Access point de pouco peso FAQ

Índice

Introdução

Este documento fornece informações sobre as perguntas mais frequentes (FAQ) sobre pontos de acesso Lightweight Cisco (LAPs).

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

DOBRE O FAQ

Q. Que é um Access point da leve Cisco (REGAÇO)?

A. O Cisco LAP é parte da arquitetura de rede Cisco Unified Wireless. Um LAP é um AP que foi projetado para ser conectado a uma controladora Wireless LAN (WLAN) (WLC). O LAP fornece suporte a banda dupla para IEEE 802.11a, 802.11b e 802.11g e monitoração simultânea no ar para o gerenciamento dinâmico e em tempo real da frequência de rádio (RF). Além, os regaços de Cisco seguram as funções sensíveis ao tempo, tais como a criptografia da camada 2, que permitem Cisco WLAN de suportar firmemente a Voz, o vídeo, e os aplicativos de dados.

Os APs são o “peso leve,” que significa que não pode atuar independentemente de um controlador do Wireless LAN (WLC). A WLC gerencia as configurações e o firmware do AP. Os APs são “toque zero” distribuído, e a configuração individual dos APs não é necessária. Os APs são igualmente lightweight no sentido em que lidam somente com a funcionalidade de MAC em tempo real. Os APs saem de toda a funcionalidade do tempo não real MAC a ser processada pelo WLC. Essa arquitetura é conhecida como “arquitetura de MAC dividido”.

Q. Posso eu configurar o REGAÇO para operar o independente de um controlador do Wireless LAN (WLC)?

A. Não, LAPs não podem funcionar separados de WLCs. Os LAPs funcionam somente em conjunto com uma WLC. A razão é que a WLC fornece todos os parâmetros de configuração e o firmware que o LAP precisa no processo de registro.

Q. O que é o Lightweight AP Protocol (LWAPP)?

A. LWAPP é um protocolo de esboço do Internet Engineering Task Force (IETF) que defina a

Mensagem do controle para operações da instalação e da autenticação e do tempo de execução do trajeto. O LWAPP também define o mecanismo de tunelamento para o tráfego de dados.

Um LAP descobre uma controladora com o uso de mecanismos de descoberta LWAPP. O LAP envia uma solicitação de união LWAPP à controladora. A controladora envia ao LAP uma resposta de união LWAPP que permite que o AP se una à controladora. Quando o LAP se une à controladora, ele baixa o software da controladora se as revisões no LAP e na controladora não combinam. Subsequentemente, o LAP está completamente sob o controle da controladora. O LWAPP protege a comunicação de controle entre o LAP e a controladora por meio de uma distribuição de chaves segura. A distribuição de chaves segura exige certificados digitais X.509 já provisionados no LAP e na controladora. Os certificados na fábrica são conhecidos pelo termo “MIC”, que é um acrônimo em inglês para Certificado Instalado na Fábrica. Os APs Cisco Aironet comercializados antes de 18 de julho de 2005 não possuem MIC. Assim, esses APs criam um certificado auto-assinado (SSC) quando são atualizados a fim de operar no modo lightweight. As controladoras são programadas para aceitar SSCs para a autenticação de APs específicos.

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, consequentemente, 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. Como eu diferencio um AP (autônomo) regular de um LAP?

A. A maneira a mais fácil de distinguir entre um AP regular e um LAP é olhar o número de peça do AP.

- LAP (Lightweight AP Protocol [LWAPP]) — Os números de peça *sempre* começam com**AIR-LAPXXXX**.
- APs autônomos (Cisco IOS® Software) — Os números de peça *sempre* começam por **AIR-APXXXX**.

Os LAPs Cisco Aironet 1000 Series são uma exceção a esses critérios. Os números de peça dos LAPs 1000 Series são:

- AIR-AP1010-A-K9 para um LAP 1010
- AIR-AP1020-A-K9 para um LAP 1020
- AIR-AP1030-A-K9 para um LAP 1030

Nota: Os números de peça podem variar, o que depende do país e do domínio regulatório. Os números de peça que esta lista fornece são apenas exemplos.

Certifique-se de fazer o pedido do AP apropriado para sua Wireless LAN (WLAN).

Q. Que modelos de AP podem executar o Lightweight AP Protocol (LWAPP)?

A. Estas plataformas do AP Cisco Aironet são capazes de executar o LWAPP:

- Aironet 1500 Series
- Cisco Aironet 1250 Series
- Aironet 1240 AG Series
- Aironet 1230 AG Series
- Aironet 1200 Series
- Aironet 1130 AG Series
- Aironet 1000 Series
- 1140 Series AP de Aironet**Nota:** O 1140 Series AP é apoiado somente com WLC que as corridas 5.2 liberam ou mais tarde.

Nota: Você pode fazer pedidos desses APs Aironet com Cisco IOS Software para operar como APs autônomos ou com o LWAPP. O número de peça determina se um AP é um AP baseado no Cisco IOS Software ou um AP baseado em LWAPP. Exemplos:

- O AIR-AP1242AG-A-K9 é um AP baseado em Cisco IOS Software.
- O AIR-LAP1242AG-P-K9 é um AP baseado em LWAPP.

Nota: Os APs 1000 Series e os APs 1500 Series são exceções a este critério. Todos os APs 1000 Series e os APs 1500 Series oferecem suporte somente ao LWAPP.

Q. Como eu instalo e configuro um Access point LWAPP-permitido?

A. os APs LWAPP-permitidos são parte da solução de rede Wireless integrada Cisco e não exigem nenhuma configuração manual antes que estejam montados. O AP é configurado por uma controladora Cisco Wireless LAN (WLC) com suporte ao LWAPP. Refira os Access point LWAPP-permitidos guia de início rápido do Cisco Aironet para obter informações sobre de como instalar e configurar inicialmente um Access point LWAPP-permitido.

Q. Como eu configuro meu LAP e minha controladora Wireless LAN (WLC) juntos?

A. Os regaços usam o protocolo de pouco peso AP (LWAPP), e quando se juntam a um WLC, o WLC envia aos regaços os todos os parâmetros de configuração e firmware. Consulte Exemplo de Configuração Básica de Controladoras Wireless LAN e Pontos de Acesso Lightweight para obter informações sobre a instalação básica.

Q. Posso conectar um AP autônomo a uma controladora Wireless LAN (WLC) e esperar que o AP funcione?

A. Não, somente os LAPs funcionam quando estão conectados a uma WLC. Os APs autônomos não compreendem o protocolo de pouco peso AP (LWAPP) ou o protocolo CAPWAP que o WLC usa. Para conectar um AP autônomo a uma WLC, você deve primeiro converter o AP autônomo para o modo lightweight.

Q. Eu tenho Cisco IOS autônomo um Access point Software-baseado. Posso convertê-lo para o modo lightweight?

A. Sim, mas nem todos os modelos autônomos de APs com base no Cisco IOS Software podem ser convertidos. Estes são os modelos que você pode converter para o modo Lightweight AP Protocol (LWAPP):

- Todos os APs Cisco Aironet 1130 AG
- Todos os APs Aironet 1240 AG
- Para todos as plataformas modulares de AP Aironet 1200 Series com base no Cisco IOS Software (upgrade do Cisco IOS Software 1200/1220 e AP 1210 e 1230), a capacidade de converter o AP depende do rádio.Se o rádio for IEEE 802.11g, haverá suporte a MP21G e MP31G.Se o rádio for IEEE 802.11a, haverá suporte a RM21A e RM22A.Você pode fazer o upgrade do AP 1200 Series com qualquer combinação de rádios com suporte:Somente GSomente AG e A

Nota: Um AP autônomo deve executar o Cisco IOS Software Release 12.3(7)JA ou posterior para poder ser convertido para o LWAPP.

Nota: Somente os Cisco 4400 e 2006 e as controladoras Wireless LAN (WLC) oferecem suporte a APs autônomos que foram convertidos para o modo lightweight. As WLCs Cisco deve executar uma versão mínima de software de 3.1. O Cisco Wireless Control System (WCS) deve executar uma versão mínima de 3.1. O utilitário de upgrade funciona nas plataformas Microsoft Windows 2000 e Windows XP.

Consulte Atualização de Pontos de Acesso Autônomos Cisco Aironet para o Modo Lightweight para obter detalhes de como fazer a conversão.

Q. Que limitações são impostas no Cisco IOS Software-basearam o Access point após a conversão do modo leve?

A. Mantenha estas diretrizes na mente quando você usa os Access point autônomos que estiveram convertidos ao modo leve:

- Os APs convertidos para o Lightweight AP Protocol (LWAPP) não oferecem suporte aos Wireless Domain Services (WDS). Os APs convertidos para LWAPP se comunicam somente com as controladoras Cisco Wireless LAN (WLAN) (WLC) e não podem se comunicar com

dispositivos WDS. No entanto, a WLC fornece funcionalidade equivalente ao WDS quando o AP se associa à WLC.

- Os Access point convertidos apoiam 2006, 4400, e controladores de WiSM somente. Quando você converte um Access point autônomo ao modo leve, o Access point pode comunicar-se com os controladores do Cisco 2006 Series, os controladores do 4400 Series, ou os controladores em Cisco WiSM somente.
- No Software Release 4.2 ou Mais Recente do controlador, todos os Access point da leve Cisco apoiam 16 BSSIDs pelo rádio e um total de 16 LAN sem fio pelo Access point. Em liberações precedentes, apoiaram somente 8 BSSIDs pelo rádio e um total de 8 LAN sem fio pelo Access point. Quando um Access point convertido associar a um controlador, simplesmente o Sem fio LAN com IDs 1 a 16 está empurrado para o Access point.
- Os APs convertidos para o LWAPP devem obter um endereço IP e descobrir a WLC com o uso do DHCP, de um Domain Name System (DNS) ou de um broadcast de sub-rede IP.
- Os APs convertidos para o LWAPP não oferecem suporte ao LWAPP da camada 2.
- Os APs convertidos para o LWAPP fornecem uma porta de console somente de leitura.
- A ferramenta da conversão da elevação adiciona a chave-mistura do certificado auto-assinado (SSC) a somente um dos controladores em Cisco WiSM. Depois que a conversão foi terminada, adicionar a chave-mistura de SSC ao segundo controlador em Cisco WiSM copiando a chave-mistura de SSC do primeiro controlador ao segundo controlador. A fim copiar a chave-mistura de SSC, abra a página das políticas AP do controlador GUI (**Segurança > políticas AAA > AP**), e copie a chave-mistura de SSC da coluna da mistura da chave SHA1 sob a lista da autorização AP. Então, com o GUI do segundo controlador, abra a mesma página e cole a chave-mistura no campo da mistura da chave SHA1 adicionam abaixo o AP à lista da autorização. Se você tem mais de um Cisco WiSM, use o WCS para empurrar a chave-mistura de SSC para todos os controladores restantes.

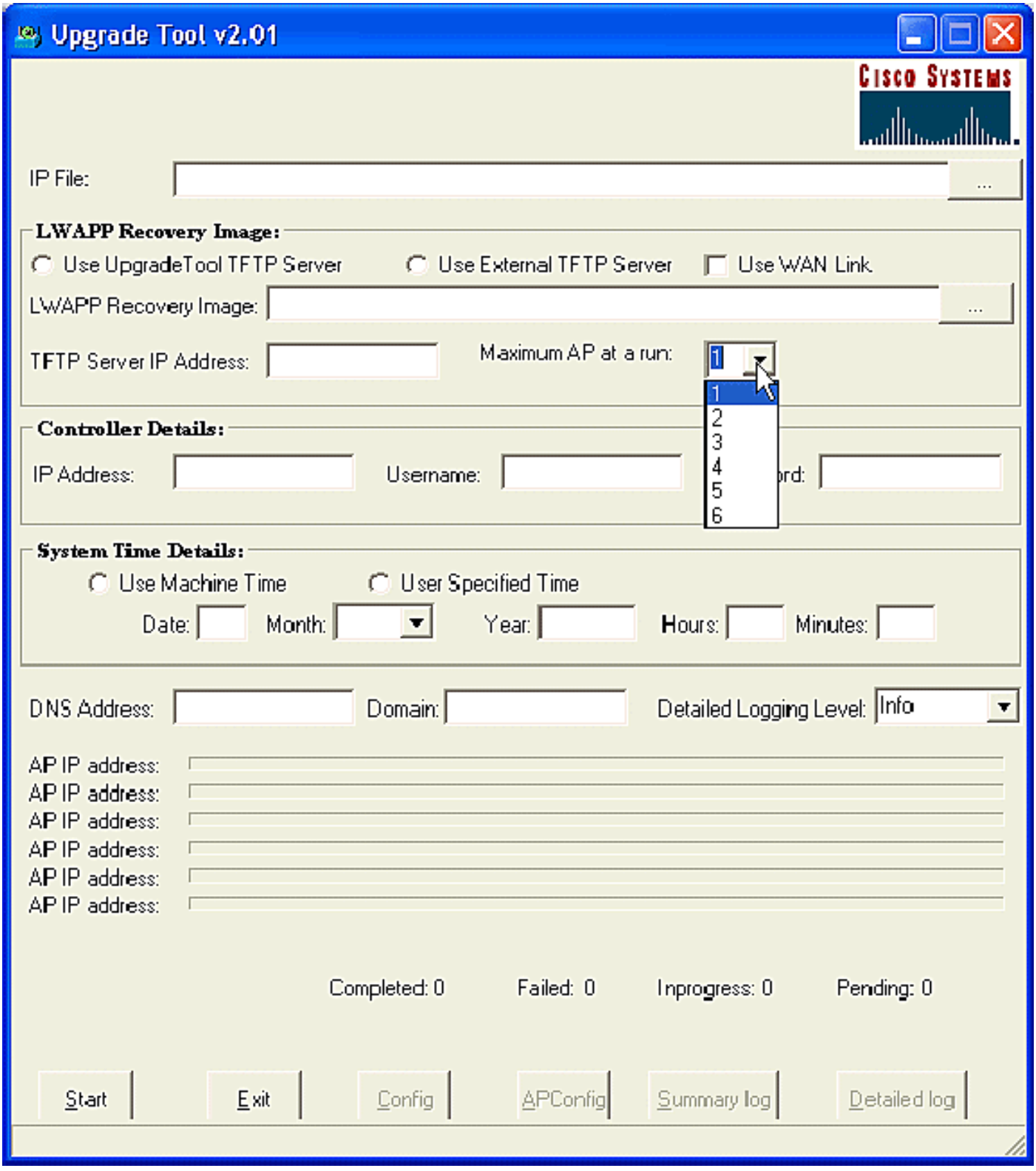
Consulte as Release Notes dos Pontos de Acesso Cisco Aironet 1130AG, 1200, 1230AG e 1240AG Series para Cisco IOS Release 12.3(7)JX para obter detalhes.

Q. Eu converti meu Access point ao modo leve, mas eu preciso de convertê-lo de volta ao modo autônomo. É possível?

A. Sim, você pode converter os AP autônomos que você converteu para o modo lightweight de volta para o modo autônomo. Conclua os passos da seção *Conversão de um Ponto de Acesso Lightweight de Volta para o Modo Autônomo de* Upgrade de Pontos de Acesso Cisco Aironet Autônomos para o Modo Lightweight.

Q. Quantos Access point podem ser convertidos através da ferramenta de upgrade ao mesmo tempo?

A. Com a versão 2.01 mais recente da ferramenta, você pode fazer o upgrade de no máximo seis AP de cada vez.



Q. Converti meu AP para o Lightweight AP Protocol (LWAPP), mas o AP não se registra na controladora. Eu recebo a mensagem "Juntar-`pedido LWAPP não incluo o certificado válido em CERTIFICATE_PAYLOAD do AP`." O que causa este problema?

A. Esse erro significa que os certificados digitais do X.509 são inválidos. Pôde-se ser que você está experimentando a identificação de bug Cisco CSCsd42296 (clientes registrados somente). A ação alternativa para esta edição é restaurar os APs aos padrões de fábrica.

Uma outra possibilidade é que o certificado auto-assinado (SSC) não está registrado na WLC. A adição manual do SSC na controladora pode ser necessária. Consulte Adição Manual do

Certificado Auto-Assinado à Controladora para APs Convertidos para o LWAPPpara obter informações sobre o procedimento.

Q. Posso configurar um AP com base no Cisco IOS Software como uma bridge de grupo de trabalho e associá-lo a APs baseados no Lightweight AP Protocol (LWAPP)?

A. Você pode configurar um Access point para operar-se como um bridge de grupo de trabalho de modo que possa fornecer a conectividade Wireless a um Access point de pouco peso em nome dos clientes que são conectados por Ethernet ao Access point do bridge de grupo de trabalho. Quando você configura o Access point para se operar como um bridge de grupo de trabalho e para conectar a uma rede unificada Cisco, pode fornecer a conectividade Wireless aos clientes prendidos que são conectados por Ethernet ao Access point do bridge de grupo de trabalho. Por exemplo, se você precisa de fornecer a conectividade Wireless para um grupo de dispositivos prendidos, você pode conectar os dispositivos a um hub ou a um interruptor, conectar o hub ou switch à porta Ethernet de ponto de acesso, e configurar o Access point como um bridge de grupo de trabalho.

Os bridges de grupo de trabalho do original em um exemplo da configuração de rede do Cisco Unified Wireless fornecem um exemplo de configuração.

Q. Pode um cliente Wireless fazer roaming entre APs LWAPP e APs autônomos?

A. Não, não há suporte ao roaming entre LAPs e APs autônomos. A razão é que, quando conectado a APs LWAPP, o tráfego é transmitido através de um túnel LWAPP. Como não há túnel da mobilidade entre a controladora Wireless LAN e os AP autônomos, o roaming não funciona.

Q. Que opções de antena estão disponíveis com os diferentes modelos de LAPs Cisco Aironet 1000 Series?

A. A caixa do LAP 1000 Series contém:

- Um IEEE 802.11a ou uma antena de rádio 802.11b/g
- Quatro antenas internas de alto ganho (duas 802.11a e duas 802.11b/g)

Você pode habilitar ou desabilitar essas antenas independentemente a fim de produzir uma área de cobertura setorizada em 180 graus ou omnidirecional em 360 graus. Alguns dos LAPs 1000 Series também podem usar antenas externas. Os LAPs 1000 Series vêm em três modelos:

- LAP 1010
- LAP 1020
- LAP 1030

As opções disponíveis de antena são:

- LAP 1010:Quatro antenas internas de alto ganhoNenhum adaptador de antena externa
- LAP 1020:Quatro antenas internas de alto ganhoUm adaptador de antena externa de 5 GHzDois adaptadores de antena externa de 2,4 GHz
- LAP 1030 (LAP de borda remota):Quatro antenas internas de alto ganhoUm adaptador de antena externa de 5 GHzDois adaptadores de antena externa de 2,4 GHz

A. External-Antenna Model B. Internal-Antenna Model

Nota: Os LAPs 1000 Series devem usar as antenas externas ou internas fornecidas pela fábrica a fim de evitar uma violação das exigências da FCC e evitar a anulação da autorização do usuário para operar o equipamento.

Q. Que opções de alimentação estão disponíveis para os LAPs Cisco Aironet 1000 Series?

A. O LAP Aironet 1000 Series pode receber energia de uma fonte de alimentação externa de 110 a 220 VCA para 48 VCC ou de equipamentos Power over Ethernet. A fonte de alimentação externa (AIR-PWR-1000) é conectada a uma tomada elétrica protegida de 110 a 220 VCA. O conversor produz os 48 VCC necessários para os LAPs 1000 Series. A saída do conversor alimenta o LAP 1000 Series através de um conector de 48 VCC.

Nota: Você pode fazer o pedido da fonte de alimentação externa AIR-PWR-1000 com os cabos de alimentação de tomada elétrica específicos do seu país. Entre em contato com a Cisco ao fazer o pedido para receber o cabo de alimentação correto.

Q. Posso executar um Telnet/SSH para um ponto de acesso baseado em LWAPP?

A. Na controladora Wireless LAN release 5.0 ou posterior, a controladora oferece suporte ao uso de protocolos Telnet ou Secure Shell (SSH) para fins de troubleshooting dos pontos de acesso lightweight. Você pode usar estes protocolos para facilitar a depuração, especialmente quando o ponto de acesso é incapaz de conectar à controladora. Você pode configurar o suporte ao Telnet e ao SSH somente através da CLI da controladora.

Para habilitar a conectividade de Telnet ou SSH em um ponto de acesso, use o comando **config ap {telnet | ssh}**. O ponto de acesso lightweight Cisco se associa a esta controladora Cisco Wireless LAN para todas as operações de rede e no caso de uma reinicialização de hardware.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Examples


```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```


Q. Como configurar credenciais globais para pontos de acesso. Quais são o nome de usuário padrão e a senha no release 5.0?

A. Os pontos de acesso Cisco IOS são enviados de fábrica com a senha de modo enable padrão Cisco. Essa senha permite que os usuários iniciem sessão no modo não privilegiado e executem comandos show e debug, o que representa uma ameaça de segurança. A senha de enable padrão deve ser mudada para impedir o acesso não autorizado e permitir que os usuários executem comandos de configuração da porta de console do ponto de acesso.

No software da controladora anterior ao release 5.0, você pode definir a senha de enable do ponto de acesso somente para os pontos de acesso que estão conectados à controladora. No software release 5.0 da controladora, você pode definir nome de acesso, senha e senha de enable globais que são herdados por todos os pontos de acesso à medida que eles se unem à controladora. Isso inclui todos os pontos de acesso unidos no momento à controladora e que possam se unir no futuro. Se desejado, você poderá cancelar as credenciais globais e atribuir um nome de usuário exclusivo, uma senha e uma senha de enable para um ponto de acesso específico.

Para obter informações sobre como configurar as credenciais globais do AP, consulte Configuração de Credenciais Globais para Pontos de Acesso.

Q. Possuo uma controladora Wireless LAN (WLC) 2006 e um ponto de acesso (AP) 1242 com versão de firmware 3.2.78.0. Eu tenho problemas com pontos de acesso que se conectam a ele e recebo estas mensagens de erro: “lwapp_clinet_error; not receive read response(3). Lwapp_image_broc; unable to open TAR file"

A. O AP 1242s é o protocolo de pouco peso convertido do Access point (LWAPP) APs. Uma vez que você os converte e tenta usá-los, eles tentam procurar a controladora para se unir a ela. Se os APs não encontrarem a controladora, este tipo de mensagem será mostrado no console. Mas, nesse caso, a controladora tem uma versão de firmware 3.2.78.0, a qual não é compatível com APs atualizados. Você precisa ter a versão de firmware 3.2.116.21 para trabalhar com APs atualizados. Uma vez que o firmware da controladora seja atualizado, esses AP se unem à controladora e começam a funcionar.

Q. Os clientes mostram um MAC address de 00:17:0f:37:65:c4 quando anexado a um Access point, mas o Access point mostra que que é tem um MAC address de rádio baixo de 00:17:0f:37:65:c0. Por que o cliente mostra um MAC diferente do

que o ponto de acesso? Há uma maneira de determinar que endereço MAC o dispositivo registra quando tenho dois pontos de acesso com endereços MAC muito próximos?

A. Se você observar um ponto de acesso em detalhes, poderá ver que ele possui um endereço MAC rádio base e um endereço MAC de FastEthernet. Além disso, é o endereço MAC do rádio base que muda com a WLAN. O cliente vê na realidade o BSSID sob a forma de um endereço MAC.

Q. Eu tenho uma rede Wireless (APs autônomos) com um ponto de acesso que está configurado como um repetidor. Esta rede deve ser migrada para uma rede Wireless LWAPP. Posso usar APs LWAPP como repetidores?

A. LWAPP APs deve juntar-se a um controlador, e não apoia um modo de repetidor desde que todo tem que ter alguma Conectividade ao controlador primeiramente. Os APs Cisco autônomos podem ser configurados como repetidores, mas devido à redução na largura de banda efetiva disponível para os clientes finais, os repetidores não são a configuração mais recomendada. Enquanto qualquer modelo de AP Cisco Aironet ou LAP pode ser usado nos modos LWAPP ou autônomo, para fazer essa mudança, uma nova imagem do software é necessária. Isso é particularmente complexo quando a mudança é do modo autônomo para o LWAPP. Assim, não, um AIR-LAP1232AG-A-K9 não oferece suporte nativo ao modo de repetidor. Ele poderia ser carregado com o software autônomo e configurado para oferecer suporte ao modo de repetidor, mas isso envolveria uma alteração de software e uma configuração separada.

Q. Quantos APs pode WLCs apoiar?

A. O número de APs apoiados por WLC depende do número de modelo:

- **2106** — Um WLC autônomo que apoie até 6 APs com 8 interfaces rápidas de Ethernet.
- **4402** — Um WLC autônomo que apoie 12, 25, ou 50 APs.
- **4404** — Um WLC autônomo que apoie 100 APs.
- **5500** — Um WLC autônomo que apoie 12, 25, 50,100, ou 250 Access point para Serviços sem fio críticos para negócio em lugar de todos os tamanhos.
- **WLCM** — Um módulo WLC que seja projetado especificamente para a série do roteador do serviço integrado de Cisco (ISR). Está atualmente disponível em uma versão 6, de 8 ou de 12 AP.
- **WS-C3750G** — Um WLC que apoie 25 ou 50 APs que vem integrado com o Catalyst 3750 Switch. As conexões da placa-mãe Do WLC aparecem como as portas Ethernet 2-Gig que podem ser configuradas separadamente como troncos do dot1q para fornecer a conexão nos 3750. Ou as portas da atuação podem ser relação agregada para fornecer uma única conexão EtherChannel aos 3750. Porque o WLC é integrado diretamente, tem o acesso a todas as características avançadas do roteamento e switching disponíveis no switch empilhável 3750. Este WLC é ideal para escritórios ou construções de tamanho médio. A versão `50 AP pode escalar até 200 APs quando quatro 3750s são empilhados junto como um virtual switch.
- **WiSM** — Um módulo WLC que seja projetado especificamente para a série do Catalyst 6500 Switch de Cisco. Apoia até 300 APs pelo módulo. Segundo a plataforma 6500, WISMs múltiplo pode ser instalado para oferecer capacidades significativas da escamação. O WiSM aparece como uma única interface de link agregada nos 6500 que podem ser configurados

como um tronco dot1 para fornecer a conexão na placa traseira 6500. Este módulo é ideal para grandes construções ou terrenos.

Q. Que é o número máximo de associações do cliente que uns Access point podem apoiar?

A. O número máximo de associações do cliente que os Access point podem apoiar depende destes fatores:

- O número máximo de associações do cliente difere para o peso leve e os Access point de Autonmous IO.
- Pôde haver um limite pelo rádio e um limite total pelo AP.
- Hardware AP (16-MB APs têm um limite mais baixo do que o 32-MB e os APs mais altos).

Para detalhes completos em limites da associação do cliente, refira a seção dos *limites da associação do cliente do* manual de configuração do controlador de LAN do Cisco Wireless, a liberação 7.0.

Q. Os 1252 AP apoiam a construção de uma ponte sobre?

A. Sim, o modo de Bridging é apoiado no 1252 Series AP.

Q. A infraestrutura de pouco peso do protocolo AP (LWAPP) apoia o PPP over Ethernet (PPPoE) (cliente de PC a um servidor PPPoE)?

A. Não, a infraestrutura do LWAPP não oferece suporte ao PPPoE. A razão é que o Ethertype PPPoE é descartado na controladora.

Q. Como posso reiniciar manualmente o LAP Cisco Aironet 1000 Series?

A. Você pode redefinir o AP para os padrões de fábrica através da controladora Wireless LAN (WLAN) (WLC). Para a redefinição, o LAP deve estar registrado na WLC.

Conclua estes passos:

1. Na GUI da WLC, clique em **Wireless**. A guia Wireless fornece acesso à configuração de rede Wireless da solução de WLAN da Cisco.
2. Escolha **Access Points > Cisco APs** e clique em **Detail** para navegar para a janela do AP específico.
3. Clique em **Clear Config** na parte inferior desta janela. Isso limpa a configuração do LAP e restaura os padrões de fábrica.

Para redefinir os LAPs para os padrões de fábrica com uso da interface de linha de comando (CLI), execute o comando **clear ap-config ap-name na** CLI da WLC.

Q. Onde posso obter mais informações sobre LAPs Cisco Aironet 1000 Series?

A. Consulte Pontos de Acesso Lightweight Cisco 1000 Series - Perguntas e Respostas. O documento fornece respostas para muitas perguntas relacionadas aos LAPs 1000 Series.

Q. Que dispositivos Cisco oferecem suporte ao modo da camada 2 do Lightweight AP Protocol (LWAPP)?

A. O modo da camada 2 LWAPP é apoiado somente nestes dispositivos Cisco:

- Controladora Wireless LAN (WLC) Cisco 4100 Series
- WLC Cisco 4400 Series
- LAP Cisco Aironet 1000 Series

Q. Eu entendo que os LAPs Cisco usam uma string de Identificador da Classe de Fornecedor (VCI) com a Opção de DHCP 43 para a descoberta de controladoras. Que é o valor da string VCI para os LAPs Cisco?

A. O Cisco Aironet série 1000 APs usa um formato da corda para a opção de DHCP 43, visto que o outro Aironet APs usa o tipo, comprimento, formato do valor (TLV) para a opção de DHCP 43. Você deve programar os servidores DHCP para retornar a opção com base na string VCI de DHCP do AP (Opção de DHCP 60). Esta tabela fornece os valores de string VCI para os diferentes LAPs:

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

Q. Que é o significado dos valores do bloco do Type Length Value (TLV) no que diz respeito à opção de DHCP 43? Como o valor TLV é calculado?

A. A opção de DHCP 43 pode ser habilitada no servidor DHCP do roteador Cisco IOS com este comando:

```
Option 43 hex <string>
```

A string hexadecimal neste comando é montada concatenando-se os valores TLV para a subopção da opção 43.

Tipo + comprimento + valor

- **Tipo** é sempre o código de subopção 0xf1.
- **O comprimento** é o número de endereços IP de gerenciamento da controladora vezes 4 em hexadecimal.
- **O valor** é o endereço IP da controladora listado sequencialmente em hexadecimal.

Por exemplo, suponha que haja duas controladoras com endereços IP 10.126.126.2 e 10.127.127.2 da interface de gerenciamento:

- O tipo é 0xf1.
- O comprimento é 2 * 4 = 8 = 0x08.
- Os endereços IP são traduzidos para 0a7e7e02 (10.126.126.2) e a 0a7f7f02 (10.127.127.2).
- A montagem da string gera então f1080a7e7e020a7f7f02. O comando do IOS adicionado então ao escopo de DHCP é:

```
option 43 hex f1080a7e7e020a7f7f02
```

Q. Faz o Balanceamento de carga AP do apoio do controlador do Wireless LAN (WLC)?

A. Sim, você pode fazer o balanceamento de carga de APs em uma WLC. Consulte Perguntas Frequentes de Troubleshooting da Controladora Wireless LAN (WLC) para obter mais informações.

Q. Como eu configuro o failover da controladora Wireless LAN (WLC) para LAPs?

A. Consulte Exemplo de Configuração de Failover de Controladora WLAN para Pontos de Acesso Lightweight para obter detalhes de como configurar o failover da WLC.

Q. Como posso eu desabilitar o botão de redefinição nos APs após a conversão de autônomo para o modo lightweight?

A. Você pode desabilitar o botão de redefinição nos APs que você converteu para o modo lightweight. O botão de redefinição chama-se “MODE” e pode ser encontrado na parte externa do AP. Use este comando para desabilitar ou habilitar o botão de redefinição em um ou em todos os APs convertidos que estão associados a uma controladora:

```
config ap reset-button {enable | disable} {ap-name | all}
```

O botão de redefinição nos APs convertidos é habilitado por padrão.

Q. Posso ter um AP compatível com o Lightweight AP Protocol (LWAPP) - AP conectado via link de WAN da controladora Wireless LAN (WLC)? Em caso afirmativo, como isso funciona?

A. Sim, alguns LAPs oferecem suporte ao recurso chamado Remote-Edge AP (REAP). Com este recurso, você pode ter um LAP através de um link de WAN da WLC à qual o LAP está conectado. O modo REAP permite que um LAP resida no outro lado de um link de WAN e ainda possa se

comunicar com a WLC e fornecer a funcionalidade de um LAP regular. Consulte Exemplo de Configuração do Remote-Edge AP (REAP) com APs Lightweight e Controladoras Wireless LAN (WLCs) para obter um exemplo detalhado desta configuração.

Nota: O modo REAP é aceito no momento somente nos LAPs Cisco Aironet 1030. A funcionalidade REAP será incluída em um número maior de LAPs no futuro.

Q. Ainda assim temos as mesmas limitações de WAN em APs no modo de monitor, da mesma forma que fazemos com APs regulares e APs H-REAP? Isto é, devemos exigir um RTD de 100 ms ou melhor entre a controladora e um AP em modo de monitor?

A. Não, o modo de monitor AP não tem a limitação de 100 Senhoras porque não há nenhuma associação do cliente, que é a razão para a limitação. A limitação da latência de 100 Senhoras foi criada fora de variado, e de frequentemente estrito, exigências da autorização do cliente, que é porque ambo o modo local e H-REAP APs têm limitações idênticas da latência. Obviamente, os APs no modo de monitor não têm as mesmas limitações que o cliente.

Q. A versão da minha WLC é 3.2. Ela está configurada para o Lightweight Access Point Protocol (LWAPP) da camada 3. A MTU da rede entre essa WLC e meu ponto de acesso lightweight (LAP) está configurado como 900 bytes. Meu AP LWAPP é incapaz de se unir a essa WLC. O que pode estar causando isso?

A. A MTU configurada em seu cenário é 900 bytes. No entanto, uma solicitação de união LWAPP é superior a 1500 bytes. Assim, o LWAPP exige um fragmento da solicitação de união LWAPP. A lógica para todos os APs LWAPP é que o tamanho do primeiro fragmento é 1500 bytes (inclui o IP e o cabeçalho de UDP) e o segundo fragmento é 54 bytes (inclui o IP e o cabeçalho de UDP). Se a rede entre os APs LWAPP e a WLC possuir um tamanho de MTU inferior a 1500 (tais como VPN, GRE, MPLS e assim por diante) como no seu caso, a WLC não poderá lidar com a solicitação de união LWAPP. Consequentemente, o LWAPP não poderá se unir à controladora.

Faça o upgrade da sua controladora para a versão 4.0 a fim de lidar com essa situação. Esta versão é capaz de lidar com fragmentos da camada 3. Consulte o bug da Cisco ID CSCsd94967 (somente clientes registrados) para obter mais informações sobre este problema.

Q. Eu tenho uma WLC que comprei em Cingapura. Com essa WLC, minha intenção era ter um escritório remoto conectado a ela (REAP) para obter conectividade Wireless. Eu tenho escritórios em outros países. No entanto, eu recebo mensagens de Erro de domínio regulatório da WLC de Cingapura. Há alguma maneira de forçar a WLC a aceitar pontos de acesso (AP) com domínios regulatórios diferentes? A mensagem de erro é: "AP 'AP_NAME' is unable to associate. **The Regulatory Domain configured on it '-R' does not match the Controller 'A.B.C.D' country code 'SG - Singapore"**

A. A WLC oferece suporte a somente um domínio regulatório. Consequentemente, uma WLC que use o domínio regulatório -A pode ser usada somente com APs que usam o domínio regulatório -A (e assim por diante). Nesse caso, a WLC está definida como -SG para Cingapura. Assim, ela oferece suporte somente a APs no domínio regulatório de Cingapura.

Ao comprar APs e WLCs, certifique-se de que eles compartilhem o mesmo domínio regulatório.

Somente assim os APs podem se registrar com a WLC.

Suporte a vários códigos de país - Nas versões 4.1.171.0 e mais recentes da WLC, o suporte a vários códigos de país foi introduzido nas WLCs. No release 4.1.171.0 ou posterior, você pode configurar até 20 códigos de país por controladora. O suporte a vários códigos de país permite gerenciar pontos de acesso em vários países a partir de uma única controladora. Não há suporte a esse recurso para o uso com pontos de acesso da malha Cisco Aironet.

Q. Quais são os modos diferentes em que um ponto de acesso lightweight (LAP) pode operar?

A. Um LAP pode operar em qualquer um destes modos:

- **Modo local** - Este é o modo padrão de operação. Quando um REGAÇO é colocado no modo local, o AP transmitirá no canal normalmente atribuído. Contudo, o AP igualmente monitora todos canais restantes na faixa durante 180 segundos para fazer a varredura de cada um dos outros canais para 60ms durante o tempo NON-transmitir. Durante esse tempo, o AP executa medidas de piso de ruído, mede a interferência e examina-as em busca de eventos de IDS.
- **COLHA o modo** — O modo remoto do Access point da borda (COLHA) permite um REGAÇO de residir através de uma relação MACILENTO e ainda de poder comunicar-se com o WLC e fornecer a funcionalidade de um REGAÇO regular. COLHA o modo é apoiado somente nos 1030 regaços.
- **Modo H-REAP** — H-REAP é uma solução Wireless para disposições do escritório filial e do escritório remoto. H-REAP permite clientes de configurar e controlar os Access point (APs) em um ramo ou em um escritório remoto do escritório corporativo com uma relação MACILENTO sem a necessidade de distribuir um controlador em cada escritório. H-Colher pode comutar o tráfego de dados do cliente localmente e executar a authenticação do cliente localmente quando a conexão ao controlador é perdida. Quando conectados ao controlador, os H-REAPs também podem enviar o tráfego por túnel de volta ao controlador.
- **Modo de monitor** - O modo de monitor é um recurso projetado para permitir que APs compatíveis com o LWAPP eliminem a si mesmos do manuseio de tráfego de dados entre os clientes e a infraestrutura. Assim eles atuam como sensores dedicados de serviços baseados em local (LB), detecção de pontos de acesso não autorizados e detecção de intrusões (IDS). Quando os AP estão no modo de monitor, eles não podem atender clientes e percorrem continuamente todos os canais configurados, escutando cada um por aproximadamente 60 ms.**Nota:** A partir do release 5.0 da controladora, os LWAPP também podem ser configurados no Modo de Monitor Otimizado para Local (LOMM), o que otimiza a monitoração e o cálculo de local de marcas RFID. Para obter mais informações sobre este modo, consulte Cisco Unified Wireless Network Software Release 5.0.**Nota:** Com controlador libere 5.2, a seção **aperfeiçoada lugar do modo de monitor (LOMM)** foi rebatizada que **segue a otimização**, e o **LOMM permitiu a** caixa suspensa foi rebatizado **permite o seguimento da otimização**.**Nota:** Para obter mais informações sobre de como configurar o seguimento da otimização, leia o RFID de aperfeiçoamento que segue na seção dos Access point.
- **Modo de detector de não autorizados**— Os LAPs que operam no modo de detector de não autorizados monitoram os APs não autorizados. Eles não transmitem nem contêm AP não autorizados. A ideia é que o detector de não autorizados possa ver todas as VLAN na rede, já que os AP não autorizados podem estar conectados a algumas das VLANs da rede (assim, nós o conectamos a uma porta de tronco). O switch envia todas as listas de endereços MAC

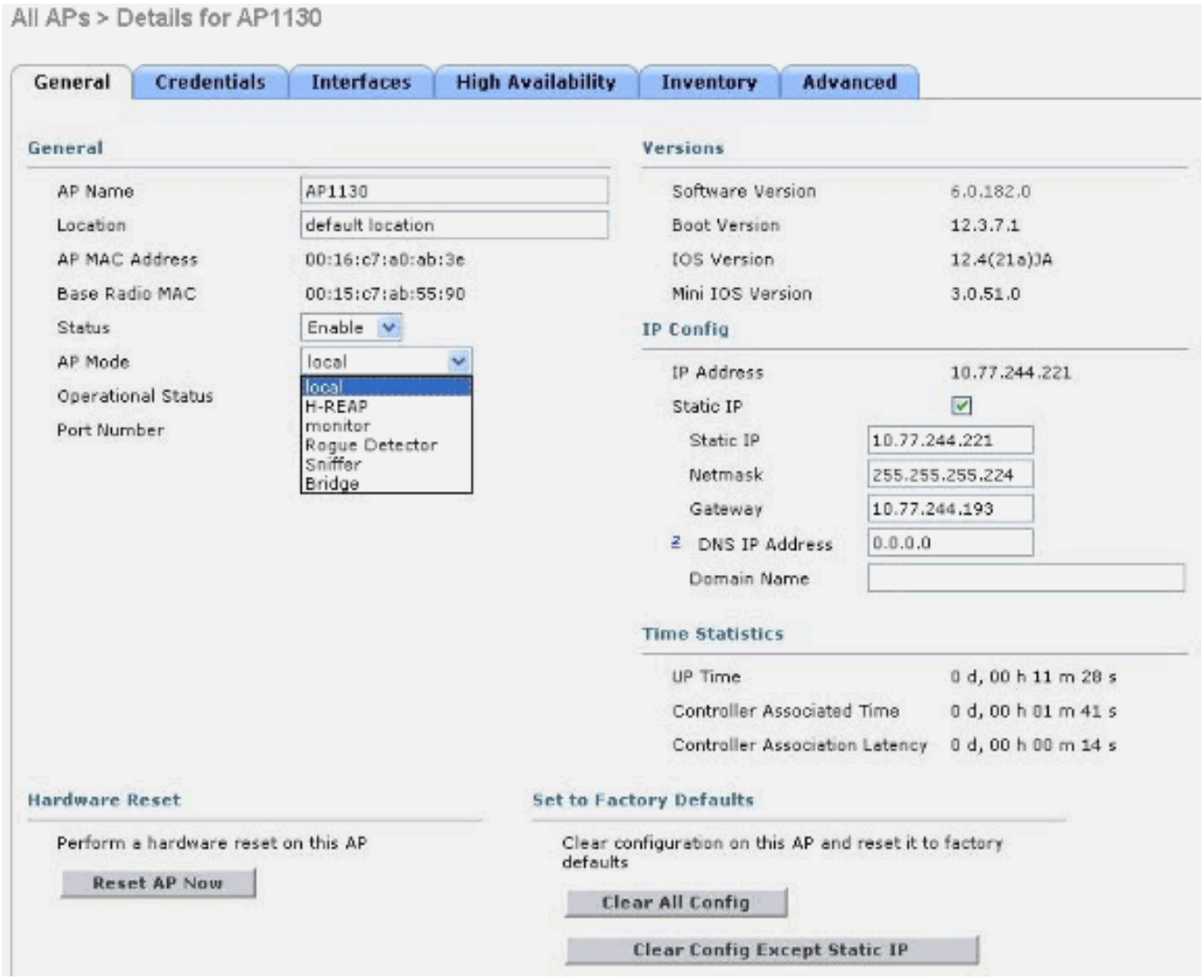
de clientes/APs não autorizados para o detector de não autorizados (RD). O RD as encaminha então para a WLC a fim de comparar com os MACs dos clientes que os APs da WLC ouviram no ar. Se os MACs combinam, a WLC sabe que o AP não autorizado ao qual esses clientes estão conectados está na rede com fio.

- **Modo sniffer** - Um LWAPP que opera no modo sniffer funciona como um sniffer e captura e encaminha todos os pacotes em um canal específico para uma máquina remota que executa o Airopeek. Esses pacotes contêm informações de marca de hora, intensidade de sinal, tamanho do pacote e assim por diante. O recurso de sniffer pode ser habilitado somente quando você executa o Airopeek, um software analisador de rede de outro fabricante que oferece suporte à decodificação de pacotes de dados.
- **Modo de Bridge** — O modo de Bridge é usado quando os Access point setup em um ambiente da malha e são usados para construir uma ponte sobre entre se.

Q. Como eu mudo o modo em um Access point de pouco peso?

A. A fim mudar o modo de um Access point de pouco peso, termine estas etapas.

1. Do WLC GUI, escolha o **Sem fio > os Access point > todos os APs**, e selecione o AP para que o modo precisa de ser mudado da lista de APs registrados.
2. **O todo o APs > detalhes para a** página **AP** aparece. **No tab geral d**esta página, selecione o **modo AP do** menu suspenso, como mostrado:



Q. Instalei recentemente pontos de acesso LAP-1131AG que foram direcionados a uma controladora específica. A versão da minha controladora é 4.0.155.5. Quando eu os inicializo com a mesma controladora Wireless LAN (WLC) para a qual eles apontam eventualmente a luz acende em verde. De acordo com a documentação, essa luz verde no LED de status significa que eles estão conectados à WLC. No entanto, não consegui encontrar esse ponto de acesso na lista de pontos de acesso da WLC. Por que isso ocorre? O Lightweight Access Point Protocol (LWAPP) se tornou associado?

A. Se o ponto de acesso estiver apontado para umaWLC na camada 3, mas não puder obter um endereço IP durante a inicialização, o LED de status da WLC acenderá em verde e não entrará sequência de busca e reinicialização até obter um endereço IP do DHCP.

Assim, nessas situações, o LED de status acender em verde não indica que o LWAPP está registrado na controladora. Após os pontos de acesso conseguirem obter seus endereços de DHCP, eles procuram a WLC e, se não a encontram, passam por um processo de reinicialização e continuam conforme o esperado. Há um bug associado a isso.

Consulte o bug da Cisco ID CSCsf10580 (somente clientes registrados) para obter mais informações.

Q. Que os diodos emissores de luz no REGAÇO indicam?

A. Esta é uma relação a um vídeo curto que explique como interpretar o diodo emissor de luz em um 1130AG AP de pouco peso:

Interpretando o diodo emissor de luz do REGAÇO - LAP1130

Q. Qual é a diferença entre pontos de acesso de telhado (RAPs) e pontos de acesso de montagem em postes (PAPs) como modos de pontos de acesso em malha (MAPs) lightweight?

A. Estes são os modos que os MAPs externos podem operar como parte da rede de malha. A solução de rede de comunicação em malha, parte da solução de rede Cisco Unified Wireless, permite que dois ou mais MAPs lightweight Cisco Aironet comuniquem-se uns com os outros via um ou mais saltos Wireless para se unirem a LAN múltiplas ou para estender a cobertura wireless 802.11b.

Esses pontos de acesso são usados como parte da rede em malha e operam em dois modos:

1. RAP
2. PAP

RAP — Os mapas de Cisco que se operam no modo RAP são o nó do pai a toda a construção de uma ponte sobre ou rede de malha e conectam uma ponte ou uma rede de malha à rede ligada com fio. Consequentemente, pode haver somente um RAP para qualquer segmento em bridge ou de rede em malha. Em uma rede em malha, os MAPs Cisco são configurados, monitorados e operados através de qualquer controladora WLAN da Cisco (WLC) implantada. Qualquer MAP que tiver uma conexão com fio para a WLC assume o papel de RAP. Esse RAP usa a interface wireless backhaul para se comunicar com os PAPs vizinhos.

PAP — Os mapas de Cisco que se operam no modo PAP não têm nenhuma conexão ligada com fio a Cisco WLC. Eles podem ser completamente wireless e oferecer suporte a clientes que se comunicam com outros PAPs ou RAPs, ou podem ser usados para conectar a dispositivos periféricos ou a uma rede com fio. A porta Ethernet é desabilitar por padrão por razões de segurança, mas você deve habilitá-la para os PAPs.

Consulte a seção de Configuração Zero Toque do Guia de Implantação da Solução de Rede em Malha da Cisco para obter mais informações sobre como um MAP assume o papel de um RAP ou PAP.

Q. Como devo interpretar o padrão de radiação das antenas dos ponto de acesso lightweight 1000 Series (LAP)?

A. Os diagramas de azimute são obtidos geralmente com o dispositivo/antena na orientação de funcionamento normal (vertical, parte superior para cima, no centro do diagrama para o omni; horizontal, montagem no centro, sentido dianteiro para "0" no diagrama). O lado A é muito provavelmente dianteiro e representado na marca 0 para o azimute e na marca 90 para a elevação. O lado B é representado na marca 180 para o azimute e 270 para a elevação. O padrão não muda no espaço livre se a unidade for invertida. No entanto, as superfícies próximas podem causar a reflexão/absorção e alterar o padrão. Os objetos metálicos perto dos radiadores (dentro de ~2 comprimentos de onda ou assim) podem igualmente distorcer o teste padrão significativamente. O Guia de Referência da Antena do Cisco Aironet contém mais informações. As antenas da 1000 Series são explicadas na última seção do documento.

Q. É possível restringir quais APs podem se unir a uma controladora? Eu vejo a página SECURITY/AAA/AP Policies, onde é possível autorizar APs com o AAA ou o certificado. Sou capaz de adicionar um AP à lista da autorização, mas fazer isso restringe somente minha lista de autorização de APs que podem se unir à controladora?

A. Não, as controladoras lidam com os APs na forma "primeiro a chegar, primeiro a ser atendido". Você possivelmente pode jogar com os campos primários, secundários e terciários para aumentar as probabilidades de conexões de APs de sua preferência.

Q. Com o LWAPP, é possível determinar os SSIDs de um AP por AP individual? O que é preciso para poder ter APs específicos em uma zona que usa um SSID exclusivo e, em todo o resto, que usa um outro conjunto de SSIDs?

A. Com a opção de substituição de WLAN, você pode escolher quais SSIDs um AP oferece. As controladoras oferecem suporte somente até 16 SSIDs cada, assim pode escolher somente entre as 16 com suporte. Isto é feito por AP.

Q. Quando eu habilito alguns comandos do LWAPP comanda em meu LAP, recebo um erro informando que o comando está desabilitado. Por que isso ocorre?

```
AccessPoint#clear lwapp ap controller ip address
ERROR!!! Command is disabled.
```

A. Uma vez que seu AP tenha se unido com sucesso a uma controladora, os comandos do

LWAPP serão desabilitados. Para habilitar novamente os comandos do LWAPP, defina o nome de usuário/senha do AP na CLI da controladora com o comando **config ap username <name> password <pwd> <cisco-ap>/all**. Em seguida, você poderá executar **clear lwapp private-config** na CLI do AP para permitir a reexecução manual dos comandos de configuração do LWAPP do AP.

Nota: Se você está executando a versão 5.0 e mais recente WLC, use este comando ajustar o nome de usuário e senha no AP:

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

Q. Quando dois AP estão no mesmo canal e podem se ver, quais são as implicações (para produtividade de roaming, etc.) sobre o uso de quatro canais em vez de três? Como os APs reagem em tal situação, e como um cliente reage?

A. Se os AP estão no mesmo canal ou não, o roaming dos clientes não é particularmente afetado. O que importa é a sobreposição suficiente das células para que os clientes possam fazer transições suaves da área de cobertura de um AP para o próximo. A intenção da mudança de um design de três canais para um projeto de quatro canais é aumentar a flexibilidade do design (devido ao canal "extra"). Essa abordagem é míope porque, quando você adiciona um pouco de flexibilidade de implantação (como você possui outro canal), você na realidade aumenta a quantidade de interferência entre canais. O que você pode ganhar na flexibilidade do design com a abordagem de quatro canais, pode perder na interferência adicionada aos canais. Resultado: não use um design de quatro canais.

Q. Podemos controlar quando os clientes fazem roaming? Podemos deixar que o cliente faça roaming baseado unicamente na intensidade de sinal baseado em APs individuais e para todos os adaptadores clientes?

A. Hoje, roaming é sempre uma função do cliente, e a escolha de fazer roaming ou não é implementada de forma diferente em vários clientes. O roaming direcionado é uma parte do CCX, mas é um recurso opcional que não é usado hoje.

Q. Há alguma exigência ou recomendação específica para um link de WAN que seja implementado entre o AP REAP/HREAP no local remoto e a WLC no local principal?

A. Estes são alguns dos principais fatores a serem considerados para o link de WAN:

- Certifique-se de que a largura de banda do link de WAN seja pelo menos 128kbps.
- Assegure-se de que a latência ou o retardo round trip entre os dois locais através da relação MACILENTO não sejam mais do que 300ms porque mais do que um atraso 300ms podem criar problemas de autenticação ao cliente, especialmente quando a autenticação central for executada.

Q. Eu tive uma rede desligada por algumas horas devido à perda de comunicação dos LAPs com as WLCs. Depois que a rede voltou a funcionar, os LAPs obtiveram o endereço IP do servidor DHCP, ainda que esses AP estivessem configurados

com um endereço IP estático. No comando "show ap config general <ap-name>", "Fallback IP Address" é mostrado. Por que isto acontece?

A. O LAP tenta se associar à WLC até 20 vezes com mensagens de descoberta LWAPP. Caso não consiga se conectar, ele tentará obter um endereço IP novo via DHCP. Se o LAP conseguir obter um endereço IP do servidor DHCP, esse endereço IP se tornará ativo, e o endereço IP atribuído estaticamente será usado como reserva. A ideia por trás disso é que, caso os LAPs sejam movidos para uma VLAN diferente (por exemplo, em outro prédio), eles sejam capazes de recuperar um endereço IP e se unir a uma WLC. Este comportamento é explicado no bug CSCse66714. Você deve fazer a atualização da WLC para o software release 4.0.206.0.

Q. É obrigatório configurar um nome de grupo de bridge para uma rede em malha?

A. Um nome de grupo de bridge (BGN) pode ser usado para agrupar logicamente os APs na malha. Embora os APs venham por padrão com um valor nulo de BGN para permitir a associação, recomendamos que você defina um BGN. Você pode fazer essa alteração de configuração com a CLI ou a GUI através deste comando:

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

Nota: Os BGNs podem conter no máximo dez caracteres. Se você entra em mais do que os caráteres 10 no BGN colocam na página da configuração do ponto de acesso da malha do controlador GUI, gerencie um Mensagem de Erro. Um erro igualmente aparece quando você configura este parâmetro com o comando CLI de **Cisco_MAP do nome de grupo do bridgegroupname ap da configuração** ou o WCS **ajustado** (CSCsk64812).

Ao configurar o BGN em uma rede ativa, certifique-se de configurar do MAP mais distante e descobrir o caminho de volta para o RAP. Isso é muito importante porque você pode travar um MAPA filho que não é capaz de se associar a um pai, o qual pode ter um BGN atualizado. Use BGNs diferentes para agrupar logicamente partes diferentes da sua rede. Isso é útil nas situações em que você possui RAPs dentro da mesma área de RF e você deseja manter separados segmentos da sua malha.

Se você desejar adicionar um AP novo a uma rede ativa, será necessário pré-configurar o BGN no AP novo. Se você ativar a rede em malha do zero com APs novos que nunca foram configurados, o BGN estará pré-definido nos APs como um valor nulo. Os AP se unem em uma nova rede com esse valor padrão do BGN. Você pode verificar o BGN de um AP com este comando:

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

Q. O que acontece se o BGN não for configurado corretamente?

A. Se o AP for provisionado incorretamente com um nome de grupo de bridge diferente daquele ao qual ele se destina, dependendo do design da rede, esse AP poderá ou não ser capaz de encontrar seu setor ou árvore corretos. Se ele não puder alcançar um setor compatível, ele poderá travar. Para recuperar esse AP travado, o conceito de nome de grupo de bridge foi introduzido. A idéia básica é que um AP que normalmente é incapaz de se conectar a qualquer

outro AP com seu nome de grupo de bridge configurado tente se conectar ao nome de grupo de bridge padrão.

Este é o algoritmo usado para detectar essa condição de travamento e a recuperação:

1. Faça a varredura passiva e encontre todos os nós vizinhos, independentemente de seus nomes de grupo de bridge.
2. O AP tenta se conectar aos vizinhos que são ouvidos com seu próprio nome de grupo de bridge com o Adaptive Wireless Path Protocol (AWPP).
3. Se o passo 2 falhar, tente conectar usando o nome de grupo de bridge padrão ao AWPP.
4. Para cada tentativa que falhar do passo 3, adicione o vizinho à lista de exclusões e tente se conectar ao melhor vizinho seguinte.
5. Se o AP falhar ao se conectar a todos os vizinhos do passo 4, reinicialize o AP.
6. Se conectado com o nome de grupo de bridge padrão por 30 minutos, faça novamente a varredura de todos os canais e tente se conectar com o nome de grupo de bridge correto.

Nota: Quando um AP consegue se conectar com o nome de grupo de bridge padrão, o nó pai relata o AP como uma entrada de filho/nó/vizinho na controladora da WLAN, de modo que um administrador de rede é informado sobre o AP travado. Tal AP não pode aceitar nenhum cliente ou outros nós da malha como seus filhos, nem pode transmitir tráfego de dados.

Q. Um LAP 1030 pode formar uma bridge com outros modelos de bridge? Da mesma forma, um LAP 1020 oferece suporte a bridges?

A. O LAP modelo 1020 não oferece suporte a bridges. O LAP 1030 oferece suporte a bridges (um salto) para outro LAP 1030, mas para o BR1310, BR1400 ou o LAP 1500 no momento.

Q. É possível configurar uma bridge wireless entre APs LAP? Eu gostaria que um rádio em meus LAPs sem fio formassem uma ponte de volta para os LAPs da bridge raiz com fio (LAP conectado a uma WLC). É isto possível?

A. No. Isso não pode ser feito em APs LAP. APs em malha podem formar bridges ponto a ponto básicas em uma rede Cisco Unified Wireless. A única outra bridge possível é com APs IOS no modo WGB (bridge de grupo de trabalho). Esses APs IOS atuam como clientes (com os dispositivos com fio por trás deles) para um AP LAP. Mas os clientes wireless não podem se conectar a esses APs IOS.

Q. Eu tenho um LAP 1131, e este ponto de acesso foi registrado com sucesso nas controladoras Wireless LAN. Quando eu conecto o Access point sem o injetor de energia, os rádios estão acima (o status LED é verde), mas quando eu conecto o AP com o injetor de energia, os rádios estão para baixo (o status LED é alaranjado). Como mim pode a resolução isto emitir?

A. Esta edição pode ser devido à potência incorretamente configurada sobre parâmetros dos Ethernet (PoE); termine estas etapas a fim resolver esta edição:

1. Clique o **Sem fio** a fim alcançar estes parâmetros.
2. Clique a relação do **detalhe do** Access point desejado. Os parâmetros novos aparecem no todo o página APs > de detalhes sob os ajustes PoE.
3. No a página APs > de detalhes do Access point para os ajustes PoE, **estado do injetor de**

energia do clique, e escolhe **instalado**.

4. Marque a caixa de verificação para habilitar o estado do injetor de potência para o ponto de acesso. Este parâmetro é obrigatório quando o switch conectado não oferece suporte ao IPM e um injetor de potência é usado. Esse parâmetro não é necessário quando o switch conectado oferece suporte ao IPM.

Q. Em AP autônomos, o encaminhamento de pacotes seguro e público (PSPF) é usado para impedir que os dispositivos clientes associados a este AP compartilhem inadvertidamente arquivos com outros dispositivos clientes na rede wireless. Há alguma característica equivalente em APs lightweight?

A. A característica ou o modo que executa a função similar de PSPF na arquitetura de pouco peso são chamados modo de bloqueio partilha de arquivos. O modo de bloqueio peer-to-peer está disponível nas controladoras que gerenciam o LAP.

Se este modo está desabilitado no controlador (que é a configuração padrão), permite que os clientes Wireless comuniquem-se um com o otro através do controlador. Se o modo estiver habilitado, ele bloqueará a comunicação entre os clientes através da controladora.

Ele funciona somente entre os AP que se uniram à mesma controladora. Quando habilitado, este modo não impede que os clientes wireless terminados em uma controladora cheguem até os clientes wireless terminados em uma controladora diferente, mesmo quando no mesmo grupo de mobilidade.

Q. Um AP LAP pode lidar com mensagens SNMP da mesma forma que um AP IOS?

A. Os APs LAP não podem lidar com mensagens SNMP por conta própria. Para lidar com mensagens SNMP, você deve configurar uma comunidade SNMP na WLC em que o LAP está registrado. Todas as informações do AP são controladas pela WLC.

Informações Relacionadas

- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Módulos de controlador de LAN do Cisco Wireless
- Controlador de LAN do Cisco Wireless (WLC) FAQ
- Guia de Configuração da Cisco Wireless LAN Controller Release 3.2
- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Suporte Técnico e Documentação - Cisco Systems