

# Gerência de recursos de rádio sob redes Wireless unificadas

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Melhoramento a 4.1.185.0 ou a mais tarde: Que a mudar ou verificar?](#)

[Gerência de recursos de rádio: Pontas e melhores prática](#)

[Agrupamento RF e ponto inicial da potência TX](#)

[Perfil da cobertura e interrupção do cliente SNR](#)

[Frequência vizinha da mensagem \(formação do grupo RF\)](#)

[Uso da opção por encomenda](#)

[Indicador do Balanceamento de carga](#)

[Gerência de recursos de rádio: Introdução](#)

[Gerência de recursos de rádio: Conceitos](#)

[Termos chaves](#)

[Uma vista aérea de RRM](#)

[Algoritmo de agrupamento RF](#)

[Algoritmo dinâmico da atribuição do canal](#)

[Algoritmo de controle da potência de transmissão](#)

[Algoritmo da detecção e correção do furo da cobertura](#)

[Gerência de recursos de rádio: Parâmetros de configuração](#)

[RF que agrupa ajustes através do WLC GUI](#)

[Ajustes da atribuição do canal RF através do WLC GUI](#)

[Ajustes da atribuição do nível de potência TX através do WLC GUI](#)

[Pontos iniciais do perfil: WLC GUI](#)

[Gerência de recursos de rádio: Troubleshooting](#)

[Verificando a atribuição dinâmica do canal](#)

[Verificando alterações de controle da potência de transmissão](#)

[Exemplo dos trabalhos do algoritmo de controle da potência de transmissão](#)

[Exemplo dos trabalhos do algoritmo da detecção e correção do furo da cobertura](#)

[Comandos debug and show](#)

[APÊNDICE A: Liberação 4.1.185.0 WLC – Realces RRM](#)

[Algoritmo de agrupamento RF](#)

[Algoritmo dinâmico da atribuição do canal](#)

[Algoritmo de controle da potência TX](#)

[Algoritmo do furo da cobertura](#)

[Realces da armadilha de SNMP](#)

[Cosmético/outros realces](#)

[Mudanças do Balanceamento de carga](#)

[APÊNDICE B: Liberação 6.0.188.0 WLC – Realces RRM](#)

[Reparos RRM para dispositivos médicos](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento detalha a funcionalidade e a operação do Gerenciamento de Recursos de Rádio (RRM) e fornece uma discussão aprofundada dos algoritmos por trás desta característica.

## [Pré-requisitos](#)

### [Requisitos](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo de pouco peso do Access point (LWAPP)
- Considerações de projeto comuns do Wireless LAN (WLAN) /radiofrequency (RF) (conhecimento comparável àquele da certificação sem fio do planeta 3 CWNA)

**Nota:** O Balanceamento de carga do cliente e a detecção do rogue/retenção agressiva (e outras características do [IPS] do sistema da prevenção de intrusão do [IDS] /Cisco IOS® do Sistema de Detecção de Intrusão da Cisco) não são funções de RRM e são além do alcance deste original.

### [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## [Melhoramento a 4.1.185.0 ou a mais tarde: Que a mudar ou verificar?](#)

1. Do CLI, verifique:

```
show advanced [802.11b|802.11a] txpower
```

O valor padrão novo é -70dbm. Se foi alterado, reverta aos padrões desde que este valor novo foi mostrado para ser ótimo sob uma escala das circunstâncias. Este valor precisa de ser o mesmo em todos os controladores em um grupo RF. Recorde salvar a configuração após ter feito mudanças. A fim mudar este valor, emita este comando:

```
config advanced [802.11b|802.11a] tx-power-control-thresh 70
```

2. Do CLI, verifique:

```
show advanced [802.11a|802.11b] profile global
```

Os resultados devem ser:

```
802.11b Global coverage threshold..... 12 dB for 802.11b
802.11a Global coverage threshold..... 16 dB for 802.11a
```

Se os resultados são diferentes, a seguir você usa estes comandos:

```
config advanced 802.11b profile coverage global 12
config advanced 802.11a profile coverage global 16
```

O parâmetro da interrupção do cliente SNR que determina se o cliente está na violação, e se a mitigação do algoritmo do furo da cobertura retrocede dentro, chamado Cobertura deve ser revertido de volta aos padrões para resultados os melhores.

### 3. Do CLI, verifique:

```
show load-balancing
```

O estado de padrão de Balanceamento de carga é *desabilitado* agora. Se permitida, a janela padrão é agora 5. Esta é a quantidade de clientes que precisam de ser associados a um rádio antes que o Balanceamento de carga em cima da associação ocorrer. O Balanceamento de carga pode ser muito útil em um ambiente high-density do cliente, e o uso desta característica deve ser uma decisão do administrador assim que a associação do cliente e o comportamento da distribuição são compreendidos.

## [Gerência de recursos de rádio: Pontas e melhores prática](#)

### [Agrupamento RF e ponto inicial da potência TX](#)

#### DICAS:

- Assegure-se de que o ponto inicial da potência TX esteja configurado o mesmos em todos os controladores que compartilham do nome do grupo RF.
- Nas versões mais cedo do que 4.1.185.0, o ponto inicial da potência TX do padrão era -65dBm, mas este valor de limiar de -65dBm pode estar demasiado “quente” para a maioria de disposições. Os melhores resultados foram observados com este conjunto de limiares entre -68dBm e -75dBm. Com versão 4.1.185.0, o ponto inicial da potência TX do padrão é agora -70dBm. Com 4.1.185.0 ou mais tarde, recomenda-se fortemente que os usuários mudam o ponto inicial da potência TX a -70 e verificam se os resultados são satisfatórios. Esta é uma recomendação forte desde que os vários realces RRM podem fazer com que sua configuração atual seja secundário-ótima agora.

#### PORQUE:

O nome do grupo RF é um string ascii configurado pelo controlador do Wireless LAN (WLC). O algoritmo de agrupamento elege o líder do grupo RF que, por sua vez, calcula o controle de potência de transmissão (TPC) e a atribuição dinâmica do canal (DCA) para o grupo inteiro RF. A exceção é o algoritmo do furo da cobertura (CHA), que é executado por WLC. Porque o agrupamento RF é dinâmico, e o algoritmo é executado nos intervalos 600-second à revelia, pôde ser um exemplo onde os vizinhos novos sejam ouvidos (ou os vizinhos existentes são ouvidos já não). Isto causa uma mudança no grupo RF que poderia conduzir à eleição de um líder novo (para um ou grupos lógicos múltiplos RF). Neste exemplo, o ponto inicial da potência TX do líder do grupo novo é usado no algoritmo TPC. Se o valor deste ponto inicial é incompatível através dos controladores múltiplos que compartilham do mesmo nome do grupo RF, este pode conduzir às discrepâncias em níveis de potência TX resultantes quando o TPC é executado.

### [Perfil da cobertura e interrupção do cliente SNR](#)

## DICA:

- Ajuste a medida da cobertura (padrões a 12dB) a 3dB para a maioria de disposições. **Nota:** Com versão 4.1.185.0, os realces tais como a potência TX acima do número do controle e dos configuráveis pelo usuário de clientes de violação do perfil SNR, os padrões de 12dB para 802.11b/g e 16dB para 802.11a devem trabalhar muito bem na maioria de ambientes.

## PORQUE:

A medida da cobertura, DB 12 à revelia, é usada para chegar no SNR tolerável máximo pelo cliente. Se o cliente SNR excede este valor, e se mesmo um cliente excede este valor, o CHA está provocado pelo WLC cujo o Access Point (AP) detecta o cliente com SNR deficiente. Nos casos onde os clientes do legado estão presente (quem têm frequentemente a lógica vagueando deficiente), ajustar o assoalho tolerável do ruído para baixo aos resultados 3dB fornece um reparo a curto prazo (este reparo não é exigido em 4.1.185.0 ou em mais tarde).

Isto é descrito mais sob a *consideração de ligação inicial do cliente pegajoso* na seção do [algoritmo da detecção e correção do furo da cobertura](#).

## Frequência vizinha da mensagem (formação do grupo RF)

### DICAS:

- Mais longo o intervalo configurado entre transmitir mensagens vizinhas, mais lenta a convergência/tempo da estabilização será durante todo o sistema.
- Se um vizinho existente não é ouvido por 20 minutos, o AP está podado fora da lista vizinha. **Nota:** Com versão 4.1.185.0, o intervalo de poda da lista vizinha é estendido agora para manter o vizinho de quem um pacote vizinho não foi ouvido por até 60 minutos.

### PORQUE:

As mensagens vizinhas, são enviadas à revelia cada 60 segundos. Esta frequência é controlada pela medida do sinal (denominada frequência vizinha do pacote em 4.1.185.0 e mais tarde) sob a seção dos intervalos do monitor na auto página RF (veja [figura 15](#) para a referência). É importante compreender que as mensagens vizinhas comunicam a lista de vizinhos que um AP ouve, que seja comunicado então a seu WLCs respectivo, que formam por sua vez o grupo RF (esta supõe que o nome do grupo RF está configurado o mesmos). O tempo de convergência RF depende inteiramente da frequência de mensagens vizinhas e este parâmetro deve apropriadamente ser ajustado.

## Uso da opção por encomenda

### DICA:

- Use o botão por encomenda para o controle mais fino, e o comportamento determinística RRM. **Nota:** Com versão 4.1.185.0, a previsibilidade pode ser conseguida através do uso do âncora-tempo do DCA, do intervalo e da configuração da sensibilidade.

### PORQUE:

Para os usuários que desejam a previsibilidade em mudanças algorítmicas durante todo o sistema, RRM pode ser executado no modo por encomenda. Quando usados, os algoritmos RRM

computam o canal o melhor e as configurações de energia a ser aplicados no intervalo 600-second seguinte. Os algoritmos são então dormentes até que a próxima vez que por encomenda a opção esteja usada; o sistema está em um estado do gelo. Veja [figura 11](#) e [figura 12](#), e as descrições respectivas para mais informação.

## Indicador do Balanceamento de carga

### DICA:

- A configuração padrão para o Balanceamento de carga está LIGADA, com o indicador do Balanceamento de carga ajustado a 0. Este indicador deve ser mudado a um número mais alto, tal como o 10 ou os 12. **Nota:** Na liberação 4.1.185.0 e mais tarde, a configuração padrão para o Balanceamento de carga está e se permitido, o tamanho de janela opta o 5.

### PORQUE:

Embora relativo a RRM, o Balanceamento de carga agressivo pode conduzir aos resultados vagueando do cliente secundário-ótimo para clientes do legado com lógica vagueando deficiente, que lhes faz clientes pegajosos. Isto pode ter efeitos adversos no CHA. O ajuste do indicador do Balanceamento de carga do padrão no WLC é ajustado a 0, que não é uma boa coisa. Isto é interpretado como o número mínimo de clientes que devem estar no AP antes que o mecanismo do Balanceamento de carga retroceda dentro. A pesquisa e a observação internas mostraram que este padrão deve ser mudado a um valor mais prático, tal como o 10 ou os 12. Naturalmente, cada desenvolvimento apresenta uma necessidade diferente e o indicador deve consequentemente ser ajustado apropriadamente. Esta é a sintaxe de linha de comando:

```
(WLC) >config load-balancing window ?  
<client count> Number of clients (0 to 20)
```

Em redes de produção densas, os controladores foram verificados para funcionar otimamente SOBRE com Balanceamento de carga e o tamanho de janela ajustado em 10. na prática, isto significa que comportamento do Balanceamento de carga está permitido somente quando, por exemplo, um grande grupo de pessoas reunido em uma sala de conferência ou em uma área aberta (reunião ou classe). O Balanceamento de carga é muito útil espalhar estes usuários entre vários APs disponíveis em tais encenações.

**Nota:** Os usuários “são jogados nunca fora” da rede Wireless. O Balanceamento de carga ocorre somente em cima da associação e o sistema tentará incentivar um cliente para um AP mais levemente carregado. Se o cliente é persistente, estará permitido juntar-se e encajado nunca à esquerda.

## Gerência de recursos de rádio: Introdução

Junto com o aumento marcado na adoção de Tecnologias WLAN, os problemas de desenvolvimento aumentaram similarmente. A especificação do 802.11 architected originalmente primeiramente com uma HOME, uso da único-pilha na mente. O projeto do canal e das configurações de energia para um único AP era um exercício trivial, mas como a cobertura patente WLAN se transformou uma das expectativas dos usuários, determinar os ajustes de cada AP necessitou uma análise de site completa. Os agradecimentos à natureza compartilhada da largura de banda 802.11's, os aplicativos que são executados agora sobre o segmento sem fio estão empurrando clientes para mover-se para mais disposições capacidade-orientadas. A adição de capacidade a um WLAN é uma edição desigual isso das redes ligadas com fio onde a prática

comum é jogar a largura de banda no problema. Os APs adicionais são exigidos adicionar a capacidade, mas se configurados incorretamente, podem realmente abaixar a potencialidade de sistema devido à interferência e aos outros fatores. Como WLAN em grande escala, densa tornou-se a norma, administradores foi desafiada continuamente com estes problemas de configuração RF que podem aumentar custos operacionais. Se segurado imprópriamente, isto pode conduzir à instabilidade WLAN e a uma experiência de usuário final deficiente.

Com espectro finito (um número limitado de canais desobrepõe) jogar com e o desejo inato do RF dado sangrar através das paredes e dos assoalhos, projetando um WLAN de todo o tamanho provou historicamente ser umas tarefas de afastamento. Dado mesmo uma análise de site sem falhas, o RF nunca-está mudando e o que pôde ser um esquema ótimo do canal e da potência AP um momento, pôde provar ser menos-do que-funcional o seguinte.

Incorpore o RRM de Cisco. RRM permite que a arquitetura unificada WLAN de Cisco analise continuamente o ambiente existente RF, automaticamente ajustando os níveis da potência dos APs e as configurações de canal para ajudar a abrandar coisas como problemas da cobertura da interferência e do sinal do co-canal. RRM reduz a necessidade de executar análises de site exaustivas, aumenta a potencialidade de sistema, e fornece a funcionalidade auto-cura automatizada para compensar zonas mortas RF e falhas AP.

## Gerência de recursos de rádio: Conceitos

### Termos chaves

Os leitores devem inteiramente compreender estes termos usados durante todo este original:

- Sinal: alguma energia transportada por via aérea RF.
- dBm: uma representação matemática absoluta, logarítmica da força de um sinal RF. o dBm é correlacionado diretamente aos miliwatts, mas é de uso geral representar facilmente energias de saída nos valores baixos mesmos comuns na rede de comunicação Wireless. Por exemplo, o valor do dBm -60 é igual a 0.000001 miliwatts.
- Indicador da força de sinal recebido (RSSI): uma medida absoluta, numérica da força do sinal. Não todo o relatório RSSI dos rádios do 802.11 o mesmos, mas para fins deste original, RSSI é suposto para correlacionar diretamente com o sinal recebido como indicado no dBm.
- Ruído: algum sinal que não puder ser decodificado como um sinal do 802.11. Isto pode ser non-802.11 de uma fonte (tal como uma micro-ondas ou um dispositivo de Bluetooth) ou de uma fonte do 802.11 cujo o sinal seja invalidado devido à colisão ou todo o outro retardamento do sinal.
- Assoalho do ruído: o nível de sinal existente (expressado no dBm) abaixo de que os sinais recebidos são incompreensíveis.
- SNR: a relação da intensidade de sinal para propalar o assoalho. Este valor é um valor relativo e porque tal está medido nos decibéis (DB).
- Interferência: o RF indesejável sinaliza na faixa de mesma frequência que pode conduzir a uma degradação ou a uma perda de serviço. Estes sinais podem ser fontes de 802.11 ou de non-802.11.

### Uma vista aérea de RRM

Antes de obter nos detalhes de como os algoritmos RRM trabalham, é importante para

primeiramente compreende um fluxo de trabalho básico de como um sistema RRM colabora para formar um RF que agrupa, assim como compreende que computações RF acontecem onde. Este é um esboço das etapas que a solução unificada de Cisco vai completamente em aprender, em agrupar, e então em computar todas as características RRM:

1. Os controladores (cujos os APs precisam de ter a configuração RF computada como um único grupo) provisioned com o mesmo nome do grupo RF. Um nome do grupo RF é um string ascii que cada AP se usará para determinar se os outros APs se ouvem são parte do mesmo sistema.
2. Os APs mandam periodicamente as mensagens vizinhas, compartilhando da informação sobre se, dos seus controladores, e do seu nome do grupo RF. Estas mensagens vizinhas podem então ser autenticadas por outros APs que compartilham do mesmo nome do grupo RF.
3. Os APs que podem se ouvir que estas mensagens vizinhas e as autenticar baseou no nome do grupo compartilhado RF, passam esta informação (consistindo primeiramente no IP address e na informação do controlador no AP que transmite a mensagem vizinha) até os controladores a que são conectados.
4. Os controladores, compreendendo agora quais outros controladores são ser parte do grupo RF, a seguir formam um grupo lógico para compartilhar desta informação RF e para eleger subsequente um líder do grupo.
5. Equipado com a informação que detalha o ambiente RF para cada AP no grupo RF, uma série de algoritmos RRM visados aperfeiçoando as configurações AP relativas ao seguinte é executada no líder do grupo RF (à exceção do algoritmo da detecção e correção do furo da cobertura que é executado no controlador local aos APs):DCATPC

**Nota:** RRM (e RF que agrupa) são uma função separada da mobilidade do inter-controlador (e da mobilidade que agrupa). A única similaridade é o uso de um string ascii comum atribuído a ambos os nomes do grupo durante o assistente inicial da configuração de controle. Isto é feito para um processo de instalação simplificado e pode ser mudado mais tarde.

**Nota:** É normal para grupos lógicos múltiplos RF existir. Um AP em um controlador dado ajudará a juntar-se a seu controlador com um outro controlador somente se um AP pode ouvir um outro AP de um outro controlador. Em grandes ambientes e terrenos da faculdade é normal para grupos múltiplos RF existir, medindo conjuntos pequenos de construções mas não através do domínio inteiro.

Esta é uma representação gráfica destas etapas:

**Figura 1: As mensagens vizinhas dos APs dão a WLCs uma opinião sistema-larga RF para fazer o canal e os ajustes de potência.**



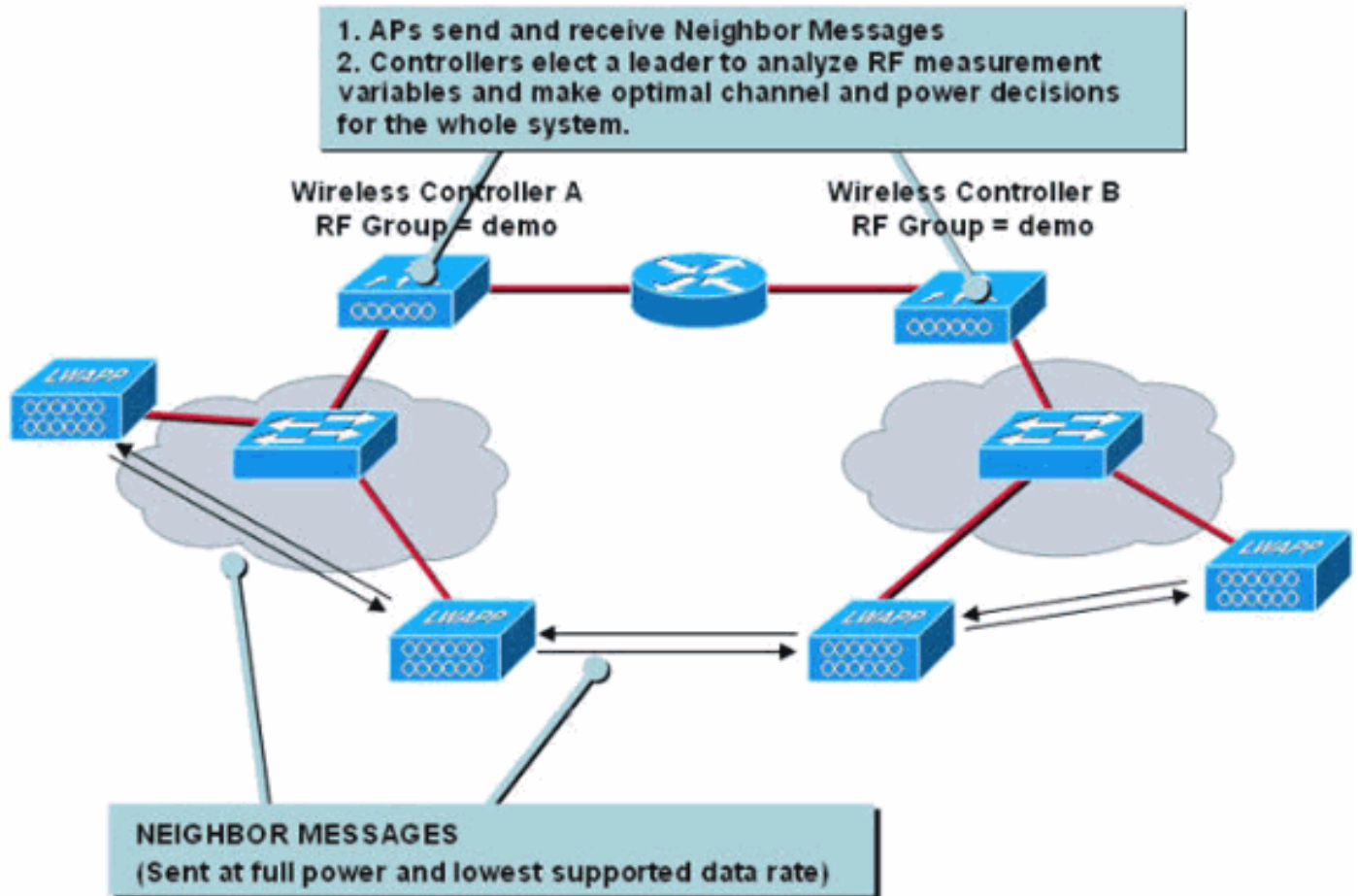


Tabela 1: Referência da divisão da funcionalidade

Funcionalidade	At/by executado:
Agrupamento RF	WLCs elege o líder do grupo
Atribuição dinâmica do canal	Líder do grupo
Controle de potência de transmissão	Líder do grupo
Detecção e correção do furo da cobertura	WLC

## Algoritmo de agrupamento RF

Os grupos RF são conjuntos de controladores que compartilham não somente do mesmo nome do grupo RF, mas os cujos os APs se ouvem.

A colocação lógica AP, e assim o controlador RF que agrupa, são determinados pelos APs que recebem as mensagens vizinhas de outros APs. Estas mensagens incluem a informação sobre o AP transmissor e seu WLC (junto com a informação adicional detalhada na [tabela 1](#)) e são autenticadas por uma mistura.

Tabela 2: As mensagens vizinhas contêm um punhado dos elementos de informação que dão a recepção dos controladores uma compreensão dos APs transmissores e dos controladores a que são conectados.

Nome do campo	Descrição



Identificador de rádio	Os APs com rádios múltiplos usam este para identificar que rádio está sendo usado para transmitir mensagens vizinhas
ID de grupo	Um contador e um MAC address do WLC
IP address WLC	Endereço IP de gerenciamento do líder do grupo RF
O canal do AP	Canal nativo em que o AP presta serviços de manutenção a clientes
Canal vizinho da mensagem	Canal em que o pacote vizinho é transmitido
Alimentação	Usado não atualmente
Teste padrão da antena	Usado não atualmente

Quando um AP receber uma mensagem vizinha (transmitida cada 60 segundos, em todos os canais, no máximo potência prestados serviços de manutenção, e na mais baixa taxa de dados apoiada), envia o quadro até seu WLC para determinar se o AP é parte do mesmo grupo RF verificando a mistura encaixada. Um AP que envia mensagens vizinhas undecipherable (indicar um nome do grupo estrangeiro RF está sendo usada) ou não envia nenhuma mensagem vizinha de todo, é determinado ser um rogue AP.

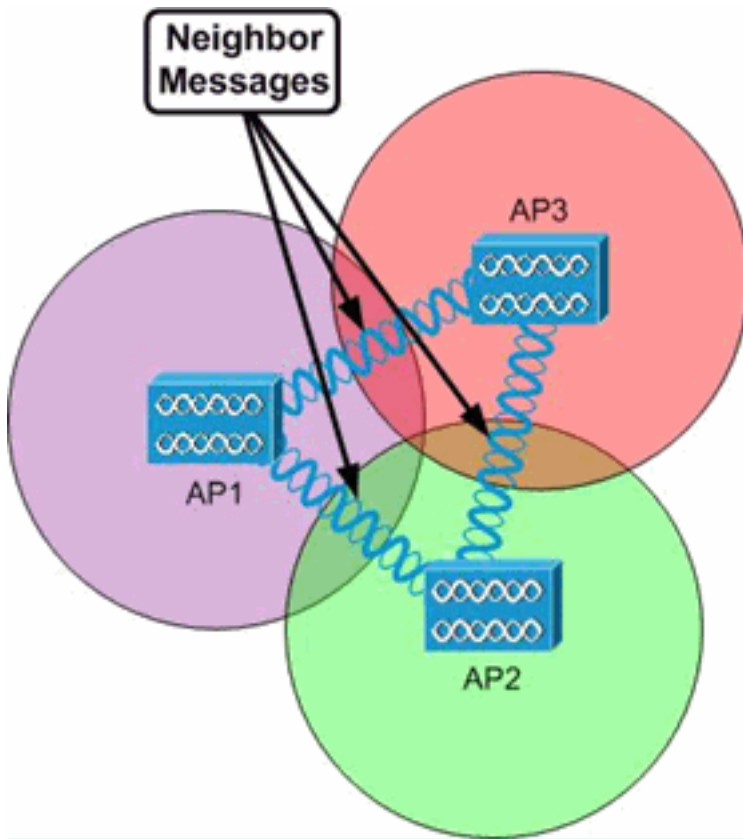
**Figura 2: As mensagens vizinhas são enviadas cada 60 segundos ao endereço de multicast de 01:0B:85:00:00:00.**

18	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0.000000
24	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:01:59.910124
29	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:02:59.915650
34	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:03:59.922653
46	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:04:59.930237
51	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:05:59.935790
56	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:06:59.946686
62	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:07:59.950317
68	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:08:59.955871
74	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:09:59.964819
80	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:10:59.971166
96	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:13:59.990219
101	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:14:59.994158
115	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:17:59.911287
120	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:18:59.919573
125	Airespace: 52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:19:59.925931

Neighbor packets being sent out at 60 second intervals

Dado todos os controladores a parte o mesmo nome do grupo RF, para que um grupo RF forme, uma necessidade WLC manda somente um único AP ouvir um AP de um outro WLC (veja figuras 3 a 8 para uns detalhes mais adicionais).

**Figura 3: Os APs enviam e recebem as mensagens vizinhas que são encaminhadas então a seus controladores para formar o grupo RF.**



As mensagens vizinhas são usadas recebendo APs e seu WLCs para determinar como criar grupos inter-WLC RF, assim como criar os subgrupos lógicos RF que consistem somente naqueles APs que podem ouvir mensagens de cada um. Estes subgrupos lógicos RF têm suas configurações RRM feitas no líder do grupo RF mas independentemente de se devido ao fato de que não têm a conectividade Wireless do subgrupo inter-RF (veja as figuras 4 e 5).

**Figura 4:** Todos os APs são conectados logicamente a um único WLC, mas dois subgrupos lógicos separados RF são formados porque os APs 1, 2, e 3 não podem ouvir mensagens vizinhas de APs 4, 5, e 6, e vice-versa.

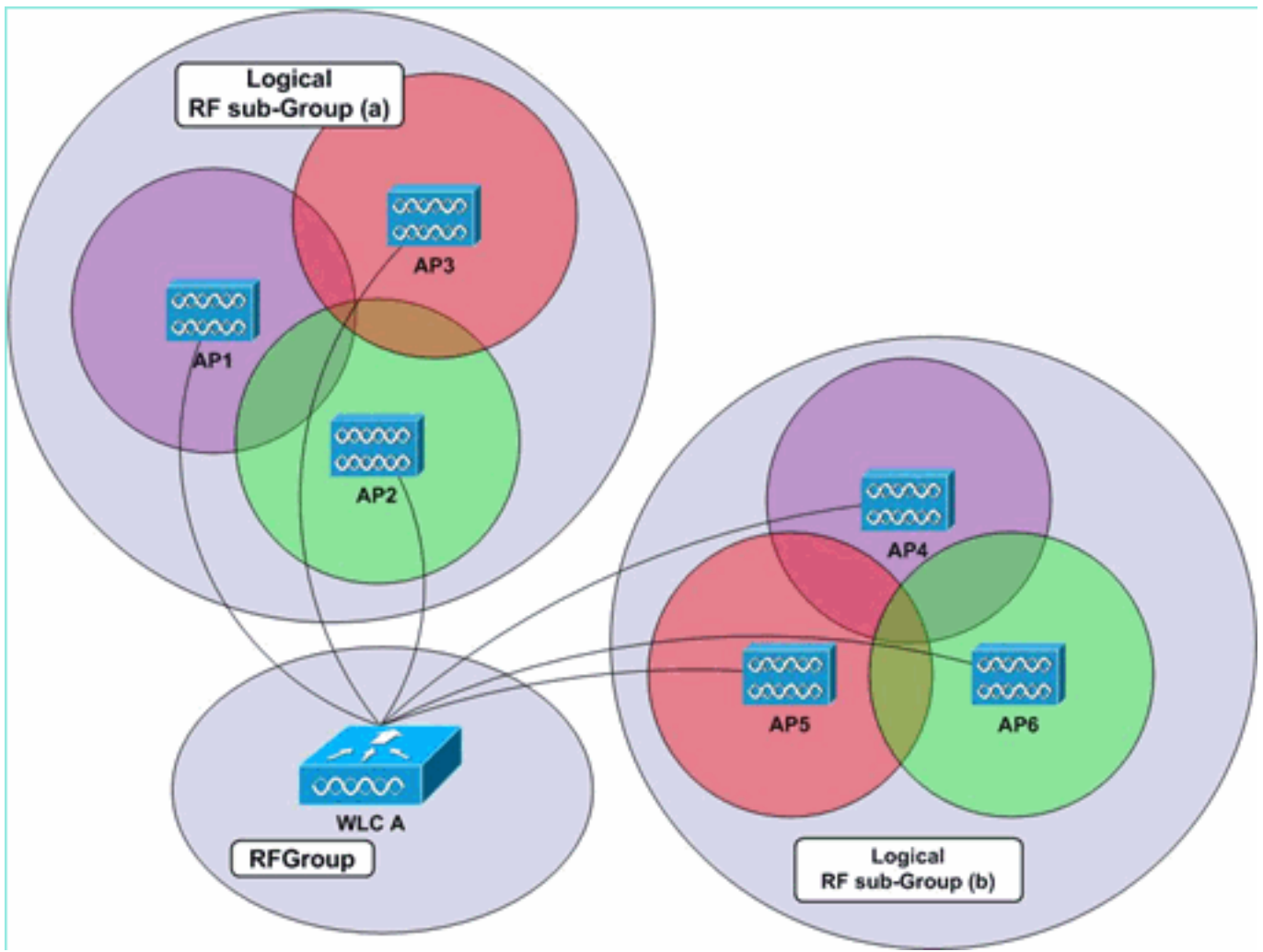
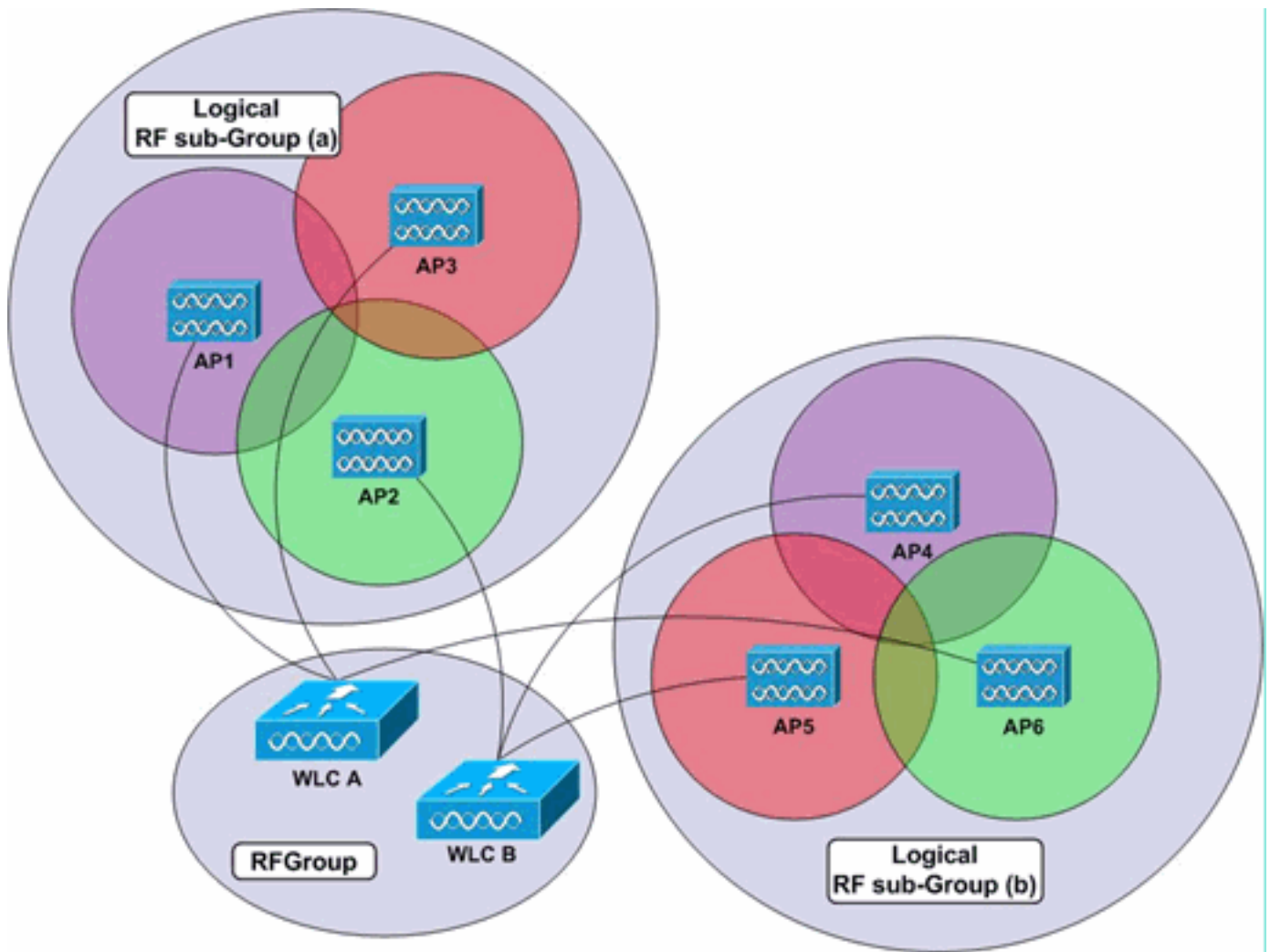
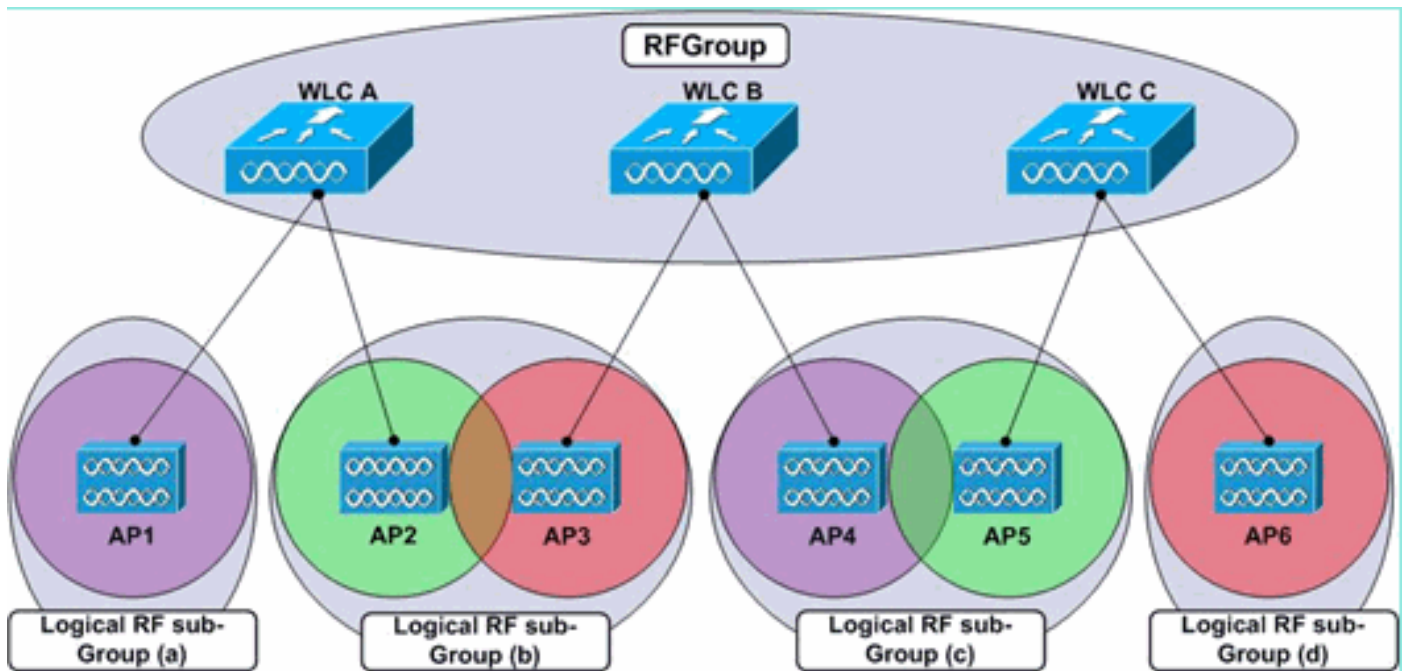


Figura 5: Os APs no mesmo subgrupo lógico RF podem compartilhar de um único WLC, cada um esteja em um WLC separado, ou para estar em uma mistura de WLCs. A funcionalidade RRM é executada em um nível sistema-largo, de modo a por muito tempo como os APs podem se ouvir, seus controladores será agrupada automaticamente. Neste exemplo, WLCs A e B está no mesmo grupo RF e seus APs estão em dois subgrupos lógicos diferentes RF.



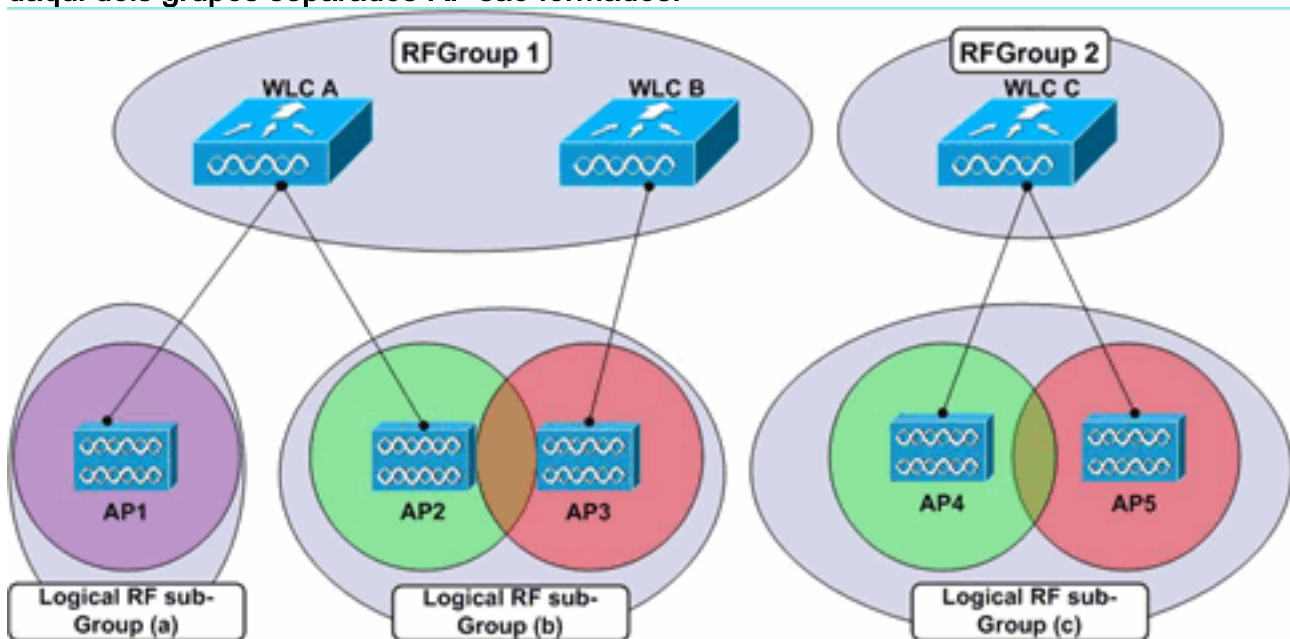
Em um ambiente com muitos WLCs e muitos APs, não todos os APs precisam de ouvir-se para que o sistema inteiro forme um único grupo RF. Cada controlador deve mandar pelo menos um AP ouvir um outro AP de todo o outro WLC. Como tal, o agrupamento RF pode ocorrer através de muitos controladores, apesar da opinião localizada de cada controlador de APs vizinhos e assim, WLCs (veja a figura 6).

**Figura 6:** Neste exemplo, os APs conectados a WLCs A e o C não podem ouvir mensagens vizinhas de se. WLC B pode ouvir WLC A e C e pode então compartilhar do outro informação com eles de modo que um único grupo RF seja formado então. Os subgrupos lógicos discretos RF são criados para cada grupo de APs que podem mensagens vizinhas de cada um.



Em uma encenação onde os controladores múltiplos sejam configurados com o mesmo nome do grupo RF, mas seus APs respectivos não podem ouvir mensagens vizinhas de cada um, dois grupos (níveis mais alto) separados RF são formados, como mostrado na figura 7.

**Figura 7:** Embora a parte de WLCs o mesmo nome do grupo RF, seus APs não possa se ouvir e daqui dois grupos separados RF são formados.

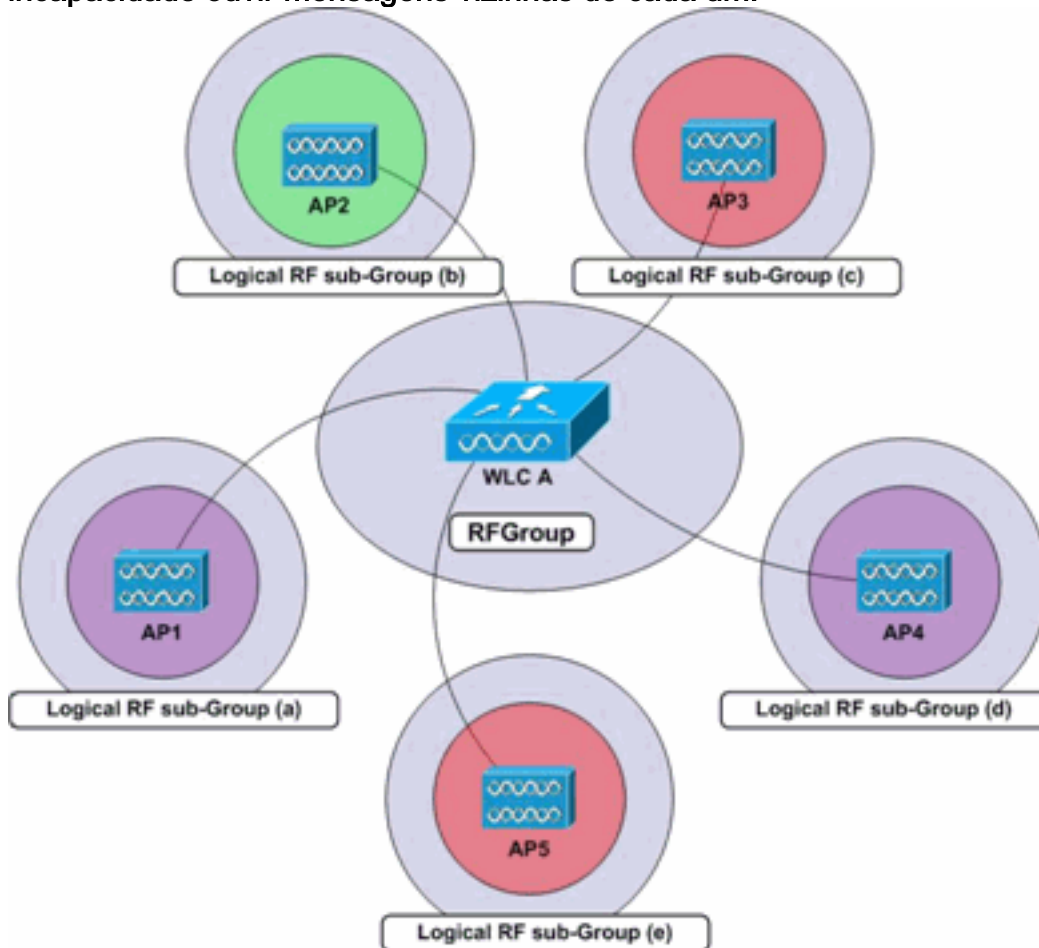


O agrupamento RF ocorre a nível do controlador, assim que significa que uma vez que informação do relatório APs nos outros APs que se ouvem (assim como os controladores a que aqueles APs são conectados) a seus controladores, cada WLC respectivo a seguir comunica-se diretamente com o outro WLCs para formar um agrupamento sistema-largo. Dentro de um único grupo sistema-largo, ou do grupo RF, muitos subconjuntos dos APs teriam seus parâmetros RF ajustados separadamente de se: considere um WLC central com os APs individuais em locais remotos. Cada AP, teria consequentemente seus parâmetros RF ajustados separadamente dos outro, assim que quando cada AP pertencer ao mesmo controlador RF que agrupa, cada AP individual (neste exemplo) estaria em seu próprio subgrupo lógico RF (veja figura 8).

**Figura 8:** Os parâmetros RF de cada AP são ajustados separadamente de outro devido a sua



incapacidade ouvir mensagens vizinhas de cada um.



Cada AP compila e mantém uma lista de até 34 APs vizinhos (pelo rádio) que seja relatada então até seus controladores respectivos. Cada WLC mantém uma lista de 24 vizinhos pelo rádio AP das mensagens vizinhas enviadas por cada AP. Uma vez a nível do controlador, este por-AP, a lista vizinha do por-rádio de até 34 APs é podado então, que deixa cair os dez APs com os sinais os mais fracos. WLCs encaminha então cada lista vizinha AP até o líder do grupo RF, o WLC eleito pelo grupo RF para executar toda a tomada de decisão da configuração RRM.

É muito importante notar aqui trabalhos desse agrupamento RF pelo tipo de rádio. O algoritmo de agrupamento é executado separadamente para os rádios 802.11a e 802.11b/g, significando que é executado pelo AP, pelo rádio, tais que cada rádio AP é responsável para povoar uma lista de vizinhos. A fim limitar o flapping, por meio de que os APs puderam frequentemente ser adicionados e podado desta lista, WLCs adicionará vizinhos a suas lista dado que estão ouvidos superior ou igual a no dBm -80 e somente as removerão então uma vez que seus sinais mergulham abaixo do dBm -85.

**Nota:** Com Software Release 4.2.99.0 ou Mais Recente do controlador do Wireless LAN, RRM apoia até 20 controladores e 1000 Access point em um grupo RF. Por exemplo, um controlador de Cisco WiSM apoia até 150 Access point, assim que você pode ter até seis controladores de WiSM em um grupo RF (controladores dos tempos 6 de 150 Access point = 900 Access point, que seja menos de 1000). Similarmente, apoios 4404 de um controlador até 100 Access point, assim que você podem ter até dez 4404 controladores em um grupo RF (100 vezes 10 = 1000). Os controladores 2100-series-based apoiam um máximo de 25 Access point, assim que você pode ter até 20 destes controladores em um grupo RF. Este limite 1000 de AP não é o número real de APs associados aos controladores, mas é calculado com base no número máximo de APs que podem ser apoiados por esse modelo específico do controlador. Por exemplo, se há 8 controladores de WiSM (4 WiSMs), cada um com 70 APs, o número real de APs é 560. Contudo,

o algoritmo calcula-o como  $8 \times 150 = 1200$  (150 que são o número máximo de APs apoiados por cada controlador de WiSM). Consequentemente, os controladores obtêm a separação em dois grupos. Um grupo com os controladores 6 e o outro com 2 controladores.

Porque o controlador que funciona enquanto o líder do grupo RF executa ambos, o algoritmo DCA e o algoritmo TPC para o sistema inteiro, controladores devem ser configurados com o nome do grupo RF em uma situação quando se antecipa que suas mensagens vizinhas estarão ouvidas por APs em um outro controlador. Se os APs (em controladores diferentes) são separados geograficamente, pelo menos a uma extensão que as mensagens vizinhas deles não podem ser ouvidas em ou melhor do que  $-80\text{dBm}$ , configurando seus controladores para estar em um grupo RF não é prático.

Se o limite superior para o algoritmo de agrupamento RF é alcançado, o controlador do líder do grupo não permitirá que nenhuns controladores ou APs novos juntem-se ao grupo existente ou contribuam-se aos cálculos do canal e da potência. O sistema tratará esta situação como um subgrupo lógico novo RF e os membros novos serão adicionados a este grupo lógico novo, configurado com o mesmo nome do grupo. Se o ambiente acontece ser dinâmico, na natureza onde as flutuações RF mudam como os vizinhos são vistos em intervalos periódicos, a probabilidade de alterações do membro do grupo e as eleições subsequentes do líder do grupo aumentarão.

### O líder do grupo

O líder do grupo RF é o controlador eleito no grupo RF que executa a análise dos dados RF dos APs, pelo grupo lógico RF, e é responsável para a configuração dos níveis da potência dos APs e dos ajustes do canal. A detecção e correção do furo da cobertura é baseada no SNR do cliente e é consequentemente a única função RRM executada em cada controlador local.

Cada controlador determina que WLC tem a prioridade a mais alta do líder do grupo baseada no elemento de informação do identificador do grupo em cada mensagem vizinha. O elemento de informação do identificador do grupo anunciado em cada mensagem vizinha é compreendido de um valor de contador (cada controlador mantém um contador de 16 bits que os começos em 0 e incrementem eventos de seguimento tais como uma saída de um grupo RF ou de uma repartição WLC) e do MAC address do controlador. Cada WLC dará a prioridade aos valores identificador do grupo de seus vizinhos baseados primeiramente neste valor de contador e então, no caso de um laço do valor de contador, no MAC address. Cada WLC selecionará o um controlador (um WLC vizinho ou próprio) com o valor identificador o mais alto do grupo, depois do qual cada controlador confer com o outro determinará que único controlador tem o ID de grupo o mais alto. Esse WLC será elegido então o líder do grupo RF.

Se o líder do grupo RF vai off line, o grupo inteiro está licenciado e os membros existentes do grupo RF tornam a colocar em funcionamento o processo de seleção do líder do grupo e um líder novo é escolhido.

Os minutos cada 10, o líder do grupo RF votará cada WLC no grupo para as estatísticas dos APs, assim como toda sua informação de mensagem vizinha recebida. Desta informação, o líder do grupo tem a visibilidade dentro ao ambiente sistema-largo RF e pode então usar os algoritmos DCA e TPC para ajustar continuamente o canal e as configurações de energia dos APs. O líder do grupo executa estes algoritmos cada dez minutos mas, como com o algoritmo da detecção e correção do furo da cobertura, as mudanças são feitas somente se necessário determinado.

### Algoritmo dinâmico da atribuição do canal



O algoritmo DCA, é executado pelo líder do grupo RF, é aplicado em uma base do por-RF-grupo para determinar ajustes ótimos do canal AP para os APs de todo o grupo RF (cada grupo de APs que podem ouvir mensagens vizinhas de cada um, referido neste original como um subgrupo lógico RF, tem sua configuração de canal feita independentemente de outros subgrupos lógicos RF devido ao fato de que os sinais não fazem sobreposição). Com o processo DCA, o líder considera um punhado do medidor AP-específico que é levado em consideração ao determinar o canal necessário muda. Este o medidor é:

- **Medida da carga** — Cada AP mede a porcentagem do tempo total ocupada transmitindo ou recebendo quadros do 802.11.
- **Ruído** — Os APs calculam valores do ruído em cada canal prestado serviços de manutenção.
- **Interferência** — Os APs relatam na porcentagem do media pegado por transmissões de interferência do 802.11 (este pode ser dos sinais de sobreposição dos APs estrangeiros, assim como dos NON-vizinhos).
- **Intensidade de sinal** — Cada AP escuta mensagens vizinhas em todos os canais prestados serviços de manutenção e grava os valores RSSI em que estas mensagens são ouvidas. Esta informação da intensidade de sinal AP é a métrica a mais importante considerada no cálculo DCA de energia do canal.

Estes valores são usados então pelo líder do grupo para determinar se um outro esquema do canal conduzirá pelo menos a um melhoramento do AP de execução o mais ruim por 5dB (SNR) ou por mais. A ponderação é dada aos APs no seu funcionamento canaliza tais que os ajustes do canal estão feitos localmente, se umedecendo mudam para impedir o efeito de dominó por meio de que uma única mudança provocaria alterações sistema-largas do canal. A preferência é dada igualmente aos APs baseados na utilização (derivada do relatório da medida da carga de cada AP) de modo que um AP menos-usado tenha uma semelhança mais elevada de ter seu canal mudado (em relação a um vizinho pesadamente utilizado) no evento que uma mudança é precisada.

**Nota:** Sempre que um canal AP é mudado, os clientes serão desligados momentaneamente. Os clientes podem ou reconectar ao mesmo AP (em seu canal novo), ou vagueie a um AP próximo, que dependa do comportamento vagueando do cliente. Jejua, vaguear seguro (oferecido pelo CCKM e pelo PKC) ajudará a reduzir este breve rompimento, dado lá é clientes compatíveis.

**Nota:** Quando os APs carreg acima de pela primeira vez (novo fora da caixa), transmitem no primeiro canal desobseposição nas faixas que apoiam (o canal 1 para 11b/g e canaliza 36 para 11a). Quando os APs põem o ciclo, usam seus ajustes precedentes do canal (armazenados na memória do AP). Os ajustes DCA ocorrerão subseqüentemente como necessário.

## [Algoritmo de controle da potência de transmissão](#)

O algoritmo TPC, é executado dez fixos em um intervalo minuto à revelia, é usado pelo líder do grupo RF para determinar os proximities RF dos APs e para ajustar mais baixo o nível de potência de transmissão de cada faixa para limitar a sobreposição da pilha e a interferência excessivas do co-canal.

**Nota:** O algoritmo TPC é somente responsável para girar níveis da potência para baixo. O aumento das energias de transmissão é parte da função do algoritmo da detecção e correção do furo da cobertura, que é explicada na seção subsequente.

Cada AP relata uma lista RSSI-pedida de todos os APs vizinhos e, desde que um AP tem APs três ou mais vizinhos (para que o TPC trabalhe, você deve ter um mínimo de 4 APs), o líder do

grupo RF aplicará o algoritmo TPC em uma por-faixa, a base por-AP para ajustar a potência AP transmite níveis para baixo tais que o terceiro vizinho que o mais alto o AP será ouvido então a nível de sinal de -70dBm (valor padrão ou o que o valor configurado é) ou mais baixo e a condição da histerese TCP é satisfeita. Consequentemente, o TCP atravessa estas fases que decidem se uma mudança da potência de transmissão é necessária:

1. Determine se há um terceiro vizinho, e se esse terceiro vizinho está acima do ponto inicial do controle de potência de transmissão.
2. Determine a potência de transmissão usando esta equação:  $Tx\_Max$  para dado AP + (o controle de potência TX trilha - o RSSI do ó vizinho o mais alto acima do ponto inicial).
3. Compare o cálculo de etapa dois com o nível de potência TX atual e verifique se excede a histerese TPC. Se a potência TX precisa de ser girada para baixo: A histerese TPC pelo menos de 6dBm deve ser encontrada. OUSE a potência TX precisa de ser aumentada: A histerese TPC de 3dBm deve ser encontrada.

Um exemplo da lógica usada no algoritmo TPC pode ser encontrado na seção do [exemplo dos trabalhos do algoritmo de controle da potência de transmissão](#).

**Nota:** Quando todos os APs carreg acima de pela primeira vez (novo fora da caixa), transmitem a seus níveis da potência máxima. Quando os APs são potência dada um ciclo, usam suas configurações de energia precedentes. Os ajustes TPC ocorrerão subseqüentemente como necessário. Veja a [tabela 4](#) para obter informações sobre dos níveis de potência de transmissão apoiados AP.

**Nota:** Há duas encenações do aumento da potência TX do cano principal que podem ser provocadas com o algoritmo TPC:

- Não há nenhum terceiro vizinho. Neste caso, o AP opta de volta a  $Tx\_max$ , e faz tão imediatamente.
- Há um terceiro vizinho. A equação TPC avalia realmente o Tx recomendado para estar em algum lugar entre  $Tx\_max$  e  $Tx\_current$  (um pouco do que mais baixo do que  $Tx\_current$ ) como dentro, por exemplo, quando o terceiro vizinho “parte” e há um terceiro vizinho possível novo. Isto conduz a um aumento da potência TX.as diminuições TPC-induzidas de Tx ocorrem gradualmente, mas os aumentos de Tx podem ocorrer imediatamente. Contudo, a precaução extra foi recolhida como a potência TX é aumentada com algoritmo do furo da cobertura, indo acima, um nível de cada vez.

### [Algoritmo da detecção e correção do furo da cobertura](#)

O algoritmo da detecção e correção do furo da cobertura é apontado nos primeiros furos de determinação da cobertura baseados na qualidade de níveis de sinal e então de aumentar do cliente a potência de transmissão dos APs a que aqueles clientes são conectados. Porque este algoritmo é estado relacionado com as estatísticas do cliente, é executado independentemente em cada controlador e sistema-não largo no líder do grupo RF.

O algoritmo determina se um furo da cobertura existe quando os níveis SNR dos clientes passam abaixo de um ponto inicial dado SNR. O ponto inicial SNR é considerado em uma base individual AP e baseado primeiramente em cada nível de potência de transmissão AP. Os níveis da potência dos APs mais altos, mais ruído são tolerados em relação à intensidade de sinal do cliente, que significa um valor tolerado mais baixo SNR.

Esse limite de SNR varia com base em dois valores: A potência de transmissão do AP e o valor do perfil de cobertura da controladora. Em detalhe, o ponto inicial é definido por cada potência de transmissão AP (representada no dBm), menos o valor constante de 17dBm, menos o valor do perfil da cobertura dos configuráveis pelo usuário (este valor é optado 12 DB e detalhado na página 20). O valor de limiar do cliente SNR é o valor absoluto (número positivo) do resultado desta equação.

### **Equação do ponto inicial do furo SNR da cobertura:**

Valor de corte de SNR do cliente (|DB|) = [Potência de transmissão do AP (dBm) - Constante (17 dBm) - Perfil de Cobertura (dB)]

Uma vez que o número configurado do SNR médio dos clientes mergulha abaixo deste ponto inicial SNR no mínimo 60 segundos, a potência de transmissão AP daqueles clientes estará aumentada a brando a violação SNR, conseqüentemente corrigindo o furo da cobertura. Cada controlador executa o algoritmo da detecção e correção do furo da cobertura para cada rádio em cada um de seus APs cada três minutos (o valor padrão de 180 segundos pode ser mudado). É importante notar que os ambientes temporários podem conduzir ao algoritmo TPC que gerencie a potência para baixo em corridas subsequentes do algoritmo.

### **“Consideração de ligação inicial do cliente pegajoso”:**

As aplicações vagueando em driveres de cliente do legado podem conduzir aos clientes “que colam” a um AP existente mesmo na presença de um outro AP que seja melhor quando se trata do RSSI, da taxa de transferência e da experiência total do cliente. Por sua vez, tal comportamento pode ter o impacto sistemático na rede Wireless por meio de que os clientes são percebidos para experimentar eventualmente o SNR deficiente (porque não vaguearam) tendo por resultado uma detecção do furo da cobertura. Em tal situação, o algoritmo põe acima a potência de transmissão do AP (para fornecer a cobertura para os clientes que se comportam ruim) que conduz (e mais altamente do que o normal) à potência de transmissão indesejável.

Até que a lógica vagueando esteja melhorada inerentemente, tais situações podem ser abrandadas aumentando o cliente Mínimo Exceção Nivelamento a um número mais alto (o padrão é 3) e igualmente aumentando o valor tolerável do cliente SNR (o padrão é DB 12 e melhorias é considerado quando mudado a DB 3). Se a versão de código é usada 4.1.185.0 ou mais tarde, os valores padrão fornece resultados os melhores na maioria de ambientes.

**Nota:** Embora estas sugestões sejam baseadas no teste interno e possam variar para disposições individuais, a lógica atrás de alterar estes ainda aplica-se.

Veja a seção do [exemplo do algoritmo da detecção e correção do furo da cobertura](#) para um exemplo da lógica envolvida na provocação.

**Nota:** O algoritmo da detecção e correção do furo da cobertura é igualmente responsável para detectar lapsos na cobertura devido à falha AP e pôr APs próximos acima como necessário. Isto permite que a rede cure em torno das interrupções de serviço.

## **Gerência de recursos de rádio: Parâmetros de configuração**

Uma vez RRM e os algoritmos são compreendidos, a próxima etapa é aprender como interpretar e alterar parâmetros necessários. Esta seção detalha operações da configuração de RRM e de ajustes básicos do relatório dos esboços, também.

A primeira etapa mesma para configurar RRM é assegurar-se de que cada um WLC tenha o mesmo nome do grupo RF configurado. Isto pode ser feito através da interface da WEB do controlador se você seleciona o **controlador | General** e entrado então um valor comum do nome do grupo. A conectividade IP entre WLCs no mesmo grupo RF é uma necessidade, também.

Figura 9: Os grupos RF são formados basearam no valor especificado pelo utilizador da “do nome RF-rede,” nome do grupo igualmente chamado RF neste original. Todo o WLCs que são exigidas participar nas operações sistema-largas RRM deve compartilhar desta mesma corda.

The screenshot shows the Cisco WLC GUI with the 'Controller' section selected. The 'General' tab is active, displaying various configuration settings. The left sidebar lists navigation options like General, Inventory, Interfaces, Network Routes, Internal DHCP Server, Mobility Management, Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP. The main content area shows the following settings:

Configuration Item	Value
802.3x Flow Control Mode	Disabled
LWAPP Transport Mode	Layer 3
LAG Mode on next reboot	Enabled
Ethernet Multicast Mode	Disabled
Broadcast Forwarding	Disabled
Aggressive Load Balancing	Disabled
Peer to Peer Blocking Mode	Disabled
Over The Air Provisioning of AP	Enabled
AP Fallback	Enabled
Apple Talk Bridging	Disabled
Fast SSID change	Disabled
Default Mobility Domain Name	mobile-demo
RF-Network Name	rrm-demo
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
802.3 Bridging	Disabled
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C

Todas as explicações de configuração e exemplos nas próximas seções são executados através da interface gráfica WLC. No WLC GUI, vá ao título principal do Sem fio e selecione a opção **RRM** para o padrão de WLAN da escolha no lado esquerdo. Seguinte, selecione o **auto RF** na árvore. As seções subsequente proveem a página resultante [Sem fio | 802.11a ou 802.11b/g RRM | Auto RF...].

## [RF que agrupa ajustes através do WLC GUI](#)

- **Modo do grupo** — A configuração de modo do grupo permite o RF que agrupa para ser

desabilitado. Desabilitar esta característica impede que o WLC agrupe com outros controladores para executar a funcionalidade sistema-larga RRM. Deficientes, todas as decisões RRM serão locais ao controlador. O agrupamento RF é permitido à revelia e os endereços MAC do outro WLCs no mesmo grupo RF estão listados à direita da caixa de seleção do modo do grupo.

- **Intervalo da atualização do grupo** — O valor do intervalo da atualização do grupo indica como o algoritmo de agrupamento RF é executado frequentemente. Este é um campo do indicador-somente e não pode ser alterado.
- **Líder do grupo** — Este campo indica o MAC address do WLC que é atualmente o líder do grupo RF. Porque o agrupamento RF é executado o por-AP, por-rádio, este valor pode ser diferente para as redes 802.11a e 802.11b/g.
- **É este controlador um o líder do grupo** — Quando o controlador é o líder do grupo RF, este valor de campo será “sim.” Se o WLC não é o líder, o campo precedente indicará que WLC no grupo é o líder.
- **Última atualização do grupo** — O algoritmo de agrupamento RF executa cada 600 segundos (minutos 10). Este campo indica somente o tempo (nos segundos) desde que o algoritmo foi executado por último e não necessariamente a última vez onde um líder do grupo novo RF foi elegido.

Figura 10: O estado do grupo RF, as atualizações, e os detalhes da sociedade são destacados na parte superior da auto página RF.

RF Grouping Algorithm		RF Group Members
Group Mode	<input checked="" type="checkbox"/> Enabled	MAC Address
Group Update Interval	600 secs	00:16:46:4b:33:40
Group Leader	00:16:46:4b:33:40	
Is this Controller a Group Leader ?	Yes	
Last Group Update	103 secs ago	

## [O RF canaliza ajustes da atribuição através do WLC GUI](#)

- **Método da atribuição do canal** — O algoritmo DCA pode ser configurado em uma de três maneiras:  
**Automático** — Esta é a configuração padrão. Quando RRM é permitido, o algoritmo DCA executa cada 600 segundos (dez minutos) e, caso necessário, as mudanças do canal serão feitas neste intervalo. Este é um campo do indicador-somente e não pode ser alterado. Note por favor as opções de 4.1.185.0 no apêndice A.  
**Por encomenda** — Isto impede que o algoritmo DCA esteja executado. O algoritmo pode manualmente ser provocado clicando em “invoca a atualização do canal agora” abotoa-se.  
**Nota:** Se você seleciona **por encomenda** e o clica então **invoca a atualização do canal agora**, as mudanças presumidas do canal são necessárias, o algoritmo DCA é executado e o plano de canal novo é aplicado 600 seguintes no segundo intervalo.  
**Fora de** — Esta opção desabilita todas as funções DCA, e não é recomendada. Isto é desabilitado tipicamente em cima de executar uma análise de site manual e subseqüentemente de configurar ajustes de cada canal AP individualmente. Embora não relacionado, isto é feito frequentemente ao lado de fixar o algoritmo TPC, também.
- **Evite a interferência estrangeira AP** — Este campo permite que a métrica da interferência do co-canal seja incluída em cálculos do algoritmo DCA. Este campo é permitido à revelia.
- **Evite a carga de Cisco AP** — Este campo permite que a utilização dos APs seja considerada ao determinar os canais de que APs precisam de mudar. A carga AP é uma métrica



frequentemente em mudança e sua inclusão não pôde sempre ser desejada nos cálculos RRM. Como tal, este campo é desabilitado à revelia.

- **Evite o ruído non-802.11b** — Este campo permite que o nível de ruído non-802.11 de cada AP seja um fator de contribuição ao algoritmo DCA. Este campo é permitido à revelia.
- **Contribuição da intensidade de sinal** — As forças de sinal dos APs vizinhos são incluídas sempre em cálculos DCA. Este é um campo do indicador-somente e não pode ser alterado.
- **Líder da atribuição do canal** — Este campo indica o MAC address do WLC que é atualmente o líder do grupo RF. Porque o agrupamento RF é executado o por-AP, por-rádio, este valor pode ser diferente para as redes 802.11a e 802.11b/g.
- **Última atribuição do canal** — O algoritmo DCA executa cada 600 segundos (minutos 10). Este campo indica somente o tempo (nos segundos) desde que o algoritmo foi executado por último e não necessariamente a última vez onde uma atribuição nova do canal foi feita.

**Figura 11: Configuração dinâmica do algoritmo da atribuição do canal**

Dynamic Channel Assignment Algorithm		
Channel Assignment Method	<input checked="" type="radio"/> Automatic Interval: 600 secs	AnchorTime: 0 (Hour of the day)
	<input type="radio"/> On Demand	<input type="button" value="Invoke Channel Update now"/>
	<input type="radio"/> OFF	
Avoid Foreign AP interference	<input checked="" type="checkbox"/> Enabled	
Avoid Cisco AP load	<input type="checkbox"/> Enabled	
Avoid non-802.11b noise	<input checked="" type="checkbox"/> Enabled	
Signal Strength Contribution	Enabled	
Channel Assignment Leader	00:16:46:4b:33:40	
Last Channel Assignment	467 secs ago	
DCA Sensitivity Level	MEDIUM (15 dB)	

## [Ajustes da atribuição do nível de potência TX através do WLC GUI](#)

- **Método da atribuição do nível da potência** — O algoritmo TPC pode ser configurado em uma de três maneiras:
  - Automático** — Esta é a configuração padrão. Quando RRM é permitido, o algoritmo TPC executa cada dez minutos (600 segundos) e, caso necessário, as mudanças da configuração de energia serão feitas neste intervalo. Este é um campo do indicador-somente e não pode ser alterado.
  - Por encomenda** — Isto impede que o algoritmo TPC esteja executado. O algoritmo pode manualmente ser provocado se você clica a **atualização do canal da invocação** se abotoa **agora**. **Nota:** Se você seleciona **por encomenda** e o clica então **invoca a atualização da potência agora**, as mudanças presumidas da potência são necessárias, o algoritmo TPC é executado e as configurações de energia novas são aplicadas 600 seguintes no segundo intervalo.
  - Fixo** — Esta opção desabilita todas as funções TPC, e não é recomendada. Isto é desabilitado tipicamente em cima de executar uma análise de site manual e subseqüentemente de configurar configurações de energia cada AP individualmente. Embora não relacionado, isto é feito frequentemente ao lado de desabilitar o algoritmo DCA, também.
- **Ponto inicial da potência** — Este valor (no dBm) é o nível de sinal da interrupção em que o algoritmo TPC ajustará níveis da potência para baixo, tais que este valor é a força em que o vizinho o mais forte de um AP terceiro é ouvido. Em determinadas ocasiões raras onde o ambiente RF foi julgado demasiado “quente”, no sentido que os APs em uma encenação

high-density provável estão transmitindo a níveis alto-do que-desejados da potência de transmissão, os **802.11b avançados configuração tx-potência-controle-trilham** o comando podem ser usados para permitir ajustes de potência descendentes. Isto permite os APs de ouvir seu terceiro vizinho com um grau maior de separação RF, que permite o AP vizinho de transmitir a nível da potência mais baixo. Este foi um parâmetro un-modificável até o Software Release 3.2. O valor configurável novo varia de -50dBm a -80dBm e pode somente ser mudado do CLI do controlador.

- **Contagem vizinha da potência** — O número mínimo de vizinhos que um AP deve ter para que o algoritmo TPC seja executado. Este é um campo do indicador-somente e não pode ser alterado.
- **Contribuição da atualização da potência** — Este campo não é atualmente em uso.
- **Líder da atribuição da potência** — Este campo indica o MAC address do WLC que é atualmente o líder do grupo RF. Porque o agrupamento RF é executado o por-AP, por-rádio, este valor pode ser diferente para as redes 802.11a e 802.11b/g.
- **Última atribuição do nível da potência** — O algoritmo TPC executa cada 600 segundos (minutos 10). Este campo indica somente o tempo (nos segundos) desde que o algoritmo foi executado por último e não necessariamente a última vez onde uma atribuição nova da potência foi feita.

**Figura 12: Configuração do algoritmo de controle da potência de transmissão**

**Tx Power Level Assignment Algorithm**

Power Level Assignment Method	<input checked="" type="radio"/> Automatic      Every 600 secs <input type="radio"/> On Demand <b>Invoke Power Update now</b> <input type="radio"/> Fixed      1
Power Threshold	-70 dBm
Power Neighbor Count	3
Power Update Contribution	SNI.
Power Assignment Leader	00:16:46:4b:33:40
Last Power Level Assignment	33 secs ago

**Pontos iniciais do perfil: WLC GUI**

Os pontos iniciais do perfil, chamados pontos iniciais RRM nos sistemas de controle sem fio (WCS), são usados principalmente alarmando-se. Quando estes valores são excedidos, as armadilhas estão enviadas até o WCS (ou algum outro sistema de administração com base em SNMP) para o diagnóstico fácil das questões de rede. Estes valores são usados unicamente para fins da alerta e não têm nenhum rolamento na funcionalidade dos algoritmos RRM qualquer.

**Figura 13: Valores de limiar alarming do perfil do padrão.**



## Profile Threshold For Traps

Interference (0 to 100%)	10
Clients (1 to 75)	12
Noise (-127 to 0 dBm)	-70
Utilization (0 to 100%)	80
Coverage Exception Level (0 to 100 %)	25

- **Interferência (0 100%)** — A porcentagem do media sem fio ocupado por sinais de interferência do 802.11 antes de um alarme é provocada.
- **Cientes (1 75)** — O número de por-faixa dos clientes, o por-AP acima de que, um controlador gerará uma armadilha de SNMP.
- **DBm do ruído (-127 a 0)** — usado para gerar uma armadilha de SNMP quando o assoalho do ruído aumentar acima do nível do grupo.
- **Cobertura (3 a DB 50)** — o nível tolerável máximo do SNR pelo cliente. Este valor é usado na geração de armadilhas para ambos os pontos iniciais mínimos do nível da exceção da cobertura e do nível da exceção do cliente. (Parte da subseção do algoritmo do furo da cobertura em 4.1.185.0 e mais tarde)
- **Utilização (0 100%)** — O valor alarming que indica o máximo desejou a porcentagem do tempo onde o rádio de um AP gasta transmitir e receber. Isto pode ser útil seguir ao longo do tempo a utilização de rede.
- **O nível da exceção da cobertura (0 100%)** — o máximo desejou a porcentagem dos clientes no funcionamento de rádio de um AP abaixo do ponto inicial desejado da cobertura (definido acima).
- **Nível mínimo da exceção do cliente** — Número desejado mínimo de clientes tolerados pelo AP cujos os SNR estão abaixo do ponto inicial da cobertura (definido acima) (parte da subseção do algoritmo do furo da cobertura em 4.1.185.0 e mais tarde).

### Canais de monitoração do ruído/interferência/rogue

Cisco APs proporciona o serviço dos dados do cliente e fá-lo a varredura periodicamente para a funcionalidade RRM (e IDS/IPS). Os canais que os APs são permitidos para fazer a varredura são configuráveis.

**Lista do canal:** Os usuários podem especificar o que a vontade APs das escalas do canal monitora periodicamente.

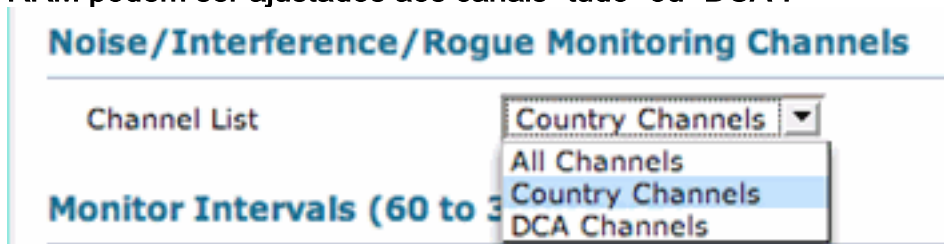
- **Todos os canais** — Este ajuste dirigirá APs para incluir cada canal no ciclo de exploração. Isto é primeiramente útil para a funcionalidade IDS/IPS (fora do âmbito deste original) e não fornece o valor adicional nos processos RRM comparados ao ajuste dos canais do país.
- **Canais do país** — Os APs farão a varredura somente daqueles canais apoiados explicitamente na configuração do domínio regulatório de cada WLC. Isto significa que os APs passarão periodicamente o tempo que escuta em cada canal permitido pelo corpo regulatório local (este pode incluir os canais de sobreposição assim como os canais desobrepõem de uso geral). Esta é a configuração padrão.

- **Canais DCA** — Isto restringe a exploração dos APs somente 2 aqueles canais a que os APs serão atribuídos baseados no algoritmo DCA. Isto significa que no Estados Unidos, os rádios 802.11b/g fariam a varredura somente nos canais 1, 6, e 11 à revelia. Isto é baseado na escola de pensamento que a exploração é centrada somente sobre os canais que o serviço está sendo proporcionado sobre, e o rogue APs não é um interesse. **Nota:** A lista de canais usados pelo algoritmo DCA (para a monitoração e a atribuição do canal) pode ser alterada na versão de código 4.0 WLC, ou mais tarde. Por exemplo, no Estados Unidos, o algoritmo DCA usa somente os canais 11b/g de 1, de 6, e de 11 à revelia. A fim adicionar os canais 4 e 8, e remover o canal 6 desta lista DCA (**esta configuração é somente um exemplo e não é recomendada**), estes comandos precisam de ser entrados no controlador CLI:

```
(Cisco Controllor) >config advanced 802.11b channel add 4
(Cisco Controllor) >config advanced 802.11b channel add 8
(Cisco Controllor) >config advanced 802.11b channel delete 6
```

Fazendo a varredura mais canais, tais como toda a seleção de canais, a quantidade total de clientes gastados tempo dos dados de conservação está diminuída levemente (em relação a quando menos canais são incluídos no processo da exploração). Contudo, a informação em mais canais pode ser garnered (em relação ao DCA canaliza o ajuste). A configuração padrão dos canais do país deve ser usada a menos que as necessidades IDS/IPS necessitem a seleção de todos os canais, ou a informação detalhada em outros canais não está precisada para a detecção e correção do alarme do perfil do ponto inicial e do algoritmo RRM. Neste caso, os canais DCA são a escolha apropriada.

Figura 14: Quando do “os canais país” forem a seleção do padrão, os canais de monitoração RRM podem ser ajustados aos canais “tudo” ou “DCA”.



### [Monitore intervalos \(60 a 3600 segundos\)](#)

Todos os APs LWAPP-baseados Cisco entregam dados aos usuários ao periodicamente ir fora canal para tomar medidas RRM (assim como para executar outras funções tais como IDS/IPS e tarefas do lugar). Esta exploração do fora-canal está completamente transparente aos usuários e limita somente o desempenho por até 1.5%, além do que ter o acessório da inteligência para adiar a exploração até que o intervalo seguinte em cima da presença de tráfego na fila da Voz no último 100ms.

Ajustar intervalos do monitor mudará como frequentemente os APs tomam medidas RRM. O temporizador o mais importante que controla a formação dos grupos RF é o campo da medida do sinal (conhecido como a frequência vizinha do pacote em 4.1.185.0 e mais tarde). O valor especificado é relacionado diretamente à frequência em que as mensagens vizinhas são transmitidas, exceto o EU, e outros domínios 802.11h, onde o intervalo da medida de ruído é considerado, também.

Apesar do domínio regulatório, o processo inteiro da exploração toma a Senhora aproximadamente 50 (pelo rádio, pelo canal) e as corridas no intervalo padrão de 180 segundos. Este intervalo pode ser mudado alterando o valor da medida da cobertura (conhecida como a

duração da varredura do canal em 4.1.185.0 e mais tarde). A escuta gastada tempo em cada canal é uma função do momento não-configurável da varredura de 50 Senhoras (mais, o 10ms que toma para comutar os canais) e do número de canais de ser feito a varredura. Por exemplo, no Estados Unidos, todos os 11 canais 802.11b/g, que incluem o um canal em que os dados estão sendo entregados aos clientes, serão feitos a varredura para 50 a Senhora cada um dentro do segundo intervalo 180. Isto significa que (no Estados Unidos, para 802.11b/g) cada 16 segundos, a Senhora 50 será escuta gastada em cada canal feito a varredura ( $180/11 = \sim 16$  segundos).

Figura 15: Intervalos da monitoração RRM, e seus valores padrão

Monitor Intervals (60 to 3600 secs)	
Noise Measurement	180
Load Measurement	60
Neighbor Packet Frequency	60
Channel Scan Duration	180

O ruído, a carga, o sinal, e os intervalos de medida da cobertura podem ser ajustados para fornecer mais ou menos informação granulada aos algoritmos RRM. Estes padrões devem ser mantidos a menos que instruído de outra maneira pelo tac Cisco.

**Nota:** Se qualquens um valores da exploração são mudados para exceder os intervalos em que os algoritmos RRM estão executados (600 segundos para o DCA e o TPC e 180 segundos para a cobertura furam a detecção e correção), os algoritmos RRM ainda serão executado, mas possivelmente com informação “velha”.

**Nota:** Quando WLCs estiver configurado para ligar interfaces Gigabit Ethernet múltiplas usando a agregação da relação (RETARDAÇÃO), o intervalo de medida da cobertura está usado para provocar a função do idle timeout do usuário. Como tal, com a RETARDAÇÃO permitida, o idle timeout do usuário é executado somente tão frequentemente como o intervalo de medida da cobertura dita. Isto aplica-se somente ao WLCs que executa versões de firmware antes de 4.1 porque, na liberação 4.1, a manipulação do idle timeout é movida do controlador para os Access point.

### [Padrão de fábrica](#)

A fim restaurar valores RRM de volta às configurações padrão, clique o grupo ao botão de padrão de fábrica na parte inferior da página.

## [Transmita por rádio a gerência de recursos: Troubleshooting](#)

As mudanças feitas por RRM podem facilmente ser monitoradas permitindo o SNMP traps necessário. Estes ajustes podem ser alcançados do Gerenciamento --> SNMP --> título de controles da armadilha no WLC GUI. Todos ajustes relacionados restantes da armadilha de SNMP detalhados nesta seção são ficados situados sob o Gerenciamento | Título SNMP onde as relações para receptores de armadilha, controles, e logs podem ser encontradas.

Figura 16: As armadilhas da auto atualização do canal e da potência RF são permitidas à revelia.

The screenshot shows the Cisco Management interface for SNMP Trap Controls. The left sidebar contains a navigation menu with categories like Management, Summary, SNMP, HTTP, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, and Tech Support. The main content area is divided into several sections:

- Miscellaneous Traps:** Includes traps for Authentication, Link Up/Down, Multiple Users, Spanning Tree, Rogue AP, and Config Save.
- Client Related Traps:** Includes traps for 802.11 Association, Disassociation, Deauthentication, Failed Authentication, Failed Association, and Exclusion.
- Auto RF Profile Traps:** Includes traps for Load Profile, Noise Profile, Interference Profile, and Coverage Profile.
- Auto RF Update Traps:** Includes traps for Channel Update and Tx Power Update.
- AAA Traps:** Includes traps for User Authentication and RADIUS Servers Not Responding.
- IP Security Traps:** Includes traps for ESP Authentication Failure, ESP Replay Failure, Invalid SPI, IKE Negotiation Failure, IKE Suite Failure, and Invalid Cookie.
- 802.11 Security Traps:** Includes a trap for WEP Decrypt Error.

## Verificando a atribuição dinâmica do canal

Depois que o líder do grupo RF (e o algoritmo DCA) sugeriram, esquema aplicamos e aperfeiçoados do canal, as mudanças podem facilmente ser monitoradas através do secundário-menu dos logs da armadilha. Um exemplo de tal armadilha é indicado aqui:

**Figura 17: As entradas de registro da mudança do canal contêm o MAC address e o canal novo do rádio de operação.**

132	Tue Jul 31 22:54:06 2007	Channel changed for Base Radio MAC: 00:19:07:06:5d:40 on 802.11b/g radio. Old Channel: 11. New Channel: 1. Why: Interference. Energy before/after change: -60/-80. Noise before/after change: -82/-82. Interference before/after change: -60/-85.
-----	--------------------------	---

A fim ver as estatísticas que detalham quanto tempo os APs retêm seus ajustes do canal entre mudanças DCA, este comando CLI-somente fornece mínimo, médio, e valores máximos do tempo de interrupção do canal em uma base do por-controlador.

```
(Cisco Controller) >show advanced 802.11b channel
```

```
Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:16:46:4b:33:40
Last Run..... 114 seconds ago

DCA Sensitivity Level: ..... MEDIUM (15 dB)
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... 0 days, 09 h 25 m 19 s
  Average..... 0 days, 10 h 51 m 58 s
  Maximum..... 0 days, 12 h 18 m 37 s
```

```
Auto-RF Allowed Channel List..... 1,6,11
Auto-RF Unused Channel List..... 2,3,4,5,7,8,9,10
```

## Verificando alterações de controle da potência de transmissão

Os ajustes atuais do algoritmo TPC, que inclui tx-potência-controle-trilhar descrito mais cedo, podem ser verificados usando este comando no controlador CLI (802.11b é indicado neste exemplo):

```
(Cisco Controller) >show advanced 802.11b txpower
```

```
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode..... AUTO
  Transmit Power Update Interval..... 600 seconds
  Transmit Power Threshold..... -70 dBm
  Transmit Power Neighbor Count..... 3 APs
  Transmit Power Update Contribution..... SNI.
  Transmit Power Assignment Leader..... 00:16:46:4b:33:40
  Last Run..... 494 seconds ago
```

Como indicado mais cedo neste original, uma área densamente distribuída que conduziu à pilha-sobreposição aumentada, que os resultados na colisão e no quadro altos experimentam de novo as taxas devido à interferência alta do co-canal, reduzindo eficazmente os níveis de ritmo de transferência do cliente poderia justificar o uso do introduzido recentemente tx-potência-controle-trilha o comando. Em tais encenações atípicas ou anômalas, os APs ouvem-se que melhor (supondo as características de propagação do sinal permaneça constante) comparou a como os clientes as ouvem.

As áreas de cobertura shrinking e conseqüentemente a diminuição da interferência do co-canal e do assoalho do ruído podem eficazmente melhorar a experiência do cliente. Contudo, este comando deve ser exercitado com análise cuidadosa dos sintomas: as taxas altas da nova tentativa, os contagens de colisão altos, uns mais baixos níveis de ritmo de transferência do cliente e o macacão aumentaram a interferência do co-canal, nos APs no sistema (os APs desonestos são esclarecidos no DCA). O teste interno indicou aquele que altera o RSSI percebido do terceiro vizinho ao dBm -70 em pesquisar defeitos tais eventos foi um valor aceitável para começar a pesquisar defeitos.

Similar às armadilhas geradas quando uma mudança do canal ocorre, as mudanças TPC gerenciem armadilhas, também, que indique claramente toda a informação necessária associada com as mudanças novas. Uma armadilha da amostra é indicada aqui:

Figura 18: O log da armadilha da potência TX indica o nível da potência novo da operação para o rádio especificado.

```
138 Thu Jul 12 07:03:24 2007 RF Manager updated TxPower for Base Radio MAC: 00:15:c7:a8:e1:70 and slotNo: 0. New Tx Power is: 3
```

## Exemplo dos trabalhos do algoritmo de controle da potência de transmissão

Baseado nas três etapas/circunstâncias definidas no algoritmo TPC, o exemplo nesta seção explica como os cálculos são feitos para determinar se a potência de transmissão de um AP precisa de ser mudada. Com a finalidade deste exemplo, estes valores são supostos:

- O Tx\_Max é 20
- A potência de transmissão atual é 20 dBm



- O ponto inicial configurado TPC é o dBm -65
- O RSSI do terceiro vizinho é o dBm -55

Obstruir isto nas três fases do algoritmo TPC conduz a:

- Circunstância uma: é verificado porque há um terceiro vizinho, e está acima do ponto inicial do controle de potência de transmissão.
- Circunstância dois:  $20 + (-65 - (-55)) = 10$
- Circunstância três: Porque a potência tem que ser diminuída um nível, e um valor de dez da circunstância dois satisfaz a histerese TPC, a potência TX é reduzida por 3dB, que derruba a potência TX nova a 17dBm.
- Na iteração seguinte do algoritmo TPC, a potência TX do AP será abaixada mais a 14dBm. Isto supõe que todas circunstâncias restantes permanecem as mesmas. Contudo, é importante notar que a potência TX não estará abaixada mais (mantendo toda a constante das coisas) a 11dBm porque a margem em 14dBm não é 6dB ou mais altamente.

### Exemplo dos trabalhos do algoritmo da detecção e correção do furo da cobertura

A fim ilustrar o processo de tomada de decisão usado no algoritmo da detecção e correção do furo da cobertura, o exemplo abaixo de primeiramente esboça o nível SNR recebido deficiente de um único cliente e como o sistema determinará se uma mudança está precisada, assim como o que essa mudança da potência pôde ser.

Recorde a equação do ponto inicial do furo SNR da cobertura:

Valor de corte de SNR do cliente (|DB|) = [Potência de transmissão do AP (dBm) - Constante (17 dBm) - Perfil de Cobertura (dB)]

Considere uma situação onde um cliente possa experimentar edições do sinal em uma área deficientemente coberta de um assoalho. Em tal encenação, estes podem ser verdadeiros:

- Um cliente tem um SNR de 13dB.
- O AP a que é conectado é configurado para transmitir em 11 dBm (nível da potência 4).
- O WLC desse AP tem um conjunto de limiares do perfil da cobertura ao padrão de DB 12.

A fim determinar se o AP do cliente precisa de ser posto acima, estes números são obstruídos na equação do ponto inicial do furo da cobertura, a que conduz:

- Interrupção do cliente SNR = 11dBm (potência de transmissão AP) – 17dBm (valor constante) – 12dB (ponto inicial da cobertura) = |-18dB|.
- Porque o SNR do cliente de 13dB é em violação da interrupção atual SNR de 18dB, o algoritmo da detecção e correção do furo da cobertura aumentará a potência de transmissão do AP a 17dBm.
- Usando a equação do ponto inicial do furo SNR da cobertura, é evidente que a potência de transmissão nova de 17dBm renderá um valor da interrupção do cliente SNR de 12dB, que satisfará o nível SNR do cliente de 13 dBm.
- Esta é a matemática para a etapa precedente: Interrupção do cliente SNR = 17dBm (potência de transmissão AP) – 17dBm (valor constante) – 12dB (ponto inicial da cobertura) = |-12dB|.

Os níveis da saída apoiados da potência na faixa 802.11b/g são esboçados na tabela 4. a fim determinar as saídas do nível da potência para 802.11a, este comando CLI podem ser sidos executado:

```
show ap config 802.11a <ap name>
```

Tabela 4: Os níveis da potência do apoio 1000-series APs até 5 visto que o 1100- e os 1200-series APs apoiam até o nível da potência 8 na banda de frequência 802.11b/g.

Níveis da potência apoiados	Potência TX (dBm)	Potência TX (mW)
1	20	100
2	17	50
3	14	25
4	11	12.5
5	8	6.5
6	5	3.2
7	2	1.6
8	-1	0.8

## Comandos debug and show

Os comandos debug do airewave-diretor podem ser usados para pesquisar defeitos e verificar mais o comportamento RRM. A hierarquia nível mais alto dos dados da linha de comando do comando do airewave-diretor **debugar** é indicada aqui:

```
(Cisco Controller) >debug airewave-director ?
```

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

Alguns comandos importantes são explicados nas subseções seguintes.

## debugar o airewave-diretor todo

O uso do airewave-diretor **que debugar o comando all** invocará todos os RRM debuga que podem ajudar a identificar quando os algoritmos RRM são executados, os que dados usam, e os que mudanças (eventualmente) são feitos.

Neste exemplo, (a saída do **comando all do airewave-diretor debugar** foi aparada para mostrar o processo dinâmico da atribuição do canal somente), o comando é executado no líder do grupo RF ganhar a introspecção nos funcionamentos internos do algoritmo DCA e pode ser dividido nestas quatro etapas:

1. Recolha e grave as estatísticas atual que serão executadas com o algoritmo.



(Cisco Controller) >**debug airewave-director ?**

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

## 2. Sugira um esquema novo do canal e armazene os valores recomendados.

(Cisco Controller) >**debug airewave-director ?**

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

## 3. Compare os valores atual contra os valores sugeridos.

(Cisco Controller) >**debug airewave-director ?**

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

## 4. Caso necessário, aplique as mudanças para que o esquema novo do canal tome o efeito.

(Cisco Controller) >**debug airewave-director ?**

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

Este comando pode ser usado para obter um detalhado, opinião do tempo real de RRM que funciona no controlador em que é executada. Estas são explicações das mensagens relevantes:

- Mensagens da manutenção de atividade que estão sendo enviadas para agrupar membros para manter a hierarquia do grupo.

```
(Cisco Controller) >debug airewave-director ?
```

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

- Estatísticas da carga que estão sendo calculadas nos vizinhos relatados.

```
(Cisco Controller) >debug airewave-director ?
```

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

- Indicadores como forte as mensagens vizinhas estão sendo ouvidas e com que APs.

```
(Cisco Controller) >debug airewave-director ?
```

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
radar        Configures debug of Airewave Director radar detection/avoidance protocol
rf-change    Configures logging of Airewave Director rf changes
profile      Configures logging of Airewave Director profile events
```

- Estatísticas do ruído e da interferência que estão sendo calculadas nos rádios relatados.

```
(Cisco Controller) >debug airewave-director ?
```

```
all           Configures debug of all Airewave Director logs
channel       Configures debug of Airewave Director channel assignment protocol
error        Configures debug of Airewave Director error logs
detail       Configures debug of Airewave Director detail logs
group        Configures debug of Airewave Director grouping protocol
manager      Configures debug of Airewave Director manager
message      Configures debug of Airewave Director messages
packet       Configures debug of Airewave Director packets
power        Configures debug of Airewave Director power assignment protocol
```

```
radar      Configures debug of Airewave Director radar detection/avoidance protocol
rf-change  Configures logging of Airewave Director rf changes
profile    Configures logging of Airewave Director profile events
```

## [debugar a potência do airewave-diretor](#)

O comando da **potência do airewave-diretor debugar** deve ser executado no WLC local ao AP que está sendo monitorado para correções do furo da cobertura. A saída do comando foi aparada com a finalidade deste exemplo.

### **Algoritmo de observação do furo da cobertura executado para 802.11a**

```
(Cisco Controller) >debug airewave-director ?
```

```
all        Configures debug of all Airewave Director logs
channel    Configures debug of Airewave Director channel assignment protocol
error      Configures debug of Airewave Director error logs
detail     Configures debug of Airewave Director detail logs
group      Configures debug of Airewave Director grouping protocol
manager    Configures debug of Airewave Director manager
message    Configures debug of Airewave Director messages
packet     Configures debug of Airewave Director packets
power      Configures debug of Airewave Director power assignment protocol
radar      Configures debug of Airewave Director radar detection/avoidance protocol
rf-change  Configures logging of Airewave Director rf changes
profile    Configures logging of Airewave Director profile events
```

### **Algoritmo de observação do furo da cobertura executado para 802.11b/g**

```
(Cisco Controller) >debug airewave-director ?
```

```
all        Configures debug of all Airewave Director logs
channel    Configures debug of Airewave Director channel assignment protocol
error      Configures debug of Airewave Director error logs
detail     Configures debug of Airewave Director detail logs
group      Configures debug of Airewave Director grouping protocol
manager    Configures debug of Airewave Director manager
message    Configures debug of Airewave Director messages
packet     Configures debug of Airewave Director packets
power      Configures debug of Airewave Director power assignment protocol
radar      Configures debug of Airewave Director radar detection/avoidance protocol
rf-change  Configures logging of Airewave Director rf changes
profile    Configures logging of Airewave Director profile events
```

## [mostre ap auto-RF](#)

A fim saber que APs são junto a outros APs, use o comando **show ap auto-RF** do controlador CLI. Na saída deste comando, há um campo chamado **Próximo RADs**. Este campo fornece a informação nos endereços próximos AP MAC e na intensidade de sinal (RSSI) entre os APs no dBm.

Esta é a sintaxe do comando:

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

Este é um exemplo:

> show ap auto-rf 802.11a AP1

```
Number Of Slots..... 2
Rad Name..... AP03
MAC Address..... 00:0b:85:01:18:b7
Radio Type..... RADIO_TYPE_80211a
Noise Information
  Noise Profile..... PASSED
  Channel 36..... -88 dBm
  Channel 40..... -86 dBm
  Channel 44..... -87 dBm
  Channel 48..... -85 dBm
  Channel 52..... -84 dBm
  Channel 56..... -83 dBm
  Channel 60..... -84 dBm
  Channel 64..... -85 dBm
Interference Information
  Interference Profile..... PASSED
  Channel 36..... -66 dBm @ 1% busy
  Channel 40..... -128 dBm @ 0% busy
  Channel 44..... -128 dBm @ 0% busy
  Channel 48..... -128 dBm @ 0% busy
  Channel 52..... -128 dBm @ 0% busy
  Channel 56..... -73 dBm @ 1% busy
  Channel 60..... -55 dBm @ 1% busy
  Channel 64..... -69 dBm @ 1% busy
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0%
  Transmit Utilization..... 0%
  Channel Utilization..... 1%
  Attached Clients..... 1 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dBm..... 0 clients
  RSSI -92 dBm..... 0 clients
  RSSI -84 dBm..... 0 clients
  RSSI -76 dBm..... 0 clients
  RSSI -68 dBm..... 0 clients
  RSSI -60 dBm..... 0 clients
  RSSI -52 dBm..... 0 clients
Client Signal To Noise Ratios
  SNR 0 dBm..... 0 clients
  SNR 5 dBm..... 0 clients
  SNR 10 dBm..... 0 clients
  SNR 15 dBm..... 0 clients
  SNR 20 dBm..... 0 clients
  SNR 25 dBm..... 0 clients
  SNR 30 dBm..... 0 clients
  SNR 35 dBm..... 0 clients
  SNR 40 dBm..... 0 clients
  SNR 45 dBm..... 0 clients
Nearby RADs
  RAD 00:0b:85:01:05:08 slot 0..... -46 dBm on 10.1.30.170
  RAD 00:0b:85:01:12:65 slot 0..... -24 dBm on 10.1.30.170
Channel Assignment Information
  Current Channel Average Energy..... -86 dBm
  Previous Channel Average Energy..... -75 dBm
```

```

Channel Change Count..... 109
Last Channel Change Time..... Wed Sep 29 12:53e:34 2004
Recommended Best Channel..... 44
RF Parameter Recommendations
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0

```

## APÊNDICE A: Liberação 4.1.185.0 WLC – Realces RRM

### Algoritmo de agrupamento RF

#### Lista vizinha “temporizador de poda”

Antes da primeira versão de manutenção do software WLC 4.1, um AP manteria outros APs em sua lista vizinha por até 20 minutos da última vez onde foram ouvidos. No caso das mudanças provisórias no ambiente RF, pôde ter havido as possibilidades onde um vizinho válido poderia fora da lista vizinha de um AP dado. A fim prever tais mudanças provisórias ao ambiente RF, o temporizador de poda para a lista vizinha de um AP (tempo desde que a última mensagem vizinha foi ouvida) foi aumentado a 60 minutos.

### Algoritmo dinâmico da atribuição do canal

#### Método da atribuição do canal

Quando no modo automático, o comportamento padrão do DCA antes de 4.1.185.0 era computar e aplicar (caso necessário) os planos de canal os minutos cada 10. Os ambientes temporários puderam potencialmente ter considerado mudanças numerosas do canal durante o dia. Conseqüentemente, a necessidade para avançado, controle mais fino na frequência do DCA elevou. Em 4.1.185.0 e mais tarde, os usuários que desejam para o controle mais fino sobre a frequência têm a capacidade para configurar estes:

- **Tempo da âncora** — Os usuários que desejam mudar o padrão de 10-minuto terão a opção para escolher uma época da âncora em que o líder do grupo executar no modo Start-up. O modo Start-up é definido como um período onde o DCA opere cada dez minutos para as primeiras dez iterações (100 minutos), com a sensibilidade DCA de 5dB. Este foi o modo normal de operação antes que os temporizadores RRM estiveram adicionados na liberação 4.1. Isto permite a rede estabilizar inicialmente e rapidamente. Após as extremidades Start-up do modo, o DCA é executado no intervalo definido pelo utilizador. A operação Start-up do modo é indicada claramente no WLC CLI através do comando **802.11[a|b] avançado mostra:**

```
(Cisco Controller) >show advanced 802.11a channel
```

```

Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds [startup]
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:16:46:4b:33:40
Last Run..... 203 seconds ago

DCA Sensitivity Level: ..... MEDIUM (5 dB)
Channel Energy Levels
Minimum..... unknown

```



Average.....	unknown
Maximum.....	unknown
Channel Dwell Times	
Minimum.....	unknown
Average.....	unknown
Maximum.....	unknown
Auto-RF Allowed Channel List.....	36,40,44,48,52,56,60,64,100,
.....	104,108,112,116,132,136,140,
.....	149,153,157,161
Auto-RF Unused Channel List.....	165,20,26

- **Intervalo** — O valor do intervalo, com as unidades definidas nas horas, permite que os usuários tenham uma rede predizível e as avaliações do plano de canal são computadas somente nos intervalos configurados. Por exemplo, se o intervalo configurado é 3 horas, o DCA computa e avalia um plano de canal novo cada 3 horas.
- **Sensibilidade** — Como descrito na seção do [algoritmo DCA](#), a histerese 5dB que está esclarecida no algoritmo para avaliar se o plano de canal é melhorado sendo executado o algoritmo é agora USER-ajustável. As configurações permitidas são baixa, sensibilidade média ou alta com um ajuste do ponto baixo que indicam o algoritmo que é muito insensível e um ajuste da elevação que indica o algoritmo que é extremamente sensível. O nível da sensibilidade do padrão é médio para ambas as faixas. Para 802.11a, os valores da sensibilidade igualam a: Baixo (35dB), médio (20dB) e alto (5dB). Para 802.11b/g, os valores da sensibilidade igualam a: Baixo (30dB), médio (15dB) e alto (5dB)

## [Algoritmo de controle da potência TX](#)

### Ponto inicial do controle de potência de transmissão do padrão

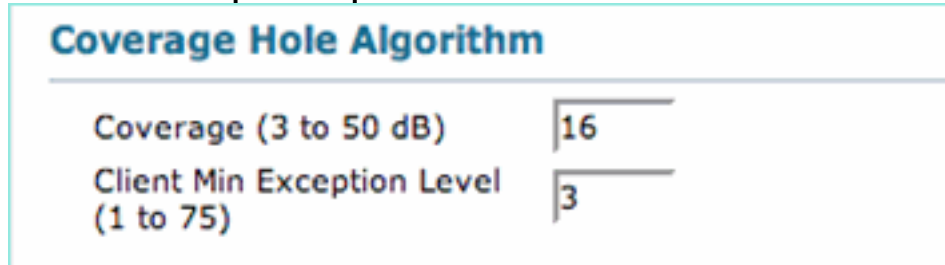
O ponto inicial do controle de potência de transmissão levou sempre a responsabilidade de como os APs ouvem seus vizinhos, que, é usado em momento oportuno para decidir a potência de transmissão do AP. Em consequência dos realces totais que foram feitos aos algoritmos RRM na versão de manutenção do software WLC 4.1, o valor padrão de -65dBm foi reconsiderado igualmente. Consequentemente, o padrão que foi julgado demasiado quente para a maioria de disposições, foi adaptado a -70dBm. Isto conduz à melhor sobreposição da pilha na maioria de disposições internas fora da caixa. Contudo, este padrão impacta somente as instalações novas enquanto o controlador mantém previamente o valor configurado se sendo promovido de 4.1.171.0 ou mais cedo.

## [Algoritmo do furo da cobertura](#)

### Cientes mínimos

Acima até de 4.1.185.0, de somente um cliente necessários ter encontrado a condição (ponto inicial mais ruim SNR do que o valor configurado, ou os padrões de 16dB para 802.11a ou 12dB para 802.11b/g) para que um furo da cobertura a ser detectados e os mecanismos da mitigação sejam retrocedidos dentro. O campo mínimo do nível da exceção do cliente é amarrado agora diretamente ao CHA (e posicionado apropriadamente na subseção recém-criado para o CHA) onde o valor configurado definirá quantos clientes têm que encontrar o ponto inicial SNR para os mecanismos da mitigação do furo da cobertura (potência de transmissão crescente AP) retrocederão dentro. Deve ser notado que a maioria de disposições devem começar com os padrões (12dB para 802.11b/g e 16dB para 802.11a, e exceção mínima do cliente em nível de 3) e ser ajustado somente caso necessário.

Figura 19: Subseção do algoritmo do furo da cobertura, separada dos pontos iniciais do perfil, com os valores padrão que fornecem resultados os melhores na maioria de instalações



### Controle da Tx-potência-Acima

Além do que permitir o número de clientes que precisam de estar na violação para que a mitigação do furo da cobertura retroceda dentro, o algoritmo foi melhorado igualmente para considerar o aumento da potência de transmissão AP em uma maneira inteligente. Quando aumentar a potência de transmissão ao máximo pôde ter sido a aposta segura para assegurar a suficientes mitigação e sobreposição, tem efeitos adversos com a presença de clientes com aplicações vagueando deficientes. Em vez de mudar sua associação a um AP diferente, tipicamente esse que fornece o sinal o mais forte, o cliente mantém-se associar ao mesmo AP velho de que se moveu mais distante longe. Consequentemente, este cliente já não está recebendo um bom sinal do AP de associação. Um cliente falhado que seja uma consequência de vaguear deficiente é um exemplo de uma encenação possível do furo da cobertura do falso positivo. Vaguear deficiente não é uma indicação que um furo genuíno da cobertura existe. O furo potencial da cobertura é genuíno se:

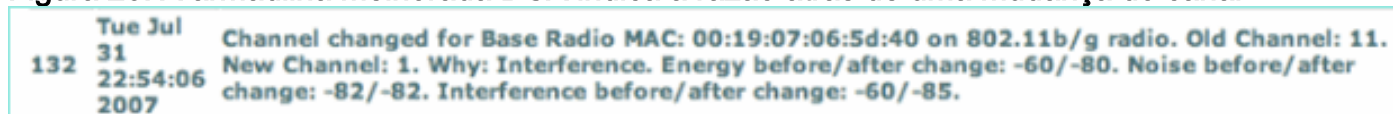
- Éficado situado dentro da área de cobertura pretendida, e
- Mesmo se o cliente neste furo da cobertura devia mudar sua associação a todo o outro AP disponível, o sinal que do downlink o cliente receberia e uplink o sinal em tal alternativa AP do cliente ainda estaria abaixo do ponto inicial da cobertura.

A fim evitar e abrandar tais encenações, a potência de transmissão AP é levantada somente um nível de cada vez (pela iteração), que permite que os furos genuínos da cobertura tirem proveito do aumento da potência sem executar a rede quente (evitando a interferência do co-canal em consequência).

### Realces da armadilha de SNMP

A armadilha de SNMP gerada no caso de uma mudança do canal foi aumentada para fornecer a informação detalhada a respeito de explica a razão para executar um plano de canal novo. Como evidente desta imagem, a armadilha aumentada inclui antes e depois de que medidor usado no algoritmo DCA e qual dos aqueles o medidor contribuiu à mudança do canal para o AP dado.

Figura 20: A armadilha melhorada DCA indica a razão atrás de uma mudança do canal



### Cosmético/outros realces

- Como um empreendimento para simplificar a configuração e melhorar a usabilidade, uma subseção nova para o CHA foi criada, que a separa da subseção dos pontos iniciais do perfil que controla diretamente os disparadores para a geração da armadilha de SNMP.

- Os termos sinalizam e as medidas da cobertura sob as subseções dos intervalos do monitor foram alteradas igualmente para refletir seus significados apropriados: A frequência e o canal vizinhos do pacote fazem a varredura da duração respectivamente.

## Mudanças do Balanceamento de carga

A configuração padrão para o Balanceamento de carga com 4.1.185.0 e está mais tarde. Quando permitido, o indicador do Balanceamento de carga optará os clientes 5.

```
(Cisco Controller) >show load-balancing
```

```
Aggressive Load Balancing..... Disabled  
Aggressive Load Balancing Window..... 5 clients
```

## APÊNDICE B: Liberação 6.0.188.0 WLC – Realces RRM

### Reparos RRM para dispositivos médicos

Esta característica melhora a maneira que QoS interage com a varredura RRM adia a característica. Nas disposições com determinados clientes da economia de energia, você precisa às vezes de adiar a exploração normal do fora-canal RRM a fim evitar faltar a informação crítica dos clientes do volume baixo, tais como os dispositivos médicos que usam o modo de economia de energia e enviam periodicamente a informação da telemetria.

Você pode usar o WMM ACIMA da marcação de um cliente a fim dizer o Access point para adiar a exploração do fora-canal por um período configurável de tempo se recebe um pacote marcado ACIMA. Use este comando CLI do controlador a fim configurar esta característica para um WLAN sepcific:

```
(Cisco Controller) >show load-balancing
```

```
Aggressive Load Balancing..... Disabled  
Aggressive Load Balancing Window..... 5 clients
```

onde prioridade = 0 com 7 para a prioridade de usuário. Este valor deve ser ajustado a 6 no cliente e no WLAN.

Use este comando a fim configurar a quantidade de tempo que fazer a varredura está adiada após um pacote ASCENDENTE na fila:

```
(Cisco Controller) >show load-balancing
```

```
Aggressive Load Balancing..... Disabled  
Aggressive Load Balancing Window..... 5 clients
```

Incorpore o valor do tempo aos miliseconds (Senhora). O intervalo válido é 100 (padrão) a 60000 (60 segundos). Este ajuste deve combinar as exigências do equipamento em seu Wireless LAN.

Você pode igualmente configurar esta característica no controlador GUI. Selecione WLAN, e edite um WLAN existente ou crie um novo. No os WLAN > editam a página, clicam o **guia avançada**. Sob fora da exploração do canal adie, selecione a varredura adiam prioridades, e incorporam o tempo do adiamento aos milissegundos.

**Nota:** a varredura de Fora-Channel é essencial à operação de RRM, que recolhe a informação sobre escolhas do canal alternativo, tais como o ruído e a interferência. Adicionalmente, a exploração do fora-canal é responsável para a detecção desonesto. Os dispositivos que precisam de adiar a exploração do fora-canal devem usar o mesmo WLAN tantas vezes quanto possível. Se há muitos destes dispositivos, e a possibilidade existe que a exploração do fora-canal poderia completamente ser desabilitada pelo uso desta característica, você deve executar uma alternativa à exploração local do fora-canal AP, tal como Access point do monitor ou outros Access point no mesmo lugar que não têm este WLAN atribuído.

A atribuição de uma política de QoS (bronze, prata, ouro, e platina) às influências WLAN como os pacotes são marcados na conexão do downlink do Access point, apesar de como foram recebidos no uplink do cliente. UP=1,2 é a mais baixa prioridade, e UP=0,3 é a prioridade mais alta seguinte. Estes são os resultados da marcação de cada política de QoS:

- O bronze marca todo o tráfego do downlink a UP= 1
- A prata marca todo o tráfego do downlink a UP= 0
- O ouro marca todo o tráfego do downlink a UP=4
- A platina marca todo o tráfego do downlink a UP=6

## [Informações Relacionadas](#)

- [Controlador do Wireless LAN e guia de integração IPS](#)
- [Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)