardware al aire libre del Punto de acceso de la malla del Cisco Aironet de la serie 1500](#)
- [Instrucciones de instalación del alimentador de corriente del Punto de acceso del Cisco Aironet de la serie 1500](#)
- [Cisco Aironet de la serie 1500 AP Q y A](#)
- [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](#)