

Guia de implantação de malha interna

Contents

[Introduction](#)

[Overview](#)

[Hardware e software suportados](#)

[Interno versus Externo](#)

[Configuração](#)

[Modo L3 da controladora](#)

[Atualize o controlador para o código mais recente](#)

[Endereço MAC](#)

[Registre o endereço MAC nos rádios](#)

[Insira o endereço MAC e os nomes dos rádios no controlador](#)

[Habilitar filtragem de MAC](#)

[Implantação de malha interna L3](#)

[Definir interfaces no controlador](#)

[Funções de rádio](#)

[Nome do grupo de bridge](#)

[Configuração de segurança](#)

[Instalação](#)

[Pré-requisitos](#)

[Instalação](#)

[Configuração de alimentação e canal](#)

[Verificação de RF](#)

[Verificar as interconexões](#)

[Segurança de acesso ao console AP](#)

[Bridging Ethernet](#)

[Aprimoramento do nome do grupo de bridge](#)

[Logs - Mensagens, Sys, AP e Trap](#)

[Logs de mensagem](#)

[Logs AP](#)

[Logs de interceptação](#)

[Desempenho](#)

[Teste de convergência de inicialização](#)

[WCS](#)

[Alarmes em malha interna](#)

[Relatório e estatísticas da malha](#)

[Teste de link](#)

[Teste de enlace nó a nó](#)

[Links de vizinhos de AP sob demanda](#)

[Teste de ping](#)

[Conclusão](#)

[Informações Relacionadas](#)

Introduction

O ponto de acesso leve 1242/1131 é um dispositivo de infraestrutura de Wi-Fi, dual-rádio, para implementações internas. É um produto baseado no Lightweight Access Point Protocol (LWAPP). Ele fornece um rádio de 2,4 GHz e um rádio de 5,8 GHz compatível com 802.11b/g e 802.11a. Um rádio pode ser usado para acesso local (cliente) para o ponto de acesso (AP) e o segundo rádio pode ser configurado para backhaul sem fio. LAP1242/LAP1131 suporta arquiteturas P2P, P2MP e de malha.

Leia o guia antes de tentar qualquer uma das instalações.

Este documento descreve a implantação da Enterprise Wireless Mesh para malha interna. Este documento permitirá que os usuários finais sem fio entendam os fundamentos da malha interna, onde configurar a malha interna e como configurar a malha interna. Malha interna é um subconjunto da malha sem fio corporativa da Cisco implantada usando controladores sem fio e APs leves.

A malha interna é um subconjunto da arquitetura de malha corporativa implantada na arquitetura Unified Wireless. Malha interna está em demanda hoje. Com malha interna, um dos rádios (normalmente 802.11b/g) e/ou o link Ethernet com fio é usado para se conectar aos clientes, enquanto o segundo rádio (normalmente 802.11a) é usado para fazer backhaul do tráfego do cliente. O backhaul pode ser um salto único ou sobre vários saltos. Malha interna traz esses valores para você:

- Não é preciso executar o cabeamento Ethernet para cada AP.
- A porta do switch Ethernet não é necessária para cada AP.
- Conectividade de rede onde os fios não podem fornecer conectividade.
- Flexibilidade na implantação - não restrita a 100m de um switch Ethernet.
- Fácil de implantar uma rede sem fio ad-hoc.

Os varejistas de grande porte são muito atraídos pela malha interna devido à economia nos custos com fiação, bem como pelos motivos mencionados anteriormente.

Os especialistas em inventário usam-na na contagem de estoque para varejistas, fábricas e outras empresas. Eles querem implantar rapidamente uma rede Wi-Fi temporária em um local do cliente para permitir a conectividade em tempo real para seus dispositivos de mão. Seminários educacionais, conferências, manufatura e hospitalidade são alguns dos lugares onde a arquitetura em malha interna é necessária.

Quando terminar de ler este guia, você vai entender onde usar e como configurar a malha interna. Você também vai entender que a malha interna em gabinetes NEMA NÃO é uma substituição para malha externa. Além disso, você também entenderá a superioridade da flexibilidade da função de malha interna sobre enlace (malha de salto único) usada por APs autônomos.

Suposições:

Você conhece a Cisco Unified Wireless Network, a arquitetura e os produtos. Você conhece os produtos de malha externa da Cisco e algumas das terminologias usadas para a rede em malha.

Glossário de acrônimos	
LWAPP	Lightweight Access Point Protocol - O protocolo de controle e tunelamento de dados entre APs e o Wireless LAN Controller.
Controlador/Controlador de WLAN /WLC	Controlador de LAN sem fio - Dispositivos da Cisco que centralizam e simplificam o gerenciamento de rede de uma WLAN ao agrupar um grande número de terminais gerenciados em um único sistema unificado, permitindo um sistema de rede WLAN de informações inteligentes e unificadas.
RAP	Ponto de acesso raiz/ponto de acesso de telhado - Os dispositivos sem fio Cisco atuam como uma ponte entre o controlador e outros APs sem fio. APs conectados ao controlador.
MAPA	APs em malha - Dispositivo sem fio da Cisco que se conecta a um RAP ou MAP sobre o ar em um rádio 802.11a e também atende clientes em um rádio 802.11b/g.
Pai	Um AP (RAP/MAP) que fornece acesso a outros APs no ar em um rádio 802.11a.
Vizinho	Todos os APs em uma rede em malha são vizinhos e têm vizinhos. O RAP não tem um vizinho, pois foi conectado ao controlador.
Filho	Um AP mais distante do controlador é sempre um filho. Uma criança terá um pai e muitos vizinhos em uma rede em malha. Se o pai morrer, o próximo vizinho com o melhor valor de facilidade será escolhido como pai.
SNR	Taxa sinal para ruído.
BGN	Nome do grupo de bridge

EAP	Protocolo de autenticação extensível
PSK	Chave pré-compartilhada
AWPP	Adaptive Wireless Path Protocol

Overview

O Cisco Indoor Mesh Network Access Point é um dispositivo de infraestrutura Wi-Fi de dois rádios para implantações internas selecionadas. É um produto baseado no Lightweight Access Point Protocol (LWAPP). Ele fornece um rádio de 2,4 GHz e um rádio de 5,8 GHz compatível com os padrões 802.11b/g, 802.11a. Um rádio (802.11b/g) pode ser usado para acesso local (cliente) para o AP e o segundo rádio (802.11a) pode ser configurado para backhaul sem fio. Ele fornece uma arquitetura em malha interna, onde diferentes nós (rádios) se comunicam via backhaul e também fornecem acesso ao cliente local. Esse AP também pode ser usado para arquiteturas de bridging ponto a ponto e ponto a multiponto. A solução Rede em malha interna sem fio é ideal para uma grande cobertura interna, pois você pode ter altas taxas de dados e boa confiabilidade com uma infraestrutura mínima. Estes são os principais recursos básicos apresentados com a primeira versão deste produto:

- Usado em ambiente interno para uma contagem de 3 saltos. Máximo 4.
- Relay node e host para clientes de usuário final. Um rádio 802.11a é usado como uma interface de backhaul e um rádio 802.11b/g para atender clientes.
- Segurança de APs em malha interna - Suporte para EAP e PSK.
- Os MAPAs LWAPP em um ambiente de malha se comunicam com os controladores da mesma forma que os APs conectados à Ethernet.
- Bridging sem fio ponto a ponto.
- Bridging sem fio ponto a multiponto.
- Seleção de pai ideal. SNR, EASE e BGN
- Melhorias do BGN. Modo NULO e Padrão.
- Acesso local.
- Lista negra pai. Lista de exclusões.
- Autocorreção com AWPP.
- Ethernet Bridging.
- Suporte básico de voz da versão 4.0.
- Seleção dinâmica de frequência.
- Anti-stranding - failover padrão de BGN e DHCP.

Nota: Estes recursos não serão suportados:

- Canal de segurança pública de 4,9 GHz
- Roteamento em torno da interferência
- Verificação em Segundo Plano
- Acesso universal
- Suporte a bridge de grupo de trabalho

Software em malha interna

O software em malha interna é uma versão especial, pois se concentra nos APs internos, especialmente em malha interna. Nesta versão, temos os APs internos trabalhando no modo local

e também no modo bridge. Alguns dos recursos disponíveis na versão 4.1.171.0 não são implementados nesta versão. Foram feitas melhorias na interface de linha de comando (CLI), na interface gráfica do usuário (GUI - navegador da Web) e na própria máquina de estado. O objetivo dessas melhorias é obter informações valiosas da sua perspectiva sobre esse novo produto e sua viabilidade funcional.

Melhorias específicas de malha interna:

- **Ambiente interno** - A malha interna é implementada usando LAP1242s e LAP1131. Eles são implementados em ambientes internos onde o cabo Ethernet não está disponível. A implementação é fácil e mais rápida para fornecer uma cobertura sem fio para áreas remotas dentro do prédio (por exemplo, Retail Distribution Centers, Education for Seminars/Conferences, Manufacturing, Hospitality).
- **Aprimoramentos de BGN (Bridge Group Name, nome do grupo de bridge)** - Para permitir que um administrador de rede organize uma rede de APs de malha interna em setores especificados pelo usuário, a Cisco fornece um mecanismo chamado BGN (Bridge Group Name, nome do grupo de bridge). O BGN, realmente o nome do setor, faz com que um AP se conecte a outros APs com o mesmo BGN. Caso um AP não encontre um setor adequado correspondente ao seu BGN, o AP opera no modo padrão e escolhe o melhor pai que responde ao BGN padrão. Esse recurso já recebeu muita apreciação do campo, pois luta contra as condições de AP retorcido (se alguém tiver configurado incorretamente o BGN). Na versão de software 4.1.171.0, os APs, ao usar o BGN padrão, não operam como um nó de malha interna e não têm acesso de cliente. Ele está no modo de manutenção para acessar através do controlador e, se o administrador não corrigir o BGN, o AP será reinicializado após 30 minutos.
- **Aprimoramentos de segurança** - a segurança no código de malha interna é configurada por padrão para EAP (Extensible Authentication Protocol). Isso é definido no RFC3748. Embora o protocolo EAP não seja limitado a LANs sem fio e possa ser usado para autenticação de LAN com fio, ele é usado com mais frequência em LANs sem fio. Quando o EAP é invocado por um dispositivo NAS (Network Access Server) habilitado 802.1X, como um ponto de acesso sem fio 802.11 a/b/g, os métodos EAP modernos podem fornecer um mecanismo de autenticação segura e negociar um PMK (Pair-wise Master Key) seguro entre o cliente e o NAS. O PMK pode então ser usado para a sessão de criptografia sem fio que usa a criptografia TKIP ou CCMP (baseada em AES). Antes da versão do software 4.1.171.0, os APs de malha externa usavam PMK/BMK para se unir à controladora. Este foi um processo de três ciclos. Agora os ciclos são reduzidos para uma convergência mais rápida. O objetivo geral da segurança em malha interna é fornecer: Configuração zero touch para segurança de provisionamento. Privacidade e autenticação para quadros de dados. Autenticação mútua entre a rede e os nós. Capacidade de usar métodos EAP padrão para autenticação de nós AP de malha interna. Desacoplando o LWAPP e a segurança de malha interna. Os mecanismos de descoberta, roteamento e sincronização são aprimorados da arquitetura atual para acomodar os elementos necessários para suportar os novos protocolos de segurança. Os APs de malha interna descobrem outros APs de malha ao verificar e ouvir atualizações gratuitas de vizinhos de outros APs de malha. Qualquer RAP ou MAPs internos conectados à rede anuncia os parâmetros de segurança principais em seus quadros NEIGH_UPD (como os quadros de beacon 802.11). Depois que essa fase terminar, um link lógico entre um AP de malha interna e o AP raiz é estabelecido.
- **Melhorias do WCS** Alarmes internos em malha foram adicionados. Os relatórios de malha

interna podem ser gerados mostrando a contagem de saltos, o pior SNR etc. O teste de link (pai para filho, filho para pai) pode ser executado entre os nós, o que mostra informações muito inteligentes. As informações do AP exibidas são muito mais do que as anteriores. Temos também a opção de ver os potenciais vizinhos. O monitoramento da saúde é aprimorado e mais conveniente para o acesso.

Hardware e software suportados

Há um requisito mínimo de hardware e software para malha interna:

- Os APs Cisco LWAPP AIR-LAP1242AG-A-K9 e AIR-LAP1131AG-A-K9 suportam configuração em malha interna.
- O software Cisco Mesh Release 2 suporta Enterprise Mesh (produtos internos e externos). Isso pode ser instalado somente no Cisco Controller, Cisco 440x/210x e WISMs.
- O software Cisco Enterprise Mesh Release 2 pode ser baixado do Cisco.com.

Interno versus Externo

Estas são algumas das principais diferenças entre malha interna e externa:

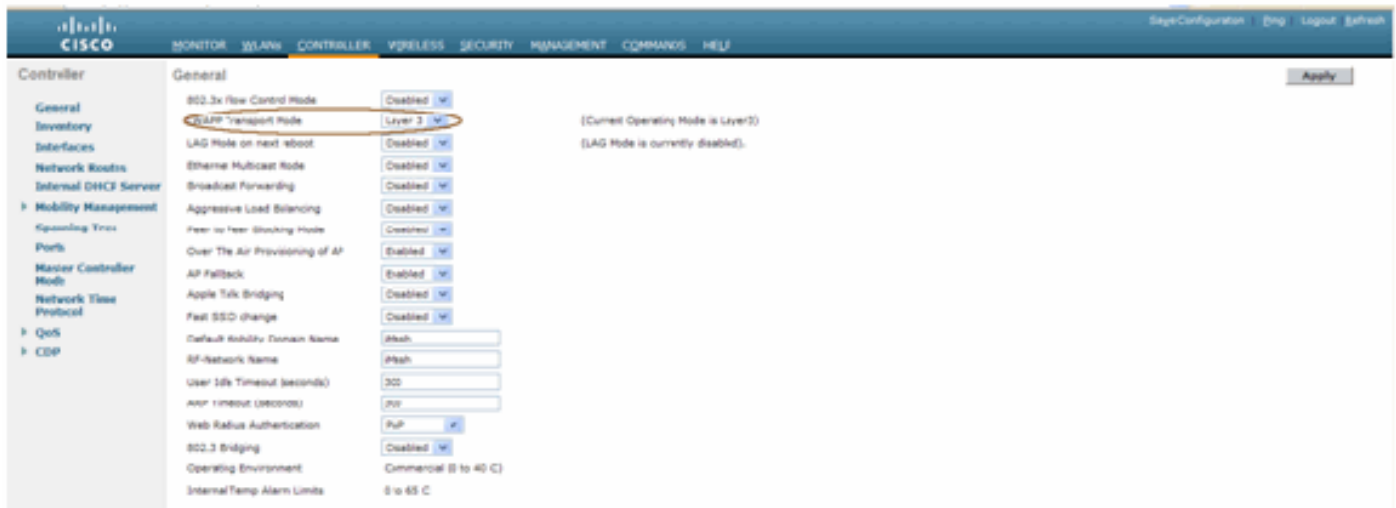
	Malha interna	Malha externa
Ambiente	SOMENTE para uso interno, classificação interna de hardware	SOMENTE externo, hardware reforçado
Hardware	AP interno usando LAP1242 e LAP1131AG	AP externo usando LAP15xx e LAP152x
Níveis de potência	2,4 Ghz:20 Dbm 5,8 Ghz:17 Dbm	2,4 Ghz:28 Dbm 5,8 Ghz:28 Dbm
Tamanhos de células	Aprox 150 pés	Aprox 1000ft
Altura da implementação	12 pés do chão	30 a 40 pés do solo

Configuração

Leia atentamente o guia antes de iniciar qualquer implementação, especialmente se você recebeu novo hardware.

Modo L3 da controladora

Os APs de malha interna podem ser implantados como uma rede L3.



[Atualize o controlador para o código mais recente](#)

Conclua estes passos:

1. Para atualizar a versão 2 da malha em uma rede em malha interna, sua rede deve estar em execução na versão 4.1.185.0 ou Mesh Release1, disponível no Cisco.com.
2. Baixe o código mais recente do controlador no servidor TFTP. Na interface GUI do controlador, clique em **Commands > Download file**.
3. Selecione o tipo de arquivo como **código** e forneça o endereço IP do servidor TFTP. Defina o caminho e o nome do arquivo.



Observação: use o servidor TFTP que suporta mais de 32 MB de transferências de tamanho de arquivo. Por exemplo, **ftpd32**. Em Caminho de arquivo colocado **"/**" conforme mostrado.

4. Ao concluir a instalação do novo firmware, use o comando **show sysinfo** na CLI para verificar se o novo firmware está 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
```

Observação: oficialmente, a Cisco não oferece suporte a downgrades para controladores.

Endereço MAC

É obrigatório usar a Filtragem MAC. Esse recurso tornou a solução de malha interna da Cisco como um verdadeiro "Zero Touch". Ao contrário das versões anteriores, a tela Mesh não terá mais a opção MAC Filtering (Filtragem de MAC).



Observação: a filtragem MAC está habilitada por padrão.

Registre o endereço MAC nos rádios

Em um arquivo de texto, registre os endereços MAC de todos os rádios de AP em malha interna implantados em sua rede. O endereço MAC pode ser encontrado na parte traseira dos APs. Isso ajuda você a realizar testes futuros, já que a maioria dos comandos CLI exige que o endereço MAC ou os nomes dos APs sejam inseridos com o comando. Você também pode alterar o nome dos APs para algo mais facilmente lembrado, como "building number-pod number-AP type: últimos quatro caracteres hexadecimais de endereço MAC."

Insira o endereço MAC e os nomes dos rádios no controlador

O Controlador Cisco mantém uma lista de endereços MAC de autorização de AP interno. O controlador responde somente às solicitações de descoberta dos rádios internos que aparecem na lista de autorização. Insira os endereços MAC de todos os rádios que você tende a usar na rede do controlador.

Na interface GUI da controladora, vá para **Security** e clique em **MAC filtering (Filtragem de MAC)**

no lado esquerdo da tela. Clique em **New** para inserir os endereços MAC como mostrado aqui:

The screenshot shows the Cisco Security Configuration interface. The 'Security' menu is highlighted, and the 'MAC Filtering' sub-menu is selected. The 'RADIUS Compatibility Mode' is set to 'Cisco ACS' and 'MAC Delimiter' is 'No Delimiter'. A table of 'Local MAC Filters' is shown with columns for MAC Address, WLAN ID, Interface, and Description. The 'Description' column is circled in red. The table contains six entries with descriptions like 'MAP1', 'Map2', 'B AP1', 'MAP3', and 'Indoor Rap1'.

Além disso, insira os nomes dos rádios por conveniência em **Description (Descrição)** (como local, nº AP, etc.) A descrição também pode ser usada para onde os Rádios foram instalados para facilitar a referência a qualquer momento.

Habilitar filtragem de MAC

A filtragem MAC está habilitada por padrão.

Também é possível escolher o modo de segurança como EAP ou PSK na mesma página.

Na interface GUI do switch, use este caminho:

Caminho da interface GUI: **Sem fio > Malha interna**

O modo de segurança SÓ pode ser verificado no CLI por 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-- o^ (quit)
Web Auth Redirect Ports..... 80
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

Implantação de malha interna L3

Para uma rede em malha interna L3, configure os endereços IP dos rádios se não quiser usar o servidor DHCP (interno ou externo).

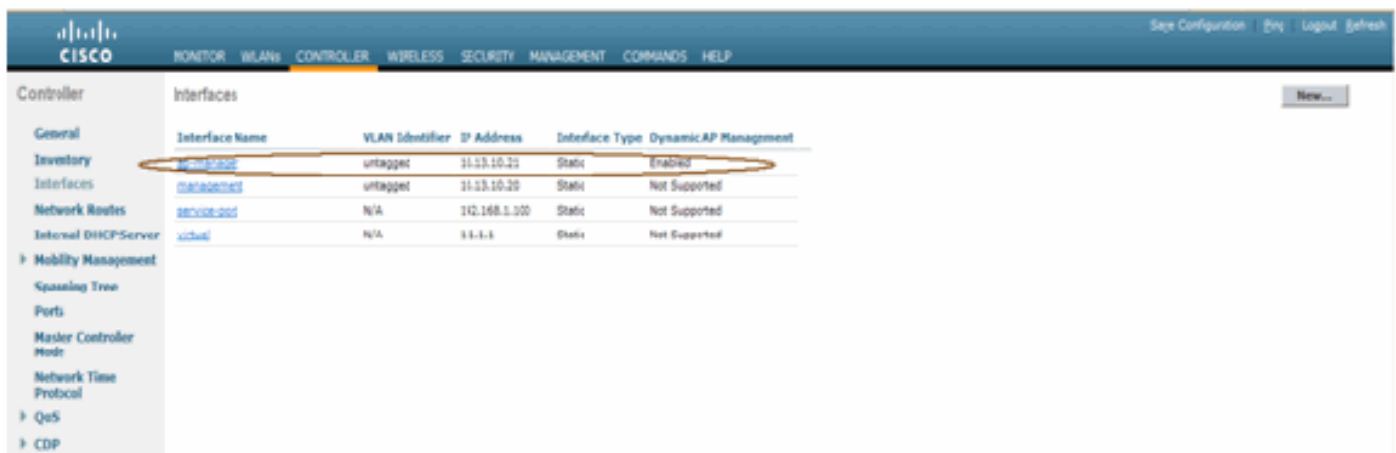
Para uma rede de malha interna L3, se você quiser usar o servidor DHCP, configure a controladora no modo L3. Salve a configuração e reinicialize o controlador. Certifique-se de configurar a Opção 43 no servidor DHCP. Depois que o controlador for reiniciado, os APs recém-conectados receberão seu endereço IP do servidor DHCP.

Definir interfaces no controlador

Gerenciador AP

Para uma implantação L3, você deve definir o **gerenciador de AP**. O AP Manager atua como um endereço IP de origem para comunicação do controlador aos APs.

Caminho: **Controlador > Interfaces > ap-manager > editar.**



The screenshot shows the Cisco Controller web interface. The 'CONTROLLER' tab is selected. On the left, the 'Interfaces' menu item is highlighted. The main area displays a table of 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 interface do **gerenciador de AP** deve receber um endereço IP na mesma sub-rede e na VLAN que a sua interface de gerenciamento.



The screenshot shows the 'Interfaces > Edit' configuration page for the 'ap-manager' interface. The 'CONTROLLER' tab is selected. The left sidebar shows the 'Interfaces' menu item highlighted. The configuration fields are as follows:

Section	Field	Value
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	<input checked="" type="checkbox"/>
DHCP Information	Primary DHCP Server	10.13.10.10
	Secondary DHCP Server	
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.

Funções de rádio

Há duas funções de rádio principais possíveis com esta solução:

- Root Access Point (RAP) - O rádio com o qual você deseja se conectar ao controlador (via switch) assumirá a função de um RAP. Os RAPs têm uma conexão com fio habilitada para LWAPP para o controlador. Um RAP é um nó pai para qualquer bridge ou rede em malha interna. Um controlador pode ter um ou mais RAP, cada um criando um parentesco com as mesmas redes sem fio ou diferentes. Pode haver mais de um RAP para a mesma rede de malha interna para redundância.
- Ponto de acesso interno em malha (MAP) - O rádio que não tem conexão com fio com o controlador assume a função de um AP em malha interna. Este AP era anteriormente chamado Pole top AP. Os MAPs têm uma conexão sem fio (através da interface de backhaul) para talvez outros MAPs e, finalmente, para um RAP e, portanto, para o controlador. Os MAPs também podem ter uma conexão Ethernet com fio para uma LAN e servir como um ponto de extremidade de ponte para essa LAN (usando uma conexão P2P ou P2MP). Isso pode ocorrer simultaneamente, se configurado corretamente como uma bridge Ethernet. Os MAPs atendem clientes na banda não usados para a Interface de Backhaul.

O modo padrão para um AP é MAP.

Observação: as funções de rádio podem ser definidas via GUI ou CLI. Os APs serão reinicializados após a alteração de função.

Observação: você pode usar a CLI do controlador para pré-configurar as funções de rádio em um AP desde que o AP esteja fisicamente conectado ao switch ou você possa ver o AP no switch como um RAP ou um 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)
```

Nome do grupo de bridge

O BGN (Bridge Group Names, nomes de grupo de bridge) controla a associação dos APs. Os BGNs podem agrupar logicamente os rádios para evitar que duas redes no mesmo canal se comuniquem entre si. Essa configuração também é útil se você tiver mais de um RAP em sua rede no mesmo setor (área). O BGN é uma string com no máximo dez caracteres.

Um nome de grupo de bridge definido de fábrica é atribuído no estágio de fabricação (VALOR NULL). Não está visível para você. Como resultado, mesmo sem um BGN definido, os rádios ainda podem ingressar na rede. Se você tiver dois RAPs em sua rede no mesmo setor (para obter mais capacidade), é recomendável configurar os dois RAPs com o mesmo BGN, mas em canais diferentes.

Observação: o nome do grupo de bridge pode ser definido na CLI e na GUI do controlador.

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

Depois de configurar o BGN, o AP será redefinido.

Observação: o BGN deve ser configurado com muito cuidado em uma rede ativa. Você deve sempre começar do nó mais distante (último nó) e mover-se em direção ao RAP. O motivo é que se você começar a configurar o BGN em algum lugar no meio do multissalto, os nós além desse ponto serão descartados, pois esses nós terão um BGN diferente (BGN antigo).

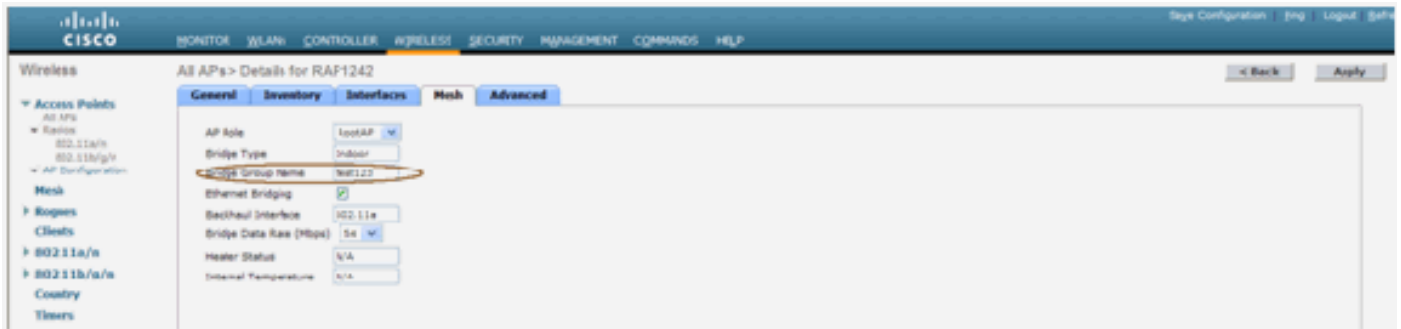
Você pode verificar o BGN emitindo este comando CLI:

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

```
(Cisco Controller) >show ap config general RAPI242  
Cisco AP Identifier..... 0  
Cisco AP Name..... RAPI242  
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 GroupName ..... 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
```

Além disso, você pode configurar ou verificar o BGN usando a GUI do controlador:

Caminho: **Sem fio > Todos os APs > Detalhes.**



Você pode ver que as informações ambientais do AP também são exibidas com essa nova versão.

Configuração de segurança

O modo de segurança de malha interna padrão é EAP. Isso significa que, a menos que você configure esses parâmetros em seu controlador, seus MAPs não participarão:



CLI de configuração de EAP em malha interna

```
(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.
```

Se precisar permanecer no modo PSK, use este comando para voltar ao 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 malha interna

No modo EAP, você pode verificar estes comandos **show** para verificar a autenticação 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 depuração EAP de malha interna

Para depurar qualquer problema no modo EAP, use estes comandos no Controlador:

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

Instalação

Pré-requisitos

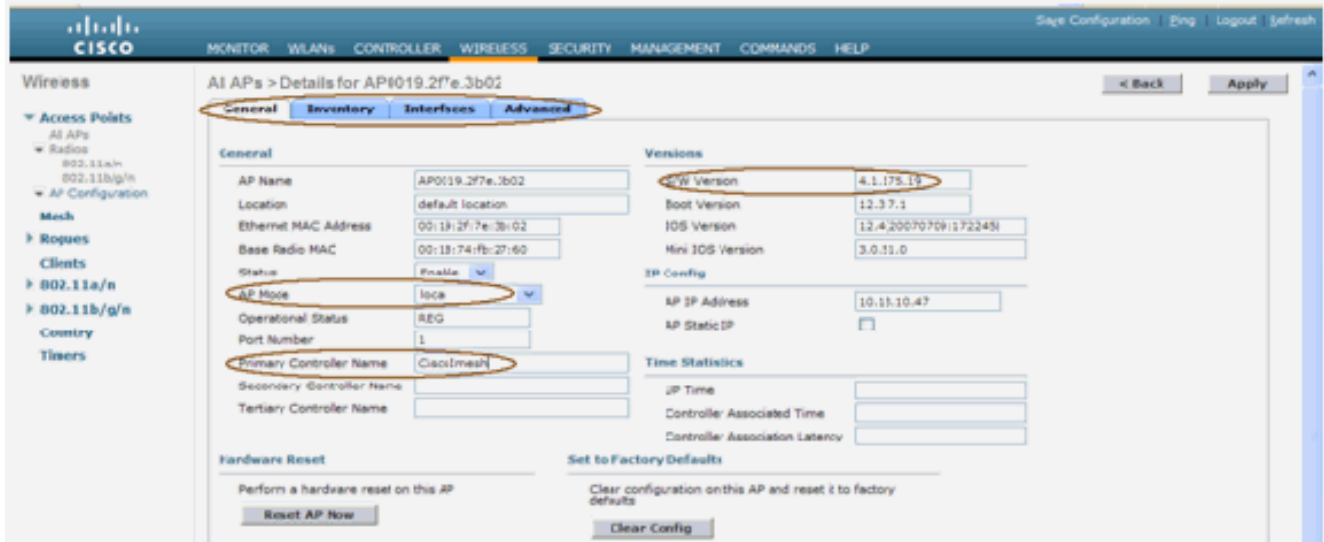
O controlador deve estar executando a versão recomendada do código. Clique em **Monitor** para verificar a versão do Software. O mesmo pode ser verificado via CLI.

```
(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..... 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
```

Sistemas como o servidor DHCP, o servidor ACS e o servidor WCS devem estar acessíveis.

Instalação

1. Conecte todos os LAPs (1131AG/1242AG) a uma rede de Camada 3 na mesma sub-rede do endereço IP de gerenciamento. Todos os APs se juntarão ao controlador como APs no modo local. Nesse modo, coloque os APs em primeiro lugar com o nome da controladora primária, o nome da controladora secundária e um nome da controladora terciária.



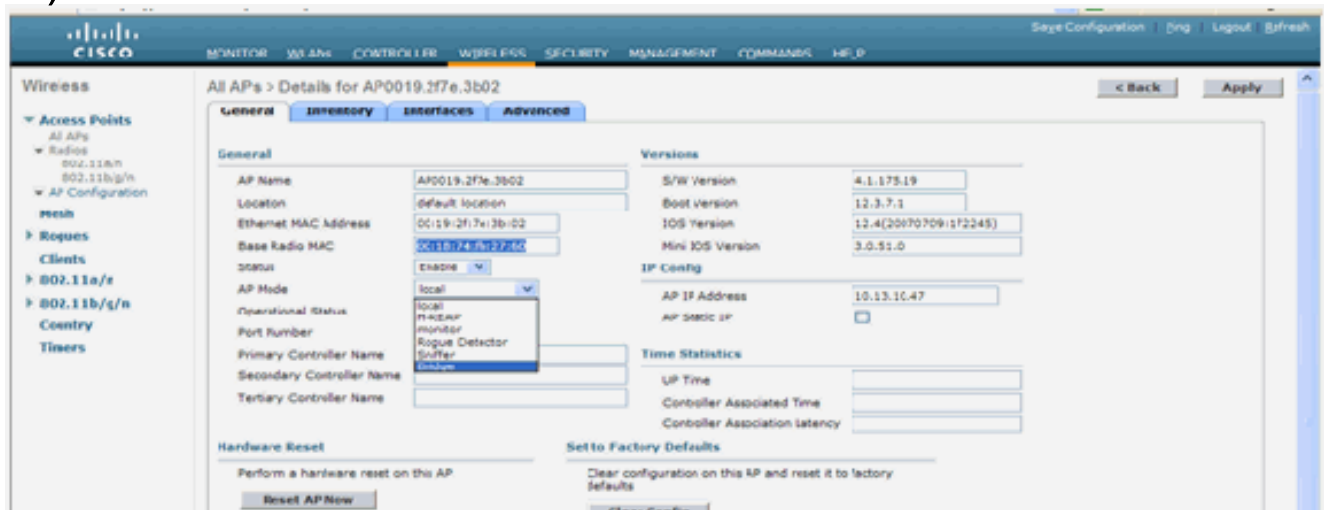
2. Capture o endereço MAC do rádio base do AP (por exemplo, 00:18:74: fb: 27:60).

3. Adicione o endereço MAC do AP para o AP ingressar no modo bridge.

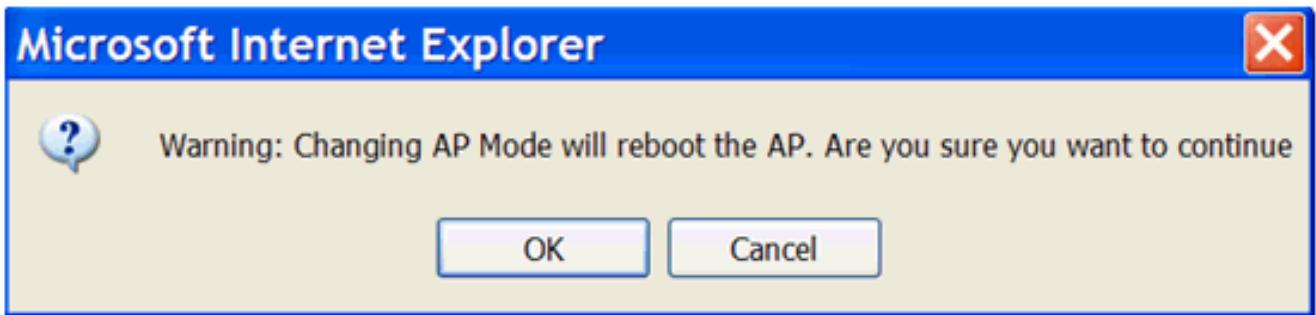
4. Clique em **Security > MAC-filtering > New**.

5. Adicione o endereço MAC copiado e nomeie os APs na lista de filtros MAC e na lista de APs.

6. Escolha **Bridge** na lista **AP Mode (Modo AP)**.



7. Ele solicitará que você confirme, pois isso reinicializará o AP.



8. O AP reinicializará e ingressará na controladora no modo Bridge. A nova janela de AP terá uma guia extra: MALHA. Clique na guia **MESH** para verificar a função, o tipo de bridge, o nome do grupo de bridge, Ethernet Bridging, interface de backhaul, taxa de dados de bridge, etc.



9. Nesta janela, acesse a lista de funções do AP e escolha a função relevante. Nesse caso, a função por padrão é um MAP. Por padrão, o nome do Grupo de Bridge está vazio. A interface de backhaul é 802.11a. A taxa de dados da bridge (ou seja, a taxa de dados do Back haul) é de 24 Mbps.
10. Conecte o AP que você deseja como RAP ao controlador. Implante os rádios (MAPs) nos locais desejados. Ligue os rádios. Você deve conseguir ver todos os rádios na controladora.

```
(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. Tente ter condições de linha de visão entre os nós. Se não existirem condições de linha de visão, crie clareamentos de zona de Fresnel para obter condições de linha próxima do local.
12. Se você tiver mais de um controlador conectado à mesma rede em malha interna, você deverá especificar o nome do controlador principal em cada nó. Caso contrário, o controlador que é visto primeiro será considerado o principal.

Configuração de alimentação e canal

O canal de backhaul pode ser configurado em um RAP. Os MAPs serão ajustados para o canal RAP. O acesso local pode ser configurado independentemente para MAPs.

Na GUI do Switch, siga o caminho: **Sem fio > rádio 802.11a > configurar**.



Observação: o nível de potência Tx padrão no backhaul é o nível de potência mais alto (Nível 1) e o RRM (Radio Resource Management, gerenciamento de recursos de rádio) está desativado por padrão.

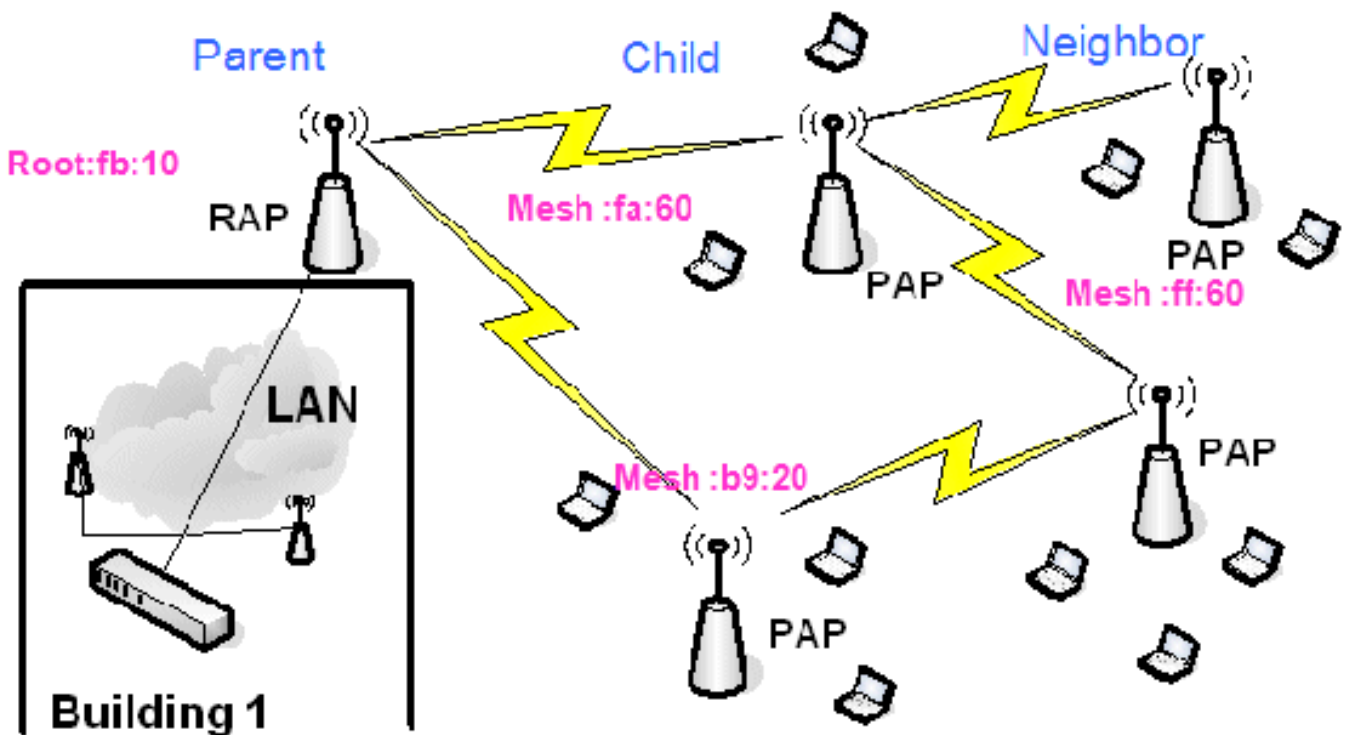
Se você estiver alocando RAPs, recomendamos o uso de canais adjacentes alternativos em cada RAP. Isso reduzirá a interferência entre canais.

Verificação de RF

Em uma rede em malha interna, devemos verificar a relação pai-filho entre os nós. **O salto** é um link sem fio entre os dois rádios. A relação pai-filho é alterada à medida que você viaja pela rede. Depende de onde você está na rede em malha interna.

O rádio mais próximo do controlador em uma conexão sem fio (salto) é um **pai** do rádio no outro lado do salto. Em um sistema de vários saltos, há uma estrutura de tipo de árvore em que o nó conectado ao controlador é um RAP (**pai**). O nó imediato no outro lado do primeiro salto é um **Filho**, e nós subsequentes no segundo salto em diante são os **Vizinhos** para esse Pai específico.

Figura 1: Rede de dois saltos



Na Figura 1, os nomes de AP são mencionados por conveniência. Na próxima captura de tela, o **RAP(fb:10)** está sendo investigado. Esse nó pode ver (na implantação real) os APs de malha interna (fa:60 & b9:20) como filhos e **MAP ff:60** como vizinhos.

Na interface GUI do switch, siga o caminho: **Sem Fio > Todos os APs > Rap1 > Informações de Vizinhos**.



Assegure-se de que as relações pai-filho sejam estabelecidas e mantidas corretamente para sua rede de malha interna.

Verificar as interconexões

show Mesh é um comando informativo para verificar a interconectividade em sua rede.

Você deve fornecer esses comandos em cada nó (AP) usando a CLI do controlador e carregar os resultados em um arquivo Word ou de texto para o site de carregamento.

```
(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.
```

Em sua rede em malha interna, escolha um link de salto múltiplo e emita esses comandos a partir do RAP. Carregue o resultado dos comandos no site de upload.

Na próxima seção, todos esses comandos foram emitidos para a rede de malha interna de dois saltos, mostrada na Figura 1.

[Mostrar caminho de malha interna](#)

Esse comando mostrará os endereços MAC, as funções de rádio dos nós, os índices de Sinal para Ruído em dBs para Uplink/Downlink (SNRUp, SNRDown) e Link SNR em dB para um caminho específico.

```
(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 Resumo do Vizinho de Malha Interno](#)

Esse comando mostrará os endereços MAC, as relações pai-filho e os SNRs Uplink/Downlink em 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
```

Até esse momento, você deve ser capaz de ver as relações entre os nós da rede e verificar a conectividade de RF ao ver os valores de SNR para cada link.

Segurança de acesso ao console AP

Esse recurso oferece segurança avançada ao acesso do console do AP. É necessário um cabo de console para o AP para usar esse recurso.

São suportados:

- Uma CLI para enviar a combinação user-id/password para o 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.
```

- Um comando CLI para enviar a combinação nome de usuário/senha para todos os APs registrados no controlador:

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

Com esses comandos, a combinação userid/password extraída do controlador é persistente durante a recarga nos APs. Se um AP for removido da controladora, não haverá modo de acesso de segurança. O AP gera uma interceptação SNMP com um login bem-sucedido. O AP também gerará uma interceptação SNMP em uma falha de login de console por três vezes consecutivas.

Bridging Ethernet

Por motivos de segurança, a porta Ethernet nos MAPs é desativada por padrão. Ele só pode ser ativado pela configuração do Ethernet Bridging no RAP e nos respectivos MAPs.

Como resultado, o Ethernet Bridging deve ser ativado para dois cenários:

- Quando quiser usar os nós de malha interna como bridges.
- Quando quiser conectar qualquer dispositivo Ethernet (como PC/Laptop, câmera de vídeo, etc.) no MAP usando sua porta Ethernet.

Caminho: **Sem fio** > Clique em qualquer AP > **Mesh**.



Há um comando CLI que pode ser usado para configurar a distância entre os nós que fazem o Bridging. Tente conectar um dispositivo Ethernet como uma câmera de vídeo em cada salto e veja o desempenho.

Aprimoramento do nome do grupo de bridge

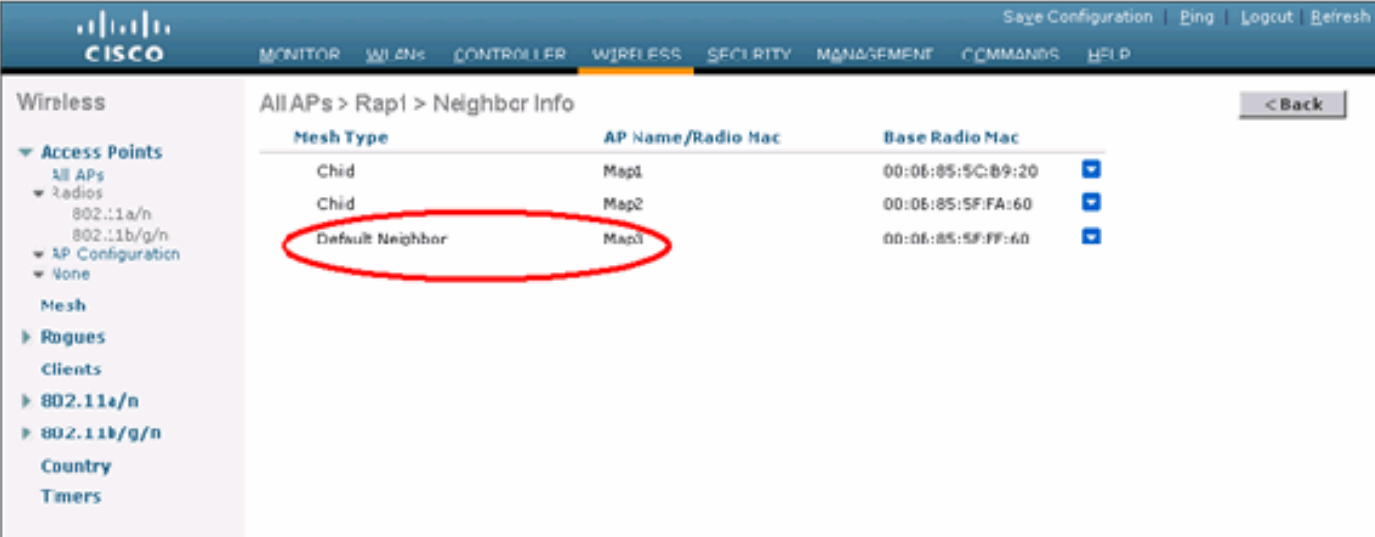
É possível que um AP seja provisionado incorretamente com um "nome de grupo de bridge" para o qual não foi planejado. Dependendo do projeto de rede, esse AP pode ou não conseguir alcançar e encontrar seu setor/árvore corretos. Se não conseguir chegar a um setor compatível, poderá ficar bloqueado.

Para recuperar esse AP retorcido, o conceito de "default" bridgegroupname foi introduzido com o código 3.2.xx.x. A ideia básica é que um AP que é incapaz de se conectar a qualquer outro AP com seu nome de grupo de bridge configurado, tenta se conectar com "default" (a palavra) como nome de grupo de bridge. Todos os nós que executam o software 3.2.xx.x e posterior aceitam outros nós com esse nome de grupo de bridge.

Esse recurso também pode ajudar a adicionar um novo nó ou um nó configurado incorreto a uma rede em execução.

Se você tiver uma rede em execução, pegue um AP pré-configurado com um BGN diferente e faça com que ele se junte à rede. Você verá esse AP na controladora usando o BGN "padrão" depois de adicionar seu endereço MAC na controladora.

```
(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 Controller GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area is titled 'All APs > Rap1 > Neighbor Info'. A table displays neighbor information:

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

O AP que usa o BGN padrão pode atuar como um AP de malha interna normal que associa clientes e forma relações pai de malha interna.

No momento em que esse AP usando o BGN padrão encontrar outro pai com o BGN correto, ele mudará para ele.

Logs - Mensagens, Sys, AP e Trap

Logs de mensagem

Habilite o nível de relatório para logs de mensagens. Na CLI da controladora, emita 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 os registros de mensagens, emita este comando da CLI do 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 carregar os registros de mensagens, use a interface GUI do controlador:

1. Clique em **Commands > Upload**.



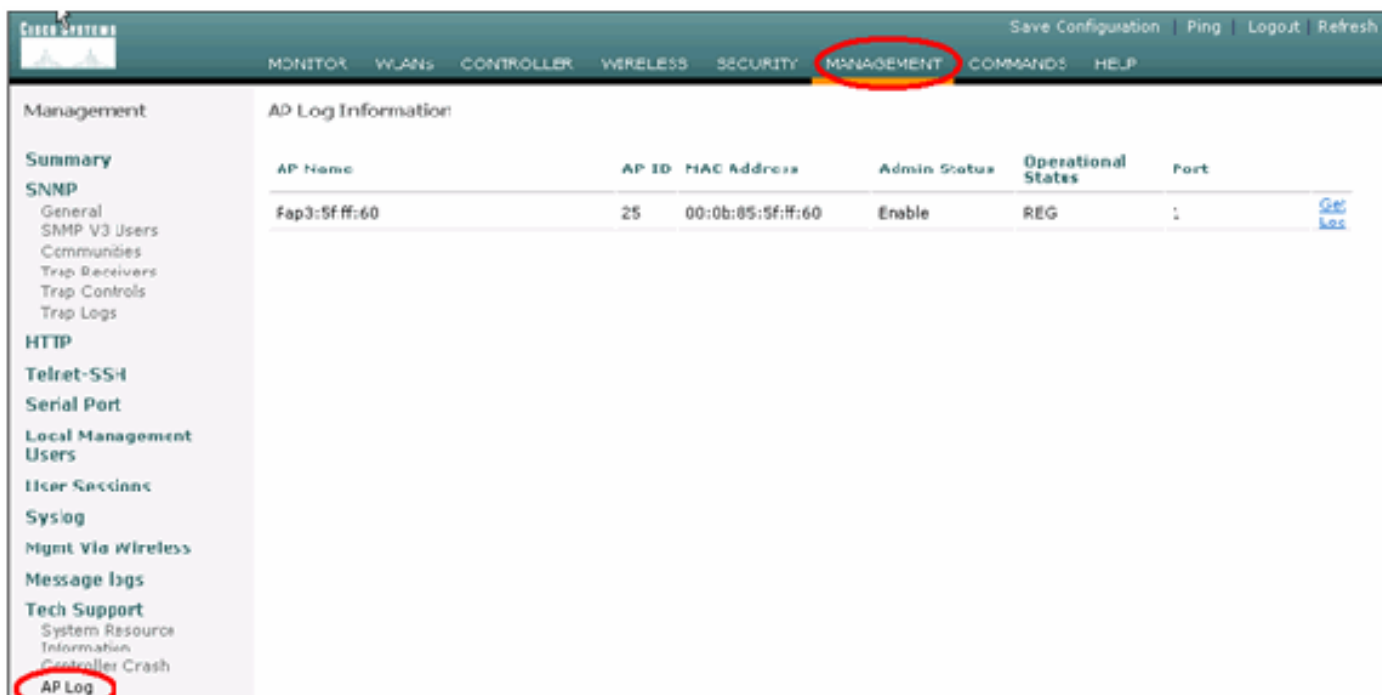
2. Insira as informações do servidor TFTP. Esta página fornecerá várias opções para carregar e você deseja que estes arquivos sejam enviados: Log de mensagens Log de eventos Registro de interceptação Arquivo de travamento (se houver) Para verificar se há

arquivos Crash, clique em **Management > Controller Crash**.



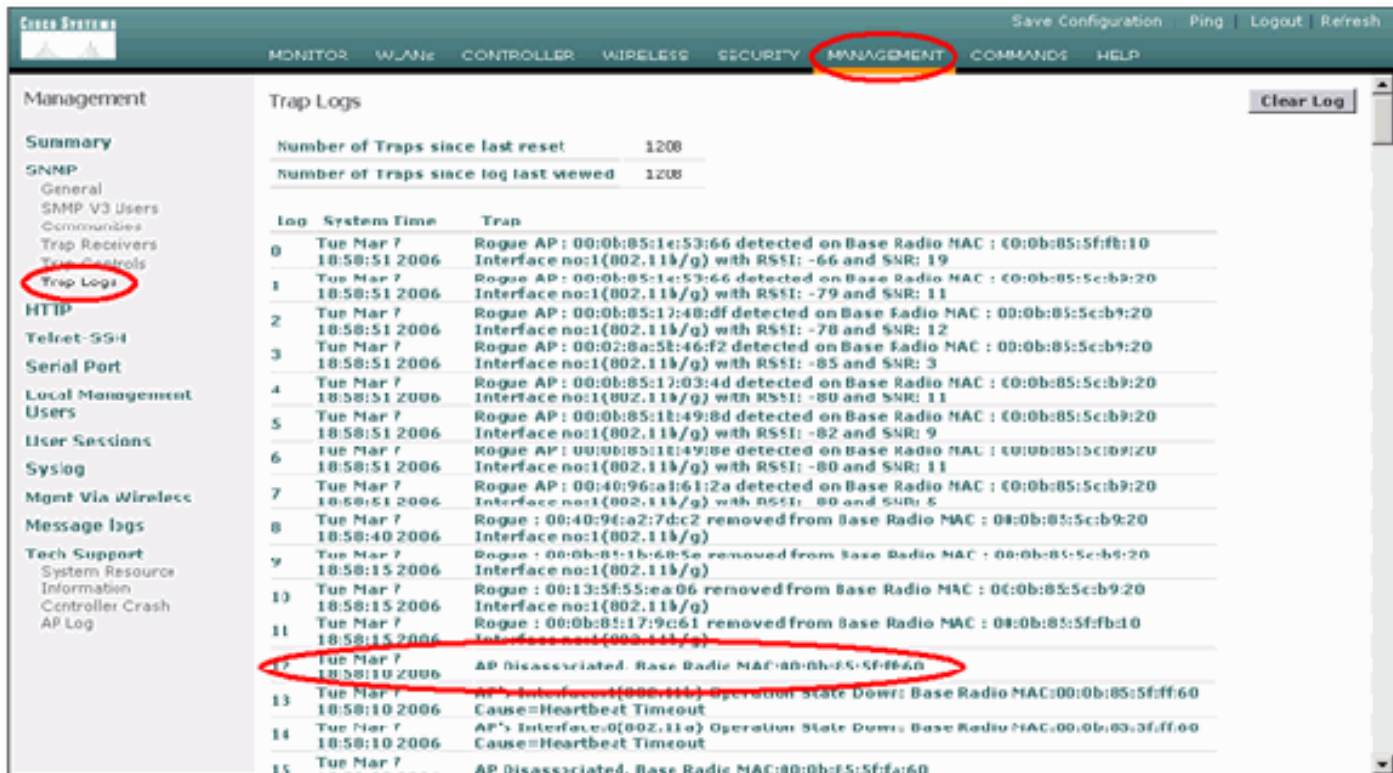
Logs AP

Vá para esta página da GUI no controlador para verificar os registros de AP para seu AP local, se houver:



Logs de interceptação

Vá para esta página GUI do controlador e verifique os Logs de interceptação:



Desempenho

Teste de convergência de inicialização

Convergência é o tempo gasto por um RAP/MAP para estabelecer uma conexão LWAPP estável com um controlador WLAN a partir do momento em que ele foi inicializado pela primeira vez, conforme listado aqui:

Teste de convergência	Tempo de convergência (min:s)			
	RAP	MAP1	MAP2	MAP3
Atualização de imagem	2:34	3:50	5:11	6:38
Reinicialização da controladora	0:38	0:57	1:12	1:32
Ligar a rede em malha interna	2:44	3:57	5:04	6:09
reinicialização de RAP	2:43	3:57	5:04	6:09
Reingressar no MAP		3:58	5:14	6:25
Alteração de MAP do pai (mesmo canal)		0:38		

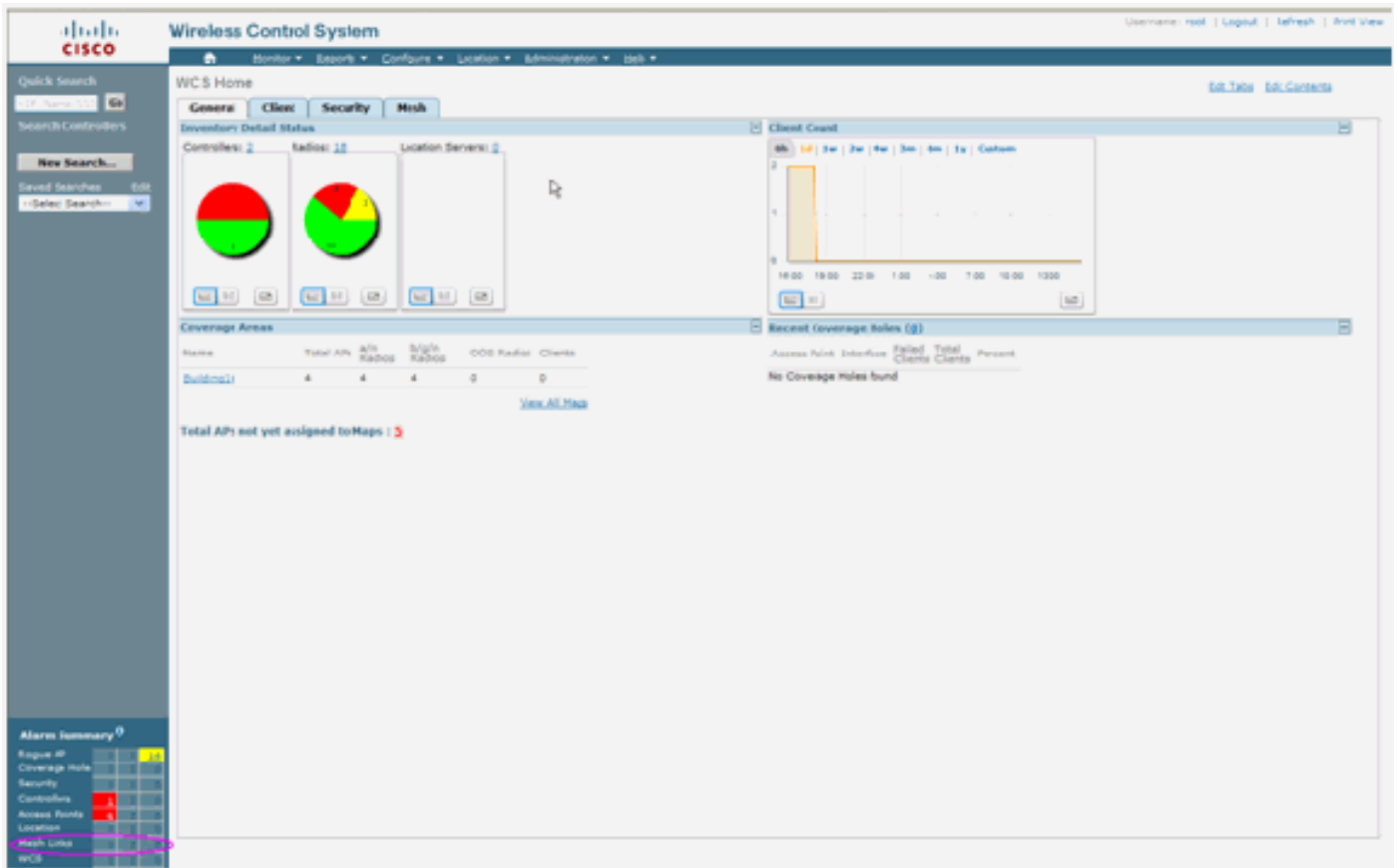
WCS

Alarmes em malha interna

O WCS gerará esses alarmes e eventos relacionados à rede em malha interna com base nas armadilhas do controlador:

- SNR de link ruim
- Pai alterado
- Filho movido
- MAP Alterações pai com frequência
- Evento da porta do console
- Falha na autorização de MAC
- Falhas de autenticação
- Pai excluído filho

Clique em **Mesh Links**. Ele mostrará todos os alarmes relacionados aos links de malha interna.



Esses alarmes se aplicam a links de malha interna:

- SNR de link ruim - esse alarme é gerado se o SNR do link cair abaixo de 12db. O usuário não pode alterar esse limite. Se um SNR ruim for detectado no link de backhaul para filho/pai, a armadilha será gerada. A armadilha conterá o valor de SNR e os endereços MAC. Gravidade do alarme é grave. A relação SNR (sinal/ruído) é importante porque a alta intensidade do sinal não é suficiente para garantir um bom desempenho do receptor. O sinal de entrada deve ser mais forte do que qualquer ruído ou interferência presente. Por exemplo, é possível ter uma alta intensidade de sinal e ainda ter um desempenho sem fio ruim se houver uma interferência forte ou um nível de ruído alto.
- Pai alterado - Este alarme é gerado quando o filho é movido para outro pai. Quando o pai for perdido, o filho se juntará a outro pai e o filho enviará uma interceptação contendo os endereços MAC do pai e do pai novos para o WCS. Gravidade do alarme: Informativo.
- Filho movido - Este alarme é gerado quando o WCS recebe uma armadilha de filho perdido. Quando o AP pai detectou a perda de um filho e não consegue se comunicar com ele, ele enviará uma interceptação do filho perdido para o WCS. A armadilha conterá o endereço MAC filho. Gravidade do alarme: Informativo.

- O pai MAP foi alterado frequentemente - esse alarme é gerado se o AP de malha interna alterar seu pai frequentemente. Quando o contador de alteração pai do MAP exceder o limite em uma determinada duração, ele enviará uma interceptação para o WCS. A armadilha conterá o número de vezes de alterações de MAP e a duração do tempo. Por exemplo, se houver 5 alterações em 2 minutos, a armadilha será enviada. Gravidade do alarme: Informativo.
- Pai Excluído Filho - Este alarme é gerado quando um filho está na lista negra de um pai. Um filho pode fazer uma lista negra de um pai quando o filho não conseguiu autenticar no controlador após um número fixo de tentativas. O filho se lembra do pai da lista negra e quando o filho ingressa na rede, ele enviará a interceptação que contém o endereço MAC pai da lista negra e a duração do período da lista negra.

Alarmes diferentes dos links de malha interna:

- Acesso à porta de console - A porta de console permite que o cliente altere o nome de usuário e a senha para recuperar o AP externo retorcido. No entanto, para impedir que qualquer usuário autorizado acesse o AP, o WCS precisa enviar um alarme quando alguém tentar fazer login. Esse alarme é necessário para fornecer proteção, já que o AP é fisicamente vulnerável enquanto está localizado em áreas externas. Esse alarme será gerado se o usuário tiver feito login com êxito na porta do console do AP ou se ele tiver falhado três vezes consecutivas.
- Falha na autorização do MAC - esse alarme é gerado quando o AP tenta se juntar à malha interna, mas não se autentica porque não está na lista de filtros do MAC. O WCS receberá uma interceptação do controlador. A interceptação conterá o endereço MAC do AP que falhou a autorização.

Relatório e estatísticas da malha

Realizamos o relatório e o quadro estatístico melhorados de 4.1.185.0:

- Nenhum caminho alternativo
- Saltos do nó da malha
- Estatísticas de erro de pacotes
- Estatísticas de pacotes
- Salto do pior nó
- Pior links SNR

The screenshot shows the Cisco WCS interface. The top navigation bar includes 'Monitor', 'Reports', 'Configure', 'Location', 'Administration', and 'Help'. The main content area is titled 'Mesh No Alternate Parent' and contains a table with the following data:

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

Below the table is an 'Alarm Summary' section with the following data:

Alarm Category	Count
Rogue AP	0
Coverage Hole	0
Security	0
Controllers	0
Access Points	2
Mesh Links	0
Location	0

[Nenhum caminho alternativo](#)

O AP em malha interna normalmente tem mais de um vizinho. Caso um AP de malha interna perca seu link pai, o AP deve ser capaz de encontrar o pai alternativo. Em alguns casos, se não houver vizinhos mostrados, o AP não poderá ir para nenhum outro pai se perder seus pais. É fundamental que o usuário saiba quais APs não têm pais alternativos. Este relatório lista todos os APs que não têm nenhum outro vizinho além do pai atual.

[Saltos do nó da malha interna](#)

Este relatório mostra o número de saltos distantes do AP raiz (RAP). Você pode criar o relatório com base nestes critérios:

- AP por controlador
- AP por andar

[Taxas de erro de pacote](#)

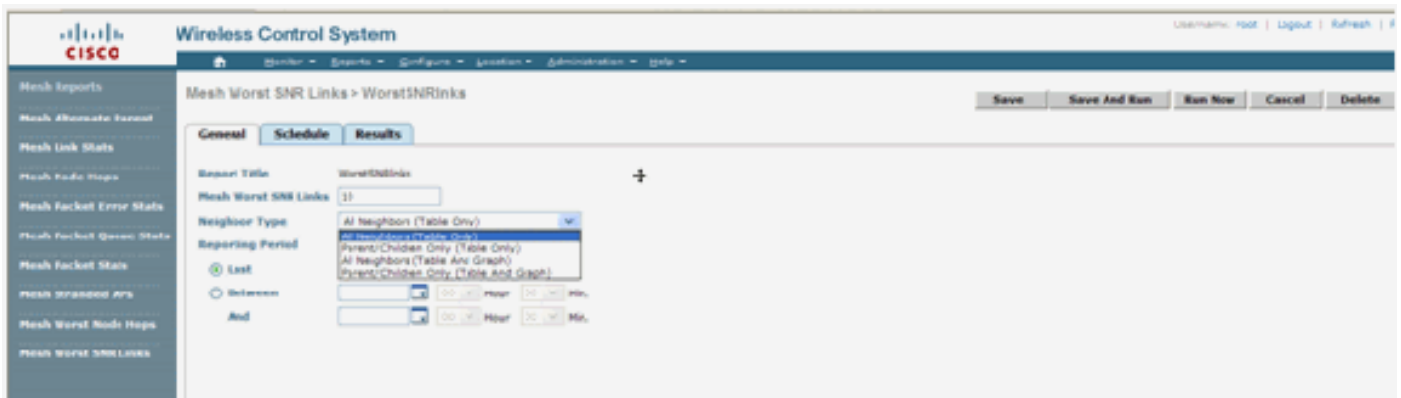
Os erros de pacote podem ser causados por interferência e quedas de pacote. O cálculo da taxa de erro do pacote baseia-se nos pacotes enviados e nos pacotes enviados com êxito. A taxa de erro do pacote é medida no link de backhaul e é coletada tanto para os vizinhos quanto para o pai. O AP envia periodicamente informações de pacote ao controlador. Assim que o pai for alterado, o AP enviará as informações de erro do pacote coletado ao controlador. Por padrão, o WCS pesquisa informações de erro de pacote do controlador a cada 10 minutos e as armazena no banco de dados por até 7 dias. No WCS, a taxa de erro do pacote é mostrada como um gráfico. O gráfico de erros de pacote é baseado nos dados históricos armazenados no banco de dados.

[Estatísticas de pacotes](#)

Este relatório mostra os valores do contador dos pacotes de transmissão total do vizinho e dos pacotes Total do vizinho transmitidos com êxito. Você pode criar o relatório com base em determinados critérios.

[Os piores links SNR](#)

Problemas de ruído podem ocorrer em diferentes momentos e o ruído pode aumentar em diferentes taxas ou durar por diferentes períodos de tempo. A próxima figura oferece a capacidade de criar relatórios para o Radio a e b/g, bem como para interfaces seletivas. O relatório lista os 10 piores links SNR por padrão. Você pode escolher entre 5 e 50 piores links. O relatório pode ser gerado para as últimas 1 hora, 6 horas, último dia, 2 dias e até 7 dias. Os dados são pesquisados a cada 10 minutos por padrão. Os dados são mantidos no banco de dados por no máximo sete dias. Os critérios de seleção de Tipo de vizinho podem ser Todos os vizinhos, Somente pai/filho.



Wireless Control System

Mesh Worst SNR Links > WorstSNRlinks

Save Save And Run Run Now Cancel Delete

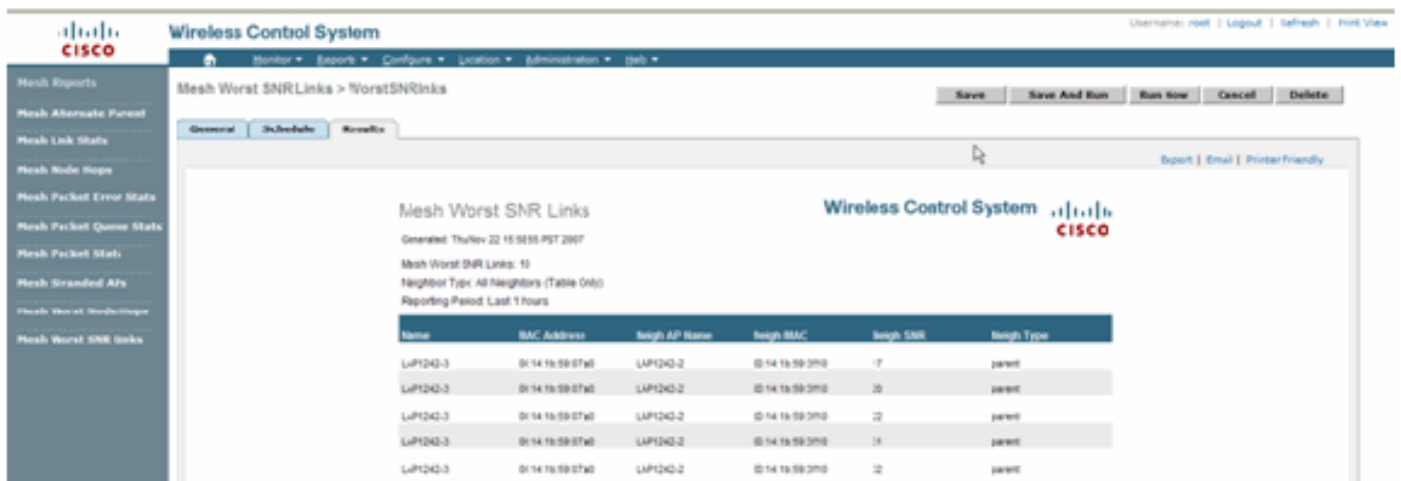
General Schedule Results

Report Title: WorstSNRlinks

Mesh Worst SNR Links: 10

Neighbor Type: All neighbors (Table Only)

Reporting Period: Last



Wireless Control System

Mesh Worst SNR Links > WorstSNRlinks

Save Save And Run Run Now Cancel Delete

General Schedule Results

Mesh Worst SNR Links

Generated: Thu/ev 22 15:53:55 PST 2007

Mesh Worst SNR Links: 10

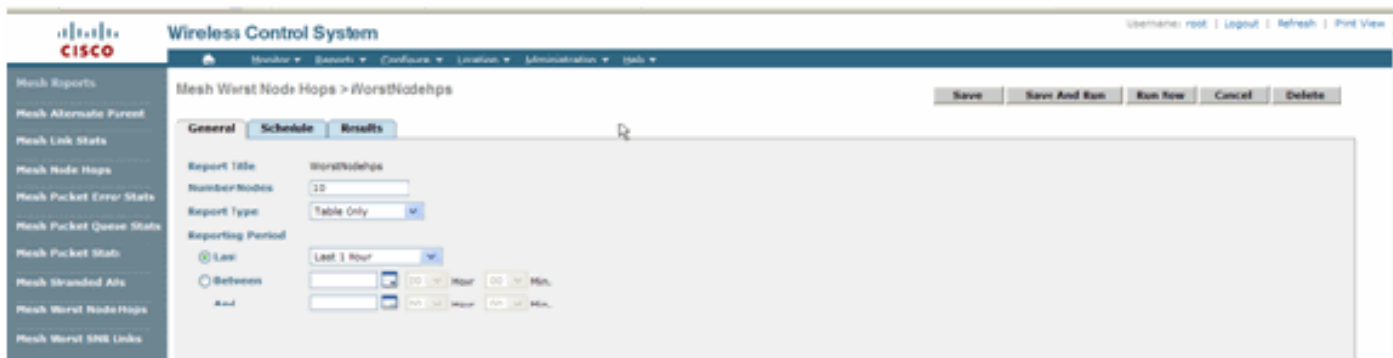
Neighbor Type: All Neighbors (Table Only)

Reporting Period: Last 1 hours

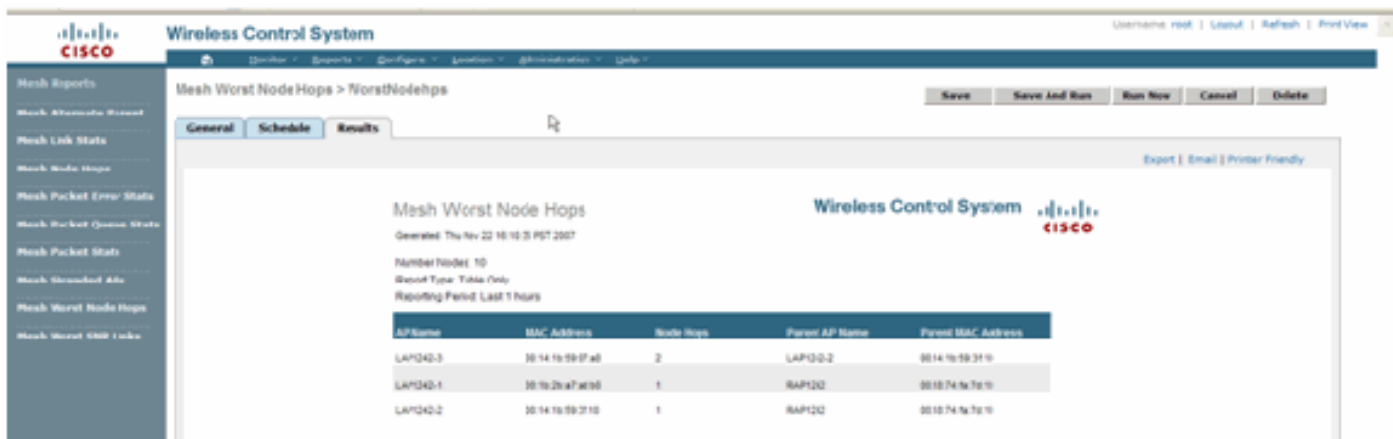
Name	MAC Address	Neighbor AP Name	Neighbor MAC	Neighbor SNR	Neighbor Type
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:31b0	-7	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:31b0	10	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:31b0	22	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:31b0	14	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:31b0	12	parent

[Saltos do pior nó](#)

Esse relatório lista os 10 piores APs de saltos por padrão. Se os APs estiverem a muitos saltos de distância, os links podem ser muito fracos. O usuário pode isolar os APs que têm muitos saltos de distância do AP raiz e tomar as medidas apropriadas. Você pode optar por alterar este critério **Número de Nós** entre 5 e 50. Os critérios de filtro **Tipo de Relatório** nesta figura podem ser Somente Tabela ou Tabela e Gráfico:



Esta figura mostra o resultado do último relatório:



[Estatísticas de segurança](#)

As estatísticas de segurança em malha interna são exibidas na página de detalhes do AP na seção de informações de Bridging. Uma entrada na tabela de estatísticas de segurança meshNode interna é criada quando um nó de malha interna filho associa ou autentica com um nó de malha interna pai. As entradas são removidas quando o nó de malha interna se desassocia do controlador.

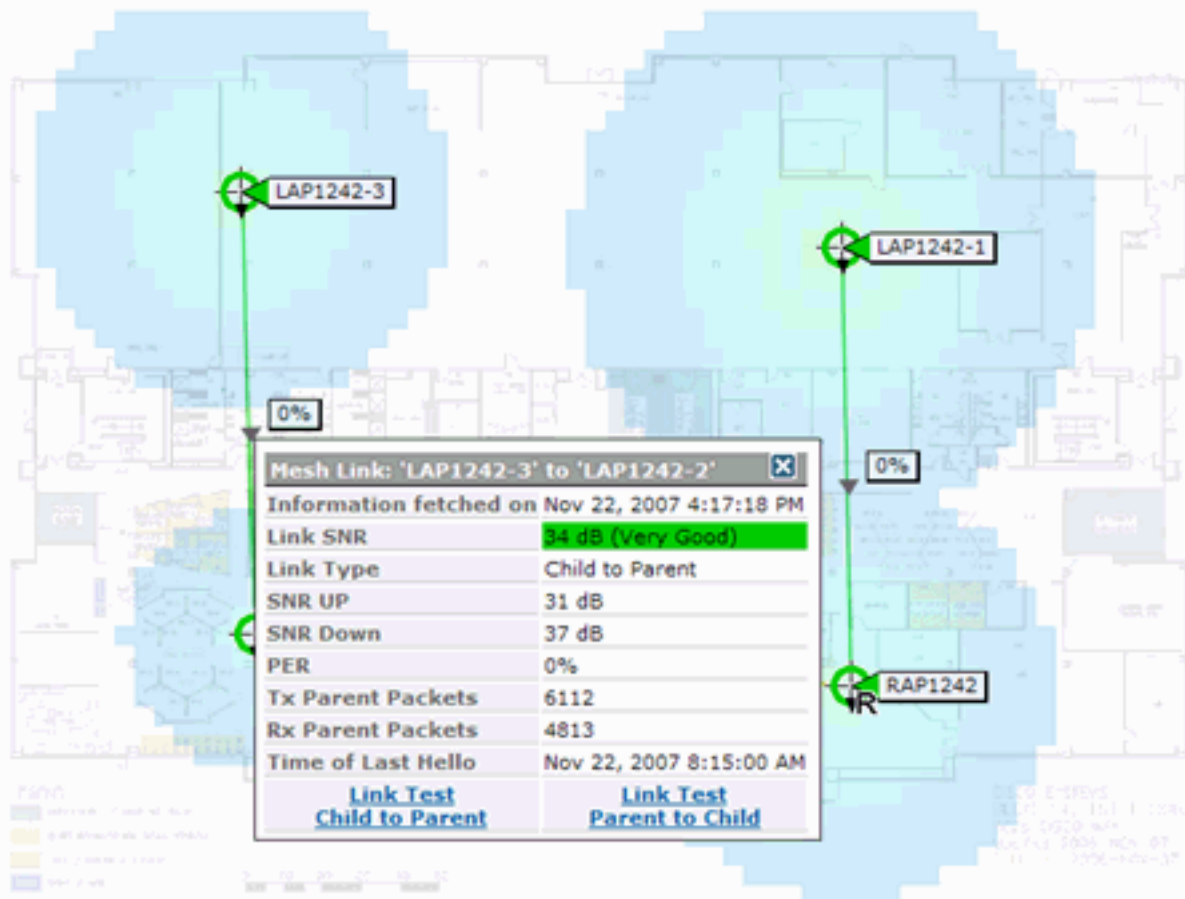
[Teste de link](#)

O teste de link AP-a-AP é suportado no WCS. É possível selecionar dois APs e chamar um teste de link entre os dois.

Se esses APs forem vizinhos de RF, o teste de link pode ter um resultado. O resultado é mostrado em uma caixa de diálogo no próprio mapa sem uma atualização completa da página. O diálogo pode ser descartado facilmente.

No entanto, se esses 2 APs não forem vizinhos de RF, o WCS não tentará descobrir um caminho entre os 2 APs para fazer um teste de vários links combinados.

Quando o mouse é movido sobre a seta no link entre os dois nós, esta janela é exibida:



Teste de enlace nó a nó

A ferramenta Link Test é uma ferramenta sob demanda para verificar a qualidade do link entre dois APs. No WCS, esse recurso é adicionado na página de detalhes do AP.

Na página de detalhes do AP, na guia **Indoor Mesh Link**, onde os links estão listados ao lado, há um link para executar o teste de link.

A ferramenta Controller CLI Link Test tem os parâmetros de entrada opcionais: Tamanho do pacote, pacotes de teste de enlace total, duração do teste e taxa de enlace de dados. O teste de link tem valores padrão para esses parâmetros opcionais. Os endereços MAC dos nós são os únicos parâmetros de entrada obrigatórios.

A ferramenta Link Test testa a intensidade, o pacote enviado e o pacote recebido entre os nós. O link para Teste de link é exibido no relatório de detalhes do AP. Quando você clica no link, há uma tela pop-up mostrando os resultados do teste de link. O teste de link só será aplicável a filho pai e entre vizinhos.

A saída do teste de enlace gera pacotes enviados, pacotes recebidos, pacotes de erro (buckets por motivos de diferenças), SNR, Noise Floor e RSSI.

O teste de link fornece estes detalhes na GUI pelo menos:

- Pacotes de teste de link enviados
- Pacotes de teste de link recebidos
- Intensidade do sinal em dBm

- Relação sinal/ruído

[Links de vizinhos de AP sob demanda](#)

Esse é um novo recurso no mapa do WCS. Você pode clicar em um AP Mesh e uma janela pop-up com informações detalhadas será exibida. Em seguida, você pode clicar em **Exibir vizinhos de malha**, que busca as informações de vizinhos para o AP selecionado e exibe uma tabela com todos os vizinhos para o AP de malha interna selecionado.

O link View Mesh Neighbor exibe todos os vizinhos do AP realçado. Esse snapshot mostra todos os vizinhos, o Tipo de vizinhos e o valor de SNR.

[Teste de ping](#)

O teste de ping é uma ferramenta sob demanda usada para fazer ping entre o controlador e o AP. A ferramenta Ping Test está disponível na página de detalhes do AP e no MAP. Clique no link **Executar teste de ping** na página de detalhes do AP ou nas informações do AP MAP para iniciar o ping do controlador para o AP atual.

[Conclusão](#)

A malha corporativa (ou seja, malha interna) é uma extensão da cobertura sem fio da Cisco para locais onde a Ethernet com fio não pode fornecer conectividade. A flexibilidade e a capacidade de gerenciamento de uma rede sem fio são obtidas com a malha corporativa.

A maioria dos recursos que os APs com fio fornecem é fornecida pela topologia em malha interna. A malha corporativa também pode coexistir com os APs com fio no mesmo controlador.

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)