

Controlador do Wireless LAN (WLC) FAQ

Índice

[Introdução](#)

[Perguntas Frequentes Gerais](#)

[Perguntas Frequentes de Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece a informação mais frequentemente nas perguntas feitas (FAQ) sobre o controlador de LAN do Cisco Wireless (WLC).

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

Perguntas Frequentes Gerais

Q. Que é um controlador do Wireless LAN (WLC)?

A. As redes Wireless se transformaram em uma necessidade nos dias de hoje. Muitos ambientes corporativos exigem a implantação de redes wireless em grande escala. A Cisco desenvolveu o conceito da solução Cisco Unified Wireless Network (CUWN) para facilitar o gerenciamento dessas implantações em larga escala. A WLC é um dispositivo que assume um papel central no CUWN. Os papéis tradicionais dos pontos de acesso, tais como a associação ou a autenticação dos clientes Wireless, são feitos na WLC. Os pontos de acesso, chamados pontos de acesso lightweight (LAPs) no ambiente unificado, registram-se em uma WLC e colocam em túneis todos os pacotes de dados e gerenciamento para as WLCs, que então comutam os pacotes entre os clientes wireless e a parte com fio da rede. Todas as configurações são feitas na WLC. Os LAPs baixam a configuração completa das WLC e atuam como uma interface Wireless para os clientes. Para obter mais informações sobre como um LAP se registra em uma WLC, consulte o documento [Registro de APs Lightweight \(LAPs\) em Controladoras Wireless LAN](#).

Q. Que é CAPWAP?

A. No software release 5.2 ou mais recente da controladora, os pontos de acesso lightweight Cisco usam o protocolo Control and Provisioning of Wireless Access Points (CAPWAP) padrão do IETF (CAPWAP) para se comunicarem entre a controladora e outros pontos de acesso lightweight na rede. As controladoras com releases de software anteriores ao 5.2 usam o Lightweight Access Point Protocol (LWAPP) para essas comunicações.

O CAPWAP, que é baseado no LWAPP, é um protocolo padrão e interoperável que permite que uma controladora gerencie uma coleção de pontos de acesso wireless. O CAPWAP está sendo implementado no software release 5.2 da controladora por estas razões:

- Para fornecer um caminho de upgrade dos produtos da Cisco que usam o LWAPP para os produtos da Cisco da próxima geração que usa o CAPWAP
- Para gerenciar leitores RFID e dispositivos semelhantes
- Para permitir que controladoras de interoperar no futuro com pontos de acesso de outros fabricantes

Os pontos de acesso com suporte ao LWAPP podem descobrir e se unir a uma controladora CAPWAP, e a conversão para uma controladora CAPWAP é direta. Por exemplo, o processo de descoberta da controladora e o processo de download de firmware quando você usa o CAPWAP são os mesmos de quando você usa o LWAPP. A uma exceção é para as implantações da camada 2, que não são aceitas pelo CAPWAP.

Você pode implantar controladoras CAPWAP e controladoras LWAPP na mesma rede. O software com suporte ao CAPWAP permite que os pontos de acesso unam-se a uma das controladoras que executam CAPWAP ou LWAPP. A única exceção é o ponto de acesso Cisco Aironet 1140 Series, o qual oferece suporte somente ao CAPWAP e, conseqüentemente, se une somente às controladoras que executam o CAPWAP. Por exemplo, um ponto de acesso 1130 Series pode se unir a uma controladora que executa CAPWAP ou LWAPP, enquanto que um ponto de acesso 1140 Series pode se unir somente a uma controladora que executa CAPWAP.

Para obter mais informações, consulte a seção [Protocolos de Comunicação de Pontos de Acesso do Guia de Configuração](#).

Q. Há alguma diretriz para usar o CAPWAP?

A. Siga estas diretrizes ao usar o CAPWAP:

- Se seu firewall estiver configurado para permitir o tráfego somente dos pontos de acesso que usam o LWAPP, você deverá mudar as regras do firewall para permitir o tráfego dos pontos de acesso que usam CAPWAP.
- Certifique-se de que as portas UDP 5246 e 5247 do CAPWAP (similar às portas UDP 12222 e 12223 do LWAPP) estejam habilitadas e não obstruídas por um dispositivo intermediário que poderia impedir que um ponto de acesso se unisse à controladora.
- Se as listas de controle de acesso (ACLs) estiverem no caminho de controle entre a controladora e seus pontos de acesso, você precisa abrir novas portas do protocolo para impedir que os pontos de acesso se tornem travados.

Os pontos de acesso usam uma porta de origem aleatória do UDP para acessar essas portas do destino na controladora. No software release 5.2 da controladora, o LWAPP foi removido e substituído pelo CAPWAP, mas se você possui um ponto de acesso novo com a configuração de fábrica, poderá tentar usar o LWAPP para entrar em contato com a controladora da nova imagem do CAPWAP ser baixada para ela. Uma vez que o ponto de acesso baixe a imagem do CAPWAP da controladora, ele usará somente o CAPWAP para se comunicar com a controladora.

Nota: Após 60 segundos da tentativa de se unir a uma controladora com o CAPWAP, o ponto de acesso voltará a usar o LWAPP. Se ele não conseguir encontrar uma controladora que usa o LWAPP dentro de 60 segundos, ele tentará outra vez se unir a uma controladora que usa o CAPWAP. O ponto de acesso repete este ciclo de troca do CAPWAP para o LWAPP e vice-versa a cada 60 segundos até se unir a uma controladora.

Um ponto de acesso com a imagem de recuperação LWAPP (um ponto de acesso convertido do modo autônomo ou um ponto de acesso com a configuração de fábrica) usa somente o LWAPP para tentar se unir a uma controladora antes da imagem do CAPWAP ser baixada da

controladora.

Q. Como eu configuro meu WLC para a operação básica?

A. A fim configurar o WLC para a operação básica, refira o [controlador do Wireless LAN e o exemplo de pouco peso da configuração básica do Access point](#).

Q. Quais são as várias opções de acesso à WLC disponíveis?

A. Esta é a lista de opções de acesso à WLC disponíveis:

- Acesso via GUI com HTTP ou HTTPS
- Acesso via CLI com Telnet, SSH ou acesso de console
- Acesso via porta de serviço

Para obter mais informações sobre como habilitar esses modos, consulte a seção [Utilização do Navegador da Web e da Interface de Linha de Comando](#) do documento [Guia de Configuração da Controladora Cisco Wireless LAN Release 5.1](#). Geralmente, o endereço IP da interface de gerenciamento é usado para o acesso via GUI e CLI. Os clientes Wireless podem acessar a WLC somente quando opção **Controller Management to be accessible from Wireless Clients** está marcada. Para habilitar esta opção, clique no menu **Management** da WLC e clique em **Mgmt via Wireless** no lado esquerdo. A WLC também pode ser acessada através de um de seus endereços IP da interface dinâmica. Use o comando **config network mgmt-via-dynamic-interface** para habilitar este recurso. Os computadores com fio podem ter acesso somente via CLI com a interface dinâmica da WLC. Os clientes wireless têm acesso via CLI e GUI com a interface dinâmica.

Q. Como eu uso a porta de Console USB no controlador do Wireless LAN do Cisco 5500 Series?

A. A porta de Console USB nos controladores do 5500 Series conecta diretamente ao conector USB de um PC usando um tipo A USB 5-pin ao mini tipo cabo B.

Nota: 4-pin o mini tipo conector B é confundido facilmente com 5-pin o mini tipo conector B. Não são compatíveis. Somente 5-pin o mini tipo conector B pode ser usado.

Para a operação com Microsoft Windows, o direcionador do console de Cisco Windows USB deve ser instalado em todo o PC conectado à porta de Console. Com este direcionador, você pode obstruir e desconectar o cabo USB e da porta de Console sem afetar operações do HyperTerminal de Windows. Somente uma porta de Console pode ser ativa em um momento. Quando um cabo é obstruído na porta de Console USB, a porta RJ-45 torna-se inativa. Inversamente, quando o cabo USB é removido do porta usb, a porta RJ-45 torna-se ativa

Para a informação detalhada, refira a [utilização da porta de Console do controlador USB do Cisco 5500 Series](#).

Q. Como eu alcanço o assistente da configuração GUI em um controlador 4400?

A. A fim configurar as configurações básicas em um controlador 4400 que usa o assistente da configuração GUI, você deve conectar à porta do serviço do controlador. Em seguida, configurar seu PC para usar a mesma sub-rede como a porta do serviço do controlador; o endereço IP de

Um ou Mais Servidores Cisco ICM NT na porta do serviço quando configurar o WLC for pela primeira vez 192.168.1.1. Comece o internet explorer 6.0 SP1 (ou mais tarde) ou Firefox 2.0.0.11 (ou mais tarde) em seu PC, e consulte a <http://192.168.1.1>. O assistente da configuração GUI aparece.

Para informações detalhadas sobre deste assunto, refira o [manual de configuração do controlador de LAN do Cisco Wireless, a liberação 6.0](#).

Q. Como eu alcanço o WLC de uma posição remota?

A. Você pode usar o telnet e o SSH para alcançar o WLC de uma posição remota. O telnet é um protocolo usado para o Acesso remoto; O SSH é igualmente um protocolo usado para o Acesso remoto, mas inclui a Segurança adicionada. Para mais informação, refira o [SSH e a seção configurando das sessões de Telnet do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 6.0](#).

Q. Posso eu configurar uma conexão da RETARDAÇÃO essa períodos através dos switch múltiplos?

A. Sim. RETARDE-SE com VSS, ou um interruptor elevador da pilha (3750/2960) setup, funcionará enquanto os fragmentos de um pacote IP são enviados à mesma porta. A ideia é que se você vai aos switch múltiplos, as portas devem pertencer ao mesmo L2 "entidade" a propósito das decisões do Balanceamento de carga.

Q. Como uma WLC comuta pacotes?

A. Todos os pacotes (802.11) do cliente (encapsulados em um pacote LWAPP pelo LAP e são enviados à WLC. A WLC desencapsula o pacote LWAPP e atua baseada no endereço IP de destino no pacote 802.11. Se o destino é um dos clientes Wireless associados à WLC, ela encapsula o pacote outra vez com o LWAPP e o envia para o LAP do cliente, onde é desencapsulado e enviado para o cliente Wireless. Se o destino estiver no lado com fio da rede, ela remove o cabeçalho 802.11, adiciona o cabeçalho Ethernet e encaminha o pacote ao switch conectado, de onde ele é enviado para o cliente com fio. Quando um pacote é proveniente do lado com fio, a WLC remove o cabeçalho Ethernet, adiciona o cabeçalho 802.11, encapsula o pacote com o LWAPP e o envia para o LAP, onde é desencapsulado e o pacote 802.11 é entregue ao cliente Wireless. Para obter mais informações sobre isso, consulte a seção [Fundamentos do LWAPP](#) do documento [Implantação de Controladoras Wireless LAN Cisco 440X Series](#).

Q. Quando devo eu usar o modo do controlador mestre em um WLC?

A. Quando há um controlador mestre permitido, todos os Access point recentemente adicionados sem preliminar, secundário, ou os controladores terciários atribuídos associam com o controlador mestre na mesma sub-rede. Isto permite que o operador verifique a configuração do ponto de acesso e atribua preliminar, secundário, e controladores terciários ao Access point usando o **todo** o página **AP > de detalhes**.

O controlador mestre é usado normalmente somente ao adicionar Access point novos à solução de LAN do Cisco Wireless. Quando não mais Access point está sendo adicionado à rede, a solução de Cisco WLAN recomenda que você desabilita o controlador mestre.

Q. Fazem os 4400 pacotes de rota WLC entre VLAN?

A. A WLC 4400 é um dispositivo que se conecta à sua rede, mas não funciona como um roteador. Deve haver um dispositivo da camada 3 para rotear pacotes entre VLANs. A WLC mapeia o SSID dos clientes na sub-rede da VLAN e coloca-os de volta na interface de gerenciamento para os roteadores upstream rotearem pacotes.

Q. Como eu configuro a WLAN em uma WLC?

A. O WLAN é similar àquele do SSID nos Access point. Ele é necessário para que um cliente se associe à sua rede wireless. Para configurar uma WLAN em uma WLC, consulte a configuração de exemplo no documento [WLAN Convidada e WLAN Interna Usando WLCs](#).

Q. Como o DHCP trabalha com a WLC?

A. A WLC é projetada para atuar como um agente de retransmissão de DHCP para o servidor DHCP externo e atua como um servidor DHCP para o cliente. Esta é a sequência de eventos que ocorre:

1. Geralmente, a WLAN é vinculada a uma interface que está configurada com um servidor DHCP.
2. Quando a WLC recebe uma solicitação de DHCP do cliente em uma WLAN, ela retransmite o pedido para o servidor DHCP com seu endereço IP de gerenciamento.
3. Quando a WLC mostra seu endereço IP virtual, o qual deve ser um endereço não roteável, normalmente configurado como 1.1.1.1, como o servidor DHCP para o cliente.
4. A WLC envia a resposta de DHCP do servidor DHCP para o cliente Wireless com seu endereço IP virtual. **Nota:** Você também pode configurar a WLC para atuar como um servidor DHCP. Para obter mais informações sobre como configurar uma WLC como um servidor DHCP, consulte a seção [Configuração de Escopos de DHCP](#) do [Guia de Configuração da Cisco Wireless LAN Controller Release 5.1](#).

Q. Como eu mudo a potência e os canais para um LAP?

A. Uma vez que um LAP se registrar em uma WLC, toda a configuração do LAP será feita na WLC. Há um recurso interno da WLC chamado RRM, onde a WLC executa internamente um algoritmo e ajusta automaticamente o canal e as configurações de potência de acordo com a implantação dos LAPs. O RRM é ativado por padrão na WLC. Você não precisa mudar o canal e as configurações de potência para um LAP, mas você pode sobrescrever o recurso RRM e atribuir estaticamente configurações de potência e canal para um LAP. Para obter mais informações sobre como configurar manualmente o canal e as configurações de energia, consulte a seção [Atribuição Automática de Canais e Configurações de Potência de Transmissão para Rádios de Pontos de Acesso](#) do documento [Guia de Configuração da Cisco Wireless LAN Controller Release 5.1](#).

Q. Eu tenho várias WLCs em minha rede. Há algum dispositivo ou software disponível para gerenciar várias WLCs em minha rede?

A. Sim, o Wireless Control System (WCS) é um software de servidor que pode gerenciar várias WLCs na rede. Ele gerencia as WLC, seus pontos de acesso associados e os clientes. Para obter

mais informações sobre o WCS, consulte o [Guia de Configuração do Cisco Wireless Control System Release 5.0](#).

Q. Como eu edito o arquivo de configuração WLC?

A. Quando você salvar a configuração WLC, o controlador armazena-a no formato XML na memória Flash. A fim permiti-lo de ler e alterar facilmente o arquivo de configuração, o software do controlador (liberação 5.2 ou mais atrasado) converte-o a um formato CLI.

Quando você transfere arquivos pela rede o arquivo de configuração a um TFTP ou a um servidor FTP, o controlador inicia a conversão do XML ao CLI. Você pode então ler ou editar o arquivo de configuração no formato CLI no server. Quando você é terminado, você transfere o arquivo de volta ao controlador, onde é convertido a um formato XML e salvar.

Para instruções passo a passo em como editar o arquivo de configuração, refira a seção de [arquivos de configuração da edição do manual de configuração 6.0 WLC](#).

Q. Posso enviar configurações de uma WLC diretamente para outras WLCs?

A. Não. Você não pode enviar configurações de uma WLC diretamente para outras WLCs. Para transferir o arquivo para outras WLCs, você deve carregar o arquivo de configuração de uma WLC para o servidor TFTP e, em seguida, baixá-lo do servidor TFTP para a WLC desejada.

Para carregar e baixar um arquivo da WLC para o servidor TFTP, consulte a seção [Gerenciamento de Software da Controladora e Configurações](#) do [Guia de Configuração da Cisco Wireless LAN Controller Release 5.0](#).

Nota: Antes de transferir o arquivo da WLC para o servidor TFTP, certifique-se de que ambas as WLCs executem a mesma versão de software.

Q. Como eu descubro a versão de código que é executado na WLC?

A. Do controlador GUI do Wireless LAN, **monitor > sumário** do clique. Na página de sumário, o campo da **versão de software** mostra a versão de firmware que é executado no controlador do Wireless LAN.

Para descobrir a versão de firmware que é executada na WLC via CLI da WLC, use o comando **show run-config**.

```
(Cisco Controller) >show run-config Press Enter to continue... System Inventory Burned-in MAC
Address..... 00:0B:85:33:52:80 Press Enter to continue Or <Ctl Z> to
abort System Information Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller Product
Version..... 4.0.217.0 RTOS
Version..... 4.0.217.0 Bootloader
Version..... 4.0.217.0 Build
Type..... DATA + WPS Compact Flash
Size..... 256 MB
```

Para exibir a imagem de inicialização ativa, use o comando **show boot**.

```
(Cisco Controller) >show boot Primary Boot Image..... 4.0.217.0
(active) Backup Boot Image..... 4.0.155.5
```

Q. O que acontece à rede wireless quando eu executo um upgrade de software?

Todos os pontos de acesso (APs) registrados em uma WLC serão desativados até serem atualizados ou eles serão atualizados um de cada vez de modo que a rede Wireless possa permanecer ativa (com exceção dos APs específicos sofrerem o upgrade)?

A. Quando a WLC é atualizada, ela deve ser reiniciada para que as alterações entrem em vigor. Ness período, a conectividade com a WLC é perdida. Os LAPs registrados em uma WLC perdem sua associação à WLC. Assim, o serviço para os clientes Wireless é interrompido. Quando você faz o upgrade do software da controladora, o software nos pontos de acesso associados à controladora são atualizados automaticamente.

Quando um ponto de acesso carrega o software, cada um de seus LEDs pisca em sequência. Até 10 pontos de acesso podem ser atualizados simultaneamente pela controladora. Não desligue a controladora ou algum ponto de acesso durante este processo. Caso contrário, a imagem do software poderá ser corrompida. O upgrade de uma controladora com um grande número de pontos de acesso pode demorar até 30 minutos, dependendo do tamanho da sua rede. No entanto, com o maior número de upgrades de pontos de acesso simultâneos aceito no software release 4.0.206.0 e posterior, o tempo de upgrade deve ser reduzido significativamente. Os pontos de acesso devem permanecer ligados e a controladora não deverá ser reiniciada nesse período.

Q. Quais são as diretrizes que devem ser seguidas antes da execução de um upgrade da controladora Wireless LAN?

A. Cisco recomenda que a elevação esteja executada sobre um LAN ou o outro de alta velocidade, link de baixa latência. Uma conexão de rede muito lenta pode causar o timeout do TFTP, fazendo com que o upgrade não seja bem sucedido.

A Cisco recomenda que a controladora seja atualizada somente de daemon tftp no mesmo segmento que o controladora wireless LAN quando você usa o TFTP como o modo de transferência.

Quando você tenta fazer o upgrade da controladora usando um cliente wireless associado como o TFTP ou o servidor FTP, o upgrade falha. A controladora Wireless LAN não permite a transferência por (T)FTP de um daemon que esteja localizado em um cliente associado a um AP unido à WLC. (Consulte [CSCsi73129](#) para obter mais informações.)

Além disso, siga as diretrizes documentadas na seção [Diretrizes de Upgrade do Software da Controladora](#) do Guia de Configuração.

Q. Que funções do controlador exigem uma repartição?

A. Depois que você executa estas funções no controlador, você deve recarregar o controlador para que as mudanças tomem o efeito:

- Permita ou desabilite a agregação do link (a RETARDAÇÃO)
- Permita uma característica que seja dependente dos Certificados (tais como https e autenticação da Web)
- Adicionar novo ou altere usuários existentes SNMP v3
- Instale uma licença, mude o conjunto de recursos da licença, ou mude a prioridade de uma

Q. Pode um ponto de acesso (AP) com base no Cisco IOS Software que foi convertido para o modo lightweight se registrar em uma WLC Cisco 4100 Series?

A. Não, os APs com base no Cisco IOS Software convertidos para o modo lightweight não podem se registrar com as Cisco 40xx, 41xx ou 3500 WLCs. Estes AP lightweight (LAPs) podem se registrar somente com WLCs Cisco 4400 e 2000 Series. Para obter informações sobre as restrições dos APs que são convertidos para o modo lightweight, consulte a seção [Restrições de Upgrade de Pontos de Acesso Autônomos Cisco Aironet para o Modo Lightweight](#).

Q. Que é o número máximo de AP apoiados nos 4402 e 4404 controladores do Wireless LAN (WLC)?

A. A limitação do número de pontos de acesso com suporte é baseada no seu hardware. Os 4402 WLC com duas portas de Ethernet Gigabit vêm nas configurações que apoiam 12, 25, e no Lightweight Access Points dos 50 pés (regaços). Os 4404 WLC com quatro apoios das portas de Ethernet Gigabit 100 regaços.

Nota: Os Access point da malha estão igualmente disponíveis em disposições internas e exteriores. Para obter mais informações sobre do número de ponto de acesso (malha including AP) apoiado em cada modelo do controlador, refira os *Access point da malha da* tabela 8-3 *apoiados pelo modelo do controlador* na seção de [controle do Access point da malha do guia de configuração de controle 6.0 do Wireless LAN](#).

Q. Eu executei um downgrade da imagem de 7.0.98.0 a 6.0.200.22 nos meus 5508 WLC. Contudo, depois que o downgrade, o número máximo de AP apoiados no WLC mudou de 500 a 250 AP. Por quê?

A. Este é um comportamento esperado. Com versão 6.0 WLC, os 5508 apoios do controlador somente até 250 Lightweight Access Points. Com versão 7.0.98.0, um controlador wireless do único Cisco 5500 Series pode apoiar até 500 Cisco Aironet AP.

Q. Como o roaming ocorre em um ambiente de WLC?

A. Vaguear é um processo onde o cliente possa reter sessões de aplicativo ininterruptos em seu movimento. Quando um cliente wireless se associa e autentica em uma WLC, ela coloca uma entrada para esse cliente em seu banco de dados de clientes. Esta entrada inclui os endereços MAC e IP do cliente, o contexto de segurança e associações, contextos de Qualidade de Serviço (QoS), a WLAN e o LAP associado. Quando um cliente faz roaming para outro LAP associado à mesmo WLC, ele apenas atualiza o banco de dados do cliente com a informação do novo LAP de modo que os dados possam ser encaminhados apropriadamente para o cliente. Quando um cliente faz roaming para um LAP associado a uma WLC diferente, seja na mesma ou em sub-redes diferentes, ele envia a informação existente no banco de dados do cliente para a nova WLC. Isto ajuda o cliente a reter seu endereço IP durante o roaming e mantém sessões de TCP ininterruptas. Para obter mais informações sobre roaming no ambiente de WLC, consulte a seção [Configuração de Grupos de Mobilidade](#) do [Guia de Configuração da Cisco Wireless LAN Controller Release 5.1](#).

Q. Como os usuários convidados são tratados pela WLC?

A. Os usuários convidado são usuários de rede da terceira, que precisa acesso limitado aos recursos de rede e à conectividade de Internet. A WLC fornece acesso wireless e com fio de convidados usando a infraestrutura de rede wireless existente. Um SSID separado é fornecido geralmente para usuários convidados wireless. Os usuários convidados nas redes wireless e com fio são atribuídos a VLANs separadas, o que fornece o isolamento do tráfego dos convidados do resto do tráfego de dados. Isso proporciona um melhor controle sobre o tráfego dos convidados e uma maior segurança de rede. Os usuários convidado são autenticados geralmente com a [autenticação da Web](#). Para obter mais informações sobre o acesso de convidados, consulte o documento [Perguntas Frequentes sobre Acesso de Convidados Wireless](#).

Para obter logs de usuário convidados, habilite a contabilidade do Radius para os usuários e use este comando: **debug aaa all enable**

Q. Como eu configuro um base de dados local no controlador do Wireless LAN (WLC)? Quais são os caracteres especiais que podem ser usados para o nome de usuário e a senha dos usuários de rede locais?

A. O banco de dados de usuários locais armazena as credenciais (nome de usuário e senha) de todos os usuários da rede local. Estas credenciais são usadas para autenticar os usuários. Você pode configurar usuários da rede local via GUI ou CLI. Você pode inserir até 24 caracteres alfanuméricos. Todos os caracteres especiais podem ser usados quando você configura o nome de usuário e a senha via CLI, mas o caractere de aspas simples não pode ser usado quando você configura o nome de usuário e a senha com a GUI.

Na CLI, use estes comandos para criar um usuário de rede local:

- **config netuser add <username> <password> wlan <wlan_id> userType permanent description <description>** — Adiciona um usuário permanente ao banco de dados de usuários locais na WLC.
- **config netuser add <username> <password> {wlan | guestlan} {wlan_id | guest_lan_id} userType guest lifetime seconds description <description>** — Adiciona um usuário convidado em uma WLAN ou LAN de convidado com fio ao banco de dados de usuários locais na WLC.

Na GUI, você pode configurar usuários de rede local na página **Security > AAA > Local Net Users**.

Q. É possível eliminar automaticamente o usuário de rede local na WLC?

A. Os usuários líquidos locais não são suprimidos automaticamente. Você deve excluí-los manualmente. Para eliminar o usuário, vá para a página **Security > AAA > Local Net Users**. Para remover um usuário, coloque o cursor do mouse sobre o ícone e clique em **Remove**. Se um usuário de rede local estiver configurado como um usuário convidado, você deverá especificar o tempo após qual o usuário será eliminado automaticamente. O intervalo configurável é entre 60 segundos e 2592000 segundos.

Q. O que é um grupo de mobilidade?

A. O grupo da mobilidade é um grupo de WLC configurados com o mesmo nome do grupo da mobilidade. O cliente fazer o roaming continuamente entre as WLCs do mesmo grupo de mobilidade. As WLC em um grupo de mobilidade proporcionam redundância entre elas mesmas. Para obter mais informações sobre grupos de mobilidade, consulte o documento [Perguntas Frequentes sobre Grupos de Mobilidade de Controladoras Wireless LAN \(WLC\)](#).

Q. Quantos WLC posso eu ter no mesmo grupo da mobilidade?

A. Você pode colocar até 24 WLCs regulares (Cisco 2000, 4100 e 4400 Series) em um único grupo de mobilidade. Você pode configurar até 12 blades Wireless Services Modules (WiSM) em um grupo de mobilidade. Conseqüentemente, um máximo de 3600 pontos de acesso (APs) é aceito em um único grupo de mobilidade.

Nota: Com a WLC release 5.1, pode haver até 72 WLCs em um domínio de mobilidade.

Q. O Cisco 4400 Series WLC apoia o protocolo das Trocas de Pacote Entre Redes IPX (IPX)? Algum produto Airspace oferece suporte ao IPX?

A. Não, o protocolo IPX não é aceito em nenhuma plataforma de WLC da Cisco.

Q. Que é o acesso das condições prévias a interface gráfica de usuário (GUI) do controlador do Wireless LAN (WLC)?

A. O controlador GUI do Wireless LAN é inteiramente - compatível com versão do Microsoft internet Explorer 6.0 SP1 (ou mais tarde) e Mozilla Firefox 2.0.0.11 (ou mais tarde).

Nota: Não há suporte ao Opera nem ao Netscape.

Nota: O Internet Explorer 6.0 SP1 (ou posterior) e o Mozilla Firefox 2.0.0.11 (ou posterior) são os únicos navegadores com suporte para acessar a GUI da controladora e para usar a autenticação da Web.

Q. Como eu recupero o MIBs do controlador de LAN do Cisco Wireless (WLC) na Web?

A. Você pode baixar MIBs da WLC Cisco na página de [downloads de wireless \(somente clientes registrados\)](#).

Conclua estes passos para baixar as MIBs de WLC:

1. Das transferências wireless pague, clique o **controlador do Wireless LAN**, e escolha a plataforma WLC para que você precisa o MIBs.
2. A página de download de software para a WLC é mostrada. Essa página contém todos os arquivos para a WLC, inclusive os MIBs.
3. Escolha uma versão de software e baixe os MIBs padrão e os MIBs específicos da Cisco. Estes dois arquivos devem ser baixados e contêm os MIBs. Os nomes de arquivo são semelhantes a este exemplo:

`standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip Cisco-WLC-MIBS-XXXX.zip`

Q. No tunelamento convidado, quantos túneis Ethernet over IP (EoIP) podem ser formados entre uma única WLC âncora para as WLCs internas diferentes?

A. Uma única WLC âncora oferece suporte a até 71 túneis de EoIP, com um túnel por WLC interna. Essas WLCs podem ser de grupos de mobilidade diferentes.

Q. Quais são as diferenças funcionais entre as WLCs 2100 Series e as WLCs 4400?

A. As diferenças principais entre as WLCs 2100 e 4400 Series estão nos recursos com suporte.

Este recurso de hardware não é aceito nas WLCs 2100 Series:

- Porta de serviço (interface Ethernet 10/100 Mbps de gerenciamento out-of-band)

Estes recursos de hardware não são aceitos nas WLCs 2100 Series:

- Terminação de VPN (como IPSec e L2TP)
- Opção da transmissão VPN
- Terminação de túneis do controlador do convidado (a origem de túneis do controlador do convidado é apoiada)
- Lista de servidores Web de autenticação da Web externa
- LWAPP da camada 2
- Spanning Tree Protocol
- Espelhamento de portas
- Apple Talk
- De QoS contratos da largura de banda por usuário
- Passagem de IPv6
- Agregação do link (RETARDAÇÃO)
- modo do Multicast-unicast

Uma WLC 4400 Series oferece suporte a todos os recursos de hardware e de software mencionados acima.

Q. A quais pontos de acesso lightweight (LAPs) as WLCs 4100 Series oferecem suporte?

A. Somente os LAPs Airespace 1200 e 1250, Cisco 1000 Series e Cisco 1500 Series LAPs funcionam com as WLCs 4100 Series.

Q. Posso usar este ASA/PIX como um servidor DHCP em vez do servidor DHCP do Windows para atribuir endereços IP a meus clientes Wireless?

A. Sim, você pode usar o ASA/PIX como um servidor DHCP para clientes wireless. Certifique-se de que a interface da WLAN à qual o cliente pertence esteja na mesma sub-rede que a interface do ASA/PIX em que o servidor está habilitado. No entanto, você não pode atribuir o gateway padrão aos clientes. O PIX/ASA declara a si mesmo como o gateway padrão dos clientes. Para obter mais informações sobre como configurar o ASA como um servidor DHCP [PIX/ASA como servidor DHCP e Exemplo de Configuração de cliente](#).

Q. É possível voltar e fazer correções no assistente de configuração da controladora Wireless LAN (WLC) no momento da configuração inicial?

A. Sim, isso pode ser feito com a tecla - (hífen). Use essa tecla para inserir novamente o valor do parâmetro anterior.

Por exemplo, você usa o assistente de configuração da WLC para configurar a WLC a partir do

zero.

Em vez de inserir o nome de usuário como **admin**, você digita **adminn**. Para corrigir isso, digite - (tecla de hífen) no prompt seguinte e clique em **Enter**. O sistema retorna ao parâmetro anterior.

(Cisco Controller)

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_e8:38:c0]: adminn
Enter Administrative User Name (24 characters max): -
System Name [Cisco_e8:38:c0] (31 characters max):
```

Q. De acordo com a RFC1907 para o Simple Network Management Protocol (SNMP), o campo de local do SNMP deve oferecer suporte a um tamanho de 1-255. No entanto, sou incapaz de inserir mais de 31 caracteres no campo de local do SNMP. Por quê?

A. Isso ocorre devido ao bug da Cisco ID [CSCsh58468](#) ([somente clientes registrados](#)). Um usuário pode inserir somente 31 caracteres. No moment, não há nenhuma solução alternativa para isso.

Q. Com o recurso de Gerenciamento via Wireless habilitado nas controladoras Wireless LAN (WLCs) em um grupo de mobilidade, eu posso acessar somente uma WLC desse grupo de mobilidade, mas não todas. Por quê?

A. Este é um comportamento esperado. Quando habilitado, o recurso de Gerenciamento via Wireless permite que um cliente wireless alcance ou gerencie somente a WLC em que seu ponto de acesso associado foi registrado. O cliente não pode gerenciar outras WLCs, mesmo que essas WLCs estejam nos mesmos grupos de mobilidade. Isso é feito por questões de segurança, e restringido recentemente para apenas uma WLC para limitar a exposição.

O recurso Cisco WLAN Solution Management over Wireless permite que os operadores da Cisco WLAN Solution monitorem e configurem WLCs locais usando um cliente Wireless. Este recurso pode ser usado em todas as tarefas de gerenciamento, exceto em carregamentos e dowloads (transferências entre) a WLC.

Isso pode ser habilitado via CLI da WLC com o comando **config network mgmt-via-wireless enable**.

Na GUI, clique em **Management**; No lado esquerdo, clique em **Mgmt Via Wireless** e marque a caixa **Enable Controller Management to be accessible from Wireless Clients**.

Nota: Ao habilitar essa opção, você pode expor os dados. Certifique-se de que você habilitou uma autenticação apropriada e um esquema de criptografia.

Q. É possível atribuir um controlador integrado em um 3750 Switch e um controlador do Wireless LAN 4400 dentro do mesmo grupo da mobilidade?

A. Sim, é possível criar um grupo de mobilidade entre um Catalyst 3750 Switch com uma controladora integrada e uma WLC 4400.

Q. Há algum requisito básico a ser mantido quando eu uso o recurso de âncora de mobilidade para configurar as controladoras Wireless LAN (WLCs) para o acesso de convidados?

A. Estes são os 2 requisitos básicos que precisam ser mantidos quando você usa a âncora de mobilidade para configurar WLCs para o acesso de convidados.

- A âncora de mobilidade da WLC local deve apontar para a WLC âncora e a âncora de mobilidade da WLC âncora deve apontar somente para ela mesma. **Nota:** Você pode configurar WLCs âncoras redundantes. A WLC local as utiliza na ordem em que as WLCs estão configuradas.
- Certifique-se de configurar a mesma política de segurança para o Service Set Identifier (SSID) nas WLCs local e âncora. Por exemplo, se o SSID for "convidado" e você ativar a autenticação da Web na WLC local, certifique-se que o mesmo SSID e a mesma política de segurança também sejam configurados na WLC âncora.
- Para que o recurso de âncora de mobilidade funcione bem, certifique-se de que a WLC âncora e a WLC local usem a mesma versão do IOS.

Q. Que são algumas das opções que podem ser configuradas em um controlador de LAN do Cisco Wireless (WLC) para melhorar sua Interoperabilidade com dispositivos que não é da Cisco?

A. A interoperabilidade de uma WLC pode ser melhorada com estas opções:

- Os recursos proprietários reduzem a possibilidade da interoperabilidade com dispositivos de outros fabricantes. Estes são os recursos proprietários da Cisco: Aironet IE - O Aironet IE contém informações como o nome do ponto de acesso, a carga, número de clientes associados e assim por diante enviadas pelo ponto de acesso nas respostas de sinalização e sondagem da WLAN. Os clientes CCX usam essas informações para escolher o melhor ponto de acesso para se associarem. MFP: O Management Frame Protection é um recurso introduzido para proteger os quadros de gerenciamento, como de autenticação, desassociação, sinalizadores e sondagens onde o ponto de acesso adiciona um elemento de informação do Message Integrity Check (MIC IE) a cada um dos quadros de gerenciamento. Qualquer discrepância no MIC IE gera um alerta. Esses recursos são habilitados por padrão para qualquer WLAN criada na WLC. Para desabilitar esses recursos, clique o menu WLAN na WLC. Uma lista de WLANs configuradas na WLC é exibida. Clique na WLAN em que o cliente deseja se associar. Na guia Advanced da página WLANs > Edit, desmarque as caixas correspondentes ao Aironet IE e MFP.
- Preâmbulo curto — Um preâmbulo curto melhora o desempenho da taxa de transferência de dados e é habilitado por padrão. Alguns dispositivos, como telefones SpectraLink, podem trabalhar somente com preâmbulos longos. Nesses casos, desmarcar os preâmbulos curtos ajuda na associação. Para desabilitar o preâmbulo curto, clique o menu **Wireless** da GUI da WLC. Em seguida, clique no menu de rede **802.11b/g** > no lado esquerdo. Desmarque a caixa **Short Preamble**.
- Habilite o broadcast do Service Set Identifier (SSID) na WLAN — Com o broadcast do SSID habilitado, as informações de WLAN/SSID são enviadas nos sinalizadores. Isso também ajuda os clientes que executam varreduras passivas (aquelas que não transmitem solicitações de sondagem), bem como os clientes configurados sem um SSID, a se

associarem à WLC através desta WLAN.**Nota:** Certifique-se de que você tenha mecanismos de autenticação forte em vigor, já que clientes indesejados poderão se associar a sua rede wireless.

- Desabilite o balanceamento de carga agressivo global na WLC.

Q. Pode um controlador do Wireless LAN (WLC) ser controlado por CiscoWorks (que é usado para controlar o Roteadores e o Switches)?

A. Sim. Os modelos do 4400 Series WLC (tais como 4402 e 4404) podem ser controlados por CiscoWorks.

Q. Que é um AP não autorizado? Os APs não autorizados em minha rede wireless podem ser bloqueados automaticamente?

A. Os AP que não são parte de seu desenvolvimento wireless são chamados AP desonestos. Eles podem ser APs autônomos ou AP lightweight que podem estar no mesmo alcance dos APs autorizados. Os APs não autorizados não podem ser bloqueados automaticamente. Isso deve ser feito manualmente. A razão para isso é que, quando um AP não autorizado é encontrado, o AP responsável pela descoberta desassocia os clientes do AP não autorizado, o que causa uma recusa de serviço para os clientes. Isso pode causar problemas legais se o AP do vizinho for detectado como um não autorizado e seus clientes tiverem os serviços negados. Para obter mais informações sobre como os AP não autorizados são detectados pela WLC, consulte o documento [Deteção de Dispositivos Não Autorizados em Redes Wireless Unificadas](#).

Q. Qual é o número máximo de pontos de acesso (APs) não autorizados aceitos por WLC?

A. O controlador do Wireless LAN do 4400 Series apoia até 625 rogues, que inclui rogues reconhecidos, quando o 2100 Series apoiar 125 rogues.

Q. Pode o controlador do Wireless LAN (WLC) enviar notificações de Email ao administrador quando um evento crítico ocorre?

A. A WLC não envia emails, mas pode enviar interceptações para as estações do Network Management System (NMS), como o HP OpenView (HPOV). O HPOV pode executar tarefas como executar scripts de envio de emails mediante o recebimento de interceptações específicas.

O HPOV é uma série de produtos da Hewlett Packard que consiste em um portfólio extensivo de produtos de gerenciamento de rede e de sistemas. O HPOV é descrito comumente como um pacote de aplicativos de software que permite o gerenciamento de rede e do sistema em grande escala dos recursos de TI de uma organização. O HPOV inclui centenas de módulos opcionais da HP, bem como milhares de complementos de terceiros, que se conectam com a estrutura bem definida e se comunicam uns com os outros.

Q. Se as WLCs no mesmo grupo de mobilidade forem separadas por limites da Tradução de Endereço de Rede (NAT), elas poderão comunicar mensagens de mobilidade umas com as outras?

A. Em software releases da controladora anteriores ao 4.2, a mobilidade entre controladoras no

mesmo grupo de mobilidade não funciona quando uma das controladoras está por trás de dispositivo de Tradução de Endereço de Rede (NAT). Este comportamento cria um problema para o recurso de âncora do convidado, onde espera-se que uma controladora esteja fora do firewall.

As cargas úteis das mensagens de mobilidade transportam a informação de endereço IP da controladora de origem. Este endereço IP é validado com o endereço IP de origem do cabeçalho IP. Este comportamento representa um problema quando um dispositivo NAT é introduzido na rede porque ele muda o endereço IP de origem no cabeçalho IP. Assim, no recurso de WLAN convidada, qualquer pacote de mobilidade roteado através de um dispositivo NAT é descartado devido à inconsistência do endereço IP.

No software release 4.2 ou posterior da controladora, a consulta do grupo de mobilidade foi alterada para usar o endereço MAC da controladora de origem. Como o endereço IP de origem é mudado devido ao mapeamento no dispositivo NAT, o banco de dados do grupo de mobilidade é pesquisado antes que uma resposta seja enviada para obter o endereço IP da controladora que faz o pedido. Isso é feito com o endereço MAC da controladora que faz o pedido.

Consulte a [Utilização de Grupos de Mobilidade em Dispositivos NAT](#) para obter mais informações.

Q. As portas físicas na WLC estão definidas para operar na velocidade de 1000 mbps. É possível mudar a velocidade dessa porta para 100 mbps?

A. Não, a velocidade da porta na WLC não pode ser mudada. Elas são configuradas somente na velocidade de 1000 mbps, full-duplex.

Q. Ajustei o Radio Resource Management (RRM) para as configurações padrão em minha WLC. No entanto, não consigo fazer com que meu RRM ajuste automaticamente o canal e os níveis de potência. Por quê?

A. RRM possivelmente não trabalha para qualquer uma das seguintes razões

- O RRM funciona somente se um AP ouvir sinais de RF de pelo menos 3 APs, com um terceiro vizinho que transmite uma intensidade de sinal superior a -65dbm. Se qualquer uma dessas condições falhar, o RRM não funcionará.
- O recurso de auto RRM inclui ajuste de canais, ajuste de potência e detecção de furos de cobertura. Esses recursos não funcionam quando estão desabilitados ou o método de atribuição escolhido é o manual.

Quando um AP novo inicializa, ele mantém inicialmente a potência no valor padrão de 1 (máximo). Ao ver 3 ou mais APs com níveis de potência superiores a -65 dBm (no mesmo domínio de mobilidade RF e no mesmo canal), ele tenta o RRM primeiro (os canais de mudança). Se não houver êxito porque os canais são fixados manualmente, ou se houver mais APs do que canais disponíveis, o AP reduzirá seu nível de potência.

Consulte [Gerenciamento de Recursos de Rádio: Conceitos](#) para obter mais informações sobre como o RRM funciona.

Q. Faz o controlador do Wireless LAN (WLC) apoiar localmente a autenticação EAP-PEAP?

A. Até a versão 4.1, o PEAP não é aceito localmente na WLC. Você precisa de um servidor RADIUS externo. Na versão 4.2 e mais recentes da WLC, o EAP local agora oferece suporte a PEAPv0/MSCHAPv2 e PEAPv1/GTC.

Q. Podemos colocar o ponto de acesso lightweight (LAP) sob a Tradução de Endereço de Rede (NAT)? O Lightweight Access Point Protocol (LWAPP) do ponto de acesso (AP) para a WLC funciona através do NAT?

A. Sim, você pode colocar o LAP sob o NAT. No lado AP, você pode ter qualquer tipo de NAT configurado, mas, no lado WLC, você pode ter somente 1:1 (NAT estático) configurado. O PAT não pode ser configurado no lado da WLC porque os LAPs não podem responder às WLC se as portas são traduzidas para portas diferentes de 12222 ou 12223, as quais se destinam a mensagens de dados e de controle.

Q. Posso eu colocar o Access point de pouco peso (REGAÇO) sob o Network Address Translation (NAT)? O controle do padrão de IETF e o abastecimento do protocolo dos pontos de acesso Wireless (CAPWAP) do Access Point (AP) ao WLC trabalham com os limites NAT?

A. Sim, você pode colocar o LAP sob o NAT. No lado AP, você pode ter qualquer tipo de NAT configurado.

Mas no lado WLC, você pode ter somente 1:1 (NAT estático) configurado e o endereço IP de Um ou Mais Servidores Cisco ICM NT externo NAT configurado na interface de gerenciamento dinâmica AP (somente para controladores do Cisco 5500 Series). A PANCADINHA não pode ser configurada no lado WLC porque os regaços não podem responder aos WLC se as portas são traduzidas às portas diferentes de 5246 ou de 5247, que estão significadas para o controle e os mensagens de dados.

Nota: Selecione a caixa de **verificação de endereço da possibilidade NAT** e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT externo NAT se você quer poder distribuir seu controlador do Cisco 5500 Series atrás de um roteador ou do outro dispositivo de gateway que está usando o Network Address Translation (NAT) do mapeamento um a um. O NAT permite que um dispositivo, tal como um roteador, atue como um agente entre o Internet (público) e uma rede local (privada). Neste caso, traça endereços IP de Um ou Mais Servidores Cisco ICM NT do intranet do controlador a um endereço externo correspondente. A relação dinâmica do gerenciador AP do controlador deve ser configurada com o endereço IP de Um ou Mais Servidores Cisco ICM NT externo NAT de modo que o controlador possa enviar o endereço IP de Um ou Mais Servidores Cisco ICM NT correto na resposta da descoberta.

Nota: Com CAPWAP, o WLC atrás do NAT não é apoiado com o 4400 Series, os controladores do Wireless LAN do 2100 Series e o WiSM.

Q. Como eu configuro a WLC para permitir somente os clientes 802.11g?

A. Use o comando **config 802.11b disable** para desabilitar ou habilitar as transmissões 802.11b/g para a rede inteira ou para um rádio individual da Cisco

Nota: Você deve usar este comando para desabilitar a rede antes de usar outros comandos config 802.11b. Este comando pode ser usado sempre que a interface CLI está ativa.

A sintaxe é a seguinte:

```
config 802.11b disable {network | Cisco_AP}
```

Exemplo de como desabilitar as transmissões 802.11b/g do AP01:

```
config 802.11b disable network
```

Para desabilitar as transmissões 802.11b/g do **AP01** , use este comando:

```
config 802.11b disable AP01
```

Alternativamente, você pode usar este comando para desabilitar as taxas de dados 802.11b:

```
config 802.11b rate {disabled | mandatory | supported} rate
```

Q. Qual é o procedimento de upgrade do software de sistema operacional (SO) em uma WLC Cisco?

A. Consulte o documento [Upgrade de Software da Controladora Wireless LAN \(WLC\)](#) para saber como fazer um upgrade de software em sua WLC.

Q. Posso fazer o upgrade da WLC de uma versão principal diretamente para outra?

A. Você pode atualizar ou reverter o software da WLC somente entre dois releases. Para atualizar ou reverter para releases não consecutivos, é necessário instalar primeiro um release intermediário. Por exemplo, se sua WLC executa o release 4.2 ou 5.0, você poderá atualizar sua WLC diretamente para o Software Release 5.1.151.0. Se a sua WLC executar o release 3.2, 4.0 ou 4.1, você deverá atualizar sua WLC para um release intermediário antes do upgrade para o 5.1.151.0. Para conhecer o caminho de upgrade para qualquer versão da WLC, consulte as Release Notes do release correspondente.

Q. Que é Beamforming?

A. Beamforming (igualmente chamado ClientLink) é um mecanismo de filtragem usado em um transmissor para melhorar a potência do sinal recebido ou a relação (SNR) de relação sinal-ruído em um receptor pretendido (cliente). Beamforming usa o múltiplo transmite Antenas para focalizar transmissões na direção de um cliente 802.11a ou 802.11g, que aumente o downlink SNR e a taxa de dados ao cliente, reduza furos da cobertura, e aumente o desempenho de sistema total. Beamforming é apoiado em Access point do 1140 e 1250 Series do Cisco Aironet e trabalha com todos os clientes 802.11a e 802.11g existentes. É desabilitado à revelia.

Para obter informações sobre de configurar Beamforming, refira a seção [configurando de Beamforming do guia de configuração de controle do Wireless LAN](#).

Q. Posso eu transferir um banner de login para o controlador do Wireless LAN?

A. Você pode transferir um arquivo do banner de login usando o controlador GUI ou o CLI. O banner de login é o texto que se publica na tela antes da autenticação de usuário quando você alcança o controlador GUI ou CLI usando o telnet, o SSH, ou uma conexão de porta de Console.

Perguntas Frequentes de Troubleshooting

Q. Nós concluímos a nossa implantação inicial de pontos de acesso lightweight (LAPs). Quando nossos clientes se deslocam de uma ponta do prédio para a outra, eles permanecem associados ao AP do qual eles estavam mais próximos. Os clientes não parecem ser entregues para o AP mais próximo seguinte até que a intensidade de sinal do AP inicial seja completamente suprimida. por que?

A. A área de cobertura de um AP é controlada inteiramente pela WLC. A WLC fala entre seus APs e controla sua intensidade de sinal com base em como cada AP detecta outros AP. Contudo, o movimento de clientes de um AP para outro é controlado inteiramente pelo cliente. O rádio interno do cliente determina quando o cliente quer migrar de um AP para o outro. Nenhuma configuração na WLC, no AP ou no resto da sua rede pode influenciar a decisão do cliente de migrar (roaming) para um AP diferente.

Q. Conectei minha WLC a switches Cat6500 configurados para roteamento e configurei o HSRP entre esses switches. No entanto, agora sou incapaz de acessar outras sub-redes com a WLC. Como eu resolvo esse problema?

A. Quando o HSRP é usado, um endereço IP virtual e um endereço MAC são normalmente configurados para o grupo HSRP, que é usado para roteamento. Os hosts continuam a encaminhar pacotes IP para esses endereços IP e MAC consistentes, mesmo quando um dos switches é desativado e uma mudança para um dispositivo de backup ocorre. Conclua estes passos para resolver o problema de roteamento:

1. Certifique-se de que o endereço IP virtual esteja configurado como o gateway padrão na WLC. **Nota:** Algumas versões antigas de WLC não encaminham pacotes para endereços MAC HSRP, o que impossibilita o roteamento de pacotes. Faça a atualização da WLC para resolver este problema.
2. Certifique-se que a interface virtual na WLC esteja configurada corretamente. Para obter mais informações sobre interfaces, consulte a seção [Configuração de Portas e Interfaces](#) do [Guia de Configuração da WLC](#).

Q. Como eu previno loops na WLC?

A. Você pode habilitar o STP na WLC para impedir a ocorrência de loops. **Do controlador do clique WLC GUI**, navegue então ao submenu **avançado** situado no lado esquerdo do aplicativo. Clique na opção **Spanning Tree** e escolha **Enable** para a opção **Spanning Tree Algorithm** localizada no lado direito do aplicativo.

Por padrão, o STP não precisa estar habilitado para prevenir loops. Como cada interface que é mapeada em uma WLAN na WLC é mapeada para as portas principal e de backup. Somente uma porta é usada em um instante de tempo específico. O tráfego da WLAN é encaminhado somente através da porta principal. A WLC nunca usa a porta secundária quando a porta principal está ativa. A WLC usa a porta secundária somente quando a porta principal está desativada. Assim, não haverá loops por padrão.

Q. Há alguma opção para fornecer a segurança adicional à rede?

A. Você pode usar a opção 82 a fim fornecer a segurança adicional. A opção 82 obstrui endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes desautorizados que alcançam a rede. Para mais informação, refira a seção [configurando da opção de DHCP 82 do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 6.0](#).

Q. Há alguma maneira de recuperar minha senha da WLC?

A. Se você esquecer a sua senha na versão 5.1 ou posterior da WLC, você poderá usar a CLI do console serial da controladora para configurar um novo nome de usuário e uma nova senha. Conclua estes passos para configurar um novo nome de usuário e uma nova senha.

1. Após a inicialização da controladora, digite **Restore-Password** no prompt de usuário.**Nota:** Por questões de segurança, o texto que você digitar não será mostrado no console da controladora.
2. No prompt Enter User Name, insira um novo nome de usuário.
3. No prompt Enter Password, digite uma nova senha.
4. No prompt Re-enter Password, digite novamente a nova senha.A controladora valida e armazena suas entradas no banco de dados.
5. Quando o prompt User for mostrado novamente, insira seu novo nome de usuário.
6. Quando o prompt Password for exibido, digite a nova senha.Você iniciará sessão na controladora com os novos nome de usuário e senha.

Nota: Para as WLC com versões anteriores do firmware (anteriores à 5.1), não há nenhuma forma de recuperar a senha. Se você usa o Sistema de controle sem fio da Cisco (WCS) a fim controlar o WLC, o módulo do controlador do Wireless LAN (WLCM) ou o módulo de Serviços sem fio (WiSM), você deve poder alcançar o WLC do WCS e criar um usuário administrativo novo sem registrar no WLC próprio. Ou, se você não salvou a configuração na WLC após eliminar o usuário, uma reinicialização (desligar e ligar) da WLC deverá reiniciar o dispositivo com o usuário eliminado ainda no sistema. Se você não possuir a conta admin padrão ou uma outra conta de usuário com a qual você pode iniciar sessão, sua unica opção será restaurar as configurações de fábrica padrão da WLC e reconfigurá-la a partir do zero.

Q. Eu mudei o modo de ponto de acesso lightweight (LAP) do ponto de acesso (AP) 1030 de Local para modo de Bridge, mas a WLC 2006 não o detecta mais. Como posso restaurar o AP 1030 de volta para seu modo de AP local?

A. A fim configurar a ponte no modo local, termine estas etapas:

1. Vá para a GUI da WLC e escolha **Wireless**. A lista de APs que estão registrados na WLC no momento é exibida. **Clique no AP para o qual você precisa mudar o modo.****Nota:** Verifique se o AP oferece suporte ao modo REAP. Ele deve ser **YES** para APs de bridging interno.
2. Verifique a opção AP mode. Se ela estiver definida como Bridge, mude-a de volta para **Local**. Isso muda o AP bridge para o AP normal.

Para obter mais informações sobre como configurar o modo de Bridging, consulte o [Exemplo de Configuração de Bridging Ethernet em Rede em Malha Wireless Ponto a Ponto](#).

Q. Configurei uma Wireless LAN convidada e a WLC está separada fisicamente da minha LAN interna. Eu decidi usar o recurso de DHCP interno desta WLC, mas meus clientes wireless não obtêm endereços IP da WLC. Como os usuários convidados Wireless obtêm endereços IP da WLC quando estão conectados

fisicamente a uma rede fisicamente separada?

- Verifique se o escopo de DHCP está habilitado na WLC. Para fazer isso, clique o menu **Controller** e clique em **Internal DHCP Server** no lado esquerdo.
- Geralmente, o servidor DHCP é especificado na interface mapeada na WLAN. Certifique-se de que o endereço da interface de gerenciamento da WLC esteja especificado como o servidor DHCP na interface mapeada na WLAN do usuário convidado. Alternativamente, você pode habilitar a opção de desvio do servidor DHCP na página **WLAN > Edit** página e especificar o endereço da interface de gerenciamento da WLC no campo do **DHCP Server IP Addr**.

Q. Eu tenho um controlador do Wireless LAN do 4400 Series (WLC) e o Lightweight Access Points (regações) registrado ao WLC. Eu configurei WLANs para que os clientes se conectem à WLC. O problema é que a WLC não faz o broadcast dos identificadores do conjunto de serviço (SSID) que configurei para as WLANs. Por quê?

A. O status administrativo e os parâmetros de broadcast do SSID estão desabilitados por padrão. Conclua estes passos para habilitar o status administrativo e o broadcast do SSID:

1. Vá para a GUI da WLC e escolha **Controller > WLANs**. A página WLANs é exibida. Esta página lista as WLANs que estão configuradas.
2. Selecione a WLAN para a qual você deseja habilitar o broadcast do SSID e clique em **Edit**.
3. Na página **WLAN > Edit**, marque **Admin Status** para habilitar a WLAN. Marque também **Broadcast SSID** para garantir que o SSID seja transmitido nas mensagens de sinalização enviadas pelo AP.

Q. A solução do Cisco Unified Wireless apoia WLC redundantes no DMZ para o Tunelamento do convidado?

A. Sim, a Cisco Unified Wireless Solution oferece suporte a WLCs redundantes na DMZ para o tunelamento de convidados. Para obter mais informações sobre como configurar WLCs redundantes, consulte a seção [Configuração da Mobilidade de Auto-Âncora](#) do documento [Guia de Configuração da Cisco Wireless LAN Controller Release 5.1](#).

Q. Os clientes do Wireless LAN associados com o Lightweight Access Points não podem obter endereços IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. O que devo fazer?

A. O servidor DHCP de um cliente é marcado geralmente na interface mapeada na WLAN em que o cliente está conectado. Verifique se a interface está configurada apropriadamente. Para obter mais informações sobre como fazer o troubleshooting de problemas relacionados ao DHCP, consulte a seção [Problemas de Endereço IP](#) do documento [Troubleshooting de Problemas de Clientes na Rede Cisco Unified Wireless](#).

Q. Há algum documento que explicar edições da conectividade de cliente do Troubleshooting em uma rede de Cisco Unified Wireless?

A. Para informações detalhadas sobre dos problemas de cliente do Troubleshooting, refira estes documentos.

- [Unified Wireless Network: Resolução de Problemas de Clientes](#)
- [Compreender debuga o cliente nos controladores do Wireless LAN \(os WLC\)](#)

Q. Meu Access point de 1131 pesos leves (REGAÇO) não se registra com meu controlador do Wireless LAN 4402 (WLC). Qual pode ser a possível razão para isso?

A. Um motivo comum é que o modo de transporte do Lightweight Access Point Protocol (LWAPP) está configurado na WLC. Uma WLC 4420 pode operar nos modos do LWAPP da camada 2 e da camada 3. No entanto, um LAP 1131 podem operar somente no modo da camada 3. O modo da camada 2 não aceito no LAP 1131. Assim, se a WLC estiver configurada com o modo de transporte do LWAPP da camada 2, seu LAP não poderá se unir à WLC. Para resolver esse problema, mude o modo de transporte do LWAPP da WLC da camada 2 para a camada 3.

Para mudar o modo de transporte do LWAPP usando a GUI, vá para a página WLC e localize a segunda seleção no campo principal, o campo LWAPP Transport Mode. Altere-o para Layer 3 e reinicialize a WLC. Agora seu LAP pode se registrar com a WLC. Para obter mais informações sobre problemas relacionado ao registro do LAP, consulte o documento [Troubleshooting de Pontos de Acesso Lightweight Incapazes de se Unir a Controladoras Wireless LAN](#).

Q. Nenhuma interceptação é gerada pela WLC para não autorizados ad-hoc e as depurações de SNMP na WLC não mostram nenhuma interceptação da WLC para o ad-hoc, mesmo que a GUI da WLC tenha relatado os não autorizados ad-hoc. A WLC executa a versão de firmware 3.2.116.21. Por que isso acontece?

A. Isso ocorre devido ao bug da Cisco ID [CSCse14889](#) ([somente clientes registrados](#)). A WLC envia consistentemente interceptações para os pontos de acesso (AP) não autorizados detectados, mas não para não autorizados ad-hoc detectados. Esse erro foi corrigido nas versões de firmware 3.2.171.5 ou posteriores da WLC.

Q. Possuímos uma infraestrutura de WLAN corporativa Cisco Airespace. Os clientes de WLAN são incapazes de consultar um domínio do Microsoft Active Directory (AD). Esse problema pode ser observado dentro de um de nossos prédios. Outros prédios não apresentam o problema. Não usamos nenhuma lista de controle de acesso (ACL) internamente. Além disso, quando um cliente que apresentou falha é conctado via cabo, ele pode consultar imediatamente o domínio do Microsoft AD. Qual poderia ser o problema?

A. Uma das razões pode ser que o modo multicast está desabilitado na WLC. Habilite o modo de multicast na WLC e verifique se você pode acessar o domínio do Microsoft AD.

Q. A mobilidade da camada 3 trabalha com uma configuração de VLAN do grupo do Access Point (AP)?

A. Sim, a mobilidade da camada 3 funciona com uma configuração de VLAN de grupo de AP. No momento, aos fontes de tráfego de um cliente wireless com roaming da camada 3 são colocadas

em uma interface dinâmica atribuída à WLAN ou à interface da VLAN do grupo de AP.

Q. Por que nossos pontos de acesso (AP) que estão registrados em outras WLCs que estão no mesmo grupo de RF são mostrados como não autorizados?

A. Isso pode ocorrer devido ao bug da Cisco ID [CSCse87066](#) ([somente clientes registrados](#)). Os APs LWAPP no mesmo grupo de RF são vistos como APs não autorizados por uma outra WLC devido a qualquer um destes motivos:

- O AP vê mais de 24 vizinhos. O tamanho da lista de vizinhos é 24. Assim o 25º AP é relatado como não autorizado.
- O AP1 pode ouvir o cliente que se comunica com o AP2, mas o AP2 não pode ser ouvido. Conseqüentemente, ele não pode ser validado como um vizinho.

A solução alternativa é definir manualmente os AP como internos conhecidos na WLC e/ou no WCS. Conclua estes passos na WLC para definir manualmente os APs como internos conhecidos:

1. Vá para a GUI da WLC e escolha **Wireless**.
2. Clique em **Rogue Aps** no menu do lado esquerdo.
3. Na lista Rogue-AP, escolha o ponto de acesso específico e clique em Edit.
4. No menu do Update Status, escolha **Known internal**.
5. Clique em Apply. Esse erro foi corrigido na versão 4.0.179.11.

Q. Eu tenho um Access point de 1200 pesos leves (REGAÇO) a ser registrado com meu controlador do Wireless LAN (WLC). Eu configurei meu servidor DHCP com a Opção 43. Como posso verificar se a Opção de DHCP 43 está funcionando corretamente?

A. Com a Opção de DHCP 43, o servidor DHCP fornece o endereço IP das WLCs junto com o endereço IP fornecido pelo DHCP. Isso pode ser verificado no LAP se o AP for um AP Lightweight Access Point Protocol (LWAPP) baseado no Cisco IOS, como o LAP 1242 ou 1131AG. Nesses casos, execute o comando **debug dhcp detail** no lado do AP para ver se o AP recebe com êxito as informações da Opção 43 e o que ele recebe.

Q. Meus WLCs 2600 mostram que diferentes canais foram atribuídos aos pontos de acesso (APs) registrados. No entanto, quando eu faço a varredura com o Aironet Desktop Utility (ADU) ou o Netstumbler, todos os APs estão no mesmo canal (1). Qual é a razão?

A. Este problema ocorre quando estes APs registrados estão muito próximos uns dos outros. Você pode ter encontrado o bug da Cisco ID [CSCsg03420](#) ([somente clientes registrados](#)).

Q. Quando eu executo o comando ipconfig/all no prompt de comandos do meu PC, um endereço de servidor DHCP diferente é mostrado. 1.1.1.1 é mostrado como o endereço IP do servidor DHCP. Este é o endereço IP da interface virtual da WLC, e não do endereço do servidor DHCP. Por que isto é mostrado como o servidor DHCP?

A. Porque o endereço da interface virtual 1.1.1.1 atua como um proxy de DHCP para o servidor DHCP original. Se quiser ver o endereço original do servidor DHCP na saída do comando **ipconfig/all**, desabilite o recurso de proxy de DHCP na WLC à qual o cliente está associado. Isso pode ser feito com o comando **config dhcp proxy disable**.

Esse comando substituirá o endereço da interface virtual 1.1.1.1, que se mostra como o servidor DHCP, pelo endereço IP de servidor DHCP real que você definiu na interface ou na opção de substituição da WLAN.

Q. Possuímos um par de servidores de controle de acesso (ACS) que autenticam os clientes wireless associados às controladoras Wireless LAN (WLC). Um ACS atua como um servidor de autenticação primário e o outro como um servidor de failover. Se o servidor primário falha, o WLC é redirecionado para o secundário para autenticar os clientes wireless. Quando o servidor primário volta a funcionar, a WLC não retorna para esse servidor primário. Por quê?

A. Este é um comportamento esperado. Estes eventos ocorrem quando um cliente é autenticado com a WLC em implantações de ACSs múltiplos:

1. Na inicialização, a WLC determina o ACS ativo.
2. Quando esse ACS ativo não responde à solicitação de RADIUS da WLC, a WLC procura e faz o failover para o ACS secundário.
3. Mesmo quando o ACS primário volta a funcionar, a WLC não retornará para ele até que o ACS no qual a WLC está autenticando falhe.

Nesses casos, reinicialize a WLC para que a WLC identifique o ACS primário novamente e passe a utilizá-lo outra vez. Isso não ocorre imediatamente após a reinicialização e pode levar algum tempo.

Q. Não consigo me conectar via Secure Shell (SSH) na controladora Wireless LAN (WLC) quando eu uso o software cliente SecureCRT SSH V2. Minha WLC executa a versão 4.0.179.8.

A. SecureCRT trabalha somente com WLC que executam a versão 4.0.206.0 ou mais tarde. Faça o upgrade da sua WLC para esta versão. Você poderá então usar o cliente SecureCRT para se conectar via SSH com a WLC.

Q. Como eu criptografo os arquivos de configuração na WLC?

A. A criptografia dos arquivos de configuração está já disponível nos WLC. Ao escolher **Commands > Upload File** na GUI da WLC, você verá a caixa de seleção **Configuration File Encryption**.

Você pode forçar o arquivo a ser criptografado via WCS dessa forma.

- Na GUI do WCS, escolha **Configure controller**. A lista de WLCs configuradas no WCS é exibida. Clique em uma WLC.
- No lado esquerdo, clique na opção **commands**. Você recebe uma lista dos comandos do controlador.
- Em **Upload/Download Commands**, escolha **download config** no menu suspenso. Nessa hora,

you will see this message: **Nota: Configuration file encryption key is not set. Downloading configuration file will fail if encryption key is needed. Please click here to setup encryption.**

Basicamente, você pode forçar o WCS a definir sempre uma chave de criptografia para as configurações de WLC. A criptografia não está habilitada por padrão, mas pode ser permitida na WLC e no WCS conforme o necessário.

Q. Como os WLC apoiam Access point desproporcionados?

A. O Software Release 5.0 ou Mais Recente do controlador permite que você promova a uma imagem de ponto de acesso desproporcionado automaticamente suprimindo a imagem de recuperação para criar o espaço suficiente. Esta característica afeta somente Access point com o 8 MB do flash (os 1100, de 1200, e de Access point do 1310 Series). Todos os Access point mais novos têm um tamanho flash maior do que o 8 MB. Em agosto 2007, não há nenhuma imagem de ponto de acesso desproporcionado, mas como os novos recursos são adicionados, o tamanho da imagem de ponto de acesso continuará a crescer. Para mais informação, refira a seção [desproporcionado de apoio das imagens de ponto de acesso do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 6.0](#).

Informações Relacionadas

- [Módulos de controlador de LAN do Cisco Wireless](#)
- [Cisco Wireless LAN Controllers - Perguntas e Respostas](#)
- [Contadores de MAC do 802.11 no WLC](#)
- [Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0](#)
- [Página de Suporte Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)