# Guia de distribuição interno da malha

## Índice

# Introdução

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). Fornece um rádio 2.4 gigahertz e um compatível de rádio 5.8 gigahertz o 802.11b/g e o 802.11a. Um rádio pode ser usado para o acesso local (do cliente) para o Access Point (AP) e o segundo rádio pode ser configurado para o regresso sem fio. LAP1242/LAP1131 apoia o P2P, o P2MP, e o tipo da malha de arquiteturas.

Certifique-se ler através do guia antes de tentar algumas das instalações.

Este original descreve o desenvolvimento da Rede sem fio da empresa para a malha interna. Este original permitirá utilizadores finais sem fio de compreender os fundamentos da malha interna, onde configurar a malha interna, e como configurar a malha interna. A malha interna é um subconjunto da Rede sem fio do Cisco enterprise distribuído usando controladores sem fio e APs de pouco peso.

A malha interna é um subconjunto da arquitetura da malha da empresa distribuído na arquitetura sem fio unificada. A malha interna está na procura hoje. Com malha interna, um dos rádios (tipicamente 802.11b/g) e/ou a relação dos Ethernet ligada com fio está usado para conectar aos clientes, quando o segundo rádio (tipicamente 802.11a) for usado ao tráfego do cliente do regresso. O regresso pode ser um salto único ou sobre lúpulos múltiplos. A malha interna traz-lhe estes valores:

- Não tendo que executar os Ethernet que prendem a cada AP.
- A porta de Ethernet switch não é exigida para cada AP.
- Conectividade de rede onde os fios não podem fornecer a Conectividade.
- Flexibilidade no desenvolvimento – não restringido a 100m de um Switch Ethernet.
- Fácil distribuir uma rede Wireless ad hoc.

os varejistas da Grande-caixa são atraídos muito à malha interna devido às economias de custos na fiação assim como para as razões mencionadas previamente.

Uso que dos especialistas do inventário n que executa o inventário conta para varejistas, usinas, e outras empresas. Querem distribuir rapidamente uma rede provisória do Wi-fi em uma site de cliente para permitir a Conectividade do tempo real para seus dispositivos handheld. Os seminários, as conferências, a fabricação, e a hospitalidade educacionais são alguns dos lugares onde a arquitetura interna da malha é precisada.

Quando você termina ler este guia, você compreenderá onde usar-se e como configurar a malha interna. Você igualmente compreenderá que a malha interna nos anexos NEMA não é uma substituição para a malha exterior. Mais, você igualmente compreenderá a superioridade da malha interna sobre a flexibilidade do papel da relação (malha do salto único) usada por APs autônomos.

**Suposições:**

Você tem o conhecimento da rede de Cisco Unified Wireless, da arquitetura, e do Produtos. Você

tem o conhecimento do Produtos exterior da malha de Cisco e o algum da terminologia usada para trabalhos em rede da malha.

| Glossário dos acrônimos | |
|---|---|
| LWAPP | Protocolo de pouco peso do Access point – O controle e o protocolo do tunelamento de dados entre APs e o controlador do Wireless LAN. |
| Controlador de WLAN /Controller /WLC | Controlador do Wireless LAN – Dispositivos Cisco que centralizam e simplificam o Gerenciamento de redes de um WLAN pelo número grande de desmoronamento de valores-limite controlados em um único, sistema unificado, permitindo um sistema inteligente unificado da rede de WLAN da informação. |
| RAP | Access point do telhado do ponto de acesso raiz – Os dispositivos de Cisco Wireless atuam como a ponte entre o controlador e o outro Sem fio APs. APs que são prendidos ao controlador. |
| MAPA | Malha APs – O dispositivo de Cisco Wireless que conecta a um RAP ou a um MAPA sobre o ar em um rádio 802.11a e também presta serviços de manutenção a clientes em um rádio 802.11b/g. |
| Pai | Um AP (um ou outro um RAP/MAP) que forneça o acesso a outros APs sobre o ar em um rádio 802.11a. |
| Vizinho | Todos os APs em uma rede de malha são vizinhos e têm vizinhos. O RAP não tem um vizinho como ele prendeu ao controlador. |
| Criança | Um AP mais distante do controlador é sempre uma |

| | |
|---|---|
| | criança. Uma criança terá um pai e muitos vizinhos em uma rede de malha. Se o pai morre, o vizinho seguinte com o melhor valor da facilidade será pai escolhido. |
| SNR | Taxa sinal para ruído. |
| BGN | Nome de grupo de bridge |
| EAP | Protocolo extensible authentication |
| PSK | Chave Preshared |
| AWPP | Protocolo sem fio adaptável do trajeto |

## Overview

O Access point interno da rede de malha de Cisco é um dispositivo de infraestrutura do Wi-fi do dois-rádio para disposições internas selecionadas. É um produto baseado no Lightweight Access Point Protocol (LWAPP). Fornece um rádio 2.4 gigahertz e um compatível de rádio 5.8 gigahertz o 802.11b/g, os padrões 802.11a. Um rádio (802.11b/g) pode ser usado para o acesso local (do cliente) para o AP e o segundo rádio (802.11a) pode ser configurado para o regresso sem fio. Fornece uma arquitetura interna da malha, onde os Nós diferentes (rádios) falem entre si através do regresso e igualmente forneçam o acesso de cliente local. Este AP pode igualmente ser usado para arquiteturas de Bridging pontos a ponto e point-to-multipoint. A solução de rede de malha interna sem fio é ideal para a grande cobertura interna como você pode ter taxas de dados altas e a boa confiança com infraestrutura mínima. Estas são as características salientes básicas introduzidas com a primeira liberação deste produto:

- Usado no ambiente interno para um contagem de saltos 3. Máximo 4.
- Nó e host do relé para clientes do utilizador final. Um rádio 802.11a é usado como uma relação do regresso e um rádio 802.11b/g para clientes de conservação.
- Segurança interna APs da malha – EAP e PSK apoiados.
- Os mapas LWAPP em um ambiente da malha comunicam-se com os controladores da mesma forma em relação aos APs Ethernet-anexados.
- Construção de uma ponte sobre do Point-to-Point Wireless.
- Construção de uma ponte sobre point-to-multipoint do Sem fio.
- Seleção ótima do pai. SNR, FACILIDADE, e BGN
- Realces BGN. ZERO e modo padrão.
- Acesso local.
- Lista preta do pai. Lista da exclusão.
- Auto que cura com AWPP.
- Ethernet Bridging.
- Suporte básico da Voz da liberação 4.0.
- Seleção dinâmica da frequência.
- Anti encalhamento – Padrão BGN e failover de DHCP.

**Nota:** Estas características não serão apoiadas:

- Canal da segurança pública 4.9 gigahertz
- Roteamento em torno da interferência
- Exploração do fundo
- Acesso universal
- Apoio do bridge de grupo de trabalho

### Software interno da malha

O software interno da malha é uma versão especial como se concentra nos APs internos, malha especialmente interna. Nesta liberação, nós temos ambos os APs internos que trabalham no modo local e igualmente no modo de Bridge. Algumas das características que estão disponíveis na liberação de 4.1.171.0 não são executadas nesta liberação. As melhorias foram feitas ao comando line interface(cli), a interface com o usuário gráfica (GUI – web browser) e na máquina de estado próprio. O objetivo para estas melhorias é ganhar a informação valiosa de sua perspectiva em relação a estes novos produtos e a sua viabilidade funcional.

Realces específicos da malha interna:

- **Ambiente interno** – A malha interna é executada usando LAP1242s e LAP1131. Estes são executados nos ambientes internos onde o cabo do Ethernet não está disponível. A aplicação é fácil e mais rápida fornecer uma cobertura sem fio às áreas remotas dentro da construção (por exemplo, centros de distribuição varejos, educação para seminários/conferências, fabricação, hospitalidade).
- **Realces do nome de grupo de bridge (BGN)** – A fim permitir que um administrador de rede organize uma rede da malha interna APs no usuário especificou setores, Cisco fornece um mecanismo chamado nome de grupo de bridge, ou o BGN. O BGN, realmente o nome do setor, faz com que um AP conecte a outros APs com o mesmo BGN. No evento um AP não encontra nenhum setor apropriado combinar seu BGN, o AP opera-se no modo padrão, e escolhe-se o melhor pai que responde ao padrão BGN. Esta característica tem recebido já muita apreciação do campo enquanto luta contra as condições encalhadas AP (se alguém tem desconfigurado o BGN). No software release de 4.1.171.0, os APs, ao usar o padrão BGN, não se operam como um nó interno da malha e não se têm nenhum acesso do cliente. Reage do modo de manutenção a alcançar através do controlador, e se o administrador não fixa o BGN, o AP recarregará após 30 minutos.
- **Aprimoramentos de segurança** - A Segurança no código interno da malha à revelia é configurada para EAP (protocolo extensible authentication). Isto é definido no RFC3748. Embora o protocolo EAP não seja limitado ao Sem fio LAN e possa ser usado para a autenticação do LAN ligado com fio, é o mais usado frequentemente no Sem fio LAN. Quando o EAP está invocado por um dispositivo permitido 802.1X NAS (servidor do acesso de rede) tal como um ponto de acesso Wireless do a/b/g do 802.11, os métodos de EAP modernos podem fornecer um mecanismo da autenticação seguro e negociar um PMK seguro (por pares chave mestre) 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 (baseado em AES).Antes do software release de 4.1.171.0, a malha exterior APs usou PMK/BMK para juntar-se ao controlador. Este era um processo do três-ciclo. Os ciclos são reduzidos agora para uma convergência mais rápida.O objetivo geral da Segurança interna da malha é fornecer:Configuração zero do toque para a Segurança do abastecimento.Privacidade e autenticação para frames de dados.Autenticação mútua entre a rede e os Nós.Capacidade para usar métodos de EAP padrão para a autenticação de Nós internos AP da malha.Decuplando LWAPP e a Segurança interna da malha.A descoberta, o roteamento, e os

mecanismos em sincronismo são aumentados da arquitetura atual para acomodar os elementos exigidos para apoiar os protocolos de segurança novos.A malha interna APs descobre a outra malha APs fazendo a varredura e escutando de atualizações vizinhas gratuitas da outra malha APs. Todo o RAP ou mapas internos conectado à rede anunciam parâmetros de segurança do núcleo em seus quadros NEIGH_UPD (bem como beacon frame do 802.11).Uma vez que esta fase se acaba, um enlace lógico entre uma malha interna AP e a raiz AP está estabelecido.
- **Realces WCS**Os alarmes internos da malha foram adicionados.Os relatórios internos da malha podem ser gerados mostrando o contagem de saltos, o SNR o mais ruim, etc.O teste da relação (Pai-à-criança, Criança-à-pai) pode ser executado entre os Nós que mostra a informação muito inteligente.A informação do AP indicada é muito mais do que mais adiantadas.Um tem uma opção para ver igualmente os vizinhos potenciais.O monitoramento de funcionamento é melhorado e mais conveniente alcançar.

## Hardware e software suportados

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

- Cisco LWAPP APs AIR-LAP1242AG-A-K9 e AIR-LAP1131AG-A-K9 apoia a configuração interna da malha.
- Cisco engrena a malha da empresa dos suportes de software da liberação 2 (Produtos interno e exterior). Isto pode ser instalado no controlador de Cisco, no Cisco 440x/210x, e no WISMs somente.
- O software da liberação 2 da malha do Cisco enterprise pode ser transferido do cisco.com.

## Interno contra exterior

Estes são algumas das diferenças salientes entre a malha interna e exterior:

| | Malha interna | Malha exterior |
|---|---|---|
| Ambiente | Interno SOMENTE, avaliado interno do hardware | Exterior SOMENTE, hardware áspero |
| Hardware | AP interno usando LAP1242 e LAP1131AG | AP exterior usando LAP15xx e LAP152x |
| Níveis de potência | 2.4 Ghz:20dbm 5.8 Ghz:17dbm | 2.4 Ghz:28dbm 5.8 Ghz:28dbm |
| Tamanhos de célula | Aproximadamente 150ft | Aproximadamente 1000ft |
| Altura da aplicação | 12ft da terra | 30-40ft da terra |

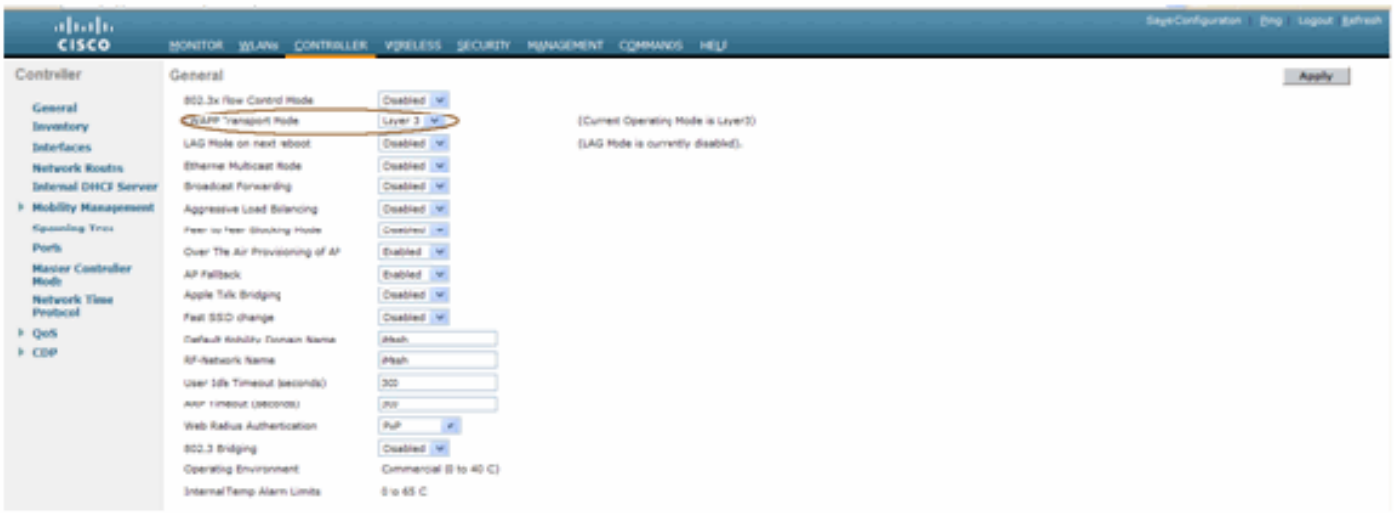
## Configuração

Certifique-se rever completamente o guia antes de começar qualquer aplicação, especialmente se

você recebeu o hardware novo.

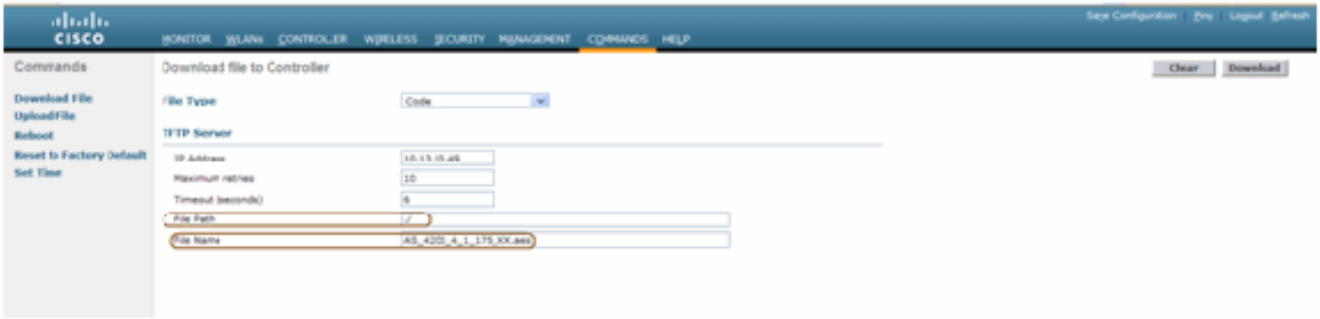
## Modo do controlador L3

A malha interna APs pode ser distribuída como uma rede L3.




## Promova o controlador ao código o mais atrasado

Conclua estes passos:

1. Para promover a liberação 2 da malha em uma rede de malha interna, sua rede deve ser executado em 4.1.185.0 ou na malha Release1, disponível em Cisco.com.
2. Transfira o código o mais atrasado para o controlador a seu servidor TFTP. Da interface GUI do controlador, clique o **arquivo dos comandos** > da **transferência**.
3. Selecione o tipo de arquivo como o **código** e dê o IP address de seu servidor TFTP. Defina o trajeto e o nome do
arquivo.


**Nota:** Use o servidor TFTP que apoia mais do que transferências do tamanho do arquivo do 32 MB. Por exemplo, **tftpd32**. Sob o caminho de arquivo posto **". /"** como mostrado.
4. Quando terminado instalar o novo firmware, use o comando do **sysinfo da mostra no** CLI verificar que 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...................................... CiscoImesh
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 WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

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

**Nota:** Oficialmente, Cisco não apoia Downgrades para controladores.

## MAC address

Éimperativo usar a filtração MAC. Esta característica fez a Cisco a solução interna da malha como “um toque zero real.” Ao contrário das liberações precedentes, a tela de malha já não terá a opção de filtragem MAC.


**Nota:** A filtração MAC é permitida à revelia.

## Grave o MAC address aos rádios

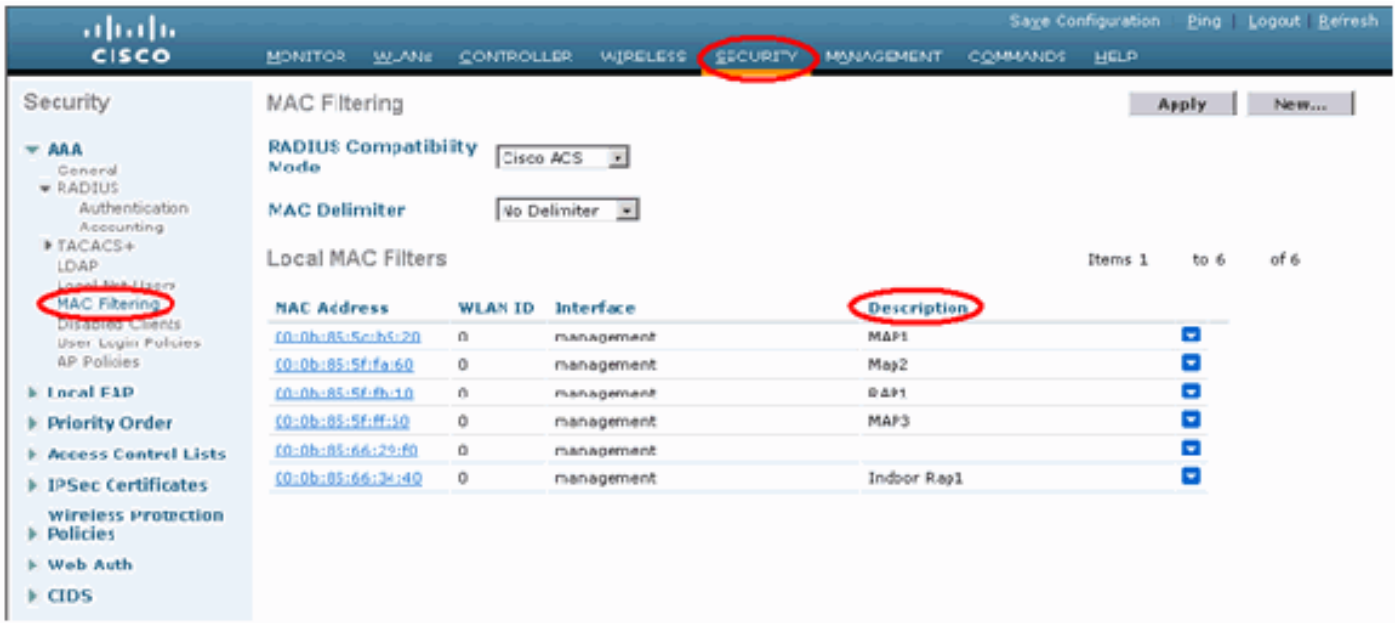
Em um arquivo de texto, grave os endereços MAC de todos os rádios AP que internos da malha você distribui em sua rede. O MAC address pode ser encontrado na parte de trás dos APs. Isto ajuda-o para os testes futuros, como a maioria dos comandos CLI exigem o MAC address APs ou os nomes sejam dados entrada com com o comando. Você pode igualmente mudar o nome dos APs a algo recordado mais facilmente, como, “tipo de construção número-AP da número-vagem: o último MAC address quatro encanta caráteres.”

## Dê entrada com o MAC address e os nomes dos rádios no controlador

O controlador de Cisco mantém uma lista interna do MAC address da autorização AP. O controlador responde somente aos pedidos da descoberta dos rádios internos que aparecem na lista da autorização. Incorpore os endereços MAC de todos os rádios que você tende a usar em sua rede no controlador.

Na interface GUI do controlador, vá à **Segurança**, e clique sobre o **MAC que filtra no** lado

esquerdo da tela. Clique **novo** a fim incorporar como mostrado os endereços MAC aqui:




Também, dê entrada com os nomes dos rádios para a conveniência sob a descrição da **descrição** (tal como o lugar, o AP #, etc.) pode igualmente ser usado para onde os rádios têm sido instalados para a referência fácil em qualquer altura que.

## Permita a filtração MAC

A filtração MAC é permitida à revelia.

Um pode igualmente fazer uma escolha do modo de segurança como o EAP ou o PSK na mesma página.

Da interface GUI do interruptor, use este trajeto:

Trajeto da interface GUI: **Sem fio > malha interna**

O modo de segurança pode SOMENTE 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-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

## Desenvolvimento interno da malha L3

Para uma rede de malha L3 interna, configurar os IP address para os rádios se você não pretende usar o servidor DHCP (interno ou externo).

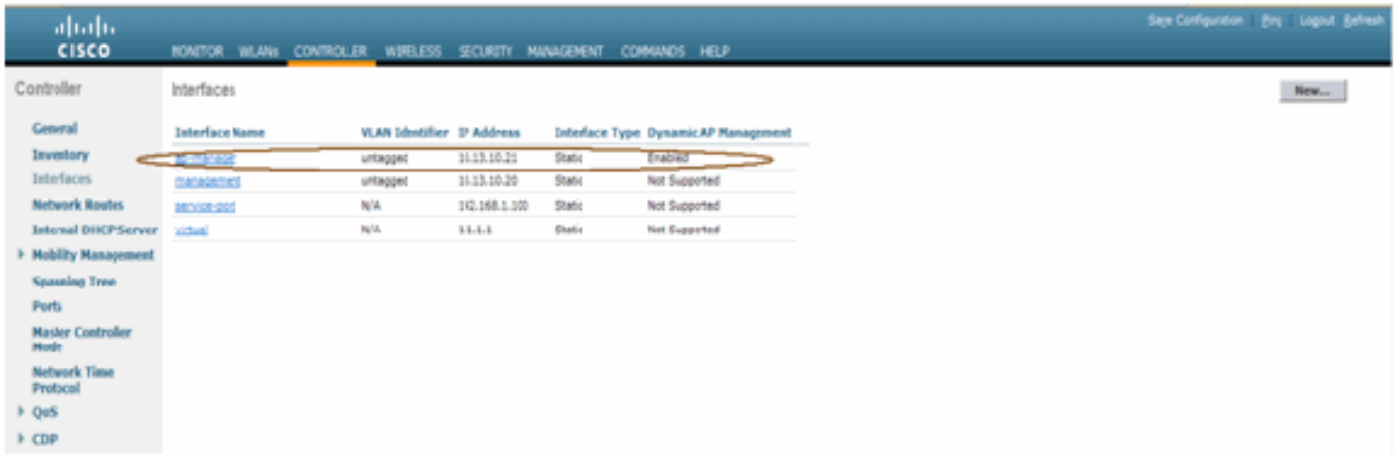
Para uma rede de malha L3 interna, se você quer usar o servidor DHCP, configurar o controlador no modo L3. Salvar a configuração e recarregue o controlador. Certifique-se de você configurar a opção 43 no servidor DHCP. Depois que o controlador reiniciou, os APs recentemente conectados receberão seu IP address do servidor DHCP.

## Defina relações no controlador

### Gerente AP

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

Caminho: **O controlador > conecta** > ap-**gerente > edita**.




A relação do **gerenciador AP** deve ser atribuída um IP address na mesma sub-rede e o VLAN como sua interface de gerenciamento.


## Papéis de rádio

Há dois papéis de rádio preliminares possíveis com esta solução:

- Ponto de acesso raiz (RAP) - O rádio com que você quer conectar ao controlador (através do interruptor) tomará o papel de um RAP. As batidas têm uma conexão prendida, LWAPP-permitida ao controlador. Um RAP é um nó do pai a toda a construção de uma ponte sobre ou rede de malha interna. Um controlador pode ter um ou vário o RAP, cada um parenting o mesmo ou as redes Wireless diferentes. Pode haver mais de um RAP para a mesma rede de malha interna para a Redundância.
- Access point interno da malha (MAPA) - O rádio que não tem nenhuma conexão ligada com fio ao controlador toma o papel de uma malha interna AP. Este AP foi chamado anteriormente a parte superior AP de Polo. Os mapas têm uma conexão Wireless (através da relação do regresso) talvez a outros mapas e finalmente a um RAP e assim ao controlador. Os mapas podem igualmente ter uma conexão dos Ethernet ligada com fio a um LAN e servir-la como um valor-limite da ponte para esse LAN (usando uma conexão P2P ou P2MP). Isto pode ocorrer simultaneamente, se configurado corretamente como um bridge Ethernet. Clientes do serviço dos mapas na faixa não usada para a relação do regresso.

O modo padrão para um AP é MAPA.

**Nota:** Os papéis de rádio podem ser ajustados através do GUI ou do CLI. Os APs recarregarão depois que a mudança do papel.

**Nota:** Você pode usar o controlador CLI PRE-para configurar os papéis de rádio em um AP forneceu o AP é conectado fisicamente ao interruptor ou você pode ver o AP no interruptor como um RAP ou um MAPA.

```
(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 de grupo de bridge

Os nomes de grupo de bridge (BGN) controlam a associação dos APs. Os BGN podem logicamente agrupar os rádios para evitar duas redes no mesmo canal da comunicação um com o otro. Este ajuste é igualmente útil se você tem mais de um RAP em sua rede no mesmo setor (área). O BGN é uma corda de dez caráteres máximos.

Um nome de grupo de bridge do fábrica-grupo é atribuído na fase da fabricação (VALOR NULO). Não é visível a você. Em consequência, mesmo sem um BGN definido, os rádios podem ainda juntar-se à rede. Se você tem duas batidas em sua rede no mesmo setor (para mais capacidade), recomenda-se que você configura as duas batidas com o mesmo BGN, mas nos canais diferentes.

**Nota:** O nome de grupo de bridge pode ser ajustado do controlador CLI e GUI.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Após ter configurado o BGN, o AP restaurará.

**Nota:** O BGN deve ser configurado muito com cuidado em uma rede viva. Você deve sempre partir do nó o mais distante (último nó) e mover-se para o RAP. A razão é que se você começa configurar o BGN em algum lugar no meio do multihop, a seguir os Nós além deste ponto estarão deixados cair como estes Nós terão um BGN diferente (BGN velho).

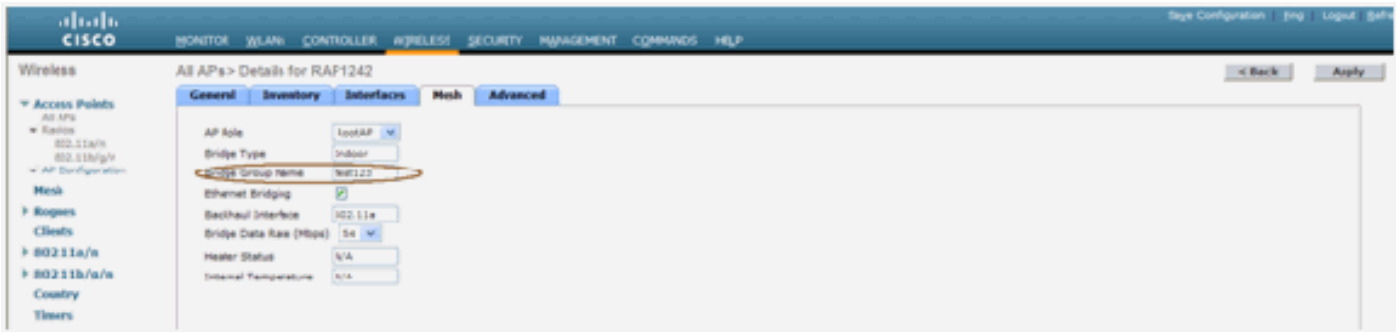
Você pode verificar o BGN emitindo este comando CLI:

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

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............
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
```

Também, você pode configurar ou verificar o BGN usando o controlador GUI:

Caminho: **Sem fio > todo o APs > detalhes**.




Você pode ver que a informação ambiental do AP está indicada igualmente com esta liberação nova.

## Configuração de segurança

O modo de segurança interno da malha do padrão é EAP. Isto significa que a menos que você configurar estes parâmetros em seu controlador, seus mapas não se juntarão:


### Configuração interna CLI da malha EAP

```
(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 você precisa de permanecer no modo PSK, use este comando ir para trás 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 internos da malha EAP

Dentro do modo EAP, você pode verificar estes **comandos show** verificar a autenticação do MAPA:

```
(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 'prfMaP1500L1EAuth93')
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 .............................. 436973636f0000000000000000000000
      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 debug internos da malha EAP

A fim debugar todos os problemas do modo EAP, use estes comandos no controlador:

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

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

# Instalação

## Condições prévias

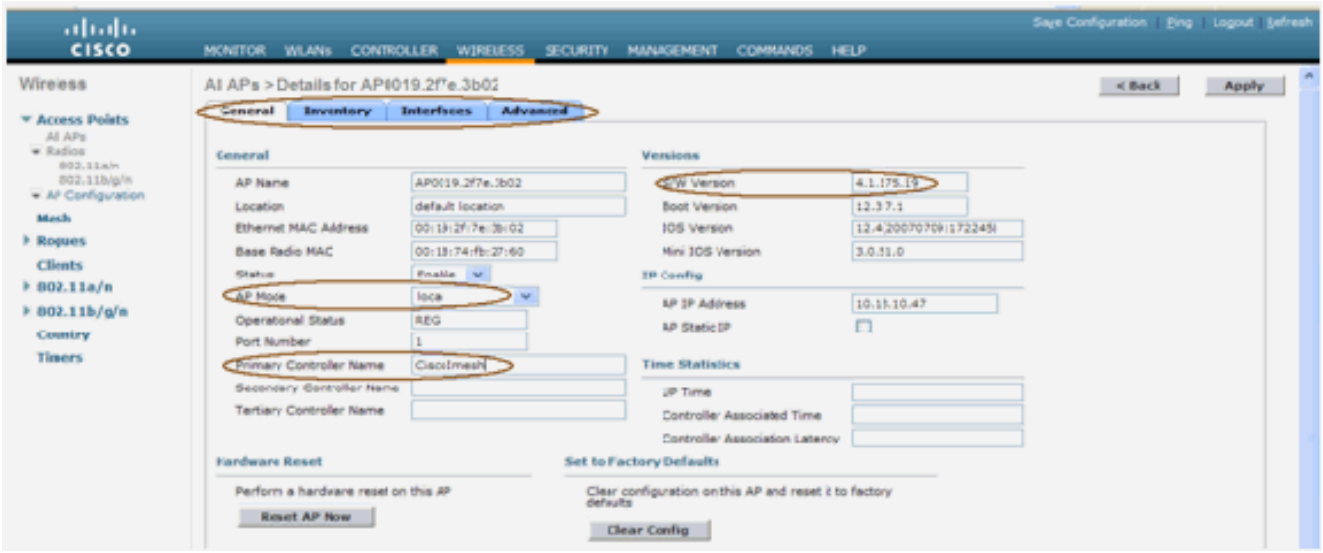
O controlador deve executar a versão recomendada do código. **Monitor do** clique para verificar a versão de software. O mesmos podem ser verificados através do CLI.

```
(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...................................... CiscoImesh
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 WLANs.................................. 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
```

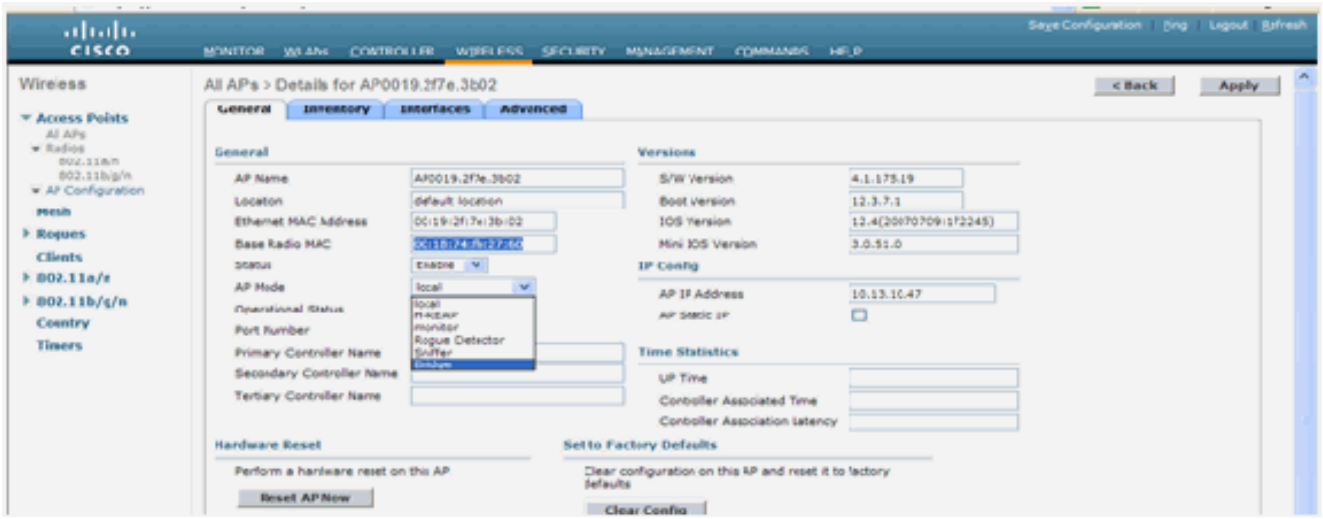
Os sistemas como o servidor DHCP, o servidor ACS, e o server WCS devem ser alcançáveis.

## Instalação

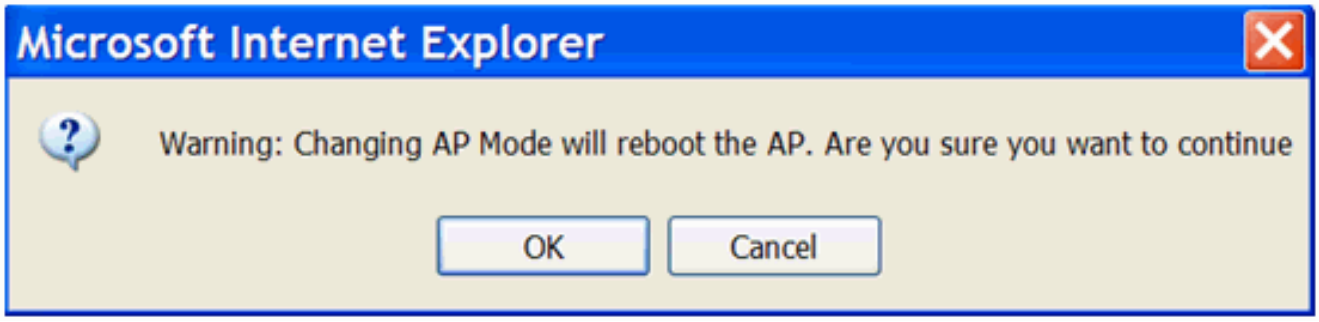
1. Conecte todos os regaços (1131AG/1242AG) a uma rede da camada 3 na mesma sub-rede como o endereço IP de gerenciamento. Todos os APs se juntarão ao controlador como APs no modo local. Neste modo, apronte os APs com o nome do controlador principal, nome do controlador secundário, e um nome do controlador terciário.




2. Capture o MAC address de rádio baixo do AP (por exemplo, 00:18:74: fb: 27:60).
3. Adicionar o MAC address do AP para que o AP junte-se no modo de Bridge.
4. Clique a **Segurança** > MAC-**filtrando** > **novo**.
5. Adicionar o MAC address copiado, e nomeie os APs na lista do MAC-filtro e na lista AP.
6. Escolha a **ponte da** lista do **modo AP**.




7. Alertá-lo-á confirmar porque este recarregará o AP.




8. O AP recarregará e juntar-se-á ao controlador no modo de Bridge. O indicador novo AP terá uma aba extra: MALHA. Clique a aba da **MALHA** para verificar o papel, o tipo da ponte, o nome de grupo de bridge, o Ethernet Bridging, a relação do transporte da parte traseira, a taxa de dados da ponte,
etc.


9. Neste indicador, alcance a lista do papel AP e escolha o papel relevante. Neste caso, o papel é à revelia um MAPA.O nome de grupo de bridge está vazio à revelia.A relação traseira do transporte é 802.11a.A taxa de dados da ponte (isto é, taxa de dados traseira do transporte) é 24Mbps.
10. Conecte o AP que você quer como um RAP ao controlador. Distribua os rádios (mapas) nos lugar desejados. Ligue os rádios. Você deve poder ver todos os rádios no controlador.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model             Ethernet MAC       Location         Port  Country
-----------------   -----  -------------------  -----------------  ---------------  ----  -------
RAP1242             2      AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1           2      AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2           2      AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. Tente ter condições da linha de vista entre os Nós. Se as condições da linha de vista não existem, crie afastamentos da zona de Fresnel para obter condições do próximo-linha--local.
12. Se você tem mais de um controlador conectado à mesma rede de malha interna, a seguir você deve especificar o nome do controlador principal em cada nó. Se não, o controlador que é primeiro visto será tomado como o preliminar.

## Potência e configuração de canal

O canal do regresso pode ser configurado em um RAP. Os mapas ajustarão ao canal RAP. O acesso local pode ser configurado independentemente para mapas.

Do interruptor GUI, siga o trajeto: **O Sem fio** > o **rádio 802.11a** > **configuram**.


**Nota:** O nível de potência TX do padrão no regresso é o nível da potência o mais alto (nível 1) e o Radio Resource Management (RRM) está à revelia.

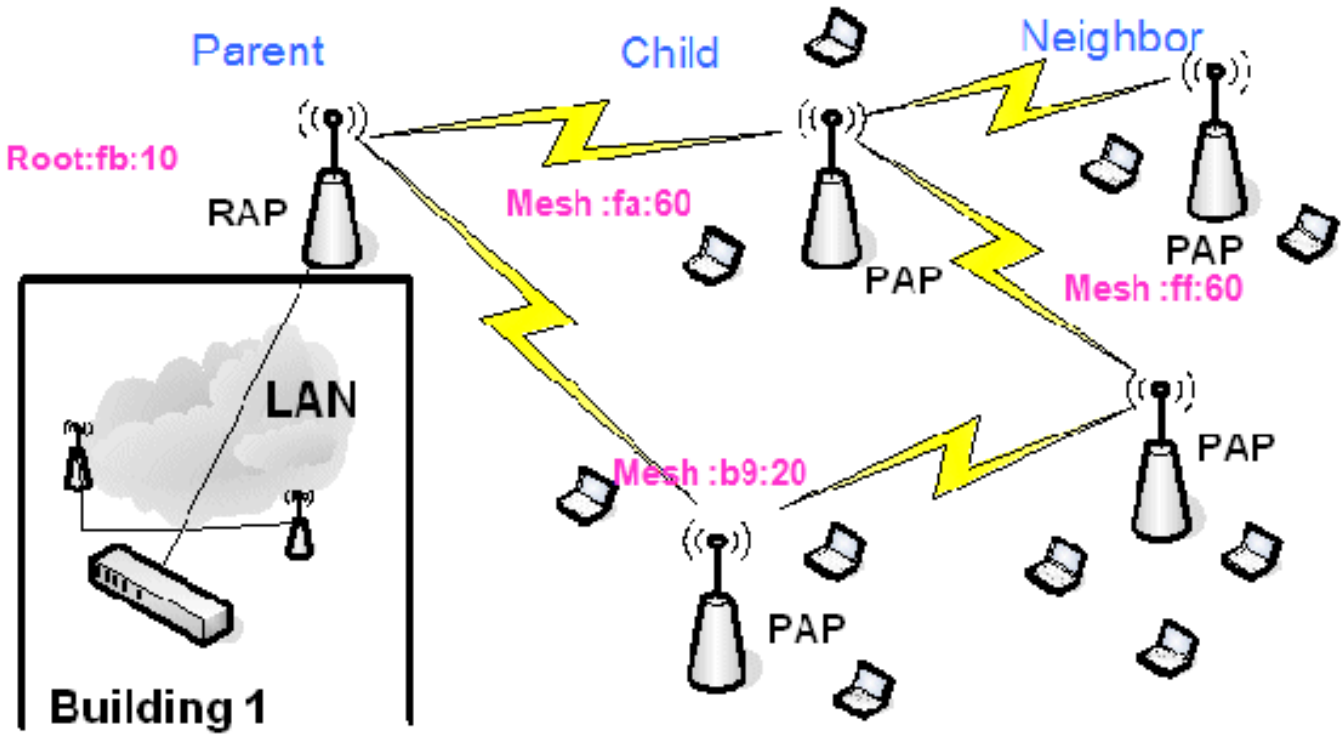
Se você está arranjando batidas, nós recomendamo-lo os canais adjacentes alternativos do uso em cada RAP. Isto reduzirá a interferência do co-canal.

## O RF verifica

Em uma rede de malha interna nós devemos verificar o relacionamento pai-filho entre os Nós. **O lúpulo** é um enlace Wireless entre os dois rádios. O relacionamento pai-filho muda enquanto você viaja através da rede. Depende em cima de onde você está na rede de malha interna.

O rádio mais perto do controlador em uma conexão Wireless (lúpulo) é um **pai do** rádio no outro lado do lúpulo. Em um sistema múltiplo do lúpulo há um árvore-tipo estrutura onde o nó conectado ao controlador seja um RAP (**pai**). O nó imediato no outro lado do primeiro lúpulo é uma **criança**, e os nós subsequente no segundo lúpulo são avante os **vizinhos** para esse pai particular.

**Figura 1: Rede de dois lúpulos**




Em figura 1, os nomes AP são mencionados para a conveniência. No tiro de tela seguinte, o **RAP(fb:10)** estão sendo investigados. Este nó pode considerar (no desenvolvimento real) a malha interna APs **(fa:60 & b9:20)** como crianças e o **MAPA ff:60 como o vizinho**.

Da interface GUI do interruptor, siga o trajeto: **Sem fio > todo o APs > Rap1 > informação vizinha**.


Assegure-se de que as relações da Pai-criança estejam estabelecidas e mantidas corretamente para sua rede de malha interna.

## Verifique as interconexões

**a malha da mostra** é um comando informativo verificar a interconexão em sua rede.

Você deve dar estes comandos em cada nó (AP) que usa o controlador CLI, e transfere arquivos pela rede os resultados em uma palavra ou em um arquivo de texto ao local transferindo arquivos pela rede.

```
(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 de malha interna, escolha uma relação múltipla do lúpulo e emita estes comandos que partem do RAP. Transfira arquivos pela rede o resultado dos comandos ao local transferindo arquivos pela rede.

Na próxima seção, todos estes comandos foram emitidos para a rede de malha interna de dois lúpulos mostrada em figura 1.

## Mostre o trajeto interno da malha

Este comando mostrar-lhe-á os endereços MAC, os papéis de rádio dos Nós, sinalizá-los-á às relações de ruído nos dBs para Uplink/downlink (SNRUp, SNRDown), e a relação SNR no DB para um caminho particular.

```
(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.
```

## Mostre o sumário interno do vizinho da malha

Este comando mostrar-lhe-á os endereços MAC, relacionamentos pai-filho, e Uplink/downlink SNR no 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
```

Entretanto, você deve poder ver os relacionamentos entre os Nós de sua rede e verificar a

Conectividade RF vendo os valores SNR para cada relação.

## Segurança do acesso de console AP

Esta característica dá a segurança avançada ao acesso de console do AP. Um cabo do console para o AP é exigido para usar esta característica.

Estes são apoiados:

- Um CLI para empurrar a USER-identificação/combinação de senha 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 empurrar a combinação de nome de usuário/senha para todos os APs registrados ao controlador:

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

Com estes comandos, o userid/combinação de senha empurrada do controlador é persistentes através do reload nos APs. Se um AP é cancelado do controlador, não há nenhum modo de acesso de segurança. O AP gerencie uma armadilha de SNMP com um login bem-sucedido. O AP igualmente gerará uma armadilha de SNMP em uma falha do console de login por três vezes consecutivas.

## Ethernet Bridging

Por razões de segurança, a porta Ethernet nos mapas é desabilitada à revelia. Pode ser permitida somente configurando o Ethernet Bridging no RAP e nos mapas respectivos.

Em consequência, o Ethernet Bridging tem que ser permitido para duas encenações:

- Quando você quer usar o interno engrene Nós como pontes.
- Quando você quiser conectar todo o dispositivo do Ethernet (tal como PC/Laptop, câmera de vídeo etc.) no MAPA usando sua porta Ethernet.

Caminho: **Sem fio** > clique algum AP > **malha**.


Há um comando CLI que possa ser usado para configurar a distância entre os Nós que fazem a construção de uma ponte sobre. Tente conectar um dispositivo do Ethernet como uma câmera de

vídeo em cada lúpulo e veja o desempenho.

## Realce do nome de grupo de bridge

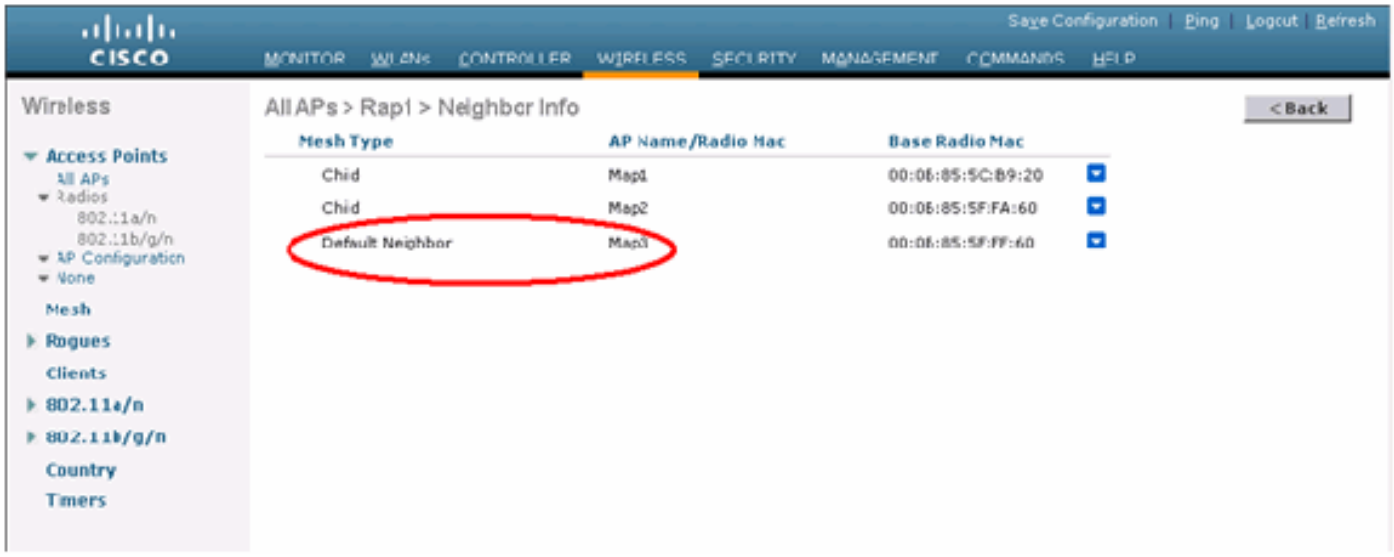
Épossível que um AP provisioned errada com um “bridgegroupname” para qual não se pretendeu. Segundo o projeto de rede, este AP pode ou não pode poder alcançar para fora e encontrar seus setor/árvore corretos. Se não pode alcançar um setor compatível, pode tornar-se encalhado.

**A fim recuperar um AP tão encalhado, o conceito do bridgegroupname do “padrão” foi introduzido com o código 3.2.xx.x.** A ideia básica é que um AP que seja incapaz de conectar a todo o outro AP com seu bridgegroupname configurado, tenta conectar com o “padrão” (a palavra) como o bridgegroupname. Todos os Nós que executam 3.2.xx.x e um software mais atrasado aceitam outros Nós com este bridgegroupname.

Esta característica pode igualmente ajudar em adicionar um novo nó ou um nó configurado errado a uma rede running.

Se você tem uma rede running, tome um AP preconfigured com um BGN diferente e faça-o juntar-se à rede. Você verá este AP no controlador que usa o “padrão” BGN depois que você adiciona seu MAC address no controlador.

```
(CiscoController) >show mesh path Map3:5f:ff:60

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




**O AP que usa o padrão BGN pode atuar como uma malha interna normal AP que associa clientes e que forma relacionamentos internos da criança do pai da malha.**

O momento onde este AP que usa o padrão BGN encontra um outro pai com o BGN correto, ele comutar-lhe-á.

## Logs - Mensagens, sistema, AP, e armadilha

## Log de mensagens

Permita o relatório em nível para log de mensagens. Do controlador CLI, emita este comando:

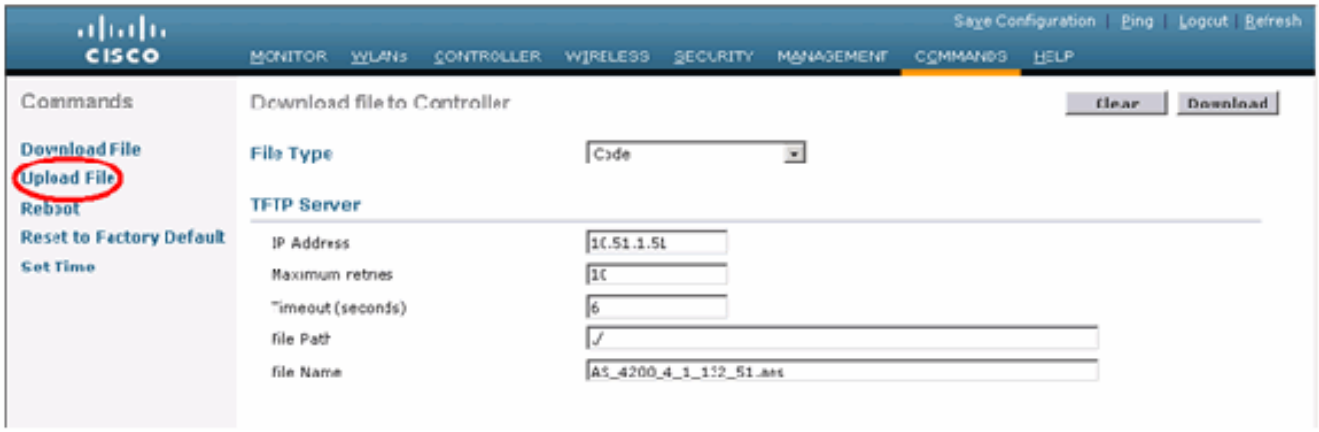
```
(Cisco Controller) >config msglog level ?

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 log de mensagens, emita este comando do controlador CLI:

```
(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 hearbeat 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 transferir arquivos pela rede os log de mensagens, use a interface GUI do controlador:

1. Clique **comandos > transferência de arquivo pela rede**.

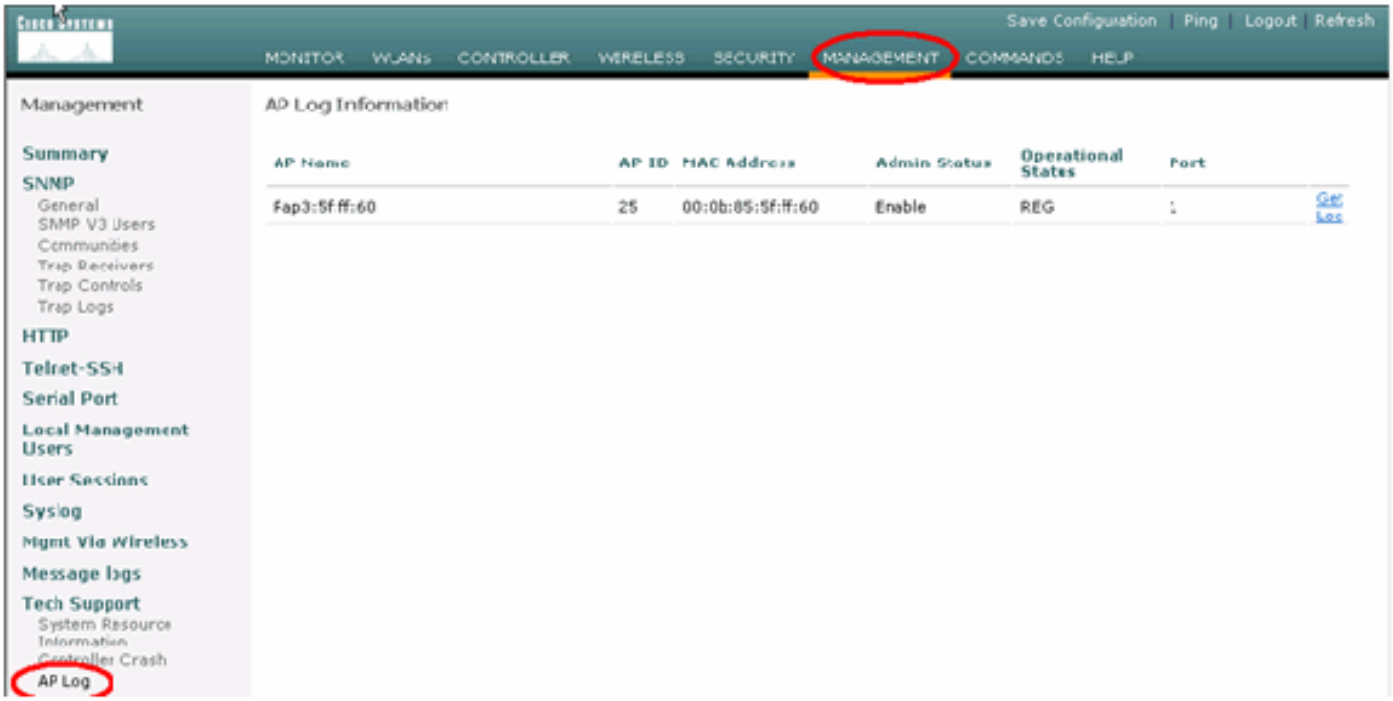



2. Incorpore sua informação do servidor TFTP. Esta página dar-lhe-á várias opções para

transferir arquivos pela rede, e você quer estes arquivos ser enviado:Log de mensagensLog de eventosLog da armadilhaArquivo do impacto (eventualmente)A fim verificar para ver se há arquivos de impacto, **Gerenciamento do** clique **> impacto do controlador**.

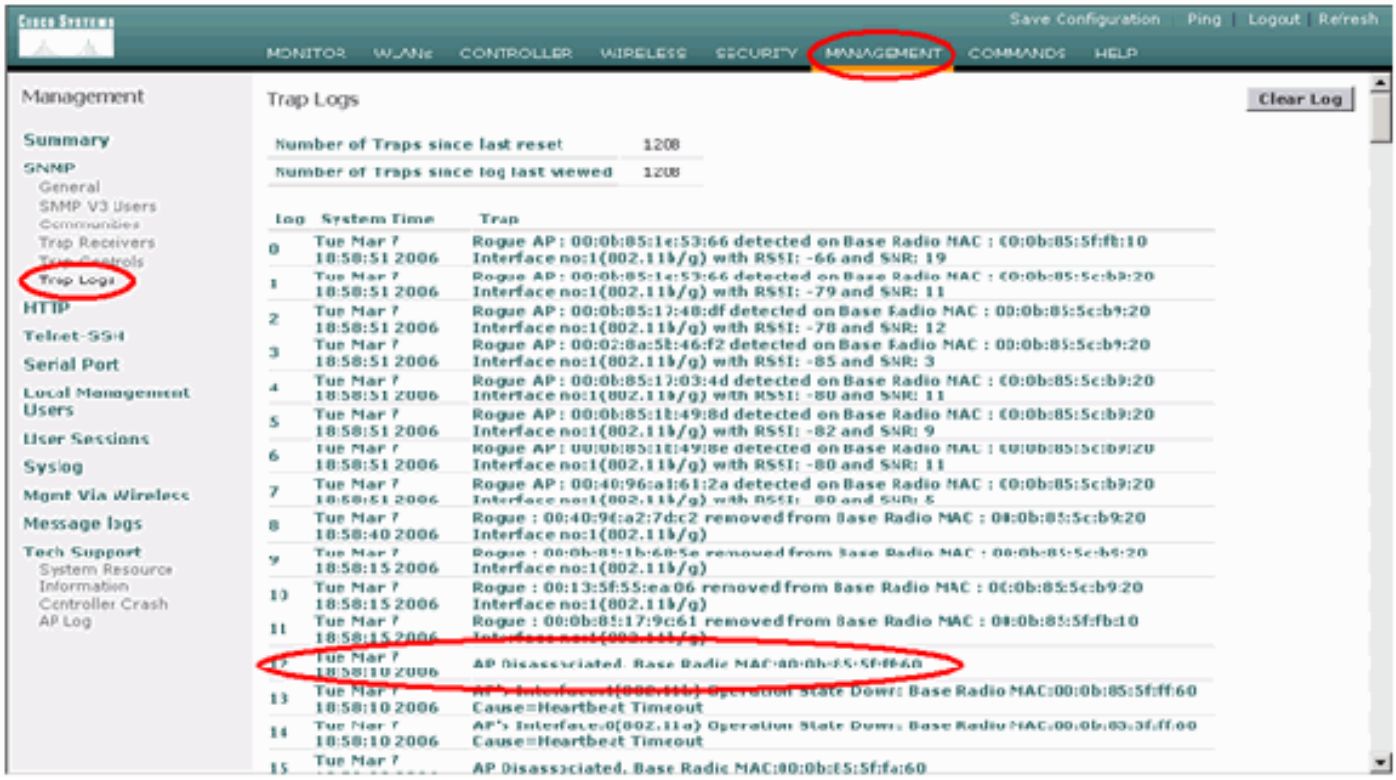

## Logs AP

Vá a esta página GUI no controlador verificar os logs AP para ver se há seu AP local, se algum:




## Prenda logs

Vá a esta página GUI do controlador e verifique os logs da armadilha:




# Desempenho

## Teste de convergência Startup

A convergência é o tempo tomado por um RAP/MAP para estabelecer uma conexão estável LWAPP com um controlador de WLAN que parte do tempo em que carreg primeiramente acima como alistado aqui:

| Teste de convergência | Tempo de convergência (minuto: segundo) | | | |
|---|---|---|---|---|
| | RAP | MAP1 | MAP2 | MAP3 |
| Upgrade da imagem | 2:34 | 3:50 | 5:11 | 6:38 |
| Repartição do controlador | 0:38 | 0:57 | 1:12 | 1:32 |
| Potência na rede de malha interna | 2:44 | 3:57 | 5:04 | 6:09 |
| Repartição RAP | 2:43 | 3:57 | 5:04 | 6:09 |
| O MAPA re-junta-se | | 3:58 | 5:14 | 6:25 |
| Mudança do MAPA do pai (o mesmo canal) | | 0:38 | | |

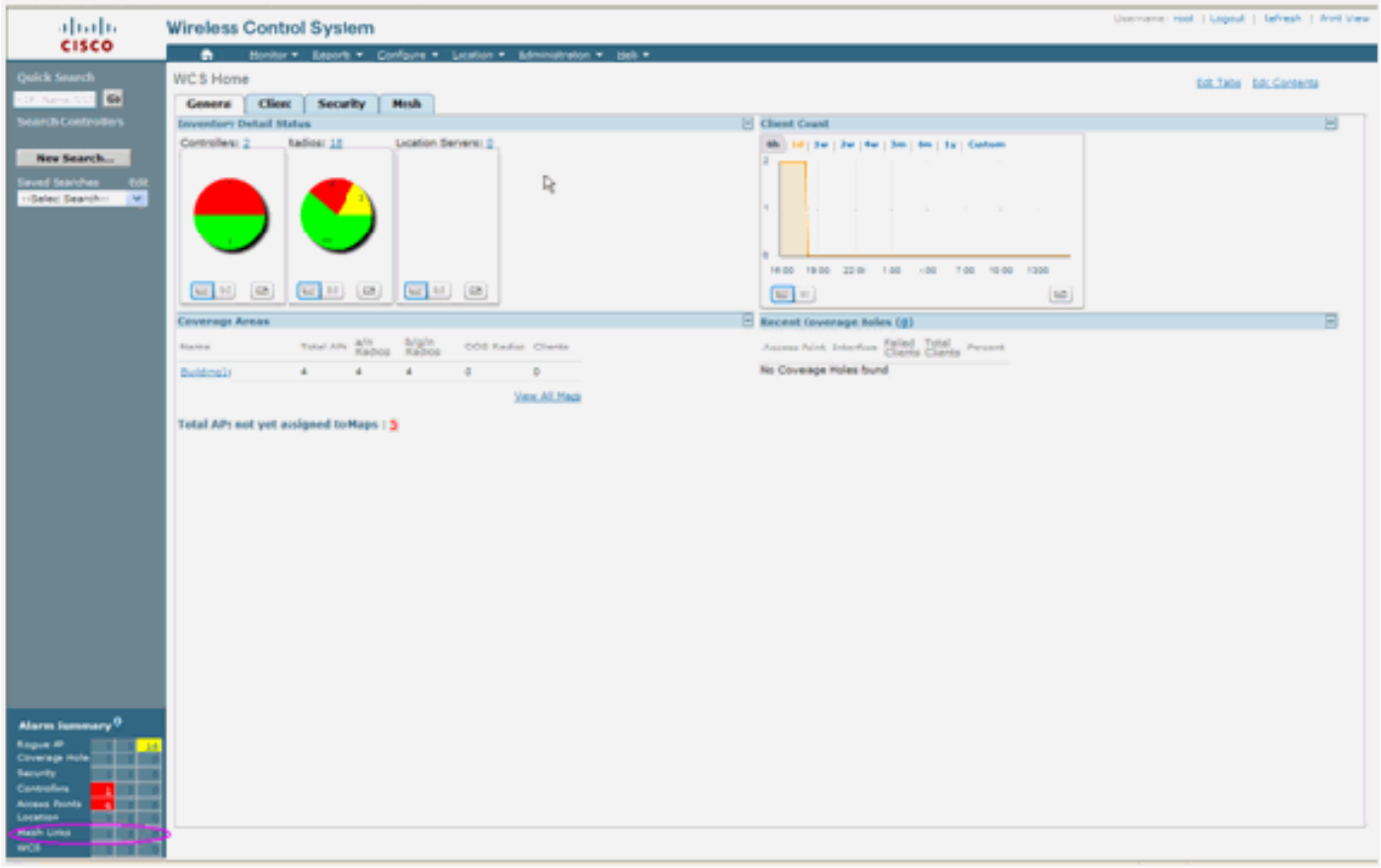
# WCS

## Alarmes internos da malha

O WCS gerará estes alarmes e eventos relativos à rede de malha interna baseada nas armadilhas do controlador:

- Relação deficiente SNR
- Pai mudado
- Criança movida
- O MAPA muda o pai frequentemente
- Evento da porta de Console
- Falha na autorização MAC
- Falhas de autenticação
- A criança excluiu o pai

**Relações da malha do** clique. Mostrará todos os alarmes relativos às relações internas da malha.




Estes alarmes aplicam-se às relações internas da malha:

- Relação deficiente SNR - Este alarme é gerado se a relação SNR cai abaixo 12db. O usuário não pode mudar este ponto inicial. Se o SNR deficiente é detectado na relação do regresso para a criança/pai, a armadilha estará gerada. A armadilha conterá o valor SNR e os endereços MAC. A severidade de alarme é principal. A relação (de relação sinal-ruído) SNR é importante porque a intensidade de sinal alta não é bastante para assegurar o bom desempenho do receptor. O sinal recebido deve ser mais forte do que todo o ruído ou interferência que estar presente. Por exemplo, é possível ter a intensidade de sinal alta e ainda ter o desempenho sem fio deficiente se há uma interferência forte ou um nível de ruído alto.
- Pai mudado - Este alarme é gerado quando a criança se transportou a um outro pai. Quando o pai é perdido, a criança juntar-se-á com um outro pai, e a criança enviará uma armadilha que contém endereços MAC do pai idoso e do pai novo ao WCS. Severidade de alarme: Informativo.
- Criança movida - Este alarme é gerado quando o WCS obtém uma armadilha perdida criança. Quando o pai AP detectou sua perda de uma criança e não capaz de se comunicar

com essa criança, enviará uma armadilha perdida criança ao WCS. A armadilha conterá o MAC address da criança. Severidade de alarme: Informativo.
- Pai do MAPA mudado frequentemente - Este alarme é gerado se a malha interna AP muda seu pai frequentemente. Quando o pai-mudança-contador do MAPA excede o ponto inicial dentro de uma duração dada, enviará uma armadilha ao WCS. A armadilha conterá o número de vezes de mudanças do MAPA e da duração do tempo. Por exemplo, se há as mudanças 5 dentro de 2 minutos, a seguir a armadilha será enviada. Severidade de alarme: Informativo.
- A criança excluiu o pai - Este alarme é gerado quando uma criança põr um pai. Uma criança pode põr um pai quando a criança não autenticou no controlador após um número fixo de tentativas. A criança recorda o pai põr e quando a criança se junta à rede, enviará a armadilha que contém o MAC address põr do pai e a duração do período da lista negra.

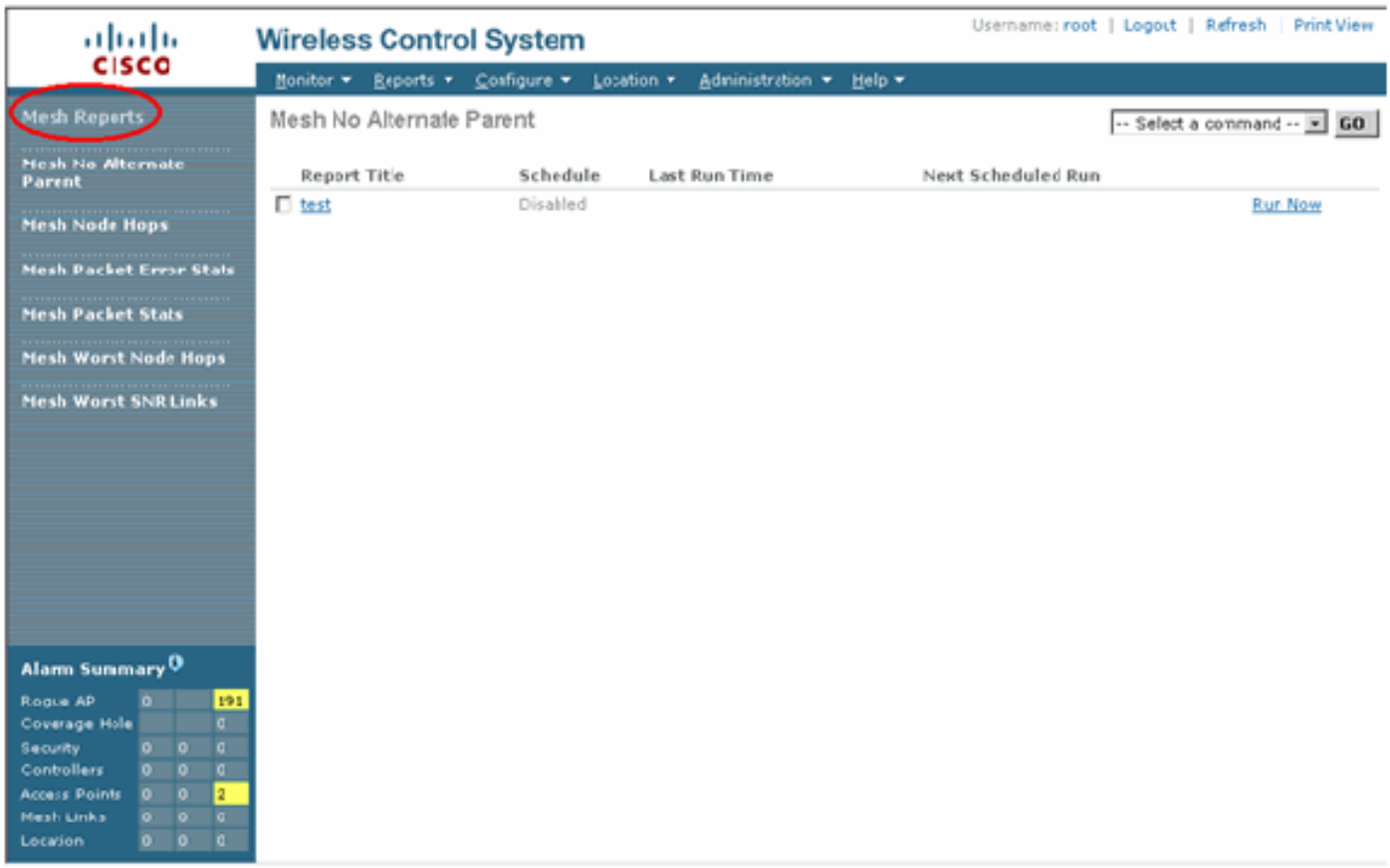
Alarmes diferentes das relações internas da malha:

- Acesso da porta de Console - A porta de Console fornece a capacidade para que o cliente mude o nome de usuário e a senha para recuperar o AP exterior encalhado. Contudo, para impedir todo o acesso de usuário autorizado ao AP, o WCS precisa de enviar um alarme quando alguém tenta entrar. Este alarme é exigido para fornecer a proteção porque o AP for fisicamente vulnerável quando encontrado fora. Este alarme estará gerado se o usuário entrou com sucesso à porta de Console AP, ou se falhou três vezes consecutivas.
- Falha na autorização MAC - Este alarme é gerado quando as tentativas AP para se juntar à malha interna mas não autenticam porque não está na lista de filtro MAC. O WCS receberá uma armadilha do controlador. A armadilha conterá o MAC address do AP que autorização falha.

## Relatório e estatísticas da malha

Nós levamos sobre a estrutura aumentada do relatório e das estatísticas de 4.1.185.0:

- Nenhum caminho alternativo
- Lúpulos do nó da malha
- Stats do erro dos pacotes
- Stats do pacote
- O lúpulo o mais ruim do nó
- As relações as mais ruins SNR




## Nenhum caminho alternativo

A malha interna AP tem tipicamente mais de um vizinho. No caso em que uma malha interna AP afrouxar sua relação do pai, o AP deve poder encontrar o pai alternativo. Em algum caso, se não há nenhum vizinho mostrado, a seguir o AP não poderá ir a nenhuns outros pais se afrouxa seus pais. É crítico para o usuário saber que APs não têm pais alternativos. Lista deste relatório para fora todos os APs que não têm nenhuns outros vizinhos diferentes do pai atual.

## Lúpulos internos do nó da malha

Este relatório mostra o número de lúpulos longe da raiz AP (RAP). Você pode criar o relatório baseado nestes critérios:

- AP pelo controlador
- AP pelo assoalho

## Taxas de erro de pacote

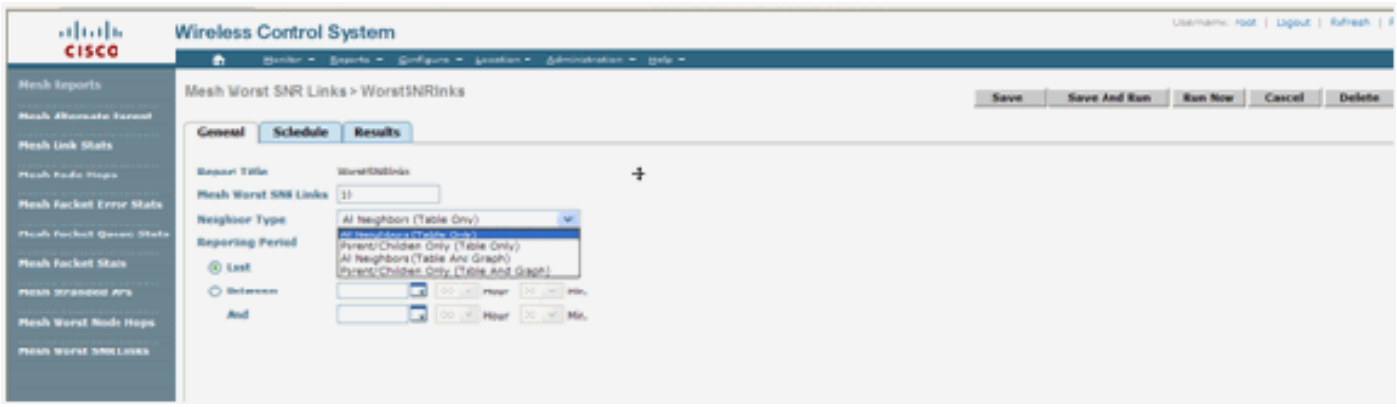
Os erros de pacote podem ser causados pela interferência e pelas quedas de pacote de informação. O cálculo da taxa de erro de pacote é baseado nos pacotes enviados e nos pacotes enviados com sucesso. A taxa de erro de pacote é medida na relação do regresso e recolhida para vizinhos e o pai. O AP envia periodicamente a informação do pacote ao controlador. Assim que o pai mudar, o AP manda a informação de erro de pacote recolhida ao controlador. O WCS vota a informação de erro de pacote do controlador os minutos cada 10 à revelia e armazena-a no base de dados por até os dias 7. No WCS, a taxa de erro de pacote é mostrada como um gráfico. O gráfico de erro de pacote é baseado nos dados históricos armazenados no base de dados.

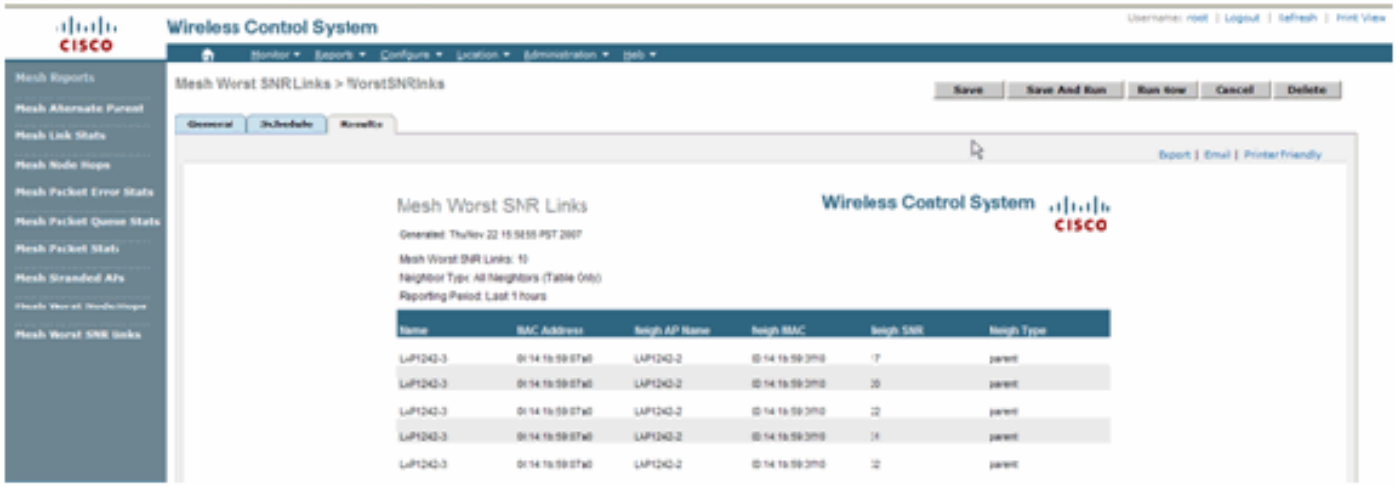
## Stats do pacote

Este relatório mostra que os valores de contador do total vizinho transmitem os pacotes e os pacotes total vizinhos transmitidos com sucesso. Você pode criar o relatório baseado em determinados critérios.

## As relações as mais ruins SNR

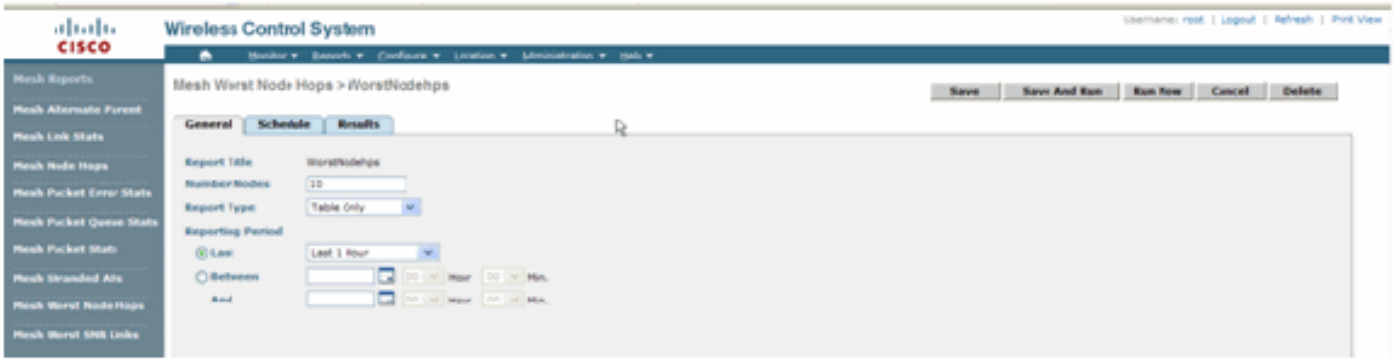
Os problemas de ruído puderam ocorrer em horas diferentes e o ruído pôde aumentar em taxas diferentes ou dura para durações diferentes. A figura seguinte fornece a capacidade para criar o relatório para o rádio a e o b/g assim como relações seletivas. As lista que de relatório o 10 o SNR o mais ruim liga à revelia. Você pode escolher de 5 a 50 relações as mais ruins. O relatório pode ser gerado para a última 1 hora, as últimas horas 6, o último dia, os últimos 2 dias, e até os dias 7. Os dados são votados os minutos cada 10 à revelia. Os dados são mantidos no base de dados para o máximo sete dias. O tipo vizinho critérios de seleção pode ser todos os vizinhos, pai/crianças somente.



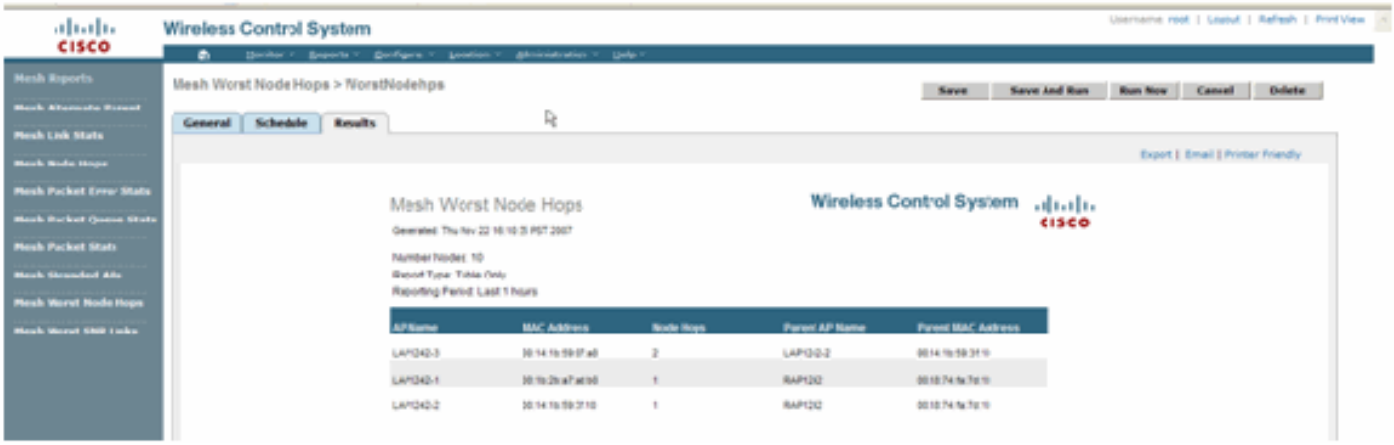




## Os lúpulos os mais ruins do nó

Este os lúpulos os mais ruins APs das lista de relatório the10 à revelia. Se os APs são lúpulos demais afastado, as relações poderiam ser muito fracas. O usuário pode isolar os APs que têm muitos lúpulos longe da raiz AP e tomam a ação apropriada. Você pode escolher mudar este **número de** critérios dos **Nós** entre 5 e 50. Os critérios do filtro do **Report Type** nesta figura podem ser tabela somente ou apresentar e representar graficamente:




Esta figura mostra o resultado para o último relatório:




## Estatísticas da Segurança

As estatísticas internas da Segurança da malha são indicadas na página do detalhe AP sob a seção de informação de construção de uma ponte sobre. Uma entrada na tabela interna da estatística de MeshNodeSecurity é criada quando um nó interno da malha da criança associa ou autentica com um nó interno da malha do pai. As entradas são removidas quando o nó interno da malha se dissocia do controlador.

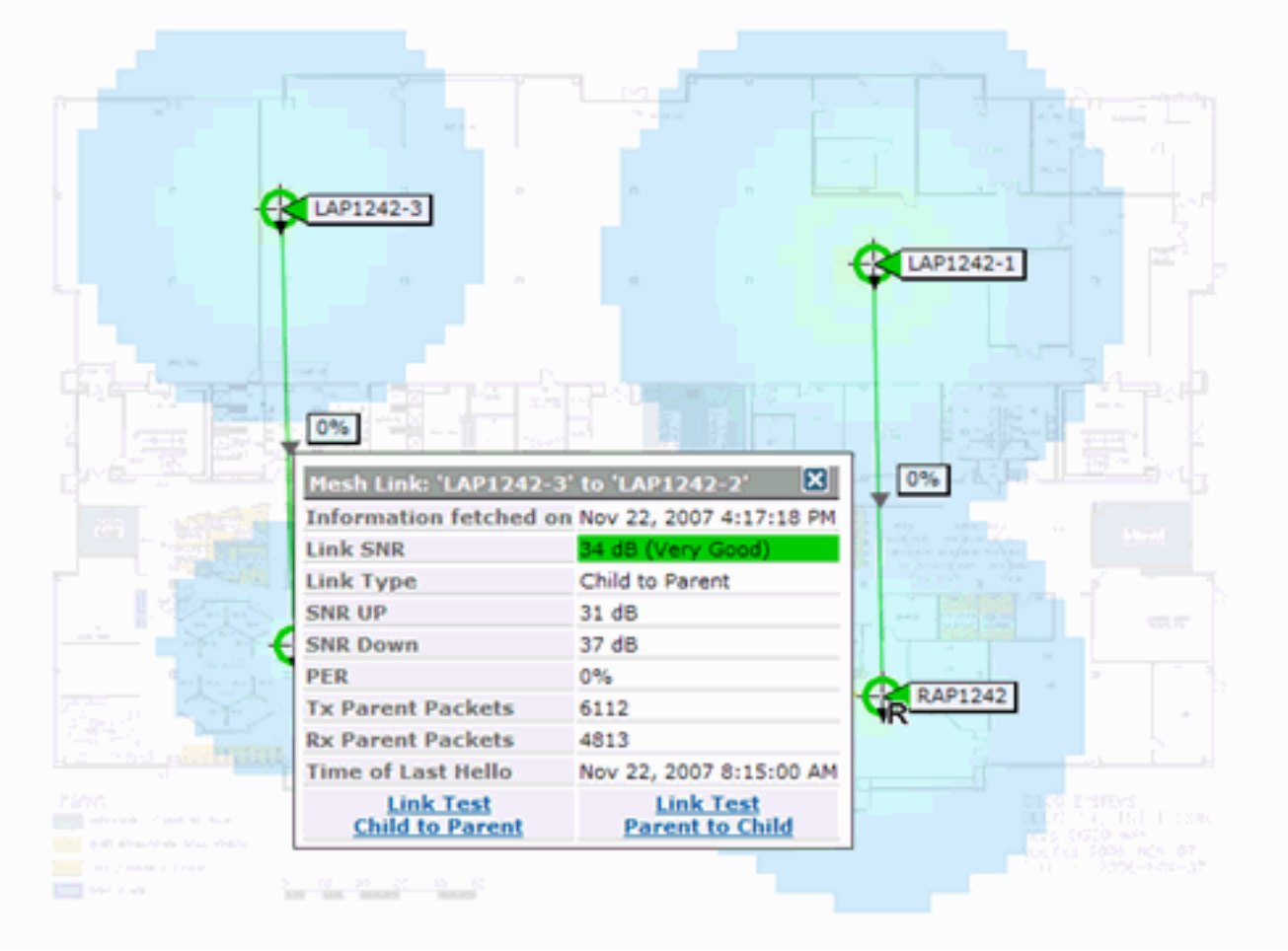
## Teste da relação

O teste da relação AP-à-AP é apoiado no WCS. Um pode selecionar quaisquer dois APs e invocar um teste da relação entre os dois.

Se aqueles APs são vizinhos RF, a seguir o teste da relação pode ter um resultado. O resultado é mostrado em um diálogo no mapa próprio sem uma página completa refresca. O diálogo pode ser disposto facilmente.

Contudo, se aqueles 2 APs não são vizinhos RF, a seguir o WCS não tenta figurar para fora um trajeto entre os 2 APs a fim fazer um teste do link múltiplo da liga.

Quando o rato é movido sobre a seta na relação entre os dois Nós, este indicador aparece:




## Teste da relação do nó para nó

A ferramenta de teste da relação é uma ferramenta por encomenda para verificar a qualidade da relação entre todos os dois APs. No WCS, esta característica é adicionada na página do detalhe AP.

Na página do detalhe AP, sob a aba **interna da relação da malha** onde as relações estão listadas ao lado dela, há uma relação para executar o teste da relação.

A ferramenta de teste da relação do controlador CLI tem os parâmetros de entrada opcionais: Tamanho do pacote, pacotes de teste do enlace total, duração do teste, e da taxa da ligação de dados. O teste da relação tem valores padrão para estes parâmetros opcionais. Os endereços MAC para os Nós são os únicos parâmetros de entrada imperativos.

A ferramenta de teste da relação testa a força, o pacote enviado, e o pacote recebido entre Nós. A relação para o teste da relação é indicada nos relatórios de detalhes AP. Quando você clica a relação, há uma tela do PNF-acima que mostra os resultados de teste da relação. O teste da relação será somente aplicável Parent – criança e entre vizinhos.

A saída do teste da relação gerencie os pacotes enviados, os pacotes recebidos, os pacotes de erro (cubetas para razões do diff), o SNR, o assoalho do ruído, e o RSSI.

O teste de Lnk fornece estes detalhes no GUI em um mínimo:

- Pacotes de teste da relação enviados
- Pacotes de teste da relação recebidos

- Intensidade de sinal no dBm
- Signal to Noise Ratio

### Relações por encomenda do vizinho AP

Este é uns novos recursos no mapa WCS. Você pode clicar sobre uma malha AP e uma janela pop-up com informação detalhada aparece. Você pode então clicar **vizinhos da malha da vista**, que busca a informação vizinha para o AP selecionado e indica uma tabela com todos os vizinhos para a malha interna selecionada AP.

A relação vizinha da malha da vista indica todos os vizinhos para o AP destacado. Este instantâneo mostra todos os vizinhos, tipo dos vizinhos, e valor SNR.

### Teste de ping

O teste de ping é uma ferramenta por encomenda usada para sibilar entre o controlador e o AP. A ferramenta de teste de ping está disponível na página do detalhe AP e no MAPA. Clique a relação do **teste de ping da corrida na** página do detalhe AP ou da informação AP do MAPA para iniciar o sibilo do controlador ao AP atual.

## Conclusão

A malha da empresa (isto é, malha interna) é uma extensão da cobertura do Cisco Wireless aos lugares onde os Ethernet ligada com fio não podem fornecer a Conectividade. A flexibilidade e a viabilidade de uma rede Wireless são realizadas com malha da empresa.

A maioria dos APs prendidos características fornecem são fornecidos pela topologia de malha interna. A malha da empresa pode igualmente coexistir com os APs prendidos no mesmo controlador.

## Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems