

Guía de implementación de malla interior

Contenido

[Introducción](#)

[Overview](#)

[Hardware y software soportados](#)

[Interior frente a exterior](#)

[Configuración](#)

[Modo de controlador L3](#)

[Actualización del controlador al último código](#)

[Dirección MAC](#)

[Grabar dirección MAC en las radios](#)

[Introduzca la dirección MAC y los nombres de las radios en el controlador](#)

[Activar filtrado de MAC](#)

[Implementación de malla interior L3](#)

[Definir interfaces en controlador](#)

[Funciones de radio](#)

[Nombre del grupo de puentes](#)

[Configuración de Seguridad](#)

[Instalación](#)

[Requisitos previos](#)

[Instalación](#)

[Configuración de alimentación y canal](#)

[Comprobación de RF](#)

[Verificar las Interconexiones](#)

[Seguridad de acceso a la consola AP](#)

[Puente Ethernet](#)

[Mejora del nombre del grupo de puentes](#)

[Registros - Mensajes, Sys, AP y Trampa](#)

[Registros de mensajes](#)

[Registros de AP](#)

[Registros de trampa](#)

[Rendimiento](#)

[Prueba de convergencia de inicio](#)

[WCS](#)

[Alarmas de malla interior](#)

[Informe y estadísticas de malla](#)

[Prueba de link](#)

[Prueba de link de nodo a nodo](#)

[Enlaces de vecino de punto de acceso a demanda](#)

[Prueba Ping](#)

[Conclusión](#)

[Información Relacionada](#)

Introducción

Lightweight Access Point 1242/1131 es un dispositivo de infraestructura del Wi-Fi de dos radios para las implementaciones interiores seleccionadas. Es un LWAPP (Lightweight Access Point Protocol) basado en el producto. Proporciona una radio de 2,4 GHz y una radio de 5,8 GHz compatible con 802.11b/g y 802.11a. Se puede utilizar una radio para el acceso local (cliente) para el punto de acceso (AP) y la segunda radio se puede configurar para la red de retorno inalámbrica. El LAP1242/LAP1131 admite arquitecturas P2P, P2MP y tipo de malla.

Asegúrese de leer la guía antes de intentar cualquiera de las instalaciones.

Este documento describe la implementación de la malla inalámbrica empresarial para la malla interior. Este documento permitirá a los usuarios finales inalámbricos entender los fundamentos de la malla interior, dónde configurar la malla interior y cómo configurar la malla interior. La malla interior es un subconjunto de la malla inalámbrica empresarial de Cisco implementado usando controladores inalámbricos y puntos de acceso ligeros.

La malla interior es un subconjunto de la arquitectura de malla empresarial implementada en la arquitectura Unified Wireless. La malla interior está en demanda hoy. Con la malla interior, una de las radios (normalmente 802.11b/g) y/o el link Ethernet cableado se utiliza para conectarse a los clientes, mientras que la segunda radio (normalmente 802.11a) se utiliza para redirigir el tráfico del cliente. La red de retorno puede ser un solo salto o a través de varios saltos. La malla interior le aporta estos valores:

- No tener que ejecutar cableado Ethernet a cada AP.
- No se requiere puerto de switch Ethernet para cada AP.
- Conectividad de red donde los cables no pueden proporcionar conectividad.
- Flexibilidad en la implementación: no se limita a 100 m de un switch Ethernet.
- Fácil implementación de una red inalámbrica ad-hoc.

Los comercios de gran tamaño se sienten muy atraídos por la malla interior debido a los ahorros en costes de cableado, así como por las razones mencionadas anteriormente.

Los especialistas en inventarios lo utilizan para realizar recuentos de inventario para minoristas, plantas de fabricación y otras empresas. Desean implementar rápidamente una red Wi-Fi temporal en el sitio del cliente para permitir la conectividad en tiempo real de sus dispositivos portátiles. Seminarios educativos, conferencias, fabricación y hospitalidad son algunos de los lugares donde se necesita una arquitectura de malla interior.

Cuando termine de leer esta guía, comprenderá dónde usar y cómo configurar la malla interior. También comprenderá que la malla interior en los recintos NEMA NO es un reemplazo de la malla exterior. Además, también comprenderá la superioridad de la malla interior sobre la flexibilidad de rol de link (malla de un solo salto) utilizada por los AP autónomos.

Suposiciones

Conozca la red inalámbrica unificada de Cisco, la arquitectura y los productos. Tiene conocimiento de los productos Cisco Outdoor Mesh y de algunos de los términos utilizados para

las redes de malla.

Glosario de acrónimos	
LWAPP	Lightweight Access Point Protocol - Protocolo de tunelización de datos y control entre los AP y el Wireless LAN Controller.
Controlador WLAN /Controlador /WLC	Controlador de LAN inalámbrica: dispositivos de Cisco que centralizan y simplifican la gestión de la red de una WLAN mediante el colapso de un gran número de terminales gestionados en un único sistema unificado, lo que permite un sistema de red WLAN de información inteligente y unificada.
RAP	Punto de acceso raíz/Punto de acceso de techo: los dispositivos inalámbricos de Cisco actúan como puente entre el controlador y otros AP inalámbricos. AP que se conectan al controlador.
MAP	AP de malla: dispositivo inalámbrico de Cisco que se conecta a un RAP o a un MAP por el aire en una radio 802.11a y también presta servicios a los clientes en una radio 802.11b/g.
Padre	Un AP (ya sea un RAP/MAP) que proporciona acceso a otros AP por el aire en una radio 802.11a.
Vecino	Todos los AP en una red de malla son vecinos y tienen vecinos. El RAP no tiene un vecino ya que está conectado al controlador.
Niño	Un AP más alejado del controlador es siempre un secundario. Un hijo tendrá un padre y muchos vecinos en una red de malla. Si el padre muere, se elegirá el vecino siguiente con el

	mejor valor de facilidad principal.
SNR	Relación señal-ruido
BGN	Nombre del grupo de puentes
EAP	Protocolo de autenticación extensible
PSK	Clave previamente compartida
AWPP	Adaptive Wireless Path Protocol

Overview

Cisco Indoor Mesh Network Access Point es un dispositivo de infraestructura Wi-Fi de dos radios para implementaciones interiores seleccionadas. Es un LWAPP (Lightweight Access Point Protocol) basado en el producto. Proporciona una radio de 2,4 GHz y una radio de 5,8 GHz compatible con los estándares 802.11b/g y 802.11a. Se puede utilizar una radio (802.11b/g) para el acceso local (cliente) para el AP y la segunda radio (802.11a) se puede configurar para la red de retorno inalámbrica. Proporciona una arquitectura de malla interior, donde los diferentes nodos (radios) se comunican entre sí a través de la red de retorno y también proporcionan acceso al cliente local. Este AP también se puede utilizar para arquitecturas de puente punto a punto y punto a multipunto. La solución Wireless Indoor Mesh Network es ideal para una amplia cobertura en interiores, ya que puede tener altas velocidades de datos y una buena fiabilidad con una infraestructura mínima. Estas son las características básicas salientes introducidas con la primera versión de este producto:

- Se utiliza en entornos interiores para un recuento de saltos de 3. Máximo 4.
- Nodo Relay y host para clientes de usuario final. Una radio 802.11a se utiliza como interfaz de red de retorno y una radio 802.11b/g para atender a los clientes.
- Seguridad de AP de malla interior - EAP y PSK soportados.
- Los MAP del LWAPP en un entorno de malla se comunican con los controladores de la misma manera que en los AP conectados a Ethernet.
- Puente inalámbrico punto a punto.
- Puente inalámbrico punto a multipunto.
- Selección primaria óptima. SNR, EASE y BGN
- Mejoras de BGN. NULL y modo predeterminado.
- Local Access (Acceso local).
- Lista negra principal. Lista de exclusión.
- Curación automática con AWPP.
- Puente Ethernet.
- Soporte básico de voz de la versión 4.0.
- Selección dinámica de frecuencia.
- Anticorrupción - Conmutación por error predeterminada de BGN y DHCP.

Nota: Estas funciones no se admitirán:

- Canal de seguridad pública de 4,9 GHz
- Routing alrededor de la interferencia

- Análisis de fondo
- Acceso universal
- Compatibilidad con puente de grupo de trabajo

Software de malla interior

Indoor Mesh Software es una versión especial ya que se concentra en los AP interiores, especialmente en la malla interior. En esta versión, tenemos los AP interiores funcionando en el modo local y también en el modo bridge. Algunas de las funciones disponibles en la versión 4.1.171.0 no se implementan en esta versión. Se han realizado mejoras en la interfaz de línea de comandos (CLI), la interfaz gráfica de usuario (GUI - navegador web) y en la propia máquina de estado. El objetivo de estas mejoras es obtener información valiosa desde su perspectiva sobre este nuevo producto y su viabilidad funcional.

Mejoras específicas de malla interior:

- **Entorno interior:** la malla interior se implementa con LAP1242s y LAP1131. Estos se implementan en entornos interiores donde el cable Ethernet no está disponible. La implementación es fácil y rápida para proporcionar una cobertura inalámbrica a áreas remotas dentro del edificio (por ejemplo, centros de distribución minorista, educación para seminarios/conferencias, fabricación, hostelería).
- **Mejoras en el nombre del grupo de puentes (BGN):** para permitir que un administrador de red organice una red de puntos de acceso de malla interiores en sectores específicos del usuario, Cisco proporciona un mecanismo llamado Nombre del grupo de puentes o BGN. El BGN, realmente el nombre del sector, hace que un AP se conecte a otros AP con el mismo BGN. En el caso de que un AP no encuentre un sector adecuado que coincida con su BGN, el AP funciona en el modo predeterminado y elige el mejor padre que responde al BGN predeterminado. Esta función ya ha recibido mucha apreciación del campo mientras lucha contra las condiciones de AP varadas (si alguien ha configurado mal el BGN). En la versión 4.1.171.0 del software, los AP, cuando utilizan el BGN predeterminado, no funcionan como un nodo de malla interior y no tienen acceso de cliente. Se encuentra en modo de mantenimiento para acceder a través del controlador, y si el administrador no arregla el BGN, el AP se reiniciará después de 30 minutos.
- **Mejoras de seguridad:** la seguridad en el código de malla interior está configurada de forma predeterminada para EAP (protocolo de autenticación extensible). Esto se define en RFC3748. Aunque el protocolo EAP no se limita a las LAN inalámbricas y se puede utilizar para la autenticación de LAN por cable, suele utilizarse en las LAN inalámbricas. Cuando EAP es invocado por un dispositivo NAS (servidor de acceso a la red) habilitado para 802.1X, como un punto de acceso inalámbrico 802.11 a/b/g, los métodos EAP modernos pueden proporcionar un mecanismo de autenticación seguro y negociar un PMK seguro (clave maestra por pares) entre el cliente y NAS. A continuación, se puede utilizar la PMK para la sesión de encriptación inalámbrica que utiliza la encriptación TKIP o CCMP (basada en AES). Antes de la versión 4.1.171.0 del software, los AP de malla exteriores utilizaban PMK/BMK para unirse al controlador. Este fue un proceso de tres ciclos. Ahora los ciclos se reducen para lograr una convergencia más rápida. El objetivo general de la seguridad de malla en interiores es proporcionar: Configuración sin intervención para el aprovisionamiento de seguridad. Privacidad y autenticación para tramas de datos. Autenticación mutua entre la red y los nodos. Capacidad de utilizar métodos EAP estándar para la autenticación de nodos AP de malla interiores. Desacoplamiento de LWAPP y seguridad de malla interior. Los mecanismos de detección, routing y sincronización se mejoran a partir de la arquitectura

actual para dar cabida a los elementos necesarios para admitir los nuevos protocolos de seguridad. Los AP de malla interior descubren otros AP de malla al escanear y escuchar las actualizaciones de vecinos gratuitas de otros AP de malla. Cualquier RAP o MAP interiores conectados a la red anuncia los parámetros de seguridad principales en sus tramas NEIGH_UPD (al igual que las tramas de baliza 802.11). Una vez que esta fase ha terminado, se establece un link lógico entre un AP de malla interior y un AP raíz.

- **Mejoras de WCS** Se han añadido alarmas de malla interior. Se pueden generar informes de malla en interiores que muestren el conteo de saltos, el peor SNR, etc. La prueba de enlace (de padre a hijo, de niño a padre) se puede ejecutar entre los nodos que muestran información muy inteligente. La información de AP mostrada es mucho más que las anteriores. Uno tiene la opción de ver también los vecinos potenciales. Se mejora la supervisión de la salud y se facilita el acceso a ella.

Hardware y software soportados

Existe un requisito mínimo de hardware y software para la malla interior:

- Los AP Cisco LWAPP AIR-LAP1242AG-A-K9 y AIR-LAP1131AG-A-K9 admiten la configuración de malla interior.
- El software Cisco Mesh Release 2 es compatible con Enterprise Mesh (productos interiores y exteriores). Esto se puede instalar solamente en Cisco Controller, Cisco 440x/210x y WISM.
- El software Cisco Enterprise Mesh Release 2 se puede descargar de Cisco.com.

Interior frente a exterior

Estas son algunas de las principales diferencias entre la malla interior y la exterior:

	Malla interior	Malla exterior
Entorno	SÓLO en interiores, con clasificación de hardware en interiores	SOLO en exteriores, hardware robusto
Hardware	AP en interiores con LAP1242 y LAP1131AG	AP exterior con LAP15xx y LAP152x
Niveles de potencia	2,4 Ghz:20 dbm 5,8 Ghz:17 dbm	2,4 Ghz:28 dbm 5,8 Ghz:28 dbm
Tamaños de células	Aprox. 150 pies	Aprox. 1000 pies
Altura de implementación	A 32 metros del suelo	A 30-40 pies del suelo

Configuración

Asegúrese de revisar detenidamente la guía antes de iniciar cualquier implementación,

especialmente si ha recibido nuevo hardware.

Modo de controlador L3

Los AP de malla interiores se pueden implementar como una red L3.



Actualización del controlador al último código

Complete estos pasos:

1. Para actualizar la versión 2 de malla en una red de malla interior, la red debe estar funcionando en la versión 4.1.185.0 o la versión 1 de malla, disponible en Cisco.com.
2. Descargue el código más reciente del controlador en su servidor TFTP. Desde la interfaz GUI del controlador, haga clic en **Comandos > Descargar archivo**.
3. Seleccione el tipo de archivo como **código** y asigne la dirección IP de su servidor TFTP. Defina la ruta y el nombre del archivo.



Nota: Utilice el servidor TFTP que admite más de 32 MB de transferencia de tamaño de archivo. Por ejemplo, **tftpd32**. En File path put **./** como se muestra.

4. Cuando haya terminado de instalar el nuevo firmware, utilice el comando **show sysinfo** en la CLI para verificar que el nuevo firmware esté instalado.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS

System Name..... CiscoMesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs

Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit
Number of VLANs..... 2
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 3

Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

Nota: Oficialmente, Cisco no soporta las Actualizaciones para los controladores.

Dirección MAC

Es obligatorio utilizar el filtrado MAC. Esta función ha convertido a la solución Cisco Indoor Mesh en un verdadero "toque cero". A diferencia de las versiones anteriores, la pantalla Malla ya no tendrá la opción MAC Filtering (Filtrado de MAC).



Nota: El filtrado de MAC está habilitado de forma predeterminada.

Grabar dirección MAC en las radios

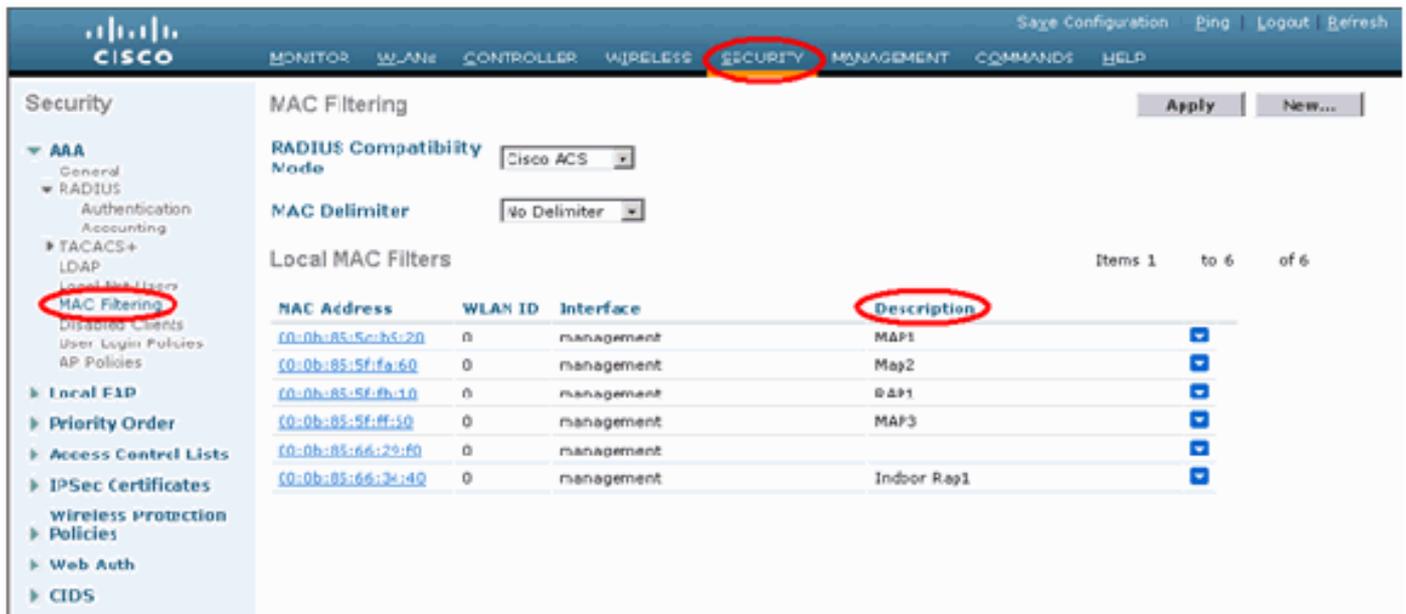
En un archivo de texto, registre las direcciones MAC de todas las radios AP de malla interiores que implemente en su red. La dirección MAC se puede encontrar en la parte posterior de los AP. Esto le ayuda a realizar futuras pruebas, ya que la mayoría de los comandos CLI requieren que se ingresen la dirección MAC de los AP o los nombres con el comando. También puede cambiar el nombre de los AP a algo más fácilmente recordado, como "construyendo número-pod número-AP tipo: últimos cuatro caracteres hexadecimales de dirección MAC".

Introduzca la dirección MAC y los nombres de las radios en el controlador

El controlador de Cisco mantiene una lista de direcciones MAC de autorización de AP en interiores. El controlador sólo responde a las solicitudes de detección de las radios interiores que aparecen en la lista de autorización. Introduzca las direcciones MAC de todas las radios que suele utilizar en la red del controlador.

En la interfaz GUI del controlador, vaya a **Seguridad** y haga clic en **filtrado MAC** en el lado

izquierdo de la pantalla. Haga clic en **Nuevo** para ingresar las direcciones MAC como se muestra aquí:



También, ingrese los nombres de las radios para mayor comodidad bajo **Descripción** (como ubicación, AP #, etc.) La descripción también se puede utilizar para el lugar en el que se han instalado las radios para facilitar la consulta en cualquier momento.

[Activar filtrado de MAC](#)

El filtrado de MAC está habilitado de forma predeterminada.

También se puede elegir el modo de seguridad como EAP o PSK en la misma página.

Desde la interfaz GUI del switch, utilice este trayecto:

Ruta de la interfaz GUI: **Inalámbrico > Malla interior**

El modo de seguridad SÓLO se puede verificar en la CLI mediante este comando:

(Cisco Controller) > **show network**

```
(Cisco Controller) >show network
RF-Network Name..... iMesh
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Ucast
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge Mac Filter Config..... Enable
Bridge Security Mode..... EAP
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
Apple Talk..... Disable
AP fallback..... Enable
--More-- of (quit)
Web Auth Redirect Ports..... 80
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

[Implementación de malla interior L3](#)

Para una red de malla interior L3, configure las direcciones IP para las radios si no pretende utilizar el servidor DHCP (interno o externo).

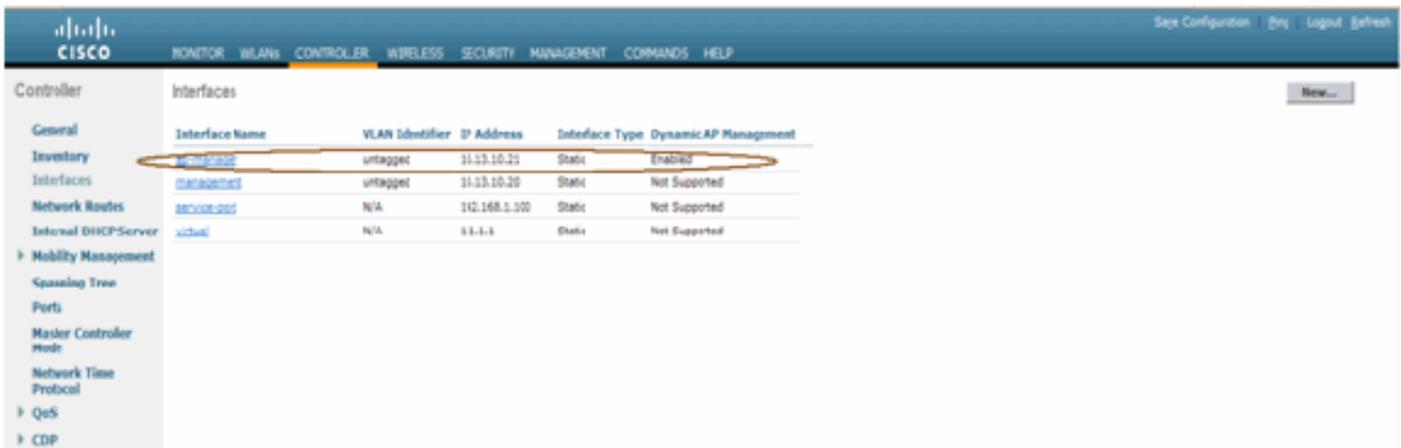
Para una red de malla interior L3, si desea utilizar el servidor DHCP, configure el controlador en modo L3. Guarde la configuración y reinicie el controlador. Asegúrese de configurar la opción 43 en el servidor DHCP. Después de que el controlador se haya reiniciado, los AP recién conectados recibirán su dirección IP del servidor DHCP.

Definir interfaces en controlador

Administrador de AP

Para una implementación L3, debe definir el **administrador AP**. El administrador AP actúa como una dirección IP de origen para la comunicación del controlador a los AP.

Ruta: **Controlador > Interfaces > administrador de ap > editar.**



The screenshot shows the Cisco Controller web interface. The 'Controller' menu is open, and the 'Interfaces' section is selected. A table lists the configured interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.13.10.21	Static	Enabled
management	untagged	10.13.10.20	Static	Not Supported
service-port	N/A	10.168.1.100	Static	Not Supported
vlan1	N/A	11.1.1	Static	Not Supported

A la interfaz **AP-manager** se le debe asignar una dirección IP en la misma subred y VLAN que a su interfaz de administración.



The screenshot shows the configuration page for the 'ap-manager' interface. The 'Interfaces > Edit' page is displayed with the following fields:

- General Information:** Interface Name: ap-manager; MAC Address: 00:18:73:34:4b:63
- Interface Address:** VLAN Identifier: 0; IP Address: 10.13.10.21; Netmask: 255.255.255.0; Gateway: 10.13.10.10
- Physical Information:** Port Number: 1; Backup Port: 0; Active Port: 1; Enable Dynamic AP Management:
- DHCP Information:** Primary DHCP Server: 10.13.10.10; Secondary DHCP Server: (empty)
- Access Control List:** ACL Name: none

Note: Changing the interface parameters causes the VLANs to be temporarily disabled and this may result in loss of connectivity for some clients.

Funciones de radio

Esta solución ofrece dos funciones principales de radio:

- Punto de acceso raíz (RAP): la radio con la que desea conectarse al controlador (a través del switch) asumirá la función de RAP. Los RAP tienen una conexión con cable y con LWAPP habilitado al controlador. Un RAP es un nodo primario para cualquier conexión en puente o red de malla interior. Un controlador puede tener uno o más RAP, cada uno de los cuales forma parte de las mismas redes inalámbricas o diferentes. Puede haber más de un RAP para la misma red de malla interior para la redundancia.
- Punto de acceso de malla interior (MAP): la radio que no tiene conexión con cables al controlador asume el papel de punto de acceso de malla interior. Este AP se llamaba anteriormente Pole top AP. Los MAP tienen una conexión inalámbrica (a través de la interfaz de red de retorno) a tal vez otros MAP y finalmente a un RAP y por lo tanto al controlador. Los MAP también pueden tener una conexión Ethernet con cables a una LAN y servir como punto final de puente para esa LAN (usando una conexión P2P o P2MP). Esto puede ocurrir simultáneamente, si se configura correctamente como un puente Ethernet. MAPs service clients en la banda no utilizados para la interfaz de red de retorno.

El modo predeterminado para un AP es MAP.

Nota: Las funciones de radio se pueden establecer mediante GUI o CLI. Los AP se reiniciarán después del cambio de rol.

Nota: Puede utilizar la CLI del controlador para preconfigurar los roles de radio en un AP siempre que el AP esté conectado físicamente al switch o puede ver el AP en el switch como un RAP o un MAP.

```
(Cisco Controller) >config ap role ?
rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?
<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Nombre del grupo de puentes

Bridge Group Names (BGN) controla la asociación de los AP. Los BGN pueden agrupar lógicamente las radios para evitar que dos redes del mismo canal se comuniquen entre sí. Esta configuración también es útil si tiene más de un RAP en su red en el mismo sector (área). El BGN es una cadena de diez caracteres como máximo.

Se asigna un nombre de grupo de puentes establecido de fábrica en la etapa de fabricación (VALOR NULO). No es visible para usted. Como resultado, incluso sin un BGN definido, las radios aún pueden unirse a la red. Si tiene dos RAP en su red en el mismo sector (para mayor capacidad), se recomienda que configure los dos RAP con el mismo BGN, pero en diferentes canales.

Nota: El nombre del grupo de puentes se puede establecer desde la CLI y la GUI del controlador.

```
(Cisco Controller) >config ap bridgegroupname set ?  
<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Después de configurar el BGN, el AP se reiniciará.

Nota: El BGN debe configurarse con mucho cuidado en una red activa. Siempre debe comenzar desde el nodo más lejano (último nodo) y avanzar hacia el RAP. La razón es que si comienza a configurar el BGN en algún lugar del centro del multisalto, los nodos más allá de este punto se caerán ya que estos nodos tendrán un BGN diferente (BGN antiguo).

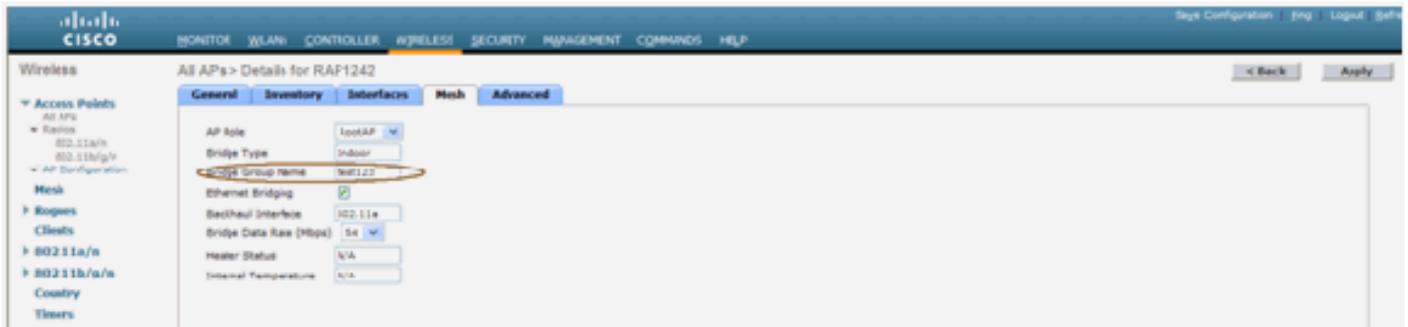
Puede verificar el BGN ejecutando este comando CLI:

```
(Cisco Controller) > show ap config general
```

```
(Cisco Controller) >show ap config general RAP1242  
Cisco AP Identifier..... 0  
Cisco AP Name..... RAP1242  
Country code..... US - United States  
Regulatory Domain allowed by Country..... 802.11bg:-AR 802.11a:-A2  
AP Country code..... US - United States  
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A  
Switch Port Number ..... 1  
MAC Address..... 00:18:74:fa:7d:1f  
IP Address Configuration..... DHCP  
IP Address..... 10.13.13.11  
IP NetMask..... 255.255.255.0  
Gateway IP Addr..... 10.13.13.10  
Cisco AP Location..... default location  
Cisco AP Group Name..... default-group  
Primary Cisco Switch..... J2106-1  
Secondary Cisco Switch.....  
Tertiary Cisco Switch.....  
Administrative State ..... ADMIN_ENABLED  
Operation State ..... REGISTERED  
Mirroring Mode ..... Disabled  
AP Mode ..... Bridge  
--More-- or (q)uit  
AP Role ..... RootAP  
Ethernet Bridging ..... Enabled  
Bridge Group Name ..... test123  
Public Safety ..... Disabled  
Remote AP Debug ..... Disabled  
S/W Version ..... 4.1.175.19  
Boot Version ..... 12.3.7.1  
Mini IOS Version ..... 3.0.51.0  
Stats Reporting Period ..... 180  
LED State..... Enabled  
PoE Pre-Standard Switch..... Disabled  
PoE Power Injector MAC Addr..... Disabled  
Number Of Slots..... 2  
AP Model..... AIR-LAP1242AG-A-K9  
IOS Version..... 12.4(20070808:082741)  
Reset Button..... Enabled  
AP Serial Number..... FTX1035B3RH  
AP Certificate Type..... Manufacture Installed  
Management Frame Protection Validation..... Disabled  
Console Login Name.....  
Console Login State..... Unknown  
AP Up Time..... 0 days, 02 h 43 m 38 s  
AP LWAPP Up Time..... 0 days, 02 h 42 m 43 s  
--More-- or (q)uit  
Join Date and Time..... Sun Aug 19 11:59:07 2007  
Join Taken Time..... 0 days, 00 h 00 m 24 s  
Ethernet Port Duplex..... Unknown  
Ethernet Port Speed..... Unknown
```

Además, puede configurar o verificar el BGN usando la GUI del controlador:

Ruta: Inalámbrico > Todos los AP > Detalles.



Puede ver que la información ambiental del AP también se muestra con esta nueva versión.

Configuración de Seguridad

El modo predeterminado de seguridad de malla interior es EAP. Esto significa que a menos que configure estos parámetros en su controlador, sus MAP no se unirán a:



CLI de configuración EAP de malla interior

```
(Cisco Controller) >config mesh local-auth enable
enable Local Auth

(Cisco controller) >config advanced eap ?
identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Si necesita permanecer en el modo PSK, utilice este comando para volver al modo PSK:

```
(Cisco Controller) >config mesh security psk ?
(Cisco Controller) >config mesh security psk

All Mesh AP will be rebooted
Are you sure you want to start? (y/N)n
```

Comandos show EAP de malla interior

Dentro del modo EAP, puede verificar estos comandos **show** para verificar la autenticación MAP:

(Cisco Controller) >show network

```
RF Network Name..... jaggi123
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Mcast 224.1.1.1
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Enable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Disable
Bridge Security Mode..... EAP otherwise PSK
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
AP Fallback..... Enable
Web Auth Redirect Ports..... 80
--More-- or (q)uit
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

(Cisco Controller) >show wlan 0

(Cisco Controller) >show wlan 0

```
WLAN Identifier..... 0
Profile Name..... Mesh_profile
Network Name (SSID)..... Mesh_ssid
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 2
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIE Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
--More-- or (q)uit
IPv6 Support..... Disabled
Radio Policy..... All
Local EAP Authentication..... Enabled (Profile 'prfMaP1500LEAuth93')
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1x..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Disabled
    WPA2 (RSN IE)..... Enabled
    TKIP Cipher..... Disabled
    AES Cipher..... Enabled
    Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
  CKIP..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
--More-- or (q)uit
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List
WLAN ID      IP Address      Status
```

(Cisco Controller) >show local-auth config

```
(Cisco Controller) >show local-auth config
User credentials database search order:
  Primary ..... Local DB
Timer:
  Active timeout ..... 300
Configured EAP profiles:
EAP Method configuration:
  EAP-FAST:
    Server key ..... <hidden>
    TTL for the PAC ..... 10
    Anonymous provision allowed ..... Yes
    Authority ID ..... 436973636f000000000000000000000000
    Authority Information ..... Cisco A-ID
(Cisco Controller) >show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 2
```

```
(Cisco Controller) >show advanced eap
```

Comandos de depuración EAP de malla interior

Para depurar cualquier problema de modo EAP, utilice estos comandos en el controlador:

```
(Cisco Controller) >debug dot1x all enable
(Cisco Controller) >debug aaa all enable
```

Instalación

Requisitos previos

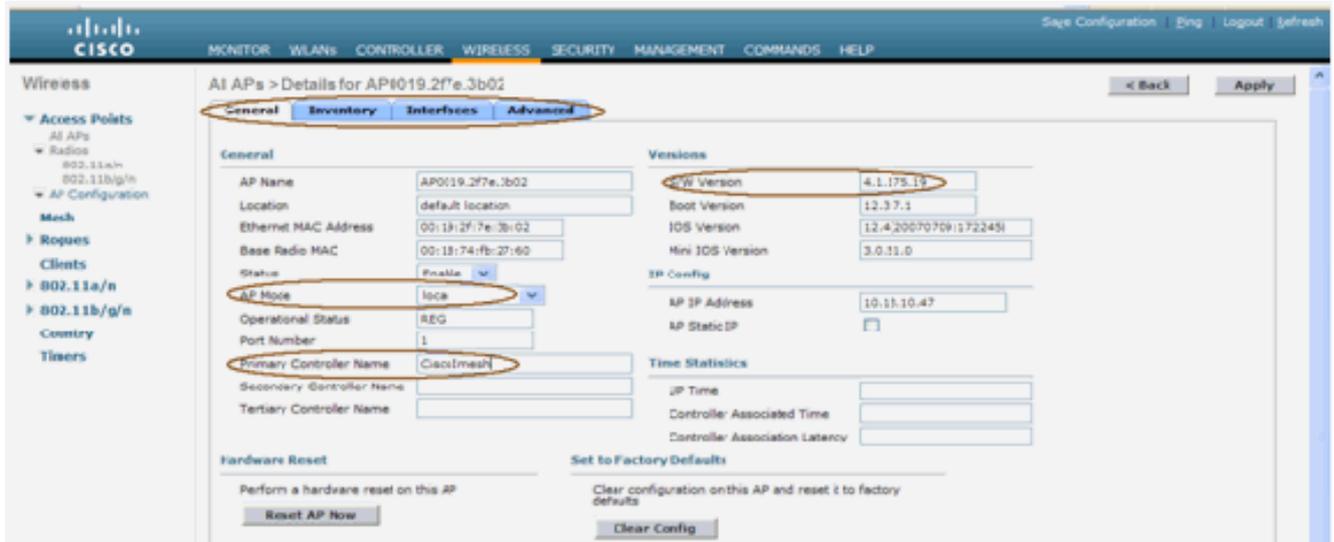
El controlador debe estar ejecutando la versión recomendada del código. Haga clic en **Monitor** para verificar la versión de Software. Lo mismo se puede verificar a través de CLI.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS
System Name..... CiscoMesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs
Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C
State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit..... 2
Number of VLANs..... Disabled
3rd Party Access Point Support..... 3
Number of Active Clients.....
Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

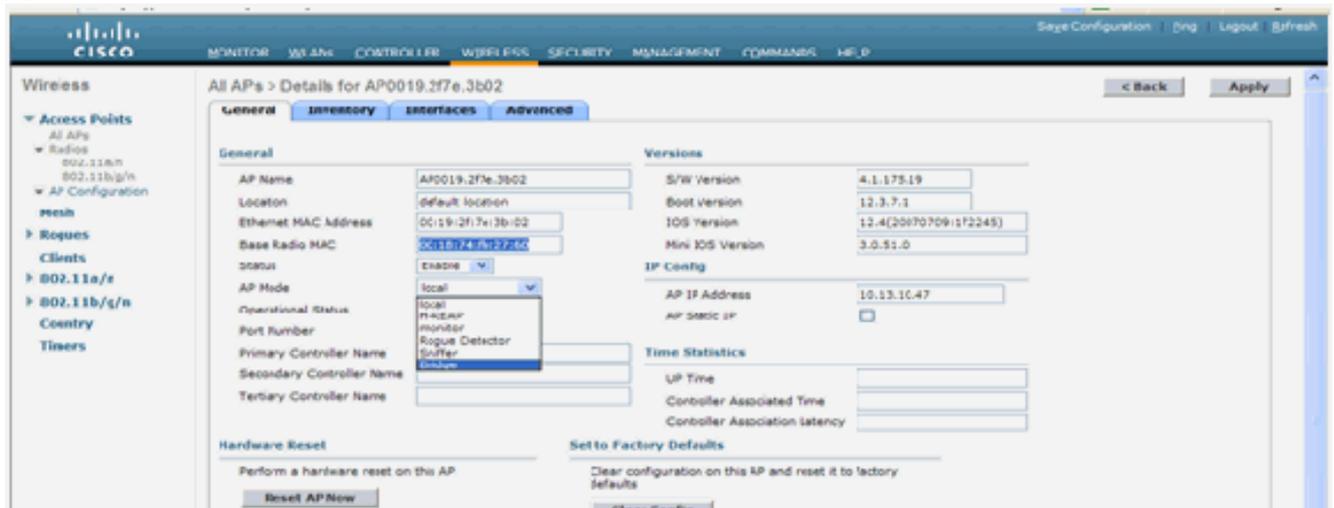
Los sistemas como el servidor DHCP, el servidor ACS y el servidor WCS deben ser accesibles.

Instalación

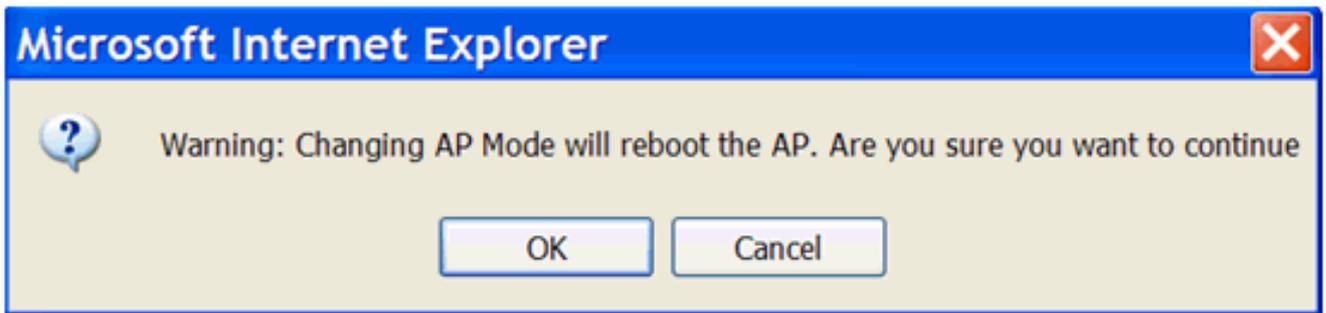
1. Conecte todos los LAP (1131AG/1242AG) a una red de capa 3 en la misma subred que la dirección IP de administración. Todos los AP se unirán al controlador como APs en el Modo Local. En este modo, priorice los AP con el nombre del controlador principal, el nombre del controlador secundario y un nombre del controlador terciario.



2. Capture la dirección MAC de radio base del AP (por ejemplo, 00:18:74:fb:27:60).
3. Agregue la dirección MAC del AP para que el AP se una en el modo bridge.
4. Haga clic en **Seguridad > filtrado de MAC > Nuevo**.
5. Agregue la dirección MAC copiada y asigne un nombre a los AP en la lista de filtros MAC y en la lista AP.
6. Elija **Bridge** de la lista Modo AP.



7. Le pedirá que confirme, ya que esto reiniciará el AP.



8. El AP se reiniciará y se unirá al controlador en el modo Bridge. La nueva ventana AP tendrá una pestaña extra: MESH. Haga clic en la pestaña **MESH** para verificar la función, el tipo de puente, el nombre del grupo de puentes, la conexión en puente Ethernet, la interfaz de red de retorno, la velocidad de datos del puente, etc.



9. En esta ventana, acceda a la lista de roles de AP y elija el rol relevante. En este caso, la función de forma predeterminada es un MAP. El nombre del grupo de puentes está vacío de forma predeterminada. La interfaz de retorno es 802.11a. La velocidad de transferencia de datos del puente (es decir, la velocidad de transferencia de datos) es de 24 Mbps.
10. Conecte el AP que desea como RAP al controlador. Implemente las radios (MAP) en las ubicaciones deseadas. Encienda las radios. Debería poder ver todas las radios en el controlador.

```
(Cisco Controller) >show ap summ
number of APs..... 3
AP Name           Slots  AP Model          Ethernet MAC      Location          Port  Country
-----
RAP1242           2      AIR-LAP1242AG-A-K9  00:18:74:fa:7d:1f default location  1      US
LAP1242-1         2      AIR-LAP1242AG-A-K9  00:1b:2b:a7:ad:bf default location  1      US
LAP1242-2         2      AIR-LAP1242AG-A-K9  00:14:1b:59:07:af default location  1      US
```

11. Intente tener condiciones de línea de visión entre los nodos. Si no existen condiciones de línea de visión, cree autorizaciones de zona de Fresnel para obtener condiciones de línea de sitio cercana.
12. Si tiene más de un controlador conectado a la misma red de malla interior, debe especificar el nombre del controlador primario en cada nodo. De lo contrario, el controlador que se ve primero se tomará como el primario.

Configuración de alimentación y canal

El canal de retorno se puede configurar en un RAP. Los MAP se ajustarán al canal RAP. El acceso local se puede configurar independientemente para los MAP.

En la GUI del switch, siga la ruta: **Inalámbrico > radio 802.11a > configurar**.



Nota: El nivel de potencia Tx predeterminado en la red de retorno es el nivel de potencia más alto (Nivel 1) y la administración de recursos de radio (RRM) está desactivada de forma predeterminada.

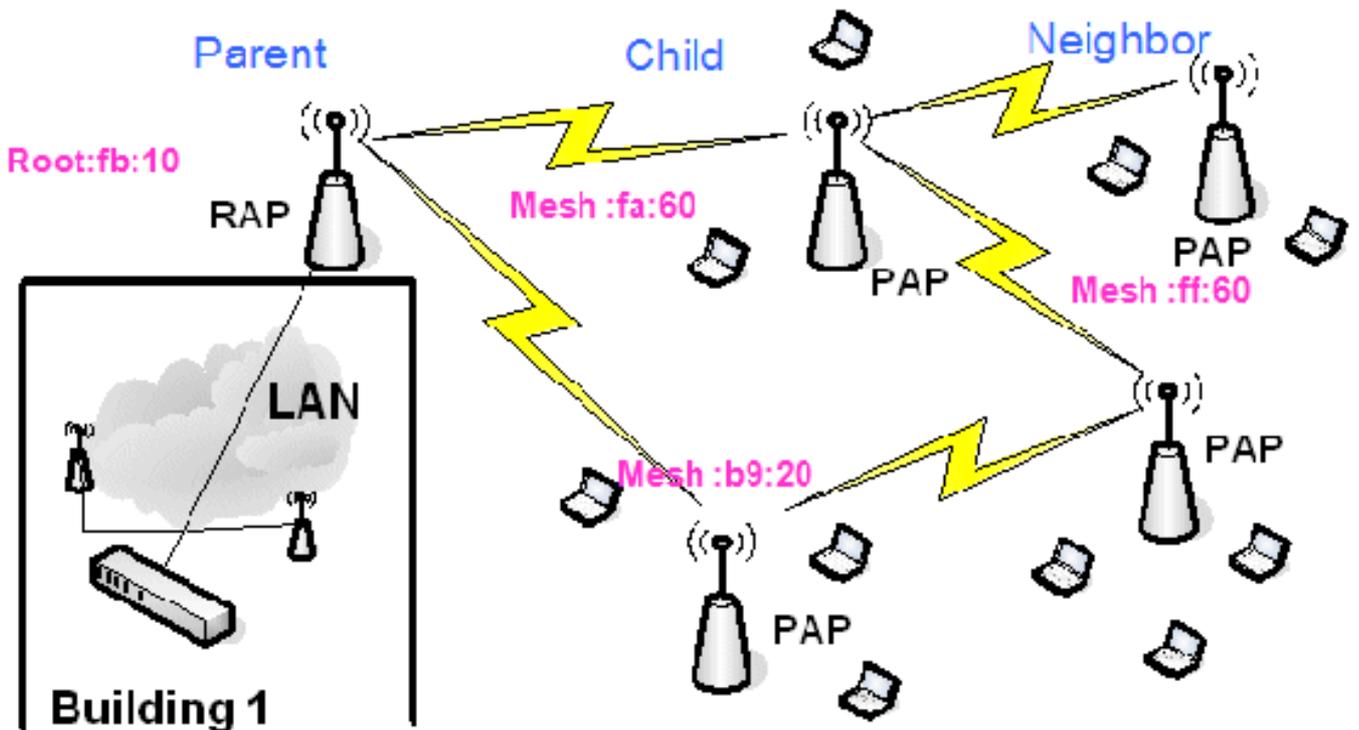
Si está recolocando RAP, le recomendamos que utilice canales adyacentes alternativos en cada RAP. Esto reducirá la interferencia del canal conjunto.

Comprobación de RF

En una red de malla interior debemos verificar la relación principal-secundario entre los nodos. **Hop** es un link inalámbrico entre las dos radios. La relación principal-hijo cambia a medida que se desplaza por la red. Depende de dónde esté en la red de malla interior.

La radio más cercana al controlador en una conexión inalámbrica (salto) es un **padre** de la radio en el otro lado del salto. En un sistema de salto múltiple hay una estructura de tipo árbol donde el nodo conectado al controlador es un RAP (**principal**). El nodo inmediato en el otro lado del primer salto es un **secundario**, y los nodos subsiguientes en el segundo salto hacia adelante son los **Vecinos** para ese padre en particular.

Figura 1: Red de dos saltos



En la Figura 1, los nombres de AP se mencionan por conveniencia. En la siguiente captura de pantalla, el **RAP(fb:10)** está siendo investigado. Este nodo puede ver (en la implementación real) los AP de malla interior (**fa:60** y **b9:20**) como hijos y **MAP ff:60** como vecinos.

Desde la interfaz GUI del switch, siga el trayecto: **Inalámbrico > Todos los AP > Rap1 > Información del Vecino**.



Asegúrese de que las relaciones padre-hijo se establecen y mantienen correctamente para su red de malla interior.

Verificar las Interconexiones

show Mesh es un comando informativo para verificar la interconectividad en su red.

Debe proporcionar estos comandos en cada nodo (AP) mediante la CLI del controlador y cargar los resultados en un archivo de texto o de Word en el sitio de carga.

```
(Cisco Controller) >show mesh ?
env          Show mesh environment.
neigh       Show AP neigh list.
path       Show AP path.
stats      Show AP stats.
secbh-stats Show Mesh AP secondary backhaul stats.
per-stats  Show AP Neighbor Packet Error Rate stats.
queue-stats Show AP local queue stats.
security-stats Show AP security stats.
config     Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access Show mesh backhaul with client access.
public-safety Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac        Show mesh cac.
```

En su red de malla interior, elija un link de salto múltiple y ejecute estos comandos comenzando desde el RAP. Cargue el resultado de los comandos en el sitio de carga.

En la siguiente sección, se han ejecutado todos estos comandos para la red de malla interior de dos saltos que se muestra en la figura 1.

[Mostrar ruta de malla interior](#)

Este comando le mostrará las direcciones MAC, las funciones de radio de los nodos, las relaciones señal-ruido en dBs para enlace ascendente/descendente (SNRUp, SNRDown) y el SNR de enlace en dB para una ruta determinada.

```
(Cisco Controller) >show mesh path RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
RAP1242 is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-1 56 29 29 27 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 56 41 32 34 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 is a Root AP.
```

[Mostrar resumen de vecino de malla interior](#)

Este comando le mostrará las direcciones MAC, las relaciones padre-hijo y los SNR de link ascendente/descendente en dB.

```
(Cisco Controller) >show mesh neigh ?
detail      Show Link rate neigh detail.
summary     Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh summary RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 0 0 0 0x860 BEACON
LAP1242-1 56 0 33 0 0x960 CHILD BEACON

(Cisco Controller) >show mesh neigh summary LAP1242-1
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 30 29 28 0x961 UPDATED CHILD BEACON
RAP1242 56 43 46 31 0x86b UPDATED NEIGH PARENT BEACON
```

Para este momento, debe poder ver las relaciones entre los nodos de su red y verificar la conectividad de RF mediante la visualización de los valores SNR para cada link.

Seguridad de acceso a la consola AP

Esta función proporciona una seguridad mejorada al acceso a la consola del AP. Se necesita un cable de consola para el AP para utilizar esta función.

Estos son compatibles:

- CLI para enviar la combinación user-id/password al AP especificado:

```
(Cisco Controller) >config ap username Cisco password Cisco ?
all          Configures the Username/Password for all connected APs.
<Cisco AP>  Enter the name of the Cisco AP.
```

- Un comando CLI para enviar la combinación nombre de usuario/contraseña a todos los AP registrados al controlador:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

Con estos comandos, la combinación userid/password enviada desde el controlador es persistente a través de la recarga en los AP. Si se borra un AP del controlador, no hay modo de acceso de seguridad. El AP genera una trampa SNMP con un login exitoso. El AP también generará una trampa SNMP en una falla de login de consola durante tres veces consecutivas.

Puente Ethernet

Por razones de seguridad, el puerto Ethernet en los MAP está inhabilitado de forma predeterminada. Sólo se puede habilitar configurando el puente Ethernet en el RAP y los respectivos MAP.

Como resultado, Ethernet Bridging debe estar habilitado para dos escenarios:

- Cuando desea utilizar los nodos de malla interiores como puentes.
- Cuando desee conectar cualquier dispositivo Ethernet (como PC/portátil, cámara de vídeo, etc.) en el MAP mediante su puerto Ethernet.

Ruta: **Wireless** > Click any AP > **Mesh**.



Hay un comando CLI que se puede utilizar para configurar la distancia entre los nodos que realizan el Bridging. Intente conectar un dispositivo Ethernet como una cámara de vídeo en cada salto y vea el rendimiento.

Mejora del nombre del grupo de puentes

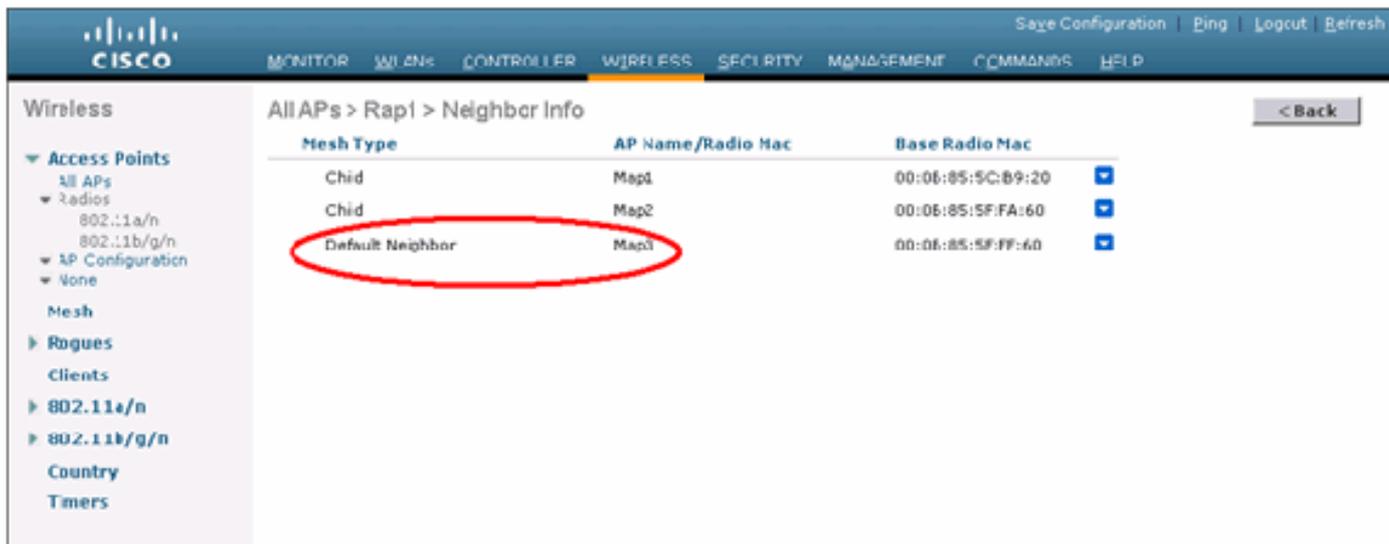
Es posible que un AP se aprovisione erróneamente con un "bridgegroupname" para el cual no estaba destinado. Dependiendo del diseño de la red, este AP puede o no ser capaz de alcanzar y encontrar su sector/árbol correcto. Si no puede alcanzar un sector compatible, puede quedar varado.

Para recuperar tal AP varado, el concepto de bridgegroupname 'predeterminado' se introdujo con el código 3.2.xx.x. La idea básica es que un AP que no puede conectarse a ningún otro AP con su bridgegroupname configurado, intenta conectarse con "default" (la palabra) como bridgegroupname. Todos los nodos que ejecutan el software 3.2.xx.x y posteriores aceptan otros nodos con este bridgegroupname.

Esta función también puede ayudar a agregar un nuevo nodo o un nodo configurado incorrecto a una red en ejecución.

Si tiene una red en ejecución, tome un AP preconfigurado con un BGN diferente y hágalo unirse a la red. Verá este AP en el controlador usando el BGN "predeterminado" después de agregar su dirección MAC en el controlador.

```
(CiscoController) >show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



The screenshot shows the Cisco Wireless LAN Controller GUI. The navigation menu on the left includes 'Wireless', 'Access Points', 'Radios', 'AP Configuration', 'Mesh', 'Rogues', 'Clients', '802.11a/n', '802.11b/g/n', 'Country', and 'Timers'. The main content area is titled 'All APs > Rap1 > Neighbor Info'. It contains a table with the following data:

Mesh Type	AP Name/Radio Mac	Base Radio Mac
Child	Map1	00:0E:85:5C:89:20
Child	Map2	00:0E:85:5F:FA:60
Default Neighbor	Map3	00:0E:85:5F:FF:60

El AP que utiliza el BGN predeterminado puede actuar como un AP de malla interior normal asociando clientes y formando relaciones secundarias de malla interior .

En el momento en que este AP usando el BGN predeterminado encuentre otro padre con el BGN correcto, se lo conmutará.

Registros - Mensajes, Sys, AP y Trampa

Registros de mensajes

Habilite el nivel de informes para los registros de mensajes. Desde la CLI del controlador, ejecute este comando:

```
(Cisco Controller) >config msglog level ?
critical      Critical hardware or software Failure.
error         Non-Critical software error.
security      Authentication or security related error.
warning       Unexpected software events.
verbose       Significant system events.

(Cisco Controller) >config msglog level verbose
```

Para ver los registros de mensajes, ejecute este comando desde la CLI del controlador:

```
(Cisco Controller) >show msglog

Message Log Severity Level ..... VERBOSE
Mon Jul 11 01:42:08 2005 [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul 8 06:12:02 2005 [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul 8 05:40:15 2005 [ERROR] spam_tmr.c 501: Did not receive heartbeat reply
from AP 00:0b:85:0e:05:80
Fri Jul 8 05:38:45 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:05:80
Fri Jul 8 05:38:40 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:14:00
Fri Jul 8 05:38:40 2005 Previous message occurred 5 times
Fri Jul 8 05:33:54 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:05:80
Fri Jul 8 05:32:23 2005 [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul 8 05:32:17 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul 8 05:32:17 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul 8 05:32:16 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul 8 05:32:16 2005 Previous message occurred 2 times
Fri Jul 8 05:31:19 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake cal
```

Para cargar los registros de mensajes, utilice la interfaz GUI del controlador:

1. Haga clic en **Comandos > Cargar**.



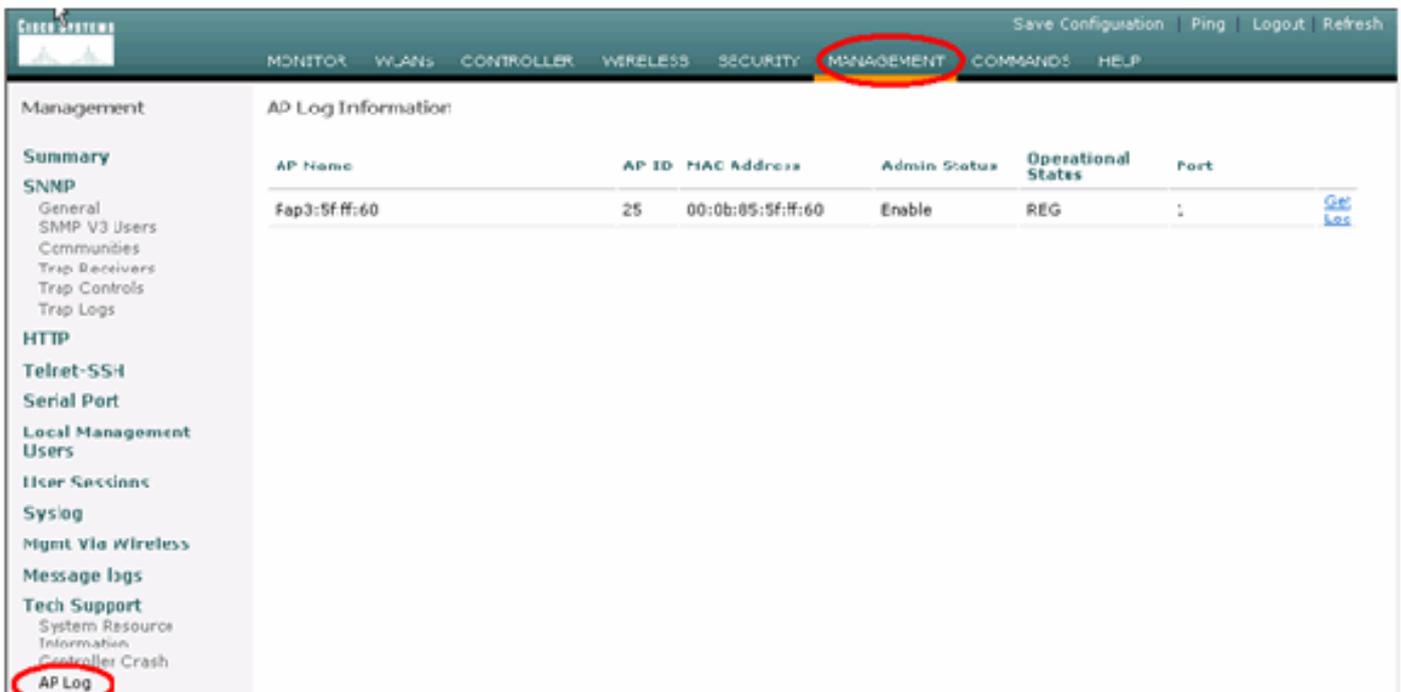
2. Introduzca la información del servidor TFTP. Esta página le dará varias opciones para cargar y desea que se envíen estos archivos: Registro de mensajes, Registro de eventos, Registro de trampa, Archivo de bloqueo (si lo hay). Para verificar los archivos Crash, haga clic en

Management > Controller Crash.



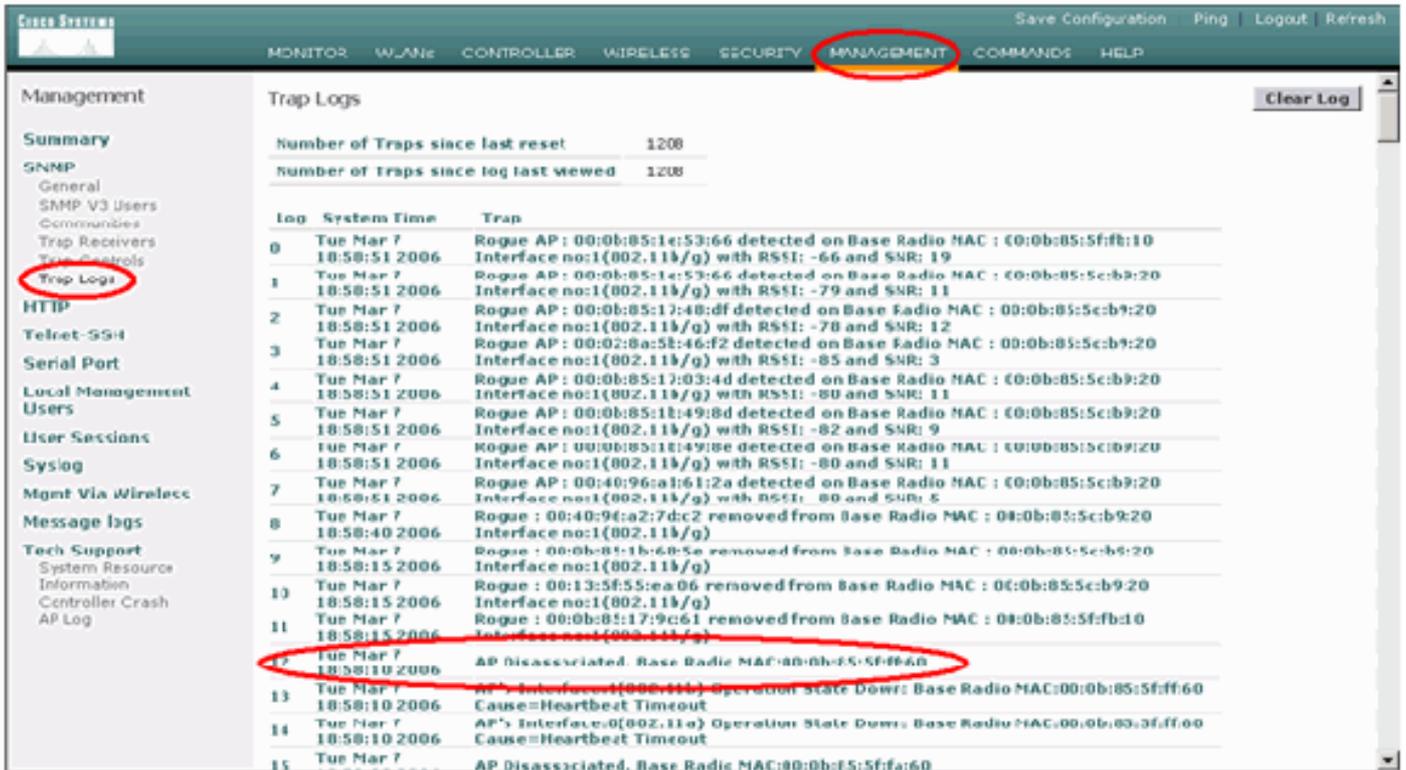
Registros de AP

Vaya a esta página de la GUI en el controlador para verificar los registros AP para su AP local, si lo hubiera:



Registros de trampa

Vaya a esta página GUI del controlador y verifique los registros de trampa:



Rendimiento

Prueba de convergencia de inicio

La convergencia es el tiempo que toma un RAP/MAP para establecer una conexión LWAPP estable con un controlador WLAN a partir del momento en que se inició por primera vez como se indica aquí:

Prueba de convergencia	Tiempo de convergencia (min:sec)			
	RAP	MAP1	MAP2	MAP3
Actualización de imagen	2:34	3:50	5:11	6:38
Reinicio del controlador	0:38	0:57	1:12	1:32
Encienda la red de malla interior	2:44	3:57	5:04	6:09
reinicio de RAP	2:43	3:57	5:04	6:09
Reincorporación de MAP		3:58	5:14	6:25
Cambio de MAP del primario (mismo canal)		0:38		

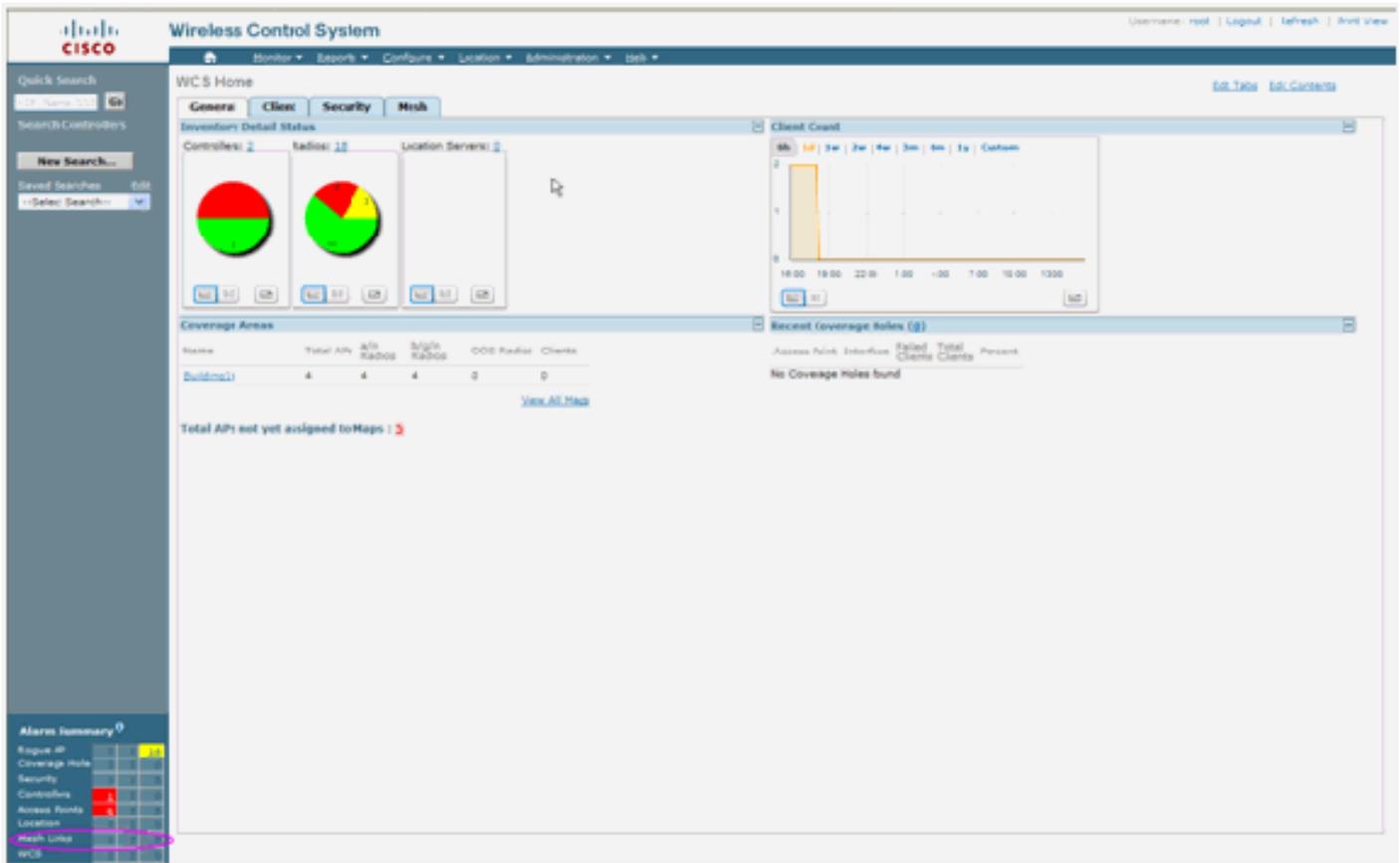
WCS

Alarmas de malla interior

WCS generará estas alarmas y eventos relacionados con la red de malla interior basándose en las trampas del controlador:

- SNR de link deficiente
- Primario cambiado
- Elemento secundario desplazado
- MAP cambia de padre con frecuencia
- Evento de puerto de consola
- Falla de Autorización MAC
- Fallos de autenticación
- Elemento secundario excluido

Haga clic en **Enlaces de malla**. Mostrará todas las alarmas relacionadas con los links de malla interiores.



Estas alarmas se aplican a los links de malla interiores:

- SNR de link deficiente - Esta alarma se genera si el link SNR cae por debajo de 12db. El usuario no puede cambiar este umbral. Si se detecta un SNR deficiente en el link de red de retorno para el elemento secundario/primario, se generará la trampa. La trampa contendrá el valor SNR y las direcciones MAC. La gravedad de la alarma es mayor. La relación SNR (señal-ruido) es importante porque la alta potencia de la señal no es suficiente para garantizar un buen rendimiento del receptor. La señal entrante debe ser más fuerte que cualquier ruido o interferencia presente. Por ejemplo, es posible tener una alta potencia de señal y seguir teniendo un rendimiento inalámbrico deficiente si hay una interferencia fuerte o un nivel de ruido alto.
- Padre cambiado: esta alarma se genera cuando el hijo se mueve a otro padre. Cuando se pierde el padre, el hijo se une a otro padre y el hijo envía una trampa que contiene las direcciones MAC del padre antiguo y del padre nuevo a WCS. Gravedad de la alarma: Informativo.
- Elemento secundario movido: esta alarma se genera cuando WCS recibe una trampa

perdida. Cuando el AP primario detectó la pérdida de un hijo y no pudo comunicarse con ese hijo, enviará una trampa perdida de Child a WCS. La trampa contendrá la dirección MAC secundaria. Gravedad de la alarma: Informativo.

- MAP parent ha cambiado con frecuencia - Esta alarma se genera si Indoor Mesh AP cambia su padre con frecuencia. Cuando MAP parent-change-counter excede el umbral dentro de una duración determinada, enviará una trampa a WCS. La trampa contendrá el número de veces que se realizan los cambios de MAP y la duración del tiempo. Por ejemplo, si hay 5 cambios en el plazo de 2 minutos, se enviará la trampa. Gravedad de la alarma: Informativo.
- Elemento principal secundario excluido: esta alarma se genera cuando un elemento secundario pone en la lista negra a un padre. Un hijo puede poner en la lista negra a un padre cuando el hijo no pudo autenticarse en el controlador después de un número fijo de intentos. El elemento secundario recuerda el elemento primario de la lista negra y cuando el elemento secundario se une a la red, enviará la trampa que contiene la dirección MAC principal de la lista negra y la duración del período de la lista negra.

Alarmas que no sean eslabones de malla interiores:

- Acceso al puerto de la consola - El puerto de la consola proporciona al cliente la capacidad de cambiar el nombre de usuario y la contraseña para recuperar el AP exterior varado. Sin embargo, para evitar cualquier acceso de usuario autorizado al AP, WCS necesita enviar una alarma cuando alguien intenta iniciar sesión. Esta alarma es necesaria para proporcionar protección ya que el AP es físicamente vulnerable mientras se encuentra en el exterior. Esta alarma se generará si el usuario ha iniciado sesión correctamente en el puerto de la consola AP, o si ha fallado tres veces consecutivas.
- MAC Authorization Failure - Esta alarma se genera cuando AP intenta unirse a la malla interior pero no autentica porque no está en la lista de filtros MAC. WCS recibirá una trampa del controlador. La trampa contendrá la dirección MAC del AP que falló la autorización.

[Informe y estadísticas de malla](#)

Transmitimos el marco mejorado de informes y estadísticas desde el 4.1.185.0:

- No hay ruta alternativa
- Saltos de nodo de malla
- Estadísticas de error de paquetes
- Estadísticas de paquetes
- Peor salto de nodo
- Los peores links SNR

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

Mesh No Alternate Parent

-- Select a command -- GO

Report Title	Schedule	Last Run Time	Next Scheduled Run
<input type="checkbox"/> test	Disabled		Run Now

Mesh Reports

Mesh No Alternate Parent

Mesh Node Hops

Mesh Packet Error Stats

Mesh Packet Stats

Mesh Worst Node Hops

Mesh Worst SNR Links

Alarm Summary

Rogue AP	0	0	191
Coverage Hole	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	0	0	2
Mesh Links	0	0	0
Location	0	0	0

No hay ruta alternativa

El AP de malla interior normalmente tiene más de un vecino. En el caso de que un AP de malla interior pierda su link principal, el AP debería ser capaz de encontrar el padre alternativo. En algún caso, si no se muestra ningún vecino, entonces el AP no podrá ir a otros padres si pierde a sus padres. Es fundamental que el usuario sepa qué AP no tienen padres alternativos. Este informe enumera todos los AP que no tienen otros vecinos que no sean el padre actual.

Salto del nodo de malla interior

Este informe muestra el número de saltos alejados del AP raíz (RAP). Puede crear el informe basándose en estos criterios:

- AP por controlador
- AP por planta

Tasas de errores de paquetes

Los errores de paquetes pueden ser causados por interferencias y caídas de paquetes. El cálculo de la velocidad de error del paquete se basa en los paquetes enviados y los paquetes enviados correctamente. La tasa de error del paquete se mide en el link de retorno y se recopila tanto para los vecinos como para el primario. El AP envía periódicamente información del paquete al controlador. Tan pronto como el padre cambia, el AP envía la información de error de paquete recolectada al controlador. WCS sondea la información de error del paquete del controlador cada 10 minutos de forma predeterminada y la almacena en la base de datos durante un máximo de 7 días. En WCS, la velocidad de error del paquete se muestra como un gráfico. El gráfico de errores de paquetes se basa en los datos históricos almacenados en la base de datos.

[Estadísticas de paquetes](#)

Este informe muestra los valores de contador de los paquetes de transmisión total vecinos y los paquetes totales vecinos transmitidos correctamente. Puede crear el informe basándose en determinados criterios.

[Los peores links SNR](#)

Los problemas de ruido pueden ocurrir en diferentes momentos y el ruido puede aumentar a diferentes velocidades o durar diferentes largos de tiempo. La siguiente figura proporciona la capacidad de crear informes para Radio a y b/g, así como para interfaces selectivas. El informe enumera los 10 peores links SNR de forma predeterminada. Puede elegir entre 5 y 50 enlaces peores. El informe se puede generar durante la última hora, las últimas 6 horas, el último día, los últimos 2 días y hasta 7 días. Los datos se sondean cada 10 minutos de forma predeterminada. Los datos se mantienen en la base de datos durante un máximo de siete días. Los criterios de selección de tipo de vecino pueden ser Todos los vecinos, Sólo elementos principales/secundarios.

The screenshot shows the 'Mesh Worst SNR Links' configuration page in the Cisco Wireless Control System. The page has a sidebar on the left with various report options. The main content area is titled 'Mesh Worst SNR Links > WorstSNRLinks'. It includes a 'General' tab and a 'Results' tab. The 'General' tab is active, showing the following configuration:

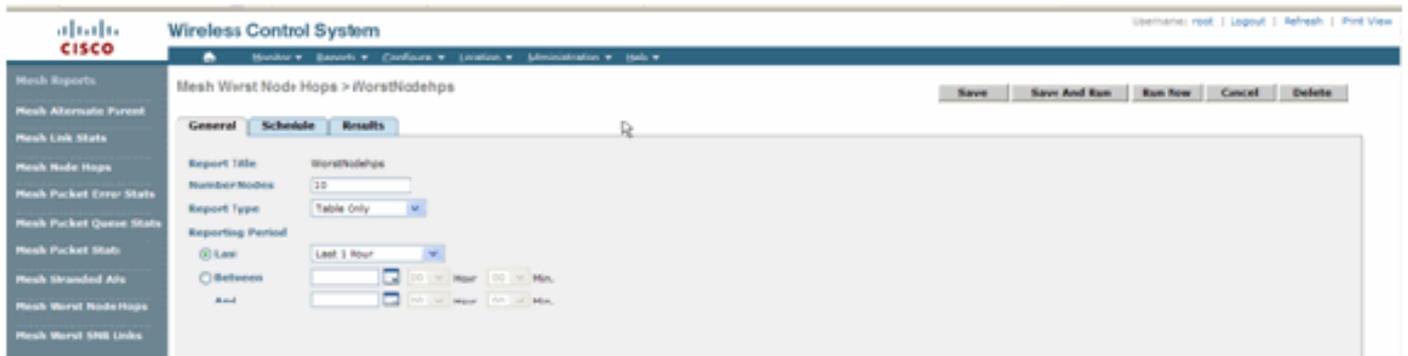
- Report Title: WorstSNRLinks
- Mesh Worst SNR Links: 10
- Neighbor Type: All Neighbors (Table Only)
- Reporting Period: Last
- And: [] Hour [] Min.

The screenshot shows the 'Results' tab of the 'Mesh Worst SNR Links' report. The report is titled 'Mesh Worst SNR Links' and was generated on 'Thu Nov 22 15:58:55 PST 2007'. The configuration shown is: Mesh Worst SNR Links: 10, Neighbor Type: All Neighbors (Table Only), Reporting Period: Last 1 hours. The results are displayed in a table with the following columns: Name, MAC Address, Neigh AP Name, Neigh MAC, Neigh SNR, and Neigh Type.

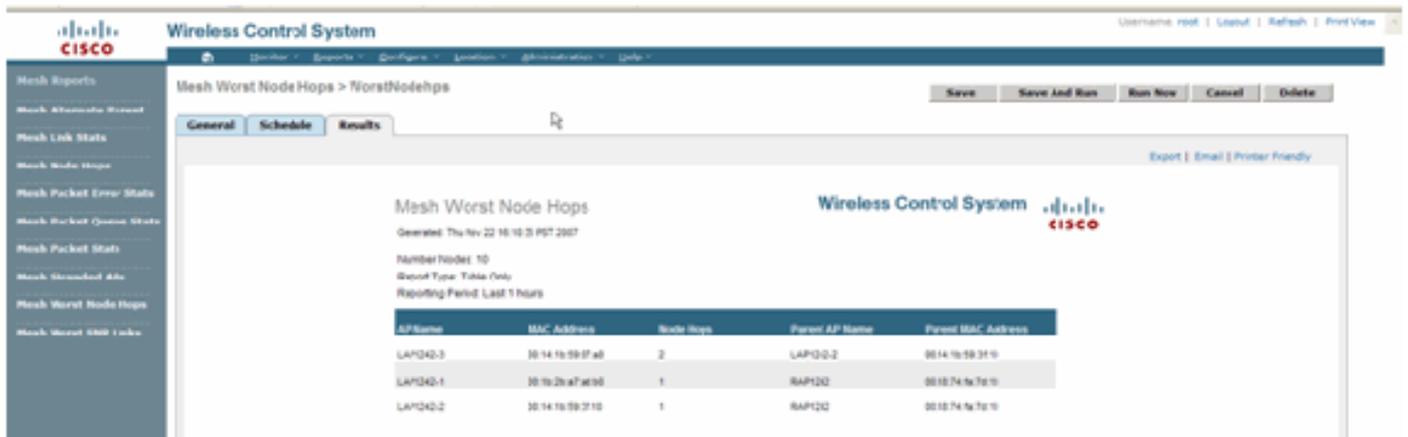
Name	MAC Address	Neigh AP Name	Neigh MAC	Neigh SNR	Neigh Type
LAP1240-3	01:14:1b:59:07a0	LAP1240-2	01:14:1b:59:07a0	-7	parent
LAP1240-3	01:14:1b:59:07a0	LAP1240-2	01:14:1b:59:07a0	-6	parent
LAP1240-3	01:14:1b:59:07a0	LAP1240-2	01:14:1b:59:07a0	-2	parent
LAP1240-3	01:14:1b:59:07a0	LAP1240-2	01:14:1b:59:07a0	-1	parent
LAP1240-3	01:14:1b:59:07a0	LAP1240-2	01:14:1b:59:07a0	-2	parent

[Peor Salto De Nodo](#)

Este informe enumera los 10 AP de saltos peores de forma predeterminada. Si los AP están a demasiados saltos de distancia, los links podrían ser muy débiles. El usuario puede aislar los APs que tienen muchos saltos lejos del AP raíz y tomar las acciones apropiadas. Puede elegir cambiar este criterio **Número de nodos** entre 5 y 50. Los criterios de filtro **Tipo de informe** de esta figura pueden ser Sólo tabla o Tabla y Gráfico:



Esta figura muestra el resultado del último informe:



[Estadísticas de seguridad](#)

Las estadísticas de seguridad de malla interior se muestran en la página de detalles de AP en la sección de información de conexión en puente. Se crea una entrada en la tabla Indoor MeshNodeSecurity Statistics cuando un nodo de malla interior secundario asocia o autentica con un nodo de malla interior primario. Las entradas se quitan cuando el nodo Malla interior se desasocia del controlador.

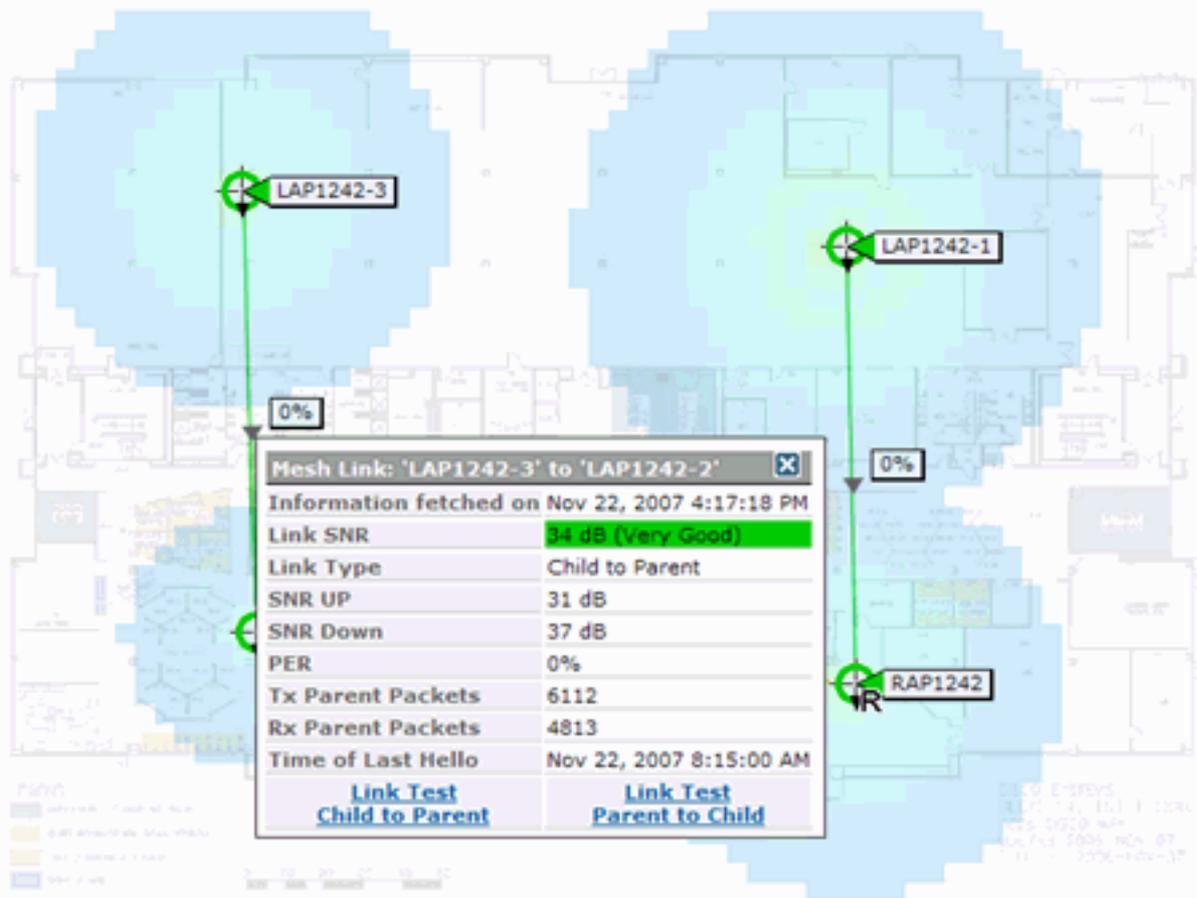
[Prueba de link](#)

La prueba de link de AP a AP es soportada en el WCS. Uno puede seleccionar dos AP cualesquiera e invocar una prueba de link entre los dos.

Si esos AP son vecinos RF, entonces la prueba de link puede tener un resultado. El resultado se muestra en un diálogo en el mapa sin una actualización completa de la página. El diálogo se puede eliminar fácilmente.

Sin embargo, si esos 2 AP no son vecinos de RF, WCS no intenta descifrar una trayectoria entre los 2 AP para hacer una prueba de link múltiple.

Cuando se mueve el ratón sobre la flecha del enlace entre los dos nodos, aparece esta ventana:



Prueba de link de nodo a nodo

La herramienta Link Test es una herramienta a petición para verificar la calidad del link entre dos AP cualesquiera. En WCS, esta función se agrega a la página de detalles de AP.

En la página de detalles de AP, bajo la pestaña **Enlace de malla interior** donde se enumeran los links junto a él, hay un link para realizar la prueba de link.

La herramienta de prueba de link CLI del controlador tiene los parámetros de entrada opcionales: Tamaño del paquete, paquetes de prueba de link total, duración de la prueba y velocidad de enlace de datos. La prueba de link tiene valores predeterminados para estos parámetros opcionales. Las direcciones MAC para los nodos son los únicos parámetros de entrada obligatorios.

La herramienta Prueba de link prueba la resistencia, el paquete enviado y el paquete recibido entre nodos. El link para la prueba de link se muestra en el informe de detalle de AP. Al hacer clic en el enlace, aparece una pantalla emergente con los resultados de la prueba de enlace. La prueba de link sólo se aplicará a Parent-Child y entre vecinos.

El resultado de la prueba de link genera paquetes enviados, paquetes recibidos, paquetes de error (bloques por razones diff), SNR, piso de ruido y RSSI.

La prueba de enlace proporciona estos detalles en la GUI como mínimo:

- Paquetes de prueba de link enviados
- Paquetes de prueba de link recibidos

- Potencia de la señal en dBm
- Relación señal-ruido

[Enlaces de vecino de punto de acceso a demanda](#)

Esta es una nueva función en el mapa de WCS. Puede hacer clic en un AP de malla y aparecerá una ventana emergente con información detallada. A continuación, puede hacer clic en **Ver vecinos de malla**, que obtiene la información del vecino para el AP seleccionado y muestra una tabla con todos los vecinos para el AP de malla interior seleccionado.

El View Mesh Neighbor Link muestra todos los vecinos para el AP resaltado. Esta instantánea muestra todos los vecinos, el tipo de vecinos y el valor SNR.

[Prueba Ping](#)

La prueba de ping es una herramienta a demanda utilizada para hacer ping entre el controlador y el AP. La herramienta Ping Test está disponible tanto en la página de detalles AP como en MAP. Haga clic en el enlace **Ejecutar prueba de ping** en la página de detalle de AP o en la información de AP de MAP para iniciar el ping desde el controlador al AP actual.

[Conclusión](#)

La malla empresarial (es decir, la malla interior) es una extensión de la cobertura inalámbrica de Cisco a lugares en los que Ethernet por cable no puede proporcionar conectividad. La flexibilidad y la capacidad de gestión de una red inalámbrica se consiguen con la malla empresarial.

La mayoría de las funciones que proporcionan los AP conectados por cable son provistas por la topología de malla interior. La malla empresarial también puede coexistir con los AP cableados en el mismo controlador.

[Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)