

Guía de despliegue interior de la malla

Contenido

[Introducción](#)

[Información general](#)

[Hardware y software soportados](#)

[Interior contra al aire libre](#)

[Configuración](#)

[Modo del regulador L3](#)

[Actualice el regulador al último código](#)

[Dirección MAC](#)

[Registre la dirección MAC a las radios](#)

[Ingrese el MAC address y los nombres de las radios en el regulador](#)

[Habilite la filtración MAC](#)

[Despliegue interior de la malla L3](#)

[Defina las interfaces en el regulador](#)

[Radie los papeles](#)

[Nombre de Grupo de Bridge](#)

[Configuración de Seguridad](#)

[Instalación](#)

[Requisitos previos](#)

[Instalación](#)

[Poder y Configuración de canal](#)

[Control RF](#)

[Verifique las interconexiones](#)

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

[Ethernet Bridging](#)

[Mejora del nombre de Grupo de Bridge](#)

[Registros - Mensajes, sys, AP, y desvío](#)

[Registros de mensajes](#)

[Registros AP](#)

[Registros del desvío](#)

[Rendimiento](#)

[Prueba de convergencia de lanzamiento](#)

[WCS](#)

[Alarmas interiores de la malla](#)

[Informe y estadísticas de la malla](#)

[Prueba del link](#)

[Prueba del link del node a node](#)

[Links a pedido del vecino AP](#)

[Prueba de 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 2.4 gigahertz y un compatible de radio 5.8 gigahertz con 802.11b/g y el 802.11a. Una radio se puede utilizar para el acceso local (del cliente) para el punto de acceso y la segunda radio se puede configurar para el regreso inalámbrico. LAP1242/LAP1131 apoya el P2P, el P2MP, y el tipo de la malla de arquitecturas.

Asegúrese leer a través de la guía antes de intentar las instalaciones unas de los.

Este documento describe el despliegue de la Malla inalámbrica de la empresa para la malla interior. Este documento permitirá a los usuarios finales inalámbricos para entender los fundamentales de la malla interior, donde configurar la malla interior, y cómo configurar la malla interior. La malla interior es un subconjunto de Malla inalámbrica del Cisco Enterprise desplegado usando los reguladores inalámbricos y los AP ligeros.

La malla interior es un subconjunto de la arquitectura de la malla de la empresa desplegado en la arquitectura inalámbrica unificada. La malla interior está en la demanda hoy. Con la malla interior, una de las radios (típicamente 802.11b/g) y/o el link de los Ethernetes de cable se utiliza para conectar con los clientes, mientras que la segunda radio (típicamente 802.11a) se utiliza al tráfico del cliente del regreso. El regreso puede ser un salto único o sobre los saltos múltiples. La malla interior le trae estos valores:

- No teniendo que funcionar con los Ethernetes que atan con alambre a cada AP.
- El puerto de un switch de Ethernet no se requiere para cada AP.
- Conectividad de red donde los alambres no pueden proporcionar la Conectividad.
- Flexibilidad en el despliegue – no restringido hasta el 100m de un switch de Ethernet.
- Fácil desplegar una red inalámbrica ad hoc.

atraen a los minoristas del Grande-cuadro muy a la malla interior debido a los ahorros de costes en el cableado así como por las razones mencionadas previamente.

Uso de los especialistas del inventario que n que realiza el inventario cuenta para los minoristas, fábricas, y otras compañías. Quieren desplegar rápidamente una red temporal del Wi-Fi en un sitio del cliente para habilitar la Conectividad en tiempo real para sus dispositivos de bolsillo. Los seminarios, las conferencias, la fabricación, y la hospitalidad educativos son algunos de los lugares donde está necesaria la arquitectura interior de la malla.

Cuando usted acaba de leer esta guía, usted entenderá donde utilizar y cómo configurar la malla interior. Usted también entenderá que la malla interior en los recintos NEMA no es un reemplazo para la malla al aire libre. Además, usted también entenderá la superioridad de la malla interior sobre la flexibilidad del papel del link (malla del salto único) usada por los AP autónomos.

Suposiciones

Usted tiene conocimiento de la red, de la arquitectura, y de los Productos del Cisco Unified Wireless. Usted tiene el conocimiento de los Productos al aire libre de la malla de Cisco y algo de

la terminología usada para el establecimiento de una red de la malla.

| Glosario de acrónimos | |
|--------------------------------------|---|
| LWAPP | Protocolo del Lightweight Access Point – El protocolo del control y de la tunelización de datos entre los AP y el regulador del Wireless LAN. |
| Controlador de WLAN /Controller /WLC | Regulador del Wireless LAN – Dispositivos de Cisco que centralizan y simplifican la Administración de redes de una red inalámbrica (WLAN) por el número grande que se derrumba de puntos finales manejadas en un sistema solo, unificado, teniendo en cuenta un sistema inteligente unificado de la red WLAN de la información. |
| RAP | Punto de acceso del tejado de la punta de acceso a raíz – Los dispositivos de tecnología inalámbrica de Cisco actúan como Bridge entre el regulador y la otra Tecnología inalámbrica AP. AP que se atan con alambre al regulador. |
| MAPA | Malla AP – El dispositivo de tecnología inalámbrica de Cisco que conecta con un RAP o un MAPA sobre el aire en una radio del 802.11a y también mantiene a los clientes en una radio 802.11b/g. |
| Padre | Un AP (cualquier un RAP/MAP) que proporciona el acceso a otros AP sobre el aire en una radio del 802.11a. |
| Vecino | Todos los AP en una red de interconexión son vecinos y tienen los vecinos. El RAP no tiene un vecino como él ató con alambre al |

| | |
|------|---|
| | regulador. |
| Niño | Un AP más lejos del regulador es siempre un niño. Un niño tendrá un padre y muchos vecinos en una red de interconexión. Si muere el padre, el vecino siguiente con el mejor valor de la facilidad será padre elegido. |
| SNR | Relación señal-ruido |
| BGN | Nombre de Grupo de Bridge |
| EAP | Protocolo extensible authentication |
| PSK | Clave del preshared |
| AWPP | Protocolo inalámbrico adaptante de la trayectoria |

Información general

El Punto de acceso interior de la red de interconexión de Cisco es un dispositivo de infraestructura del Wi-Fi de la dos-radio para las implementaciones interiores seleccionadas. Es un LWAPP (Lightweight Access Point Protocol) basado en el producto. Proporciona una radio 2.4 gigahertz y un compatible de radio 5.8 gigahertz con 802.11b/g, los estándares del 802.11a. Una radio (802.11b/g) se puede utilizar para el acceso local (del cliente) para el AP y la segunda radio (802.11a) se puede configurar para el regreso inalámbrico. Proporciona una arquitectura interior de la malla, donde diversos Nodos (radios) hablan el uno al otro vía el regreso y también proporcionan el acceso de cliente local. Este AP se puede también utilizar para las arquitecturas de Bridging del Punto a punto y de la punta a de múltiples puntos. La solución de red de interconexión interior inalámbrica es ideal para la cobertura interior grande como usted puede tener las altas velocidades de datos y buena confiabilidad con la infraestructura mínima. Éstas son las características salientes básicas introducidas con la primera versión de este producto:

- Utilizado en el entorno interior para un conteo saltos 3. Máximo 4.
- Nodo y host de la retransmisión para los clientes del usuario final. Una radio del 802.11a se utiliza como una interfaz del regreso y radio 802.11b/g para los clientes de mantenimiento.
- Seguridad interior de la malla AP – EAP y PSK soportados.
- Los mapas del LWAPP en un entorno de la malla comunican con los reguladores igual que comparado a los AP adjuntos a Ethernet.
- Bridging de la red inalámbrica punto a punto.
- Bridging inalámbrico de la punta a de múltiples puntos.
- Selección óptima del padre. SNR, FACILIDAD, y BGN
- Mejoras BGN. FALTA DE INFORMACIÓN y modo predeterminado.
- Acceso local.
- Anuncio negro del padre. Lista de la exclusión.
- Uno mismo que cura con AWPP.
- Ethernet Bridging.
- Soporte básico de la Voz de la versión 4.0.

- Selección dinámica de la frecuencia.
- Encalladura anti – BGN predeterminado y falla de DHCP.

Note: Estas características no serán soportadas:

- Canal de la seguridad pública 4.9 gigahertz
- Encaminamiento alrededor de interferencia
- Análisis en segundo plano
- Acceso universal
- Soporte del Work Group Bridge

Software interior de la malla

El software interior de la malla es una versión especial como concentra en los AP interiores, especialmente malla interior. En esta versión, tenemos ambos los AP interiores que trabajan en el modo local y también en el modo Bridge. Algunas de las características que están disponibles en la versión de 4.1.171.0 no se implementan en esta versión. Mejoras se han llevado a cabo al comando line interface(cli), la interfaz del usuario (GUI – buscador Web) y en la máquina de estado sí mismo. El objetivo para estas mejoras es ganar la información valiosa de su perspectiva con respecto este producto nuevo y a su viabilidad funcional.

Mejoras específicas de la malla interior:

- **Entorno interior** – La malla interior se implementa usando LAP1242s y LAP1131. Éstos se implementan en los entornos interiores donde no está disponible el cable Ethernet. La implementación es fácil y más rápida proporcionar una cobertura de red inalámbrica a las áreas remotas dentro del edificio (por ejemplo, los centros de distribución al por menor, educación para los seminarios/las conferencias, fabricación, hospitalidad).
- **Mejoras del nombre de Grupo de Bridge (BGN)** – Para permitir que un administrador de la red ordene una red de la malla interior AP en el usuario especificó los sectores, Cisco proporciona un mecanismo llamado nombre de Grupo de Bridge, o el BGN. El BGN, realmente el nombre del sector, hace un AP conectar con otros AP con el mismo BGN. En el evento un AP no encuentra ningún sector conveniente el corresponder con de su BGN, el AP actúa en el modo predeterminado, y elige al mejor padre que responde al valor por defecto BGN. Esta característica ha recibido ya mucho aprecio del campo mientras que lucha contra las condiciones trenzadas AP (si alguien tiene mis configurado el BGN). En la versión de software de 4.1.171.0, los AP, al usar el valor por defecto BGN, no actúan como nodo interior de la malla y no tienen ningún acceso al cliente. Está en el modo de mantenimiento a acceder vía el regulador, y si el administrador no repara el BGN, el AP reiniciará después de 30 minutos.
- **Mejoras de la seguridad** - La Seguridad en el código interior de la malla por abandono se configura para EAP (protocolo extensible authentication). Esto se define en el RFC3748. Aunque el protocolo EAP no se limite a la Tecnología inalámbrica LAN y se pueda utilizar para la autenticación del LAN cableado, es el más de uso frecuente en Tecnología inalámbrica LAN. Cuando el EAP es invocado por un dispositivo habilitado 802.1x NAS (servidor de acceso a la red) tal como un unto de acceso de red inalámbrica del a/b/g del 802.11, los métodos EAP modernos pueden proporcionar un mecanismo de autenticación seguro y negociar un PMK seguro (en parejas clave principal) entre el cliente y el NAS. El PMK se puede entonces utilizar para la sesión de encriptación inalámbrica que utiliza el cifrado TKIP o del CCMP (basado en el AES). Antes de la versión de software de 4.1.171.0, la malla al aire libre AP utilizó PMK/BMK para unirse al regulador. Esto era un proceso del tres-ciclo.

Ahora los ciclos se reducen para una convergencia más rápida. El objetivo general de la Seguridad interior de la malla es proporcionar: Configuración cero del tacto para la Seguridad de disposición. Aislamiento y autenticación para los marcos de datos. Autenticación recíproca entre la red y los Nodos. Capacidad de utilizar los métodos EAP estándar para la autenticación de los Nodos interiores de la malla AP. Desemparejamiento del LWAPP y de la Seguridad interior de la malla. La detección, la encaminamiento, y sincronizar los mecanismos se aumentan de la arquitectura actual para acomodar los elementos requeridos para soportar los nuevos protocolos de Seguridad. La malla interior AP descubre la otra malla AP analizando y estando atentas las actualizaciones vecinas gratuitas de la otra malla AP. Cualquier RAP o mapa interior conectado con la red hace publicidad de los parámetros de seguridad de la base en sus tramas NEIGH_UPD (como las tramas de recuperación de problemas del 802.11). Una vez que esta fase ha terminado, un link lógico entre una malla interior AP y el AP raíz se establece.

- **Mejoras WCSS** Se han agregado las alarmas interiores de la malla. Los informes interiores de la malla se pueden generar mostrando el conteo saltos, el SNR peor, el etc. La prueba del link (Padre-a-niño, Niño-a-padre) se puede funcionar con entre los Nodos que muestra la información muy inteligente. La información AP visualizada es mucho más que las anteriores. Uno tiene una opción también para ver a los vecinos potenciales. Mejoran al control de salud y más conveniente acceder.

Hardware y software soportados

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

- El LWAPP AP AIR-LAP1242AG-A-K9 y AIR-LAP1131AG-A-K9 de Cisco soporta la configuración interior de la malla.
- Malla de la empresa del software support de la versión 2 de la malla de Cisco (Productos interiores y al aire libre). Esto se puede instalar en el regulador de Cisco, Cisco 440x/210x, y WISMs solamente.
- El software de la versión 2 de la malla del Cisco Enterprise se puede descargar del cisco.com.

Interior contra al aire libre

Éstos son algunas de las diferencias salientes entre la malla interior y al aire libre:

| | Malla interior | Malla al aire libre |
|---------------------|---|---|
| Entorno | Interior SOLAMENTE, clasificado interior del hardware | Al aire libre SOLAMENTE, hardware rugoso |
| Hardware | AP interior usando LAP1242 y LAP1131AG | AP al aire libre usando LAP15xx y LAP152x |
| Niveles de potencia | 2.4 Ghz:20dbm 5.8 Ghz:17dbm | 2.4 Ghz:28dbm 5.8 Ghz:28dbm |
| Tamaños de | El aproximadamente | El |

| | | |
|-----------------------------|----------------------|--------------------------|
| celda | 150ft | aproximadamente 1000ft |
| Altura de la implementación | el 12ft de la tierra | los 30-40ft de la tierra |

Configuración

Asegúrese de revisar la guía a conciencia antes de comenzar cualquier implementación, especialmente si usted ha recibido el nuevo hardware.

Modo del regulador L3

La malla interior AP se puede desplegar como red L3.

Actualice el regulador al último código

Complete estos pasos:

1. Para actualizar la versión 2 de la malla en una red de interconexión interior, su red debe ejecutarse en 4.1.185.0 o la malla Release1, disponible en Cisco.com.
2. Descargue el último código para el regulador a su servidor TFTP. De la interfaz GUI del regulador, haga clic el **archivo de los comandos >** de la **descarga**.
3. Seleccione el tipo de archivo como **código** y dé la dirección IP de su servidor TFTP. Defina la trayectoria y el nombre del archivo. **Note:** Utilice al servidor TFTP que soporta más que las transferencias del tamaño del archivo del 32 MB. Por ejemplo, **ftpd32**. Bajo el trayecto del archivo puesto “. /” como se muestra.
4. Cuando está acabado de instalar el nuevo firmware, utilice el comando del **sysinfo de la demostración** en el CLI de verificar que el nuevo firmware está instalado. **Note:** Oficialmente, Cisco no soporta los Downgrades para los reguladores.

Dirección MAC

Es obligatorio utilizar la filtración MAC. Esta característica ha hecho Cisco la solución interior de la malla como “tacto cero real.” A diferencia de las versiones anteriores, la pantalla de malla tendrá no más la opción de filtro MAC.

Note: La filtración MAC se habilita por abandono.

Registre la dirección MAC a las radios

En un archivo de texto, registre las direcciones MAC de todas las radios AP interiores de la malla que usted despliega en su red. La dirección MAC se puede encontrar en la parte de atrás de los AP. Esto le ayuda para la prueba futura, como la mayoría de los comandos CLI requieren el MAC address AP o los nombres se ingresen con el comando. Usted puede también cambiar el nombre de los AP algo recordado más fácilmente, por ejemplo, “tipo constructivo de la número-vaina número-AP: caracteres hexadecimales de la dirección MAC del último cuatro.”

[Ingrese el MAC address y los nombres de las radios en el regulador](#)

El regulador de Cisco mantiene una lista interior de la dirección MAC de la autorización AP. El regulador responde solamente a las peticiones de la detección de las radios interiores que aparecen en la lista de la autorización. Ingrese los direccionamientos MAC de todas las radios que usted tiende a utilizar en su red en el regulador.

En la interfaz GUI del regulador, vaya a la **Seguridad**, y haga clic en el **MAC que filtra** en el lado izquierdo de la pantalla. Haga clic **nuevo** para ingresar los direccionamientos MAC como se muestra aquí:

También, ingrese los nombres de las radios para la conveniencia bajo descripción de la **descripción** (tal como ubicación, AP #, etc.) puede también ser utilizado para donde las radios han estado instaladas para la referencia fácil en cualquier momento.

[Habilite la filtración MAC](#)

La filtración MAC se habilita por abandono.

Uno puede también tomar una decisión del modo seguro como EAP o del PSK en lo mismo página.

De la interfaz GUI del Switch, utilice esta trayectoria:

Trayectoria de la interfaz GUI: **Tecnología inalámbrica > malla interior**

El modo seguro puede ser comprobado SOLAMENTE el CLI por este comando:

```
(Cisco Controller) > show network
```

[Despliegue interior de la malla L3](#)

Para una red de interconexión interior L3, configure los IP Addresses para las radios si usted no se prepone utilizar al servidor DHCP (interno o externo).

Para una red de interconexión interior L3, si usted quiere utilizar al servidor DHCP, configure el regulador en el modo L3. Salve la configuración y reinicie el regulador. Asegúrese le la opción 43 de la configuración en el servidor DHCP. Después de que el regulador haya recommenzado, los AP nuevamente conectados recibirán su dirección IP del servidor DHCP.

[Defina las interfaces en el regulador](#)

Administrador AP

Para un despliegue L3, usted debe definir el **AP manager**. El administrador AP actúa como dirección IP de origen para la comunicación del regulador a los AP.

Ruta: **El regulador > interconecta > ap-administrador > edita.**

La interfaz del **AP manager** se debe asignar una dirección IP en la misma subred y el VLA N

como su interfaz de administración.

Papeles de radio

Hay dos papeles de radio primarios posibles con esta solución:

- Punta de acceso a raíz (RAP) - La radio con la cual usted quiere conectar con el regulador (vía el Switch) tomará el papel de un RAP. Los rap tienen una conexión atada con alambre, Lwapp-habilitada al regulador. UN RAP es un nodo primario a cualquier bridging o red de interconexión interior. Un regulador puede tener uno o más RAP, cada uno parenting el mismo o las diversas redes inalámbricas. Puede haber más de un RAP para la misma red de interconexión interior para la Redundancia.
- Punto de acceso interior de la malla (MAPA) - La radio que no tiene ninguna conexión alámbrica al regulador toma el papel de una malla interior AP. Este AP fue llamado antes el top AP de poste. Los mapas tienen una conexión de red inalámbrica (a través de la interfaz del regreso) quizás a otros mapas y finalmente a un RAP y así al regulador. Los mapas pueden también tener una conexión de los Ethernetes de cable a un LAN y servir como punto final del Bridge para ese LAN (usando una conexión P2P o P2MP). Esto puede ocurrir simultáneamente, si está configurada correctamente como puente de Ethernet. Clientes del servicio de los mapas en la banda no usada para la interfaz del regreso.

El modo predeterminado para un AP es MAPA.

Note: Los papeles de radio se pueden fijar vía el GUI o el CLI. Los AP reiniciarán después de que el cambio del papel.

Note: Usted puede utilizar el regulador CLI para preconfigurar los papeles de radio en un AP proporcionó al AP está conectado físicamente con el Switch o usted puede ver el AP en el Switch como un RAP o MAPA.

Nombre de Grupo de Bridge

Los nombres de Grupo de Bridge (BGN) controlan la asociación de los AP. Los BGN pueden agrupar lógicamente las radios para evitar dos redes en el mismo canal de la comunicación con uno a. Esta configuración es también útil si usted tiene más de un RAP en su red en el mismo sector (área). El BGN es una cadena de diez caracteres máximos.

Un nombre de Grupo de Bridge del fábrica-conjunto se asigna en la etapa de la fabricación (VALOR NULO). No es visible a usted. Como consecuencia, incluso sin un BGN definido, las radios pueden todavía unirse a la red. Si usted tiene dos rap en su red en el mismo sector (para más capacidad), se recomienda que usted configura los dos rap con el mismo BGN, pero en diversos canales.

Note: El nombre de Grupo de Bridge se puede fijar del regulador CLI y GUI.

Después de configurar el BGN, el AP reajustará.

Note: El BGN se debe configurar muy cuidadosamente en una red en funcionamiento. Usted debe salir del nodo más lejano (el nodo más reciente) y moverse siempre hacia el RAP. La razón es que si usted comienza a configurar el BGN en alguna parte en el medio del multihop, después los Nodos más allá de esta punta serán caídos como estos Nodos tendrán un diverso BGN (BGN

viejo).

Usted puede verificar el BGN publicando este comando CLI:

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

También, usted puede configurar o verificar el BGN usando el regulador GUI:

Ruta: **Tecnología inalámbrica > todo el AP > detalles.**

Usted puede ver que la información del entorno AP también está visualizada con esta nueva versión.

[Configuración de Seguridad](#)

El modo seguro interior predeterminado de la malla es EAP. Esto significa que a menos que usted configure estos parámetros en su regulador, sus mapas no se unirán a:

Configuración interior CLI de la malla EAP

Si usted necesita permanecer en el modo del PSK, utilice este comando de volver al modo del PSK:

Comandos show interiores de la malla EAP

Dentro del modo EAP, usted puede marcar estos **comandos show** de verificar la autenticación del MAPA:

```
(Cisco Controller) >show wlan 0
```

```
(Cisco Controller) >show local-auth config
```

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

Comandos debug interiores de la malla EAP

Para hacer el debug de cualquier problema del modo EAP, utilice estos comandos en el regulador:

[Instalación](#)

[Requisitos previos](#)

El regulador debe funcionar con la versión recomendada del código. **Monitor del teclado** para verificar la versión de software. Lo mismo se pueden verificar vía el CLI.

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

Instalación

1. Conecte todos los revestimientos (1131AG/1242AG) con una red de la capa 3 en la misma subred como el IP Address de administración. Todos los AP se unirán al regulador como AP en el modo local. En este modo, prepare los AP con el nombre del controlador primario, el nombre del controlador secundario, y un nombre del controlador terciario.
2. Capture la dirección MAC de radio baja del AP (por ejemplo, 00:18:74:fb:27:60).
3. Agregue la dirección MAC del AP para que el AP se una a en el modo Bridge.
4. Haga clic la **Seguridad > MAC-filtrando > nuevo**.
5. Agregue la dirección MAC copiada, y nombre los AP en la lista del MAC-filtro y la lista AP.
6. Elija el **Bridge modo AP de la lista**.
7. Le indicará a que confirme pues éste reiniciará el AP.
8. El AP reiniciará y se unirá al regulador en el modo Bridge. La nueva ventana AP tendrá una lengüeta adicional: MALLA. Haga clic la lengüeta de la **MALLA** para verificar el papel, el tipo del Bridge, el nombre de Grupo de Bridge, el Ethernet Bridging, la interfaz del recorrido de la parte posterior, la velocidad de datos del Bridge, el etc.
9. En esta ventana, acceda la lista del papel AP y elija el papel relevante. En este caso, el papel por abandono es un MAPA. El nombre de Grupo de Bridge está vacío por abandono. La interfaz posterior del recorrido es 802.11a. La velocidad de datos del Bridge (es decir, velocidad de datos posterior del recorrido) es 24Mbps.
10. Conecte el AP que usted quiere como RAP al regulador. Despliegue las radios (mapas) en las ubicaciones deseadas. Switch en las radios. Usted debe poder ver todas las radios en el regulador.
11. Intente tener condiciones de la visión entre los Nodos. Si no existen las condiciones de la visión, cree las liquidaciones de la zona de Fresnel para obtener las condiciones del cercano-línea-de-sitio.
12. Si usted tiene más de un regulador conectado con la misma red de interconexión interior, después usted debe especificar el nombre del controlador primario en cada nodo. Si no, el regulador que es primer vista será tomado como el primario.

Poder y Configuración de canal

El canal del regreso se puede configurar en un RAP. Los mapas ajustarán al canal del RAP. El Acceso local se puede configurar independientemente para los mapas.

Del Switch GUI, siga la trayectoria: **Tecnología inalámbrica > radio > configuración del 802.11a**.

Note: El valor por defecto Alimentación de TX llano en el regreso es el nivel de potencia más alto (el nivel 1) y el Administración de recursos de radio (RRM) está apagado por abandono.

Si usted está colocando los rap, le recomendamos los canales adyacentes alternos del uso en cada RAP. Esto reducirá interferencia del cocanal.

Control RF

En una red de interconexión interior debemos verificar la relación controlante/subordinado entre los Nodos. **El salto** es un link de red inalámbrica entre las dos radios. La relación controlante/subordinado cambia mientras que usted viaja a través de la red. Depende de donde

usted está en la red de interconexión interior.

La radio más cercano al regulador en una conexión de red inalámbrica (salto) es un **padre de la radio** en el otro lado del salto. En un sistema múltiple del salto hay una estructura del árbol-tipo donde está un RAP el nodo conectado con el regulador (**padre**). El nodo inmediato en el otro lado del primer salto es un **niño**, y los nodos subsiguientes en el segundo salto hacia adelante son los **vecinos** para ese padre determinado.

Figura 1: Red de dos saltos

En el cuadro 1, los nombres AP se mencionan para la conveniencia. En el tiro de siguiente pantalla, se está investigando el **RAP(fb:10)**. Este nodo puede considerar (en el despliegue real) la malla interior AP (**fa:60 y b9:20**) como niños y **ASOCIAR ff:60** como vecino.

De la interfaz GUI del Switch, siga la trayectoria: **Tecnología inalámbrica > todo el AP > Rap1 > información de vecino**.

Asegúrese de que las relaciones del Padre-niño estén establecidas y mantenidas correctamente para su red de interconexión interior.

Verifique las interconexiones

la **malla de la demostración** es un comando informativo de verificar la interconexión en su red.

Usted debe dar estos comandos en cada nodo (AP) usando el regulador CLI, y carga los resultados en una palabra o un archivo de texto al sitio que carga.

En su red de interconexión interior, elija un link múltiple del salto y publique estos comandos a partir del RAP. Cargue el resultado de los comandos al sitio que carga.

En la siguiente sección, todos estos comandos se han publicado para la red de interconexión interior de dos saltos mostrada en el cuadro 1.

Muestre la trayectoria interior de la malla

Este comando le mostrará las direcciones MAC, el papeles de radio de los Nodos, los ratios señal/ruidos en los dBs para el uplink/SNR del link descendente (SNRUp, SNRDown), y del link en el DB para un trayecto determinado.

Muestre el resumen interior del vecino de la malla

Este comando le mostrará las direcciones MAC, las relaciones controlante/subordinado, y el uplink/link descendente SNRs en el DB.

Para entonces, usted debe poder ver las relaciones entre los Nodos de su red y verificar la Conectividad RF viendo los valores del SNR para cada link.

Seguridad del acceso a la consola AP

Esta característica da la seguridad mejorada al acceso a la consola del AP. Un cable de la consola para el AP se requiere para utilizar esta característica.

Se soportan éstos:

- Un CLI para avanzar la identificación del usuario/la combinación de la contraseña al AP especificado:
- Un comando CLI de avanzar la Combinación de nombre de usuario/contraseña a todos los AP registrados al regulador:

Con estos comandos, el user/la combinación de la contraseña avanzada del regulador es persistentes a través de la recarga en los AP. Si un AP se borra del regulador, no hay modo de acceso a la seguridad. El AP genera un SNMP trap con una registración satisfactoria. El AP también generará un SNMP trap en un error del acceso a la consola por tres veces consecutivas.

Ethernet Bridging

Por razones de seguridad, el acceso de Ethernet en los mapas se inhabilita por abandono. Puede ser habilitado solamente configurando el Ethernet Bridging en el RAP y los mapas respectivos.

Como consecuencia, el Ethernet Bridging tiene que ser habilitado para dos escenarios:

- Cuando usted quiere utilizar los Nodos interiores de la malla como Bridges.
- Cuando usted quiere conectar cualquier dispositivo Ethernet (tal como PC/Laptop, cámara de video etc.) en el MAPA usando su acceso de Ethernet.

Ruta: **Tecnología inalámbrica** > tecleo cualquier AP > **mall**.

Hay un comando CLI que puede ser utilizado para configurar la distancia entre los Nodos que hacen el bridging. Intente conectar un dispositivo Ethernet como un cámara de video en cada salto y vea el funcionamiento.

Mejora del nombre de Grupo de Bridge

Es posible que un AP es incorrecto provisionado con un "bridgegroupname" para cuál no fue pensado. Dependiendo del diseño de red, este AP puede o no puede poder alcanzar hacia fuera y encontrar su sector/árbol correctos. Si no puede alcanzar un sector compatible, puede trenzarse.

Para recuperar un AP tan trenzado, el concepto de bridgegroupname "predeterminado" fue introducido con el código 3.2.xx.x. La idea básica es que un AP que no puede conectar con cualquier otro AP con su bridgegroupname configurado, intenta conectar con el "valor por defecto" (la palabra) como bridgegroupname. Todos los Nodos que funcionan con y posterior el software 3.2.xx.x validan otros Nodos con este bridgegroupname.

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

Si usted tiene una red corriente, tome un AP preconfigurado con un diverso BGN y haga que se une a la red. Usted verá este AP en el regulador que usa el "valor por defecto" BGN después de que usted agregue su dirección MAC en el regulador.

El AP usando el valor por defecto BGN puede actuar como malla interior normal AP que asocia a los clientes y que forma las relaciones interiores del niño del padre de la malla.

El momento que este AP usando el valor por defecto BGN encuentra a otro padre con el BGN

correcto, conmutará a él.

Registros - Mensajes, sys, AP, y desvío

Registros de mensajes

Habilite la información llana para los registros de mensajes. Del regulador CLI, publique este comando:

Para ver los registros de mensajes, publique este comando del regulador CLI:

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

1. Haga clic los **comandos** > la **carga**.
2. Ingrese su información del servidor TFTP. Esta página le dará las diversas opciones para cargar, y usted quisiera que estos archivos fueran enviados: Registro de mensajes Registro de acontecimientos Registro del desvío Archivo de la caída (eventualmente) Para marcar para saber si hay archivos de la caída, **Administración del teclado** > **caída del regulador**.

Registros AP

Vaya a esta página GUI en el regulador a marcar los registros AP para su AP local, si lo hay:

Atrape los registros

Vaya a esta página GUI del regulador y marque los registros del desvío:

Rendimiento

Prueba de convergencia de lanzamiento

La convergencia es el tiempo llevado por un RAP/MAP para establecer una conexión estable del LWAPP con un controlador de WLAN a partir del tiempo en que primero arrancó según lo enumerado aquí:

| Prueba de convergencia | Tiempo de convergencia (minuto: sec) | | | |
|---|--------------------------------------|------|------|------|
| | RAP | MAP1 | MAP2 | MAP3 |
| Actualización de la imagen | 2:34 | 3:50 | 5:11 | 6:38 |
| Reinicialización del regulador | 0:38 | 0:57 | 1:12 | 1:32 |
| Poder en la red de interconexión interior | 2:44 | 3:57 | 5:04 | 6:09 |
| Reinicialización del RAP | 2:43 | 3:57 | 5:04 | 6:09 |
| El MAPA re-se une a | | 3:58 | 5:14 | 6:25 |
| Cambio del MAPA del | | 0:38 | | |

| | | | | |
|------------------------|--|--|--|--|
| padre (el mismo canal) | | | | |
|------------------------|--|--|--|--|

WCS

Alarmas interiores de la malla

El WCS generará estas alarmas y eventos relacionados con la red de interconexión interior basada en los desvíos del regulador:

- SNR del link de los pobres
- Padre cambiado
- Niño movido
- El MAPA cambia al padre con frecuencia
- Evento del puerto de la consola
- Falla de autorización MAC
- Fallas de autenticación
- El niño excluyó al padre

Links de la malla del tecleo. Mostrará todas las alarmas relacionadas con los links interiores de la malla.

Estas alarmas se aplican a los links interiores de la malla:

- SNR del link de los pobres - Se genera esta alarma si baja el SNR del link abajo 12db. El usuario no puede cambiar este umbral. Si el SNR pobre se detecta en el link del regreso para el niño/el padre, el desvío será generado. El desvío contendrá el valor del SNR y las direcciones MAC. La gravedad de la alarma es principal. La relación de transformación (de relación señal/ruido) del SNR es importante porque la alta potencia de la señal no es bastante para asegurar el buen funcionamiento del receptor. La señal entrante debe ser más fuerte que cualquier ruido o interferencia que esté presente. Por ejemplo, es posible tener alta potencia de la señal y todavía tener funcionamiento inalámbrico pobre si hay interferencia fuerte o un alto nivel de ruido.
- Padre cambiado - Se genera esta alarma cuando el niño se trasladó a otro padre. Cuando pierden al padre, el niño se unirá a con otro padre, y el niño enviará un desvío que contiene las direcciones MAC del viejo padre y del nuevo padre al WCS. Gravedad de la alarma: Informativo.
- Niño movido - Se genera esta alarma cuando el WCS consigue un desvío perdido niño. Cuando el padre AP detectó su pérdida de un niño y no capaz de comunicar con ese niño, enviará un desvío perdido niño al WCS. El desvío contendrá la dirección MAC del niño. Gravedad de la alarma: Informativo.
- Padre del MAPA cambiado con frecuencia - Se genera esta alarma si la malla interior AP cambia a su padre con frecuencia. Cuando el padre-cambio-contador del MAPA excede el umbral dentro de una duración dada, enviará un desvío al WCS. El desvío contendrá la cantidad de veces de cambios del MAPA y de la duración del tiempo. Por ejemplo, si hay 5 cambios en el plazo de 2 minutos, después el desvío será enviado. Gravedad de la alarma: Informativo.
- El niño excluyó al padre - Se genera esta alarma cuando un niño puso a un padre. Un niño puede poner a un padre cuando el niño no pudo autenticar en el regulador después de un

número fijo de tentativas. El niño recuerda al padre puesto y cuando el niño se une a la red, enviará el desvío que contiene la dirección MAC puesta del padre y la duración del período de la lista negra.

Alarmas con excepción de los links interiores de la malla:

- Acceso del puerto de la consola - El puerto de la consola proporciona la capacidad para que el cliente cambie el Nombre de usuario y la contraseña para recuperar el AP al aire libre trenzado. Sin embargo, para prevenir cualquier acceso de usuario autorizado al AP, el WCS necesita enviar una alarma cuando alguien intenta iniciar sesión. Esta alarma se requiere para proporcionar la protección pues el AP es físicamente vulnerable mientras que está localizado al aire libre. Esta alarma será generada si el usuario ha abierto una sesión con éxito al puerto de la consola AP, o si él ha fallado tres veces consecutivas.
- Falla de autorización MAC - Se genera esta alarma cuando los intentos AP para unirse a la malla interior pero no pueden autenticar porque no está en la lista de filtros MAC. El WCS recibirá un desvío del regulador. El desvío contendrá la dirección MAC del AP que autorización fallida.

[Informe y estadísticas de la malla](#)

Transportamos el marco aumentado del informe y de las estadísticas de 4.1.185.0:

- Ningún trayecto alternativo
- Saltos del nodo de la malla
- Stats del error de los paquetes
- Stats del paquete
- El salto peor del nodo
- Los links peores del SNR

[Ningún trayecto alternativo](#)

La malla interior AP tiene típicamente más de un vecino. En caso de que una malla interior AP suelte su link del padre, el AP debe poder encontrar al padre alternativo. En un poco de caso, si no hay vecinos mostrados, después el AP no podrá ir a ninguna otra padres si suelta a sus padres. Es crítico que el usuario sepa qué AP no tienen los padres alternos. Este informe enumera hacia fuera todos los AP que no tienen ninguna otra vecinos con excepción del padre actual.

[Saltos interiores del nodo de la malla](#)

Este informe muestra el número de saltos lejos del AP raíz (RAP). Usted puede crear el informe basado en estos criterios:

- AP por el regulador
- AP por el suelo

[Tarifas de error de paquete](#)

Los errores de paquete se pueden causar por la interferencia y las caídas de paquetes. El cálculo de la tarifa de error de paquete se basa en los paquetes enviados y los paquetes enviados con

éxito. La tarifa de error de paquete se mide en el link del regreso y se recoge para los vecinos y el padre. El AP envía periódicamente la información del paquete al regulador. Tan pronto como el padre cambie, el AP envía la información de error de paquete recogida al regulador. El WCS sondea la información de error de paquete del regulador cada 10 minutos por abandono y la salva en la base de datos por hasta 7 días. En el WCS, la tarifa de error de paquete se muestra como gráfico. El gráfico de error de paquete se basa en los datos históricos salvados en la base de datos.

[Stats del paquete](#)

Este informe muestra que los valores de contador del total vecino transmiten los paquetes y los totales de paquetes vecinos transmitidos con éxito. Usted puede crear el informe basado en ciertos criterios.

[Los links peores del SNR](#)

Los problemas de ruido pudieron ocurrir en los momentos diferentes y el ruido pudo aumentar a diversas tarifas o dura para diversas longitudes del tiempo. La figura siguiente proporciona la capacidad de crear el informe para la radio a y b/g así como las interfaces selectivas. Los informes enumera los 10 links peores del SNR por abandono. Usted puede elegir a partir del 5 a 50 links peores. El informe se puede generar para el último 1 hora, dura 6 horas, el día más pasado, dura 2 días, y hasta 7 días. Los datos se sondean cada 10 minutos por abandono. Los datos se mantienen la base de datos para el máximo siete días. El Criterio de selección vecino del tipo puede ser todos los vecinos, padre/los niños solamente.

[Los saltos peores del nodo](#)

Este los saltos peores AP de los informes enumera the10 por abandono. Si los AP son demasiados saltos lejos, los links podrían ser muy débiles. El usuario puede aislar los AP que tienen muchos saltos lejos del AP raíz y toman la acción apropiada. Usted puede elegir cambiar este **número de** criterios de los **Nodos** entre 5 y 50. Los criterios del filtro del **Report Type** en esta figura pueden ser tabla solamente o presentar y representar gráficamente:

Esta figura muestra el resultado para el informe más reciente:

[Estadísticas de la Seguridad](#)

Las estadísticas interiores de la Seguridad de la malla se visualizan en la página del detalle AP conforme a la sección de información que interliga. Una entrada en la tabla interior de la estadística de MeshNodeSecurity se crea cuando un nodo interior de la malla del niño se asocia o autentica con un nodo interior de la malla del padre. Se quitan las entradas cuando el nodo interior de la malla desasocia del regulador.

[Prueba del link](#)

La prueba del link AP-a-AP se soporta en el WCS. Uno puede seleccionar cualesquiera dos AP e invocar una prueba del link entre los dos.

Si esos AP son vecinos RF, después la prueba del link puede tener un resultado. El resultado se muestra en un diálogo en la correspondencia sí mismo sin una página completa restaura. El

diálogo se puede disponer fácilmente.

Sin embargo, si esos 2 AP no son vecinos RF, después el WCS no intenta imaginar una trayectoria entre los 2 AP para hacer una prueba del link múltiple de la cosechadora.

Cuando el ratón se mueve sobre la flecha en el link entre los dos Nodos, esta ventana aparece:

[Prueba del link del node a node](#)

La herramienta de evaluación del link es una herramienta a pedido para verificar la calidad del link entre cualquier dos AP. En el WCS, esta característica se agrega en la página del detalle AP.

En la página del detalle AP, bajo lengüeta **interior del link de la malla** donde están mencionados los links al lado de ella, hay un link para realizar la prueba del link.

La herramienta de evaluación del link del regulador CLI tiene los parámetros de entrada opcionales: Tamaño de paquetes, paquetes de prueba del link total, duración de la prueba, y de la tarifa del link de datos. La prueba del link tiene valores predeterminados para estos parámetros optativos. Las direcciones MAC para los Nodos son los únicos parámetros de entrada obligatorios.

La herramienta de evaluación del link prueba la fuerza, el paquete enviado, y el paquete recibido entre los Nodos. El link para la prueba del link se visualiza en el informe de la reunión AP. Cuando usted hace clic el link, hay una pantalla móvil que muestra los resultados de la prueba del link. La prueba del link será solamente aplicable Parent – niño y entre los vecinos.

La salida de la prueba del link genera los paquetes enviados, los paquetes recibidos, los paquetes de errores (compartimientos por las razones del diff), el SNR, el suelo del ruido, y el RSSI.

La prueba de Lnk proporciona estos detalles en el GUI en un mínimo:

- Paquetes de prueba del link enviados
- Paquetes de prueba del link recibidos
- Potencia de la señal en el dBm
- Relación señal-ruido

[Links a pedido del vecino AP](#)

Esto es una nueva función en el mapa WCS. Usted puede hacer clic en una malla AP y una ventana emergente con la información detallada aparece. Usted puede entonces hacer clic a los **vecinos de la malla de la visión**, que trae la información de vecino para el AP seleccionado y visualiza una tabla con todos los vecinos para la malla interior seleccionada AP.

El link vecino de la malla de la visión visualiza a todos los vecinos para el AP resaltado. Esta foto muestra todos los vecinos, el tipo de los vecinos, y el valor del SNR.

[Prueba de ping](#)

La prueba de ping es una herramienta a pedido usada para hacer ping entre el regulador y el AP. La herramienta de prueba de ping está disponible en ambos la página del detalle AP y en el MAPA. Haga clic el link de la **prueba de ping del funcionamiento** en la página del detalle AP o de

la información del MAPA AP para iniciar el ping del regulador al AP actual.

Conclusión

La malla de la empresa (es decir, malla interior) es una extensión de la cobertura de la tecnología inalámbrica de Cisco a los lugares en donde los Ethernetes de cable no pueden proporcionar la Conectividad. La flexibilidad y la manejabilidad de una red inalámbrica se logra con la malla de la empresa.

La mayor parte de los AP atados con alambre las características proporcionan son proporcionados por la topología de interconexión interior. La malla de la empresa puede también coexistir con los AP atados con alambre en el mismo regulador.

Información Relacionada

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