

Ethernetes que puentean 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 APs](#)

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

[Registre el AP con el WLC](#)

[Configure el papel AP y otros parámetros que puentean](#)

[Active los Ethernetes que puentean en los APs](#)

[Active 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 LAN de la Tecnología inalámbrica (WLC) se configura para la operación básica.
- El WLC se configura en el modo de la capa 3.
- El conmutador 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 de Cisco WLCs
- 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 del Switches de Cisco

Componentes Utilizados

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

- Cisco 2000 Series WLC que funciona con los firmwares 4.0.217.0
- Dos (2) revestimientos de las 1510 Series de Cisco Aironet
- 2 Switch de la capa 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 Cisco unificó la solución de red inalámbrica, permite a dos o más Puntos de acceso ligeros de la malla de Cisco Aironet (en lo sucesivo llamados los Puntos de acceso de la malla) 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 vigilan, y se actúan desde y a través de cualquier regulador inalámbrico LAN de Cisco que se despliegue en la solución de interconexión de redes de la malla.

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

- Despliegue de punto a punto
- despliegue Punta-a-de múltiples puntos
- Despliegue de la malla

Este documento se centra en cómo configurar el despliegue de punto a punto y los Ethernetes de la malla que puentean en lo mismo. En el despliegue de punto a punto de la malla, los Puntos de acceso de la malla proporcionan al acceso de red inalámbrica y al regreso a los clientes de red inalámbrica, y pueden utilizar simultáneamente puentear 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 de Cisco Aironet es un dispositivo de red inalámbrica diseñado para el acceso de cliente de red inalámbrica y puentear de punto a punto, puentear punta-a-de múltiples puntos, y la conectividad de red inalámbrica punta-a-de múltiples puntos de la malla. 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 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 regulador inalámbrico LAN de Cisco. Utilizan el interfaz inalámbrico del regreso para comunicar con los mapas próximos. Los rap son el nodo primario a cualquier puentear o red de interconexión y conectan un puente o la red de interconexión a la red alámbrica, tan allí puede ser solamente un RAP para cualquier segmento puenteado o de la red de interconexión.

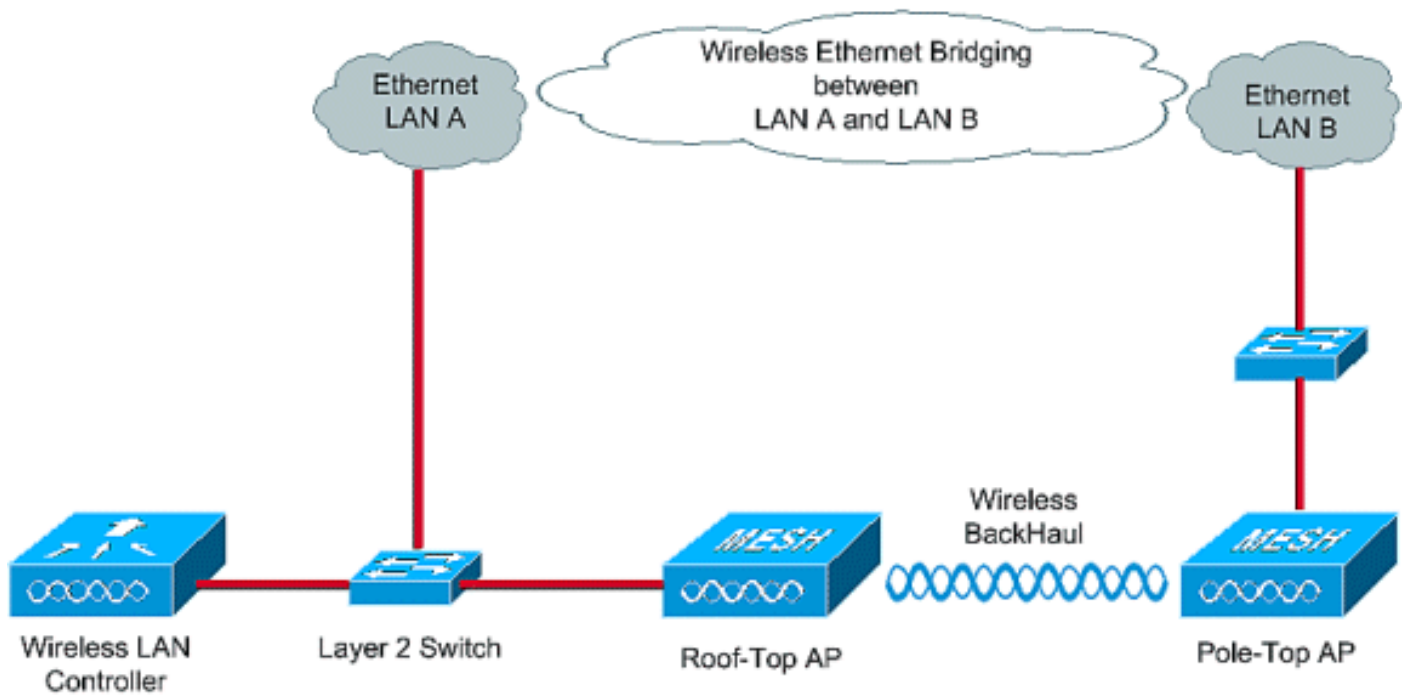
Los mapas no tienen ninguna conexión alámbrica a un regulador inalámbrico LAN de Cisco. Pueden ser los clientes totalmente inalámbricos y ayuda que comunican con otros mapas o rap, o pueden ser utilizados para conectar con los dispositivos periféricos o una red alámbrica. El puerto Ethernet se inhabilita por abandono por razones de seguridad, pero usted puede activarlo para los PAPs.

[Configurar](#)

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

En esta disposición, 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 LAN A de los Ethernetes locales 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 APs del hacia fuera-de-cuadro 1510 para los Ethernetes que puentean, realice estos pasos:

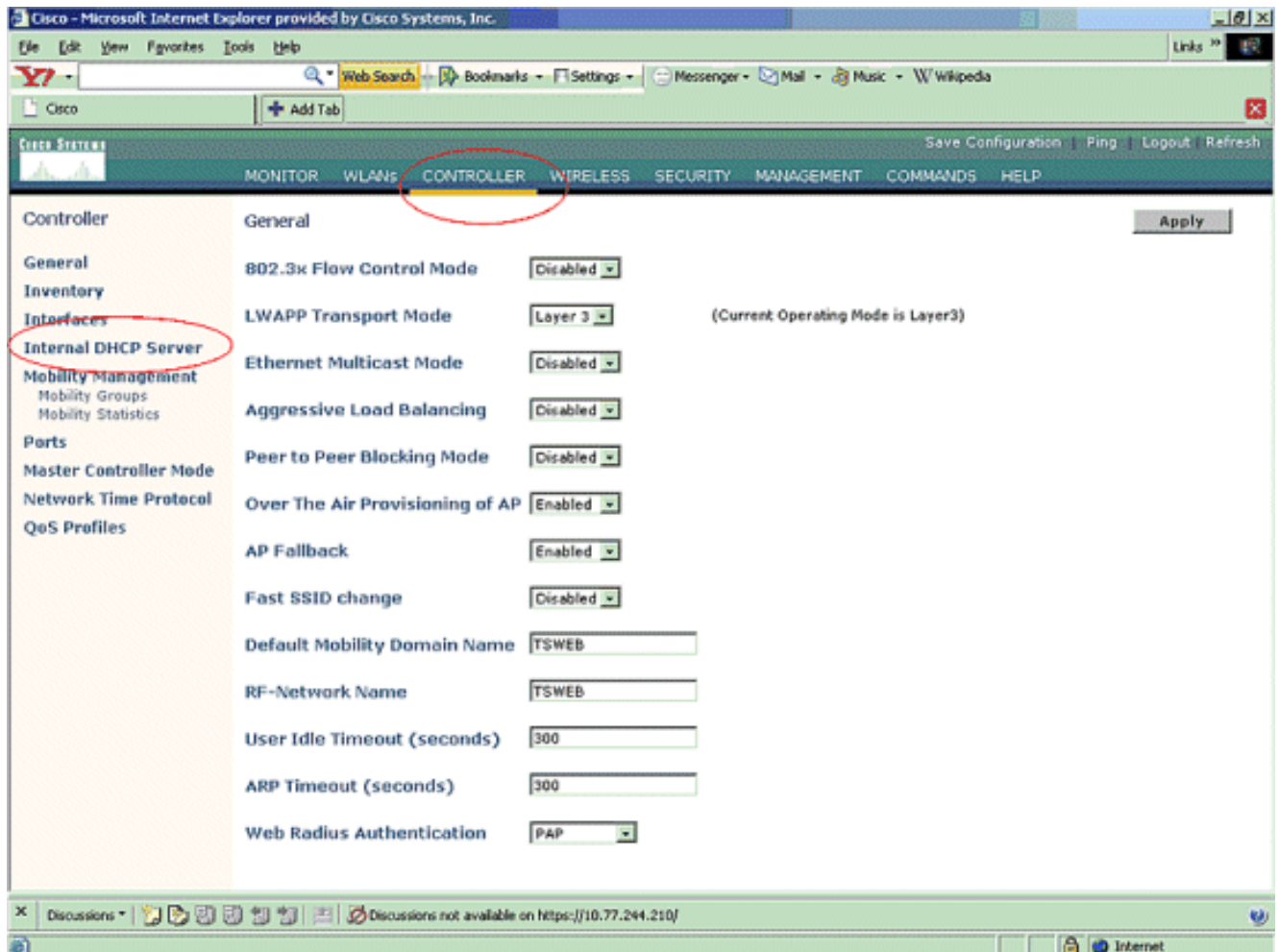
1. [Asigne la dirección IP a los APs](#)
2. [Agregue la dirección MAC de los APs a la lista de filtración MAC del WLC](#)
3. [Registre los APs con el WLC](#)
4. [Configure el papel AP y otros parámetros que puentean](#)
5. [Active los Ethernetes que puentean en los APs](#)
6. [Active la configuración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

[Asigne la dirección IP a los APs](#)

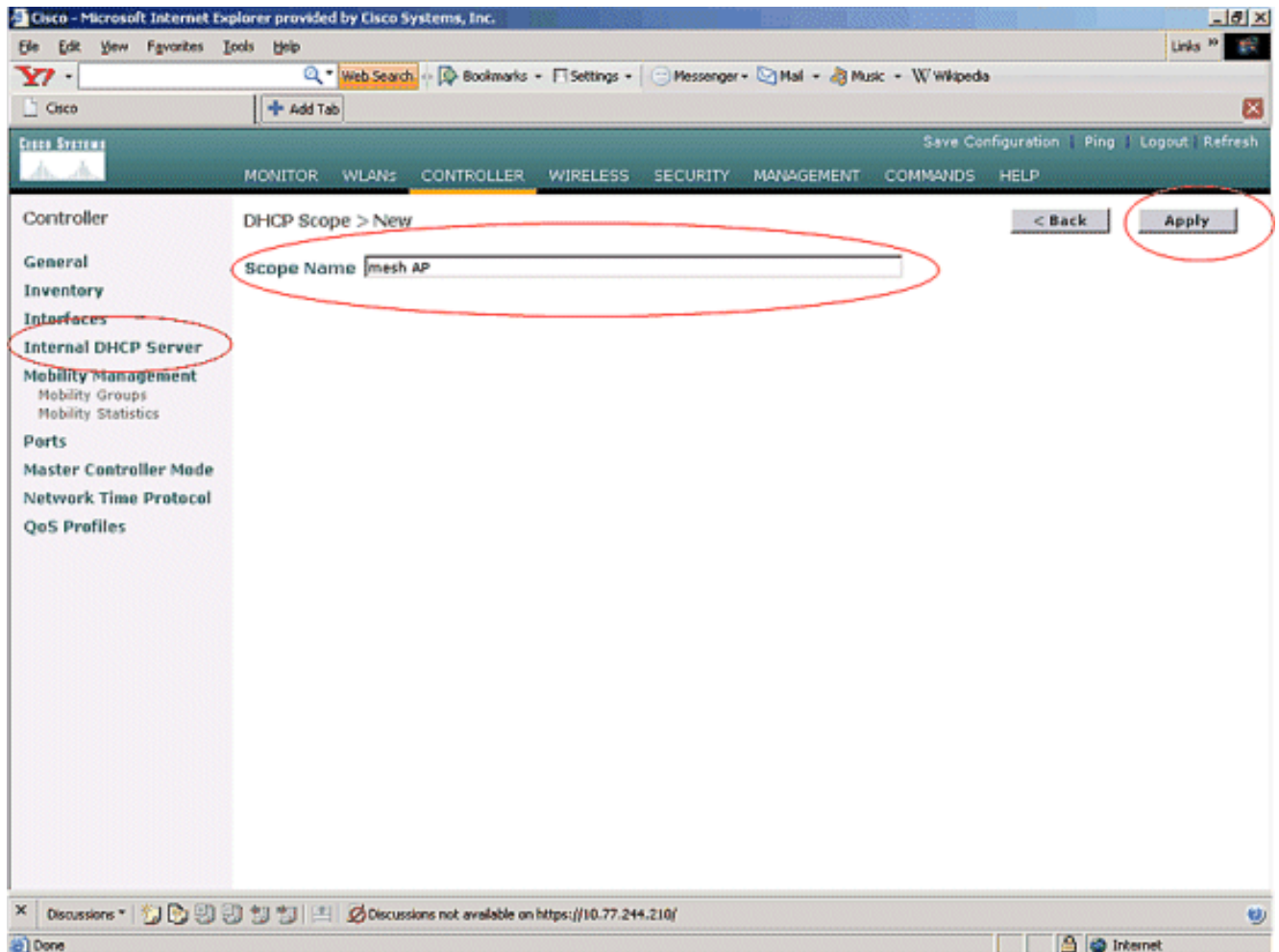
Cuando cualquier AP arranca, primero busca una dirección IP. Esta dirección IP se puede asignar dinámicamente con un DHCP interno externo como el servidor del DHCP del [®] de Microsoft Windows. La última versión WLC (4.0 y más adelante) puede asignar la dirección IP a los APs con el servidor interno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

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

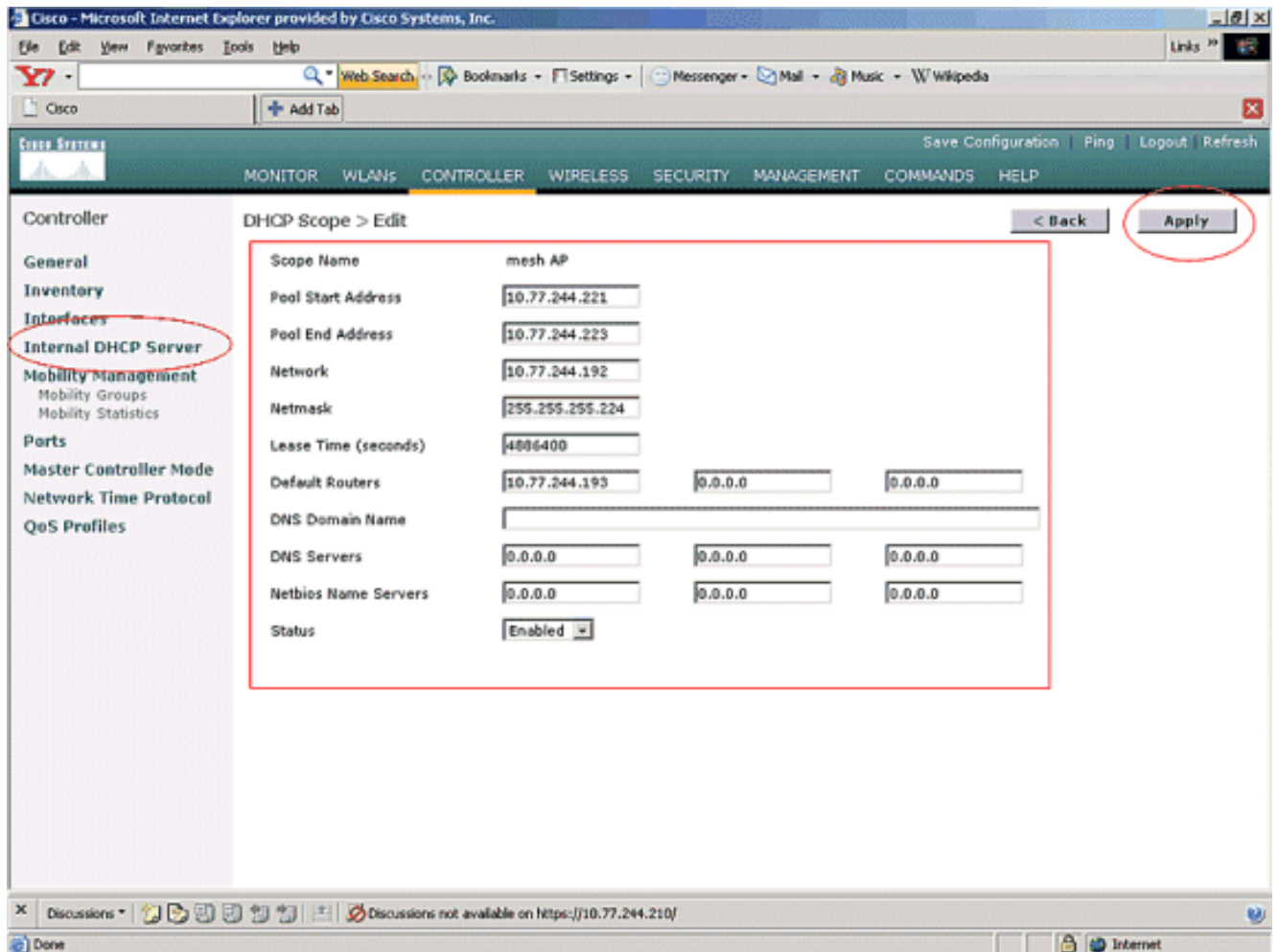
1. Haga clic el **REGULADOR** del menú principal del GUI WLC. Elija el **servidor interno del DHCP de la** esquina del lado izquierdo de la página principal del regulador.



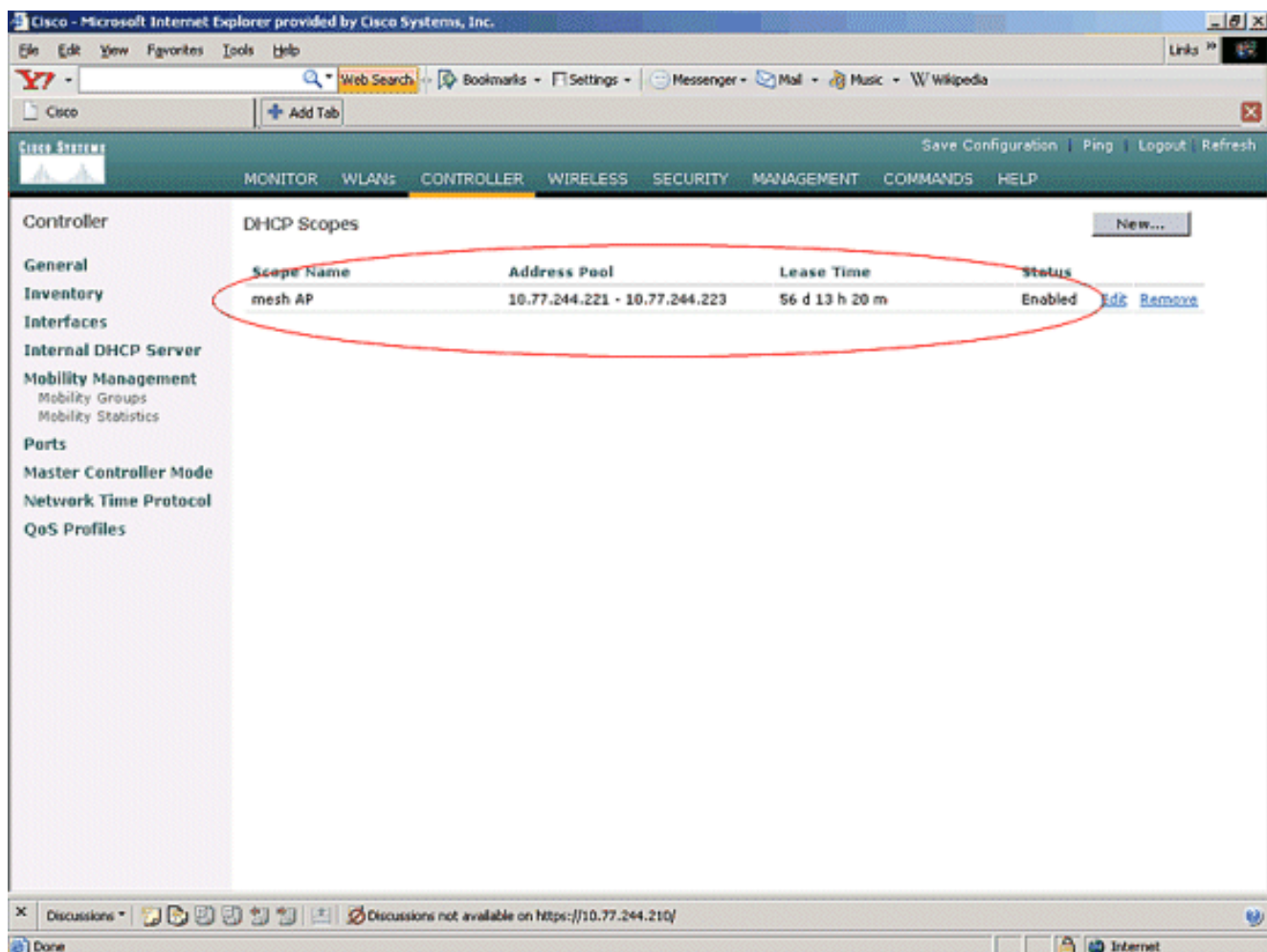
2. En la **página del servidor interna del DHCP**, clickNew para crear un nuevo alcance del DHCP. Este ejemplo asigna el nombre del alcance como **malla AP**. Haga clic en Apply (Aplicar). Esto le lleva al alcance del DHCP de la malla AP corrige la página.



3. En el **alcance del DHCP > corrija la página**, configure la Dirección de inicio del pool, reúna el direccionamiento del final, red y máscara de red, Routers del valor por defecto, y el resto de parámetros necesarios según lo dado en este ejemplo. Elija el estatus del servidor del DHCP según lo **activado de la casilla desplegable del estatus**. Haga clic en Apply (Aplicar).



4. Ahora, el servidor interno del DHCP se configura para asignar los IP Addresses a la malla APs.



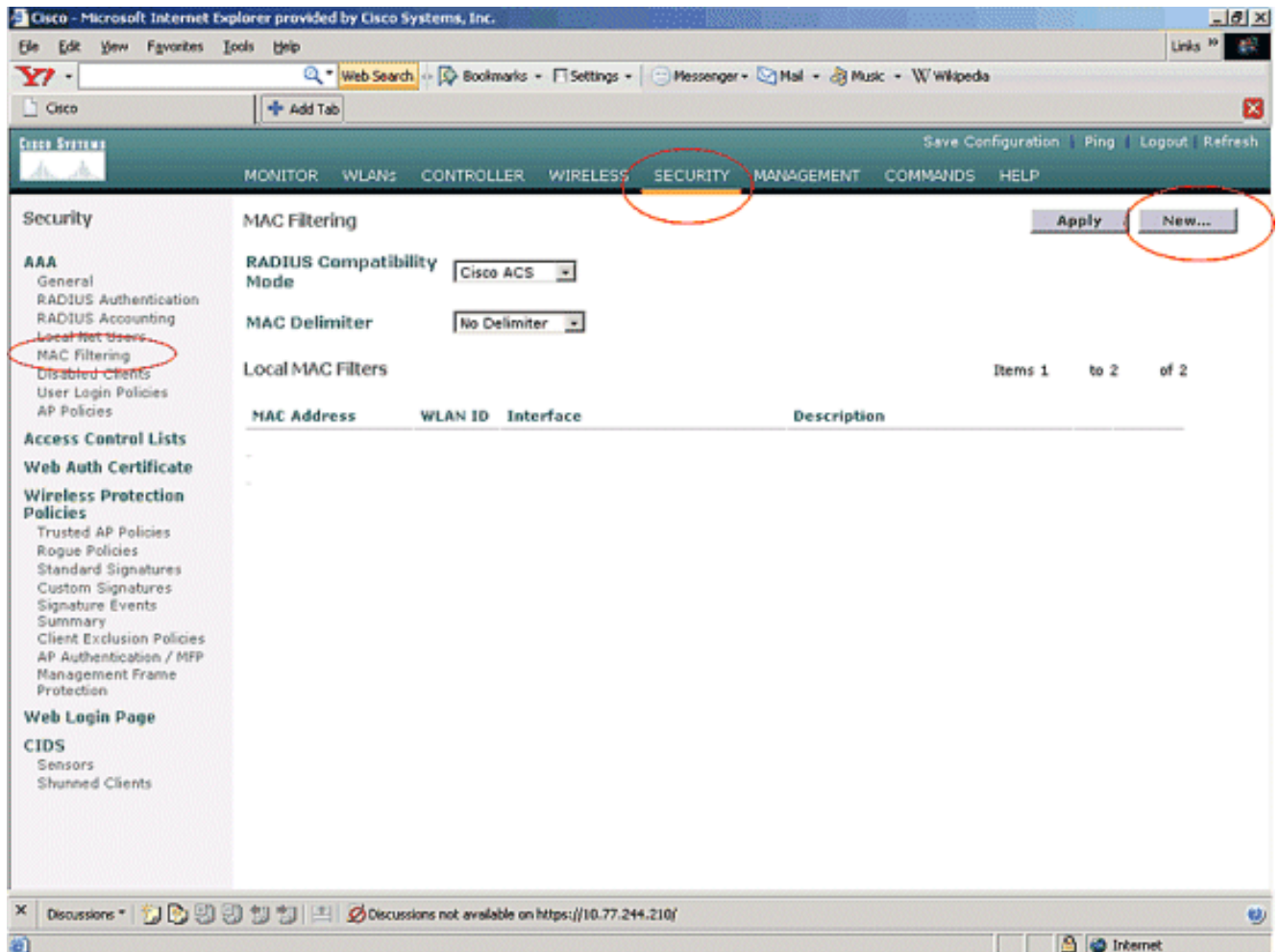
5. Una vez que los APs se registran con el regulador, asigne la dirección IP estática a los APs a través del GUI del regulador. Si usted asigna los IP Addresses estáticos para enredar los APs, proporcionan a una convergencia más rápida de los APs la próxima vez que se registran con el regulador.

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

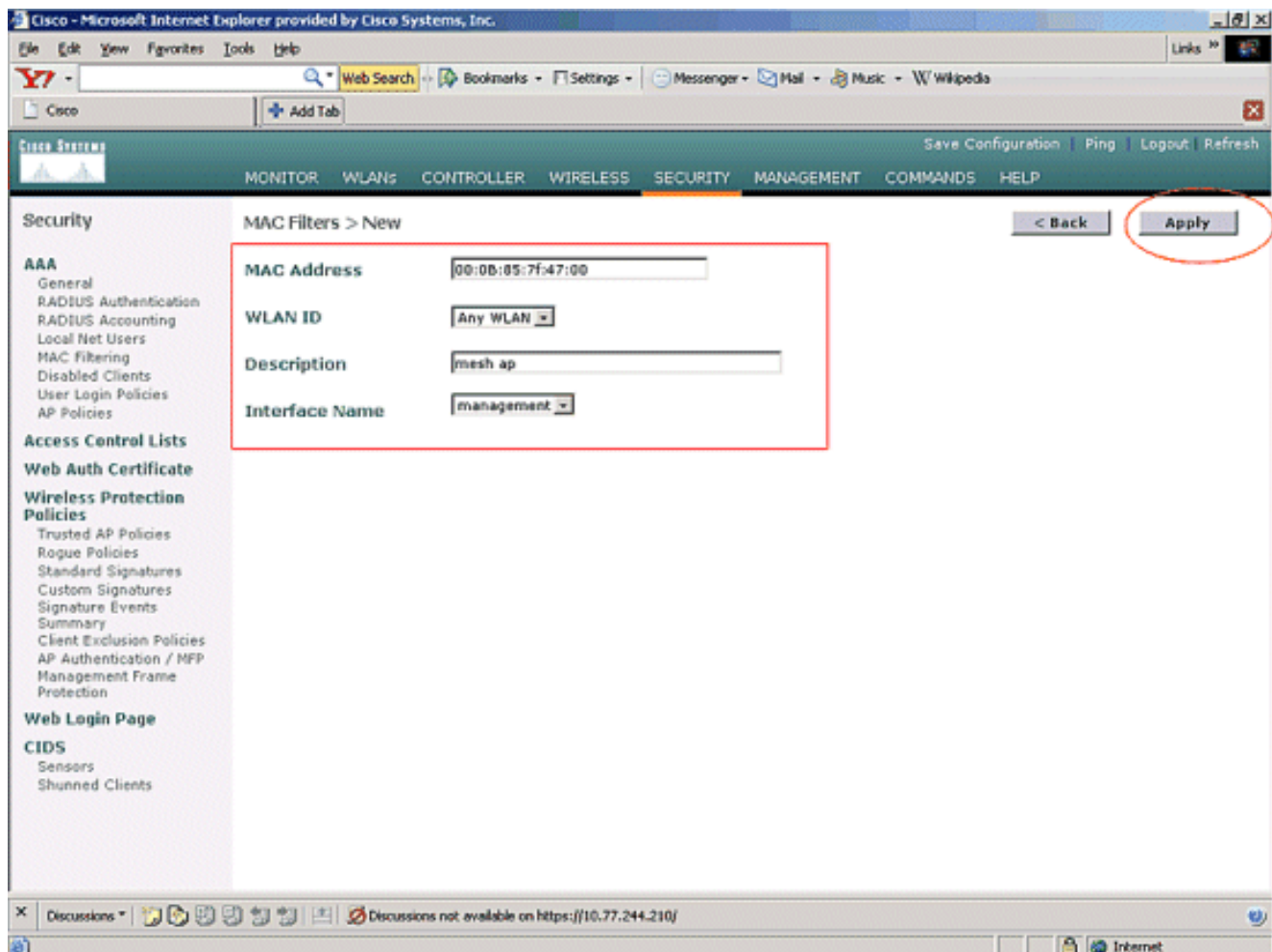
Para registrar la malla APs con el WLC, usted necesita primero agregar la dirección MAC de los APs a la lista de filtración MAC del WLC. Usted puede encontrar la dirección MAC etiquetada en el lado superior de la malla AP.

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

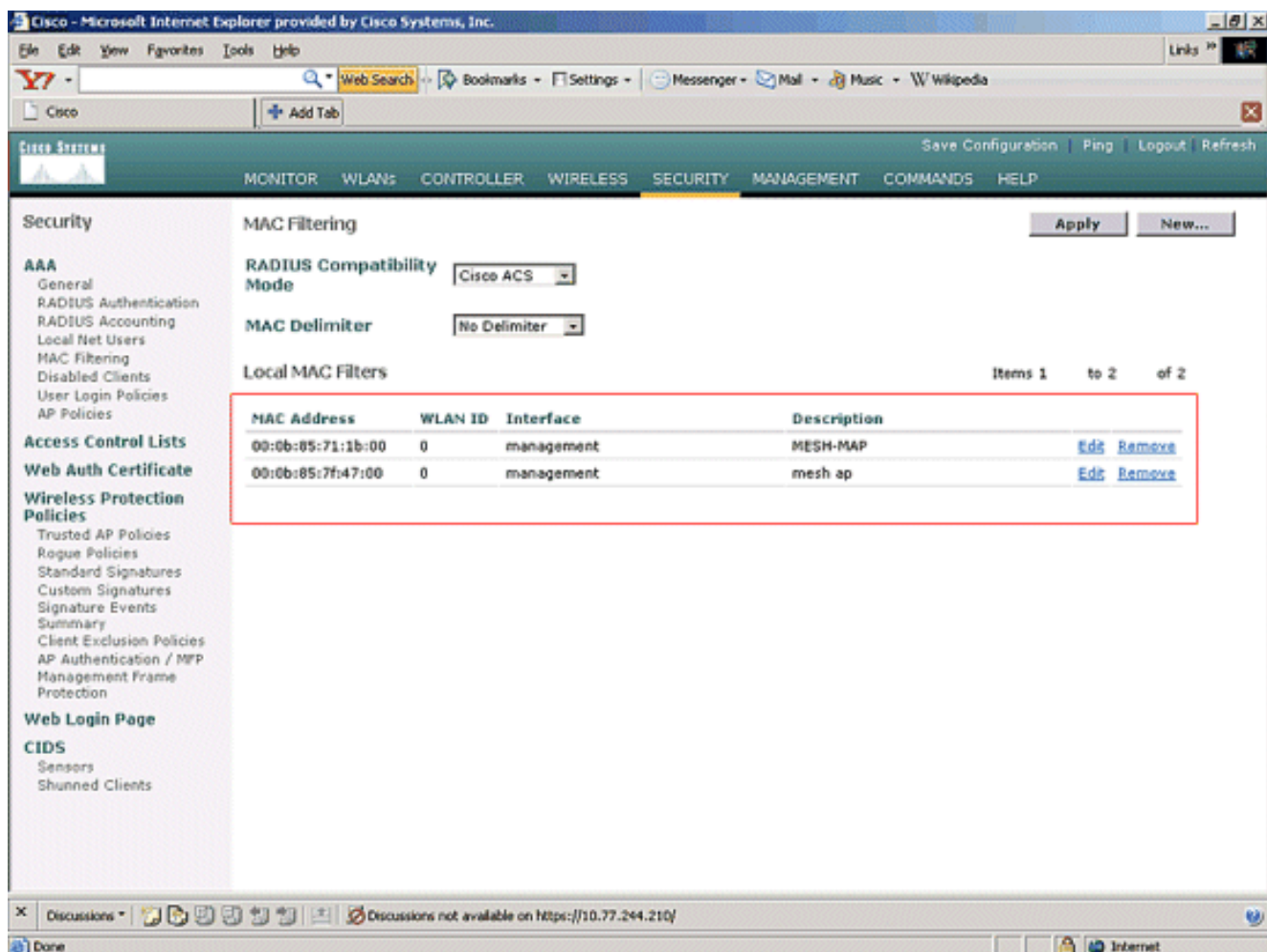
1. Haga clic la **SEGURIDAD** del menú principal del regulador. En la página Seguridad, elija el **MAC que filtra** bajo sección **AAA**. Esto le lleva a la página de filtración MAC. Haga clic **nuevo** para crear los filtros MAC para la malla APs.



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 un **interfaz dinámico de los menús desplegables** del nombre identificación y del interfaz de la red inalámbrica (WLAN), respectivamente. Haga clic en Apply (Aplicar).



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



[Registre el AP con el WLC](#)

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

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

Si usted no ha podido agregar el AP a la lista de filtración MAC del regulador, los APs no pueden unirse al WLC a la hora del registro con 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 APs de las 1500 Series, se recomienda para inhabilitar la **permit APs que puentean 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-puente-aps de la red de los config**

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

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

(Resumen ap del >show del regulador de Cisco)

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	LAP1510	00:0b:85:7f:47:00	default_locat
ap:71:1b:00 ion 2	2	LAP1510	00:0b:85:71:1b:00	default_locat

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

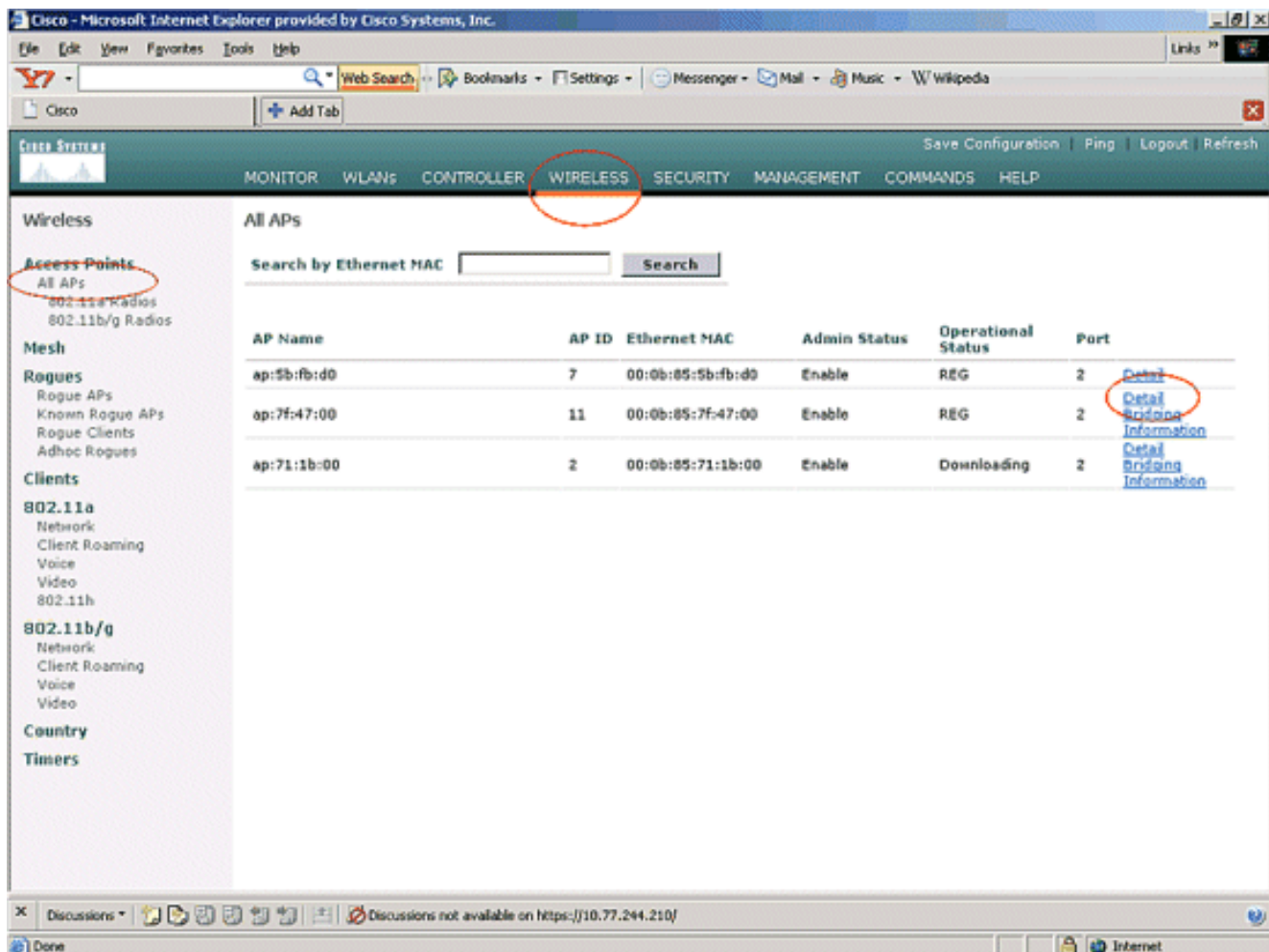
AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:5b:fb:d0	7	00:0b:85:5b:fb:d0	Enable	REG	2
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2

[Configure el papel AP y otros parámetros que puentean](#)

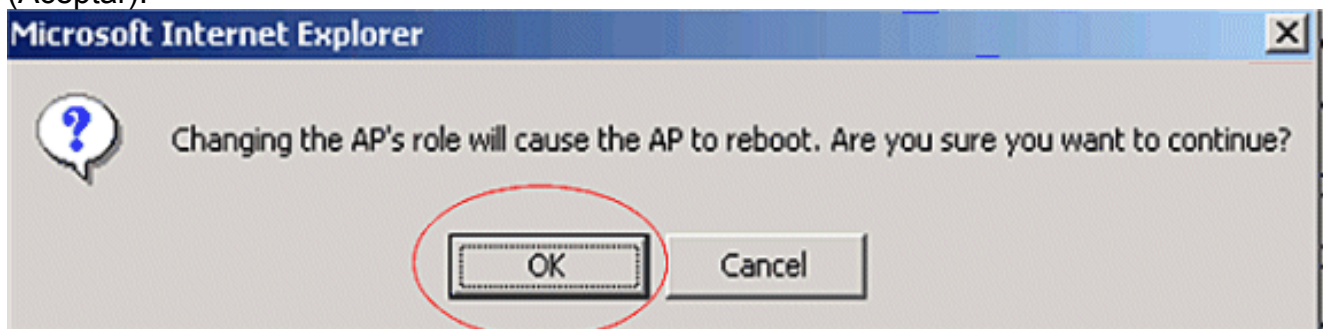
Una vez que los APs se registran al WLC, usted necesita configurar el papel AP y otros parámetros que puentean. Usted necesita configurar los APs como los rap y mapas, como sea necesario.

Complete estos pasos para configurar esos parámetros AP:

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



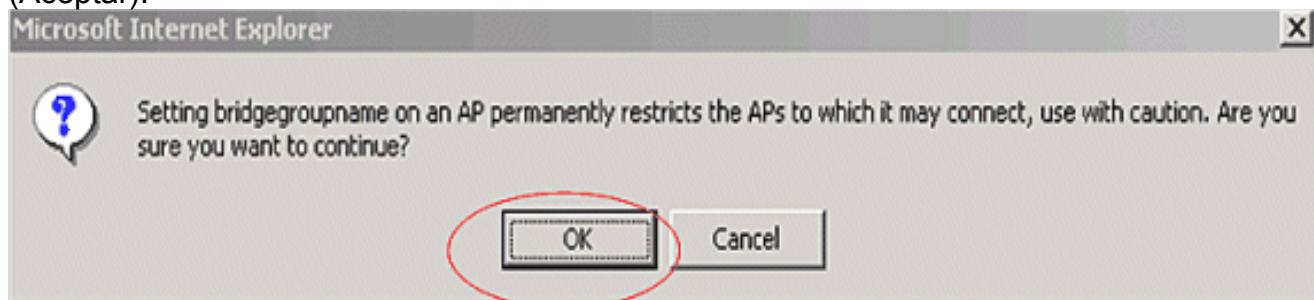
3. En la página de los **detalles** de sus 1510 AP, **modo AP** bajo fijan al **general** automáticamente **para puentear** para los APs que tienen funciones del puente, tales como el AP1510. Esta página también muestra esta información bajo puentear la información. Bajo **puentear la información**, elija una de estas opciones para especificar el papel de este AP en la red de interconexión: MeshAP (MAPA) RootAP (RAP) Los APs configurados como RootAPs deben tener conexión alámbrica al WLC a la hora de la puesta en práctica de la disposición 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 APs, por abandono, asumen el papel de los mapas cuando suben y se registran con el WLC. Mientras que usted configura el papel del puente, 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.

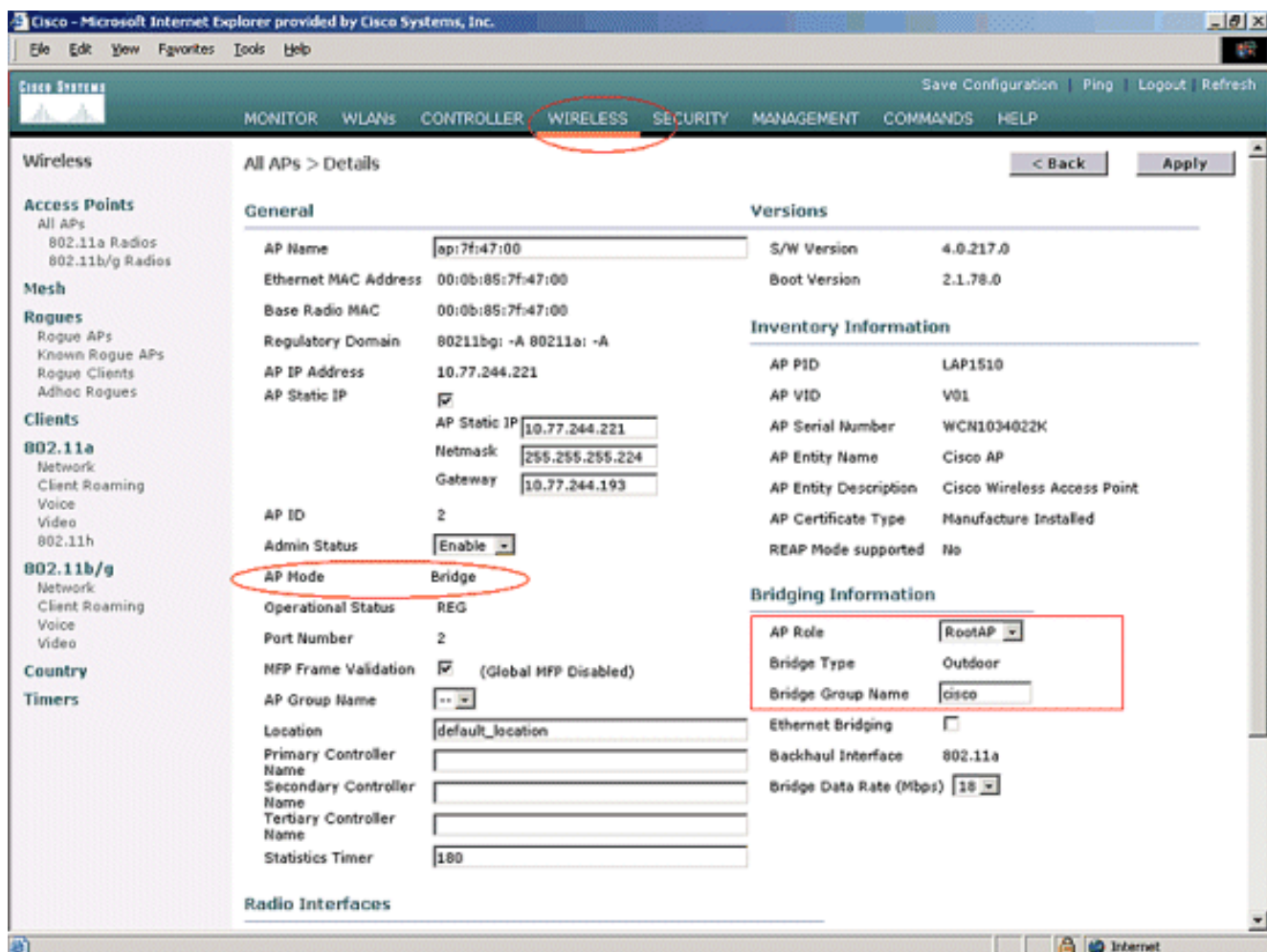
4. Configure el parámetro del **nombre del grupo del puente**. Esto es una cadena de un máximo de 10 caracteres. Utilice los nombres del grupo del puente para agrupar lógicamente los Puntos de acceso de la malla para evitar dos redes en el mismo canal de la comunicación

con uno a. **Para que los Puntos de acceso de la malla comuniquen, deben tener el mismo nombre del grupo del puente.** Un nombre del grupo del puente del Punto de acceso de la malla del valor por defecto se asigna en la etapa de la fabricación. No es visible a usted. El campo de nombre del grupo del puente 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 puente del valor por defecto. Este ejemplo utiliza el nombre del grupo **Cisco** del puente en todos los APs implicados en esta red de interconexión. Mientras que usted configura el nombre del grupo del puente, un cuadro alerta visualiza esto: **La determinación del nombre del grupo del puente restringe permanentemente el AP con el cual puede conectar.** Para continuar, haga clic en OK (Aceptar).



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

5. **La tarifa de datos del puente** es la tarifa en la cual los datos se comparten entre los Puntos de acceso de la malla. Esto es fijo para una red completa. **La tarifa de datos del valor por defecto 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 del **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.

Ethernetes del permiso que puentean en los APs

El siguiente paso es activar los Ethernetes que puentean en el RAP y todos los mapas cuyo puerto Ethernet está conectado con un dispositivo de los Ethernetes. Una de las características fundamentales de la malla APs es el uso de un puerto Ethernet en el MAPA para conectar los dispositivos externos y para proporcionar a los Ethernetes que puentean entre todos los puertos Ethernet de los APs implicados en la red de interconexión.

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

Complete estos pasos para configurar los Ethernetes que puentean en el RAP y la malla APs:

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

Save Configuration | Ping | Logout | Refresh

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

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

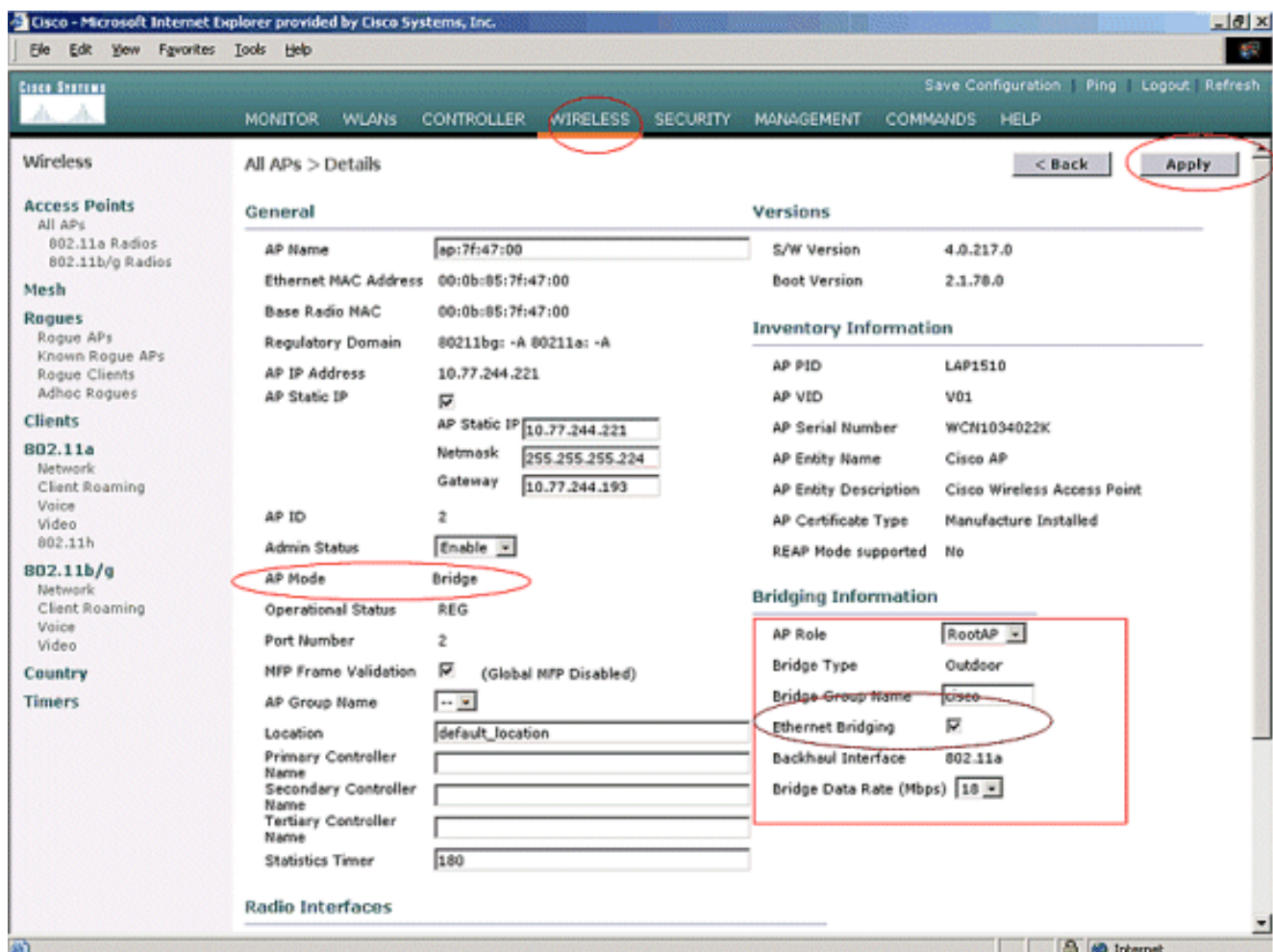
All APs

Search by Ethernet MAC 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	Details
ap:7f:47:00	11	00:0b:85:7f:47:00	Enable	REG	2	Details Rogue Information
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2	Details Rogue Information

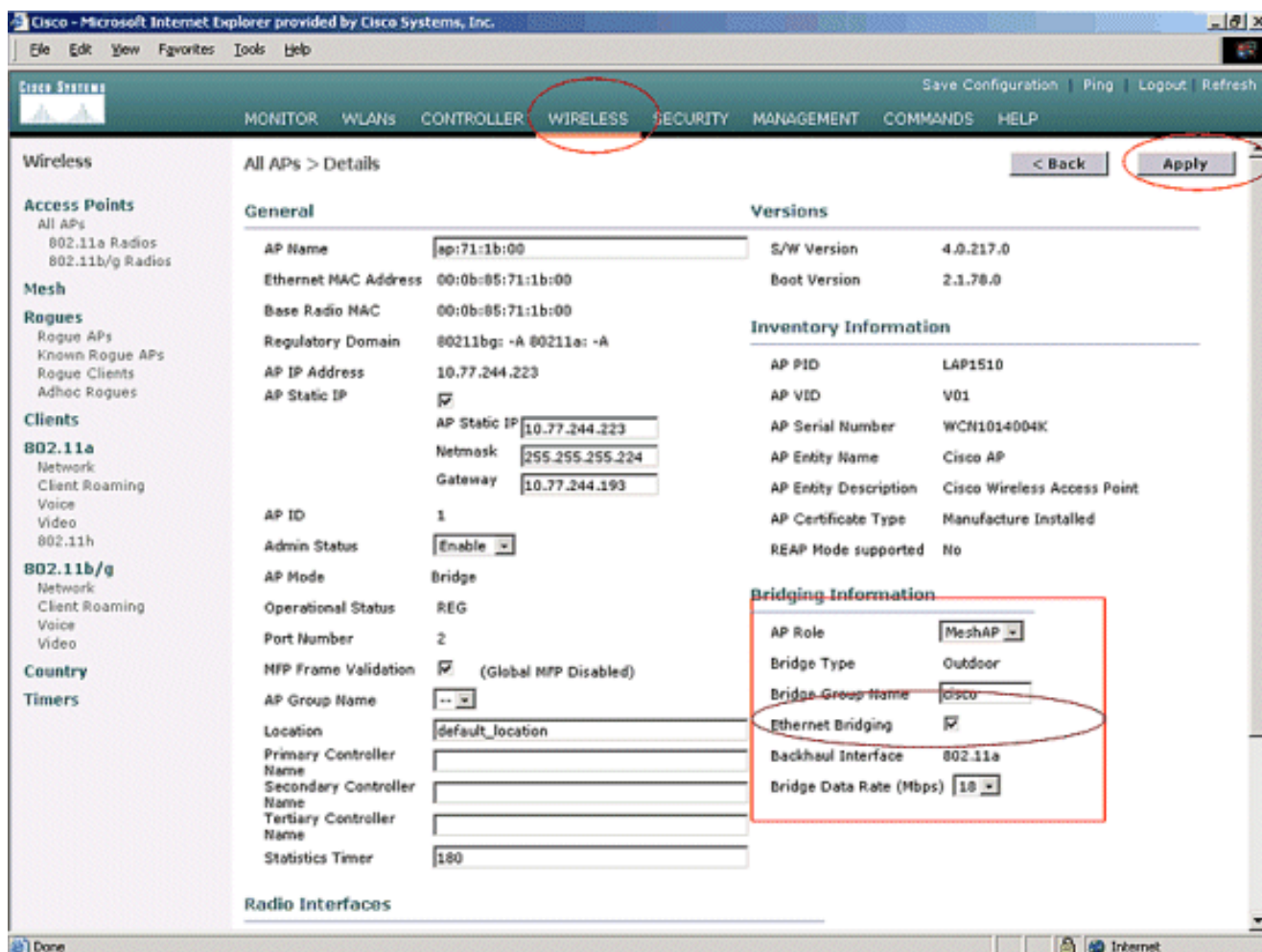
Discussions not available on https://10.77.244.210/

3. Bajo puentear la información, controle el cuadro al lado de puentear de los Ethernetes. Esto activa los Ethernetes que puentean en el AP.



Si usted utiliza una punta a la red de interconexión de múltiples puntos, active los Ethernetes que puentean en los rap y solamente en los mapas con los cuales los dispositivos de los Ethernetes están conectados. No es necesario activar los Ethernetes que puentean en todos los mapas en una red de interconexión. Si usted ha activado los Ethernetes que puentean para utilizar la red para puentear (P2P o P2MP), usted debe activar los Ethernetes que puentean en todos los Nodos (los mapas y los rap). En el decorado que puentea, un RAP que actúa como puente de la raíz conecta los mapas múltiples como puentes de la no-raíz con su LANs atado con alambre asociado. Usted puede activar los Ethernetes que puentean en los APs del regulador CLI con este comando: **config ap que puentean el permiso.** Nota: Ninguna switches conectados a los puertos Ethernet de sus mapas no deben HACER el protocolo VLAN trunking (VTP). El VTP puede configurar de nuevo el VLAN 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. Active puentear de los Ethernetes y todos los parámetros que puentean explicados en la sección anterior en el MAPA, también.



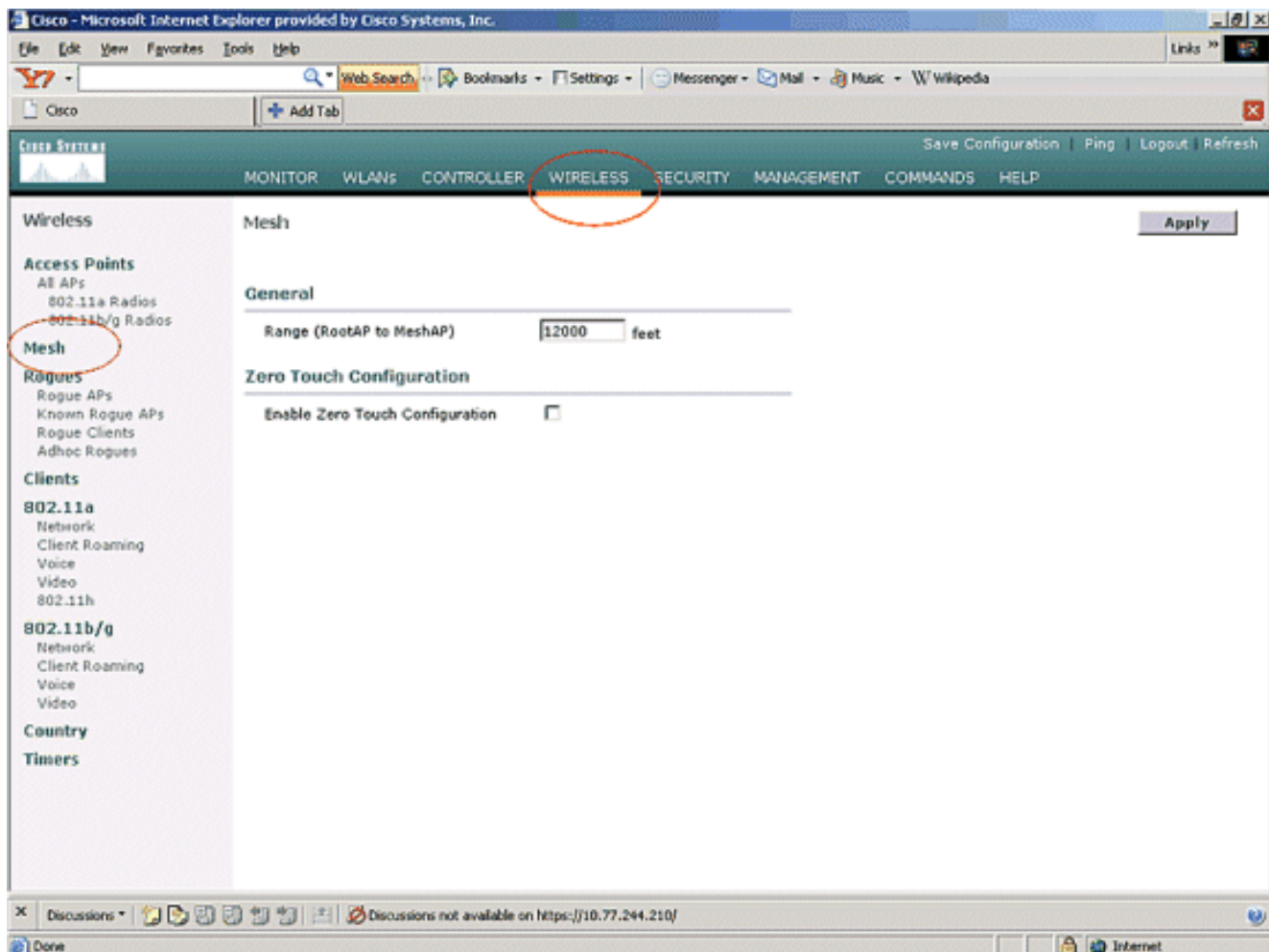
Una vez que usted acaba las configuraciones de los parámetros del puente y de los parámetros bridging de los Ethernetes en cada AP, el tecléo **se aplica** para salvar las configuraciones. Esto causa el AP al unregister del WLC, reinicialización, y reregister con el WLC.

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

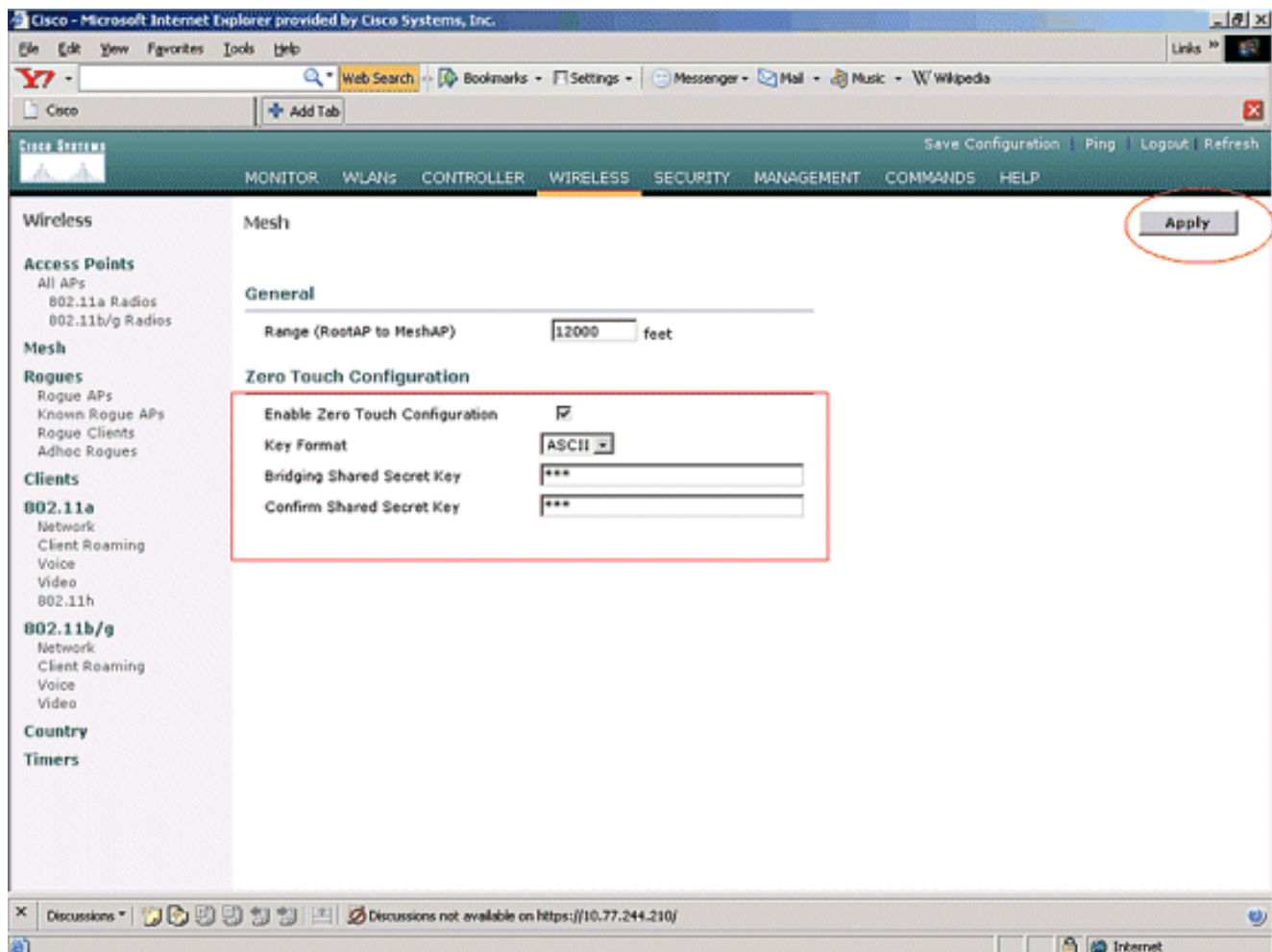
Ahora usted ha configurado sus APs como los rap y mapas, según las necesidades, así como ha configurado sus parámetros que puenteaban. Active la **configuración del Cero-tacto en el WLC** para, quitar una vez el MAPA de su conexión alámbrica con el WLC y llevado la red de producción (al otro extremo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

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

1. Del GUI del regulador, 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 que puentea. Se activa este campo solamente si se activa 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 LWAPP con el regulador inalámbrico LAN 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 del valor por defecto se asigna en la etapa de la fabricación. No es visible a usted. Este ejemplo utiliza la clave secreta compartida que puentea **Cisco**. Cuando usted cambia la clave secreta compartida, el regulador inalámbrico LAN de Cisco envía automáticamente el cambio a todos los rap, que hace los PAPs perder la Conectividad hasta que puedan obtener la nueva clave secreta compartida del regulador inalámbrico LAN de Cisco.
4. Ingrese la clave secreta compartida que puentea 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 activa en el regulador inalámbrico LAN 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 LWAPP al regulador inalámbrico LAN de Cisco y utiliza ya el interfaz configurado del regreso del RAP (valor por defecto: 802.11a).
2. Si es un MAPA, analiza los 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 del grupo del puente** (configurado como parte de puentear los parámetros) y una trayectoria de nuevo al regulador inalámbrico LAN de Cisco, hace ese Punto de acceso de la malla a su padre. Si el MAPA 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 regulador inalámbrico LAN de Cisco. Para poner una conexión segura LWAPP con el regulador inalámbrico LAN de Cisco, el MAPA envía su clave secreta compartida del valor por defecto, que está ya disponible en la etapa de la fabricación AP, y la dirección MAC para poner una conexión asegurada temporal. El regulador inalámbrico LAN 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 de la configuración del Cero-tacto al MAPA y desconecta. El MAPA salva la clave secreta compartida y la utiliza para poner una conexión segura LWAPP. Si un MAPA pierde la conexión al regulador inalámbrico LAN de Cisco, busca para los vecinos válidos que utilizan el nombre del grupo del puente del Punto de acceso de la malla y analiza los 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 poner una conexión segura LWAPP al regulador inalámbrico LAN de Cisco. Si la clave secreta compartida no trabaja,

utiliza la clave secreta compartida del valor por defecto 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. Potencia en la malla. Con todas las configuraciones adecuadas, el MAPA puede localizar el RAP como su padre y registrar 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 APs 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 que el AP **ap:7f:47:00** está conectado 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 que el 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
Vector ease 1 -1, FWD: 00:0B:85:7F:47:00

```

Esta salida dice que el 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 GUI del regulador con estos pasos: Del GUI WLC, **Tecnología inalámbrica del teclado > todos los APs**. Haga clic el link de información que **puntea** para su AP1510 para tener acceso a la **página de información** que **puntea** del AP.

The screenshot shows the Cisco WLC GUI. The 'WIRELESS' tab is selected and circled in red. In the left sidebar, the 'Access Points' link is circled in red. The main content area displays a table of APs:

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
ap:71:1b:00	2	00:0b:85:71:1b:00	Enable	Downloading	2	Detail

El AP que **puntea** los **detalles** pagina las listas todos los detalles que **puntean** 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 APs están registrados con el WLC:

Para verificar si sus Ethernetes que puentean los trabajos correctamente, realicen estos pasos:

1. Conecte una red de Ethernet (LAN Ethernet B según lo dado en el diagrama de la red) con el puerto Ethernet del MAPA a través de un conmutador. Asegúrese de que el conmutador 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 los Ethernetes que puentean los trabajos muy bien.

Troubleshooting

Estos comandos de Troubleshooting pueden ser útiles:

Comandos para resolución de problemas

- **permiso de los errores del lwapp de la depuración** — Muestra la depuración de los errores LWAPP.
- **permiso del pki de la depuración P.M.** — Muestra la depuración 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
    >cscsDefaultMfgCaCert<
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 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 de la depuración** — Utilizado para configurar las opciones de la depuración del encargado de la política de acceso. **permiso de los eventos PEM de la depuración** — Utilizado para configurar las opciones de la depuración del encargado de la política de acceso. **permiso del mensaje DHCP de la depuración** — Muestra la depuración de los mensajes DHCP que se intercambian a y desde el servidor del DHCP. **permiso del paquete DHCP de la depuración** — Muestra la depuración de los detalles del paquete del DHCP que se envían a y desde el servidor del 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 inalámbrico de la configuración de red de interconexión del regulador LAN](#)
- [Guía de inicio rápido: Puntos de acceso al aire libre ligeros de la malla del Cisco Aironet de la serie 1500](#)
- [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](#)