Perguntas freqüentes sobre o ponto de acesso Cisco Aironet

Índice

Introdução

Este documento dá respostas às perguntas mais frequentemente feitas (FAQ) sobre os Pontos de Acesso do Cisco Aironet (AP).

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

Projete o FAQ

Q. Que é o nome de usuário padrão e a senha para Cisco IOS® Software-based APs?

A. O Cisco IOS AP com base no software tem uma configuração padrão que inclua um nome de usuário e uma combinação de senha, ambos são **Cisco** (diferenciando maiúsculas e minúsculas). Depois que você restaura aos padrões de fábrica, esteja pronto para dar à Cisco como ambos o nome de usuário e senha quando o GUI ou a interface de linha de comando (CLI) o alertam.

Q. Que cabo devo usar para uma conexão de console?

A. Use um cabo direto com o conector macho de nove pinos ao conector fêmea da nove pinos com o objetivo de conectar a porta COM1 ou COM2 em seu computador à porta RS-232 no AP. Use um programa de simulação terminal em seu computador, como:

- Microsoft Windows Hyper Terminal
- Symantec ProComm
- Minicom

Use estas configurações de porta:

Velocidade:	9.600 bps (bits por segundo)
Bit de dados:	8

Bit de interrupção:	1
Paridade	Nenhum
Controle de fluxo:	Xon/Xoff

Nota: Se o controle de fluxo Xon/Xoff não funciona, tente usar o controle de fluxo Nenhum.

Q. Eu tenho um Aironet 1231 AP. A Cisco faz um cabo de extensão 50-pés para que eu possa ter o AP em uma área e a antena em outra?

A. Sim, o número da peça do cabo 50-pés é AIR-CAB050LL-R. Você pode usar este cabo para conectar seu AP à antena.

Q. Como você verifica o tipo de rádio no AP autônomo?

A. Você pode usar o **mostrar o comando controllers do** modo de EXEC privilegiado no AP PARA obter a informação no tipo de rádio.

Q. Como você estabelece um endereço IP no AP?

A. Por padrão, o AP pede um endereço IP por DHCP.

Os Cisco IOS Versão 12.3(2)JA e mais recente mudam o comportamento padrão dos APs solicitando um endereço IP de um servidor DHCP:

- Quando você conecta um 1200 ou 1230 series AP com configuração padrão a seu LAN, o AP pede um endereço IP de seu servidor DHCP. Se não receber um endereço, continua a enviar pedidos indefinidamente.
- Quando você conecta um 1100 Series AP com uma configuração padrão a seu LAN, o 1100 Series AP faz diversas tentativas de obter um endereço IP do servidor DHCP. Se não receber um endereço, ele irá atribuir o endereço IP 10.0.0.1 por cinco minutos. Durante esta janela de cinco minutos, você pode navegar pelo endereço IP padrão e configurar um endereço estático. Se após cinco minuto o AP não for reconfigurado, ele irá rejeitar o endereço de 10.0.0.1 e reverter solicitando um endereço do servidor DHCP. Se não receber um endereço, irá enviar pedidos indefinidamente. Se você perder a janela de cinco minutos para navegar ao AP em 10.0.0.1, você pode virar o ciclo de energia do AP para repetir o processo.

Você também pode ajustar o endereço IP do AP manualmente. Em Microsoft Windows PC que está conectado ao segmento de Ethernet, do prompt do DOS, prepare o comando:

```
arp -s a.b.c.d 00-12-34-56-78-90
```

Nota: O termo *a.b.c.d representa o* IP address que deve ser ajustado no AP, e 00-12-34-56-78-90is o MAC address. Este endereço aparece no painel na parte inferior do AP.

Emita este comando a fim verificar o endereço:

```
ping a.b.c.d
```

Nota: Este procedimento não funciona se o AP já tenha sido atribuído ao endereço IP por um outro método.

Q. Como você habilita o acesso HTTPS no AP?

A. A fim permitir o HTTPS, você deve adicionar este comando a seu AP:

```
AP(config)#ip http secure-server
```

Quando você adiciona o comando **ip http secure-server**, você vê as chaves RSA exigidas para uma comunicação segura regenerada nos APs.

Q. Como um cliente escolhe um ponto de acesso (AP) a ser associado?

A. A escolha do Access Point (AP) é feita na máquina de rádio do cliente. Baseado no fabricante, motorista, tipo de cartão, e assim por diante, pode usar métricas diferentes para fazer a escolha. O mecanismo o mais comum da afiliação AP usado na maioria de clientes é baseado na intensidade de sinal recebida pelo cliente dos AP. O padrão 802.11 exige somente que o cartão do cliente Wireless relate a intensidade do sinal com uma métrica simples chamada Receiver Signal Strenght Indicator (RSSI). O cliente se associa então com o AP com o sinal o mais forte. É conhecido que estes algoritmos podem conduzir a um desempenho ruim. O motivo principal é devido a sua falta do conhecimento da carga em APs diferentes.

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. Desde que não há nenhum túnel da mobilidade entre o controlador do Wireless LAN e os AP autônomos, o roam não funciona.

Q. Como você estende a cobertura do AP?

A. Há diversas maneiras de estender a área de cobertura para um AP. Estes são os métodos os mais importantes:

- Use APs no modo de repetição.
- Use um AP secundário no modo AP com canais não sobrepostos.
- Mude o parâmetro de nível da potência do transmissor do AP existente a fim estender a cobertura.
- Posicione o APs de forma otimizada.

Refira aos métodos WLAN Radio Coverage Area Extension para uma descrição completa de como executar estes métodos.

Q. Que são as implicações se seu AP está no modo repetição?

A. A porta Ethernet é desativada no modo de repetição. O throughput efetivo é cortado ao meio uma vez para cada salto longe do AP pai.

A fim de estabelecer repetição, você deve habilitar extensões Aironet no ponto de acesso do pai (raiz) e nos pontos de acesso de repetição. As extensões Aironet, que são permitidas por padrão, melhoram a capacidade do ponto de acesso para compreender as capacidades dos dispositivos do cliente Cisco Aironet associados ao ponto de acesso. Se você desabilitar as extensões Aironet, você pode às vezes melhorar a interoperabilidade entre o ponto de acesso e os dispositivos cliente não-Cisco. Os dispositivos cliente não-Cisco podem encontrar uma comunicação difícil com os pontos de acesso de repetição e o ponto do acesso raiz a que a repetição foi associada.

A infra-estrutura SSID deve ser atribuída ao VLAN nativo. Se mais de um VLAN for criado em um ponto de acesso ou ponte Wireless, uma infra-estrutura SSID não pode ser atribuída a um VLAN não-nativo. Esta mensagem aparece quando a infra-estrutura SSID é configurada no VLAN não-nativo:

```
AP(config)#ip http secure-server
```

Porque os pontos de acesso criam uma interface virtual para cada interface de rádio, os pontos de acesso do repetidor associam ao ponto do acesso raiz duas vezes: uma vez para a relação real e uma vez para a interface virtual.

Nota: Você não pode configurar VLAN múltiplos em pontos de acesso de repetição. Os pontos de acesso de repetição suportam somente o VLAN nativo.

Q. Que são as características apoiadas pela opção da Extensão Aironet?

A. A Extensão Aironet é uns recursos proprietários executados pela Cisco. As extensões Aironet contêm os elementos de informação que apoiam estas características.

- **Balanceamento de carga:** O ponto de acesso usa extensões Aironet para dirigir dispositivos do cliente a um ponto de acesso que forneça a melhor conexão à rede baseada na rede em fatores tais como o número de usuários, de taxas de erros de bits, de carga e de intensidade do sinal.O balanço de carga é propriedade entre os dispositivos que compreendem as extensões Aironet. O balanço de carga é executado por extensões nas balizas AP e/ou prova-resposta, que fornecem a informação nestes:Intensidade de sinal da estação-baseCarga da estação base (% do transmissor ocupado)Número de saltos ao backboneNúmero de associações clienteO cliente avalia estes e associa-os ao “melhor”. Os clientes não-Cisco não compreendem estas extensões.
- **MIC:** Cisco Proprietary Message Integrity Check (MIC) - O MIC é uns recursos de segurança adicional WEP que previne o ataque aos pacotes criptografados chamados ataques bit-flip. O MIC é executado no ponto de acesso e em todos os dispositivos cliente associados.
- **O Cisco Proprietary Temporal Key Integrity Protocol (CKIP)**, também é conhecido como o chave hashing de WEP, é um recurso de segurança WEP adicional que defende contra um ataque no WEP, em que o intruso usa um segmento não criptografado chamado de vetor de inicialização (iv) em pacotes criptografado para calcular a chave de WEP.
- Além destes, as extensões Aironet levam mais informações que incluem:Carga atualmente suportada pelo APNúmero de saltos da rede cabeadaTipo de dispositivo, que as ajudas identificam o produto sob Cisco system para a gestãoNome de dispositivoNúmero de clientes associadosTipo de rádio, uma característica usada para determinar certas características sobre o rádio, tal como a taxa de dados, o tipo de rádio (1310, 1200, 352 ou 342), o tipo da

segurança (WEP/802.1x), etc.

Os dispositivos que são CCX compatível também podem aproveitar-se de algumas das características da extensão Aironet. Está aqui uma lista das características disponíveis com as versões diferentes das extensões compatível Cisco:

Extensões compatíveis Cisco - Versões e Características

Q. Você pode conectar dois computadores sem um AP através das placas de interface Wireless?

A. Yes. Pelo Aironet Client Utility (ACU) você pode configurar os clientes para ser executado no modo adhoc. Esta conexão é somente uma conexão peer-to-peer. Um PC transforma-se o pai e controla-se a conexão. Os outros PCs no modo adhoc são estações filhos.

Q. Você precisa o hardware especial de apoiar a criptografia?

A. O modelo de hardware específico determina o nível de criptografia para a unidade:

- Os modelos 341 e 351 apoiam somente a criptografia 40-bit.
- Os 342 e 352 modelos apoiam amba a criptografia de 40- e de 128-bit.
- Todos os modelos 1100, 1200, e 1300 series apoiam a criptografia de 40- e de 128-bit.

Q. É possível ver todos os AP e seus clientes associados que pertencem a essas rede particular/infra-estrutura apenas de um único AP?

A. Isto é possível de um VxWorks AP. Um único VxWorks AP pode indicar todos os clientes e seus AP em uma rede. Isto pode ser conseguido se você clicar em **Association > Entire Netowork > Apply**. Em um AP com base em IOS, não indica todos os clientes associados nessa rede sem a ajuda de um gerenciador de dispositivo, tal como o WLSE, com um AP como o WDS ou um controlador se a imagem no AP é uma imagem LWAPP.

Q. Eu uso o CCKM em minha rede, mas o processo de autenticação inteiro ocorre sempre que o dispositivo do cliente estiver em roaming. Resumindo, o roaming rápido e seguro não funciona como esperado. Por que?

A. Isto é possivelmente devido ao erro CSCsg10128. Este erro é fixado na versão 3.1.03.

Q. Os pontos de acesso da Cisco dão suporte à característica UniDirectional Link Detection (UDLD) para desligar a conexão Ethernet aos interruptores se há uma falha de cabo da C amada 1/Camada 2?

A. Não, pontos de acesso da Cisco não suportam a característica UDLD.

Q. Como você fornece energia ao Aironet AP?

A. As opções de energia para seu AP dependem do modelo AP que você tem. Refira ao Cisco Aironet e às opções de energia do WLAN Controller Product para mais informação.

Q. Eu tenho um AP1010, AP1030, e um AIR-LAP-1232AG. É possível usar um WS-PWR-PANEL para a potência sobre Ethernet (PoE)?

A. O WS-PWR-PANEL apoia somente pontos de acesso com um único rádio. Refira à matriz de compatibilidade disponível no *Cisco PoE e Cisco Intelligent Power Management* seção de Cisco Aironet Power Over Ethernet Application Note para mais informações.

Q. Como você salva a configuração do AP?

A. As alterações à configuração são salvas imediatamente. Você pode despejar a configuração atual em formato de texto no **menu de instalação**. Então, escolha **Cisco Services > Manage System Configuration** e faça o download da configuração de sistema.

Q. Como eu determino a freqüência específica ou a canalizo para meu AP ou ponte?

A. Use o **comando show controllers dot11Radio0** a fim mostrar a freqüência e canalizá-la que o AP ou a ponte estão ligada. Este exemplo de saída mostra onde encontrar a informação:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Q. Como eu faço meu trabalho AP com outros dispositivos do IEEE 802.11B?

A. A fim permitir que o AP se comunique com outro dispositivo 802.11b, desligue extensões Aironet. Verifique a caixa de verificação **Non-Aironet 802.11** no indicador da instalação expressa. Alternativamente, você pode clicar o botão de rádio da **usar extensão Aironet** na janela Advanced AP Radio.

Q. Que dispositivos podem se associar a um AP?

- AP ao cliente
- AP ao AP (no modo de repetição)
- AP (no modo de repetição) à estação base (no modo AP)
- AP à ponte do grupo de trabalho

Q. Qual a freqüência em que um AP comunica-se?

A. Nos Estados Unidos, o IEEE 802.11B AP transmite e recebe em um de 11 canais dentro da frequência 2,4 GHz. O IEEE 802.11a AP transmite e recebe em um de oito canais na freqüência 5GHz. O IEEE 802.11g APs transmite e recebe em um de 11 canais dentro das frequência 2,4 GHz. Estas são áreas de freqüência pública e são não-licenciadas pelo FCC.

Q. Como você fixa os dados através de um link do rádio AP?

A. Há diversos métodos para fazer seus dados seguros através de uma conexão AP Wireless. A fim aprender mais sobre os diferentes métodos de segurança, refira ao FAQ em Cisco Aironet Wireless Security.

Q. Quantos clientes podem se associar ao AP?

A. O AP tem a capacidade física para cuidar de 2048 endereços MAC, mas, por o AP ser um meio compartilhado e atuar como um hub Wireless, o desempenho de cada usuário é reduzido conforme o número de usuários aumenta em um AP individual. Idealmente, não mais de 24 clientes podem associar com o AP porque a produção do AP é reduzida com cada cliente que associa ao AP.

Q. Há uma limitação no número de filtros de endereços MAC que podem ser configurados no AP?

A. Você pode usar o CLI a fim configurar até 2.048 endereços MAC para filtrar, mas, com o uso da relação do web browser, você pode configurar somente até 43 endereços MAC para filtrar.

Q. Qual é o intervalo típico para um AP?

A. A resposta a esta pergunta depende de muitos fatores, que incluem:

- A taxa de dados (largura de faixa) desejado
- Tipo de antena
- Comprimento do cabo de antena
- O dispositivo que recebe a transmissão

Numa instalação ideal, o alcance pode ser de até 90 m.

Q. Quais são os ajustes disponíveis do nível de potência de transmissão para o 1200 AP?

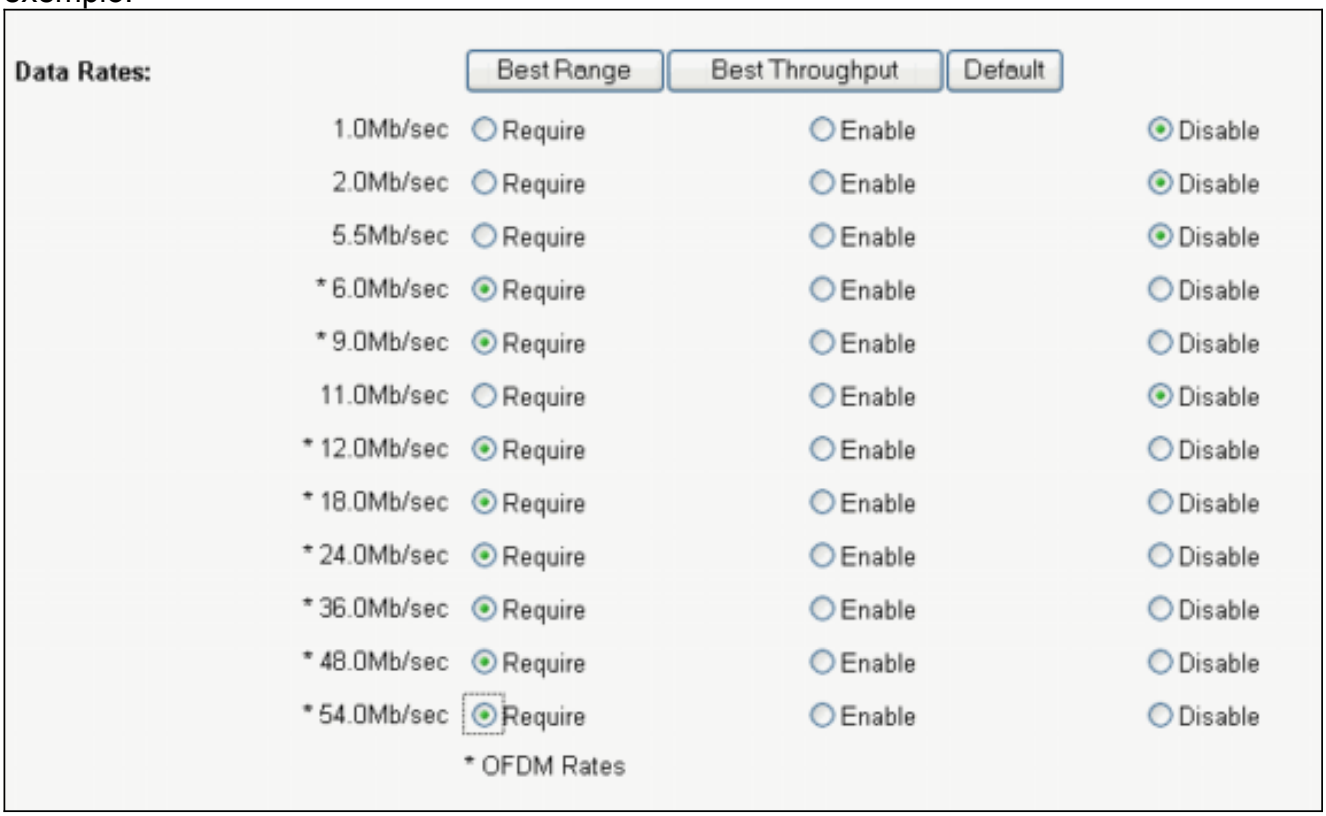
A. Os ajustes de potência de transmissão são diferentes e dependem do rádio que é usado. Refira a Cisco Airnet 1200 Series Access Point Data Sheet para a lista completa de níveis da configuração de energia. Devido às configurações de energia variarem com base no canal, execute uma análise do local. A análise de local é importante a fim conseguir informação precisa referente ao ajuste a ser usado. Refira ao Wireless Site Survey FAQ para detalhes na análises do local.

Q. Como eu posso ajustar o AP de modo que somente os clientes de IEEE 802.11g possam se conectar? Eu não quero que os clientes do IEEE 802.11B se conectem e retardem a rede Wireless. Há uma segunda rede paralela 802.11b para clientes não seguros.

A. Para que o AP receba somente os clientes 802.11g, complete estas etapas no GUI:

1. Vá à seção das interfaces de rede e clique o **Radio0-802.11G**.

2. Clique na aba dos **ajustes** na parte superior do indicador do Radio0-802.11G.
3. Selecione **Desabilitar** para estas taxas de dados: 1.02.05.511.0
4. Escolha **Requerido** para todas as taxas de dados restantes. Estas são as outras taxas de dados: 6.09.012.018.024.036.048.054.0
5. Clique em**Aplicar** na parte inferior da janela. Esta janela oferece um exemplo:



Q. É verdade que se eu permito somente clientes IEEE 802.11g em uma rede Wireless, estes não podem interferir com uma rede paralela do IEEE 802.11B porque usam esquemas de modulação diferentes?

A. Não, isto não é verdade. Estes clientes 802.11g podem interferir se usarem a mesma freqüência. Certifique-se usar canais diferentes. Os três canais nonoverlapping são 1, 6, e 11.

Q. Que é a velocidade da porta Ethernet AP?

A. A porta Ethernet AP suporta o 10 Mbps ou o 100 Mbps sobre um conector RJ-45, ou um meio duplex ou duplex completo. Configure a velocidade e duplex aos mesmos ajustes que seu interruptor ou hub.

Q. Há um mecanismo para o falha ou redundância para meu AP?

A. Sim, você pode configurar o hot standby a fim fornecer a redundância caso o AP preliminar falhar. Refira os Release Note para Access point do Cisco Aironet para mais informação.

Q. O que é uma chave de WEP?

A. O WEP representa o Wired Equivalent Privacy. Você pode usar o WEP para criptografar e decifrar os sinais de dados que transmitem entre dispositivos do Wireless LAN (WLAN). O WEP é

uma característica opcional do IEEE 802.11 que previne a divulgação e a alteração dos pacotes no trânsito e também forneça o controle de acesso para o uso da rede. O WEP faz um link WLAN tão seguro como um link cabeado. Conforme especificado pelo padrão, o WEP usa o algoritmo RC4 com uma chave 40-bit ou 10-bit. O RC4 é um algoritmo simétrico porque o RC4 usa a mesma chave para a criptografia e a decifração dos dados. Quando o WEP é habilitado, cada estação de rádio tem uma chave. A chave é usada para misturar os dados antes da transmissão dos dados através das ondas de rádio. Se uma estação recebe um pacote que não esteja misturado com a chave apropriada, a estação rejeita o pacote e nunca entrega tal pacote ao host. Refira ao Wired Equivalent Privacy (WEP) em Aironet Access Points e o Exemplo de Configuração de Pontes para obter informações sobre de como configurar o WEP.

Q. Quando você usar o protocolo light extensible authentication (LEAP), que número de porta você especifica a fim se comunicar com seu Cisco Secure Access Control Server (ACS)?

A. Por padrão, o ACS escuta um pedido de autenticação na porta 1645 e a contabilidade na porta 1646, mas você pode configurar a porta 1812 para a autenticação e 1813 para contabilidade. Confirme que estas portas estão ajustadas corretamente na página de instalação do Authentication Server no AP.

Q. No Cisco IOS Software-based AP, você pode executar as chaves do Wired Equivalent Privacy (WEP) e o Extensible Authentication Protocol (EAP) junto na mesma autenticação para AP? Isto funcionou com AP com base em VxWorks.

A. Não, você não pode executar chaves de WEP estáticas para a criptografia e EAP para a autenticação no mesmo Service Set Identifier (SSID). VxWorks permitiu esta configuração devido à vulnerabilidade de software, mas esta capacidade não é uma característica. O que você pode fazer é criar dois SSID e dois VLAN (um pelo SSID). Então, configurar a autenticação aberta com o WEP para um SSID e a autenticação de EAP para o outro SSID.

Q. Você realmente precisa realizar uma análise de site?

A. Yes. Devido à natureza sensível de transmissões da freqüência de rádio (fr), você deve conhecer os outros tipos de tráfego RF que podem estar em seu ambiente, mesmo sem seu conhecimento da presença do tráfego. Uma análise de site permite uma compreensão melhor desta ameaça invisível ao bom desempenho de seus dispositivos Wireless. A análise de site igualmente ajuda seu instalador profissional a assegurar a cobertura RF desejada. Refira à análise de site Wireless FAQ.

Q. Se você tentar alterar o AP e você está alertado para um nome de usuário e senha, o que você deve digitar?

A. Uma alerta para o nome de usuário e senha indica que o gerenciador de usuário foi habilitado. Refira seu administrador AP a fim encontrar o nome de usuário e senha para usar-se. Se você é o administrador AP e não conhece o que estas contas de usuário são, você precisa de executar uma recuperação de senha. Refira ao procedimento de recuperação de senha para o equipamento Cisco Aironet.

Q. Você pode usar duas antenas externas a fim cobrir duas células de rádio (por exemplo, antena 1 para a pilha 1 e antena 2 para a pilha 2)?

A. Você não pode usar duas antenas em um AP a fim cobrir duas células de rádio. As tentativas de usar as antenas para cobrir duas células de rádio podem resultar em problemas de conectividade. A finalidade das duas antenas é aumentar a cobertura de uma pilha em um esforço para superar as edições que elevaram com distorção de multipath e o sinal anula. Refira a Multipath e a diversidade para obter mais informações sobre da diversidade e das distorções de multipath.

Q. Qual é o uso do comando mobility network-id em um AP?

A. Você usa o **comando mobility network-id** a fim configurar a mobilidade da camada 3 em uma rede Wireless. Você usa o **comando mobility network-id ssid** a fim associar um Service Set Identifier (SSID) a um ID de rede da mobilidade da camada 3. Com mobilidade da camada 3, os clientes podem fazer o roaming aos diferentes APs que residem em sub-redes diferentes. Os clientes em roaming ficam conectados a sua rede e não mudam endereços IP.

Você deve usar um módulo de serviços (WLSM) do Wireless LAN (WLAN) como seu dispositivo dos serviços do domínio Wireless (WDS) a fim configurar corretamente a mobilidade da camada 3. A mobilidade da camada 3 não é apoiada quando você usa um AP como seu dispositivo WDS. Para obter mais informações sobre da mobilidade da camada 3, refira a *Compreendendo a Mobilidade da Camada 3*seção Configurando o WDS, Roaming Rápido e Seguro, e Gestão de Rádio.

O comando deve ser usado quando o AP participa em uma infra-estrutura WDS com um módulo WLSW (que atua no dispositivo WDS) onde há uma mobilidade da camada 3. Se você usa este comando incorretamente, resulta em problemas de conectividade na rede de WLAN como:

- Os clientes não obtêm endereços IP do DHCP.
- Em alguns casos, os clientes não podem se associar ao AP.
- Os clientes Wireless não podem se associar ao AP.
- A autenticação do Extensible Authentication Protocol (EAP) não acontece. Com o **comando mobility network-id** configurado, o AP tenta construir um túnel de encapsulamento de roteamento genérico (GRE) para a transmissão dos pacotes EAP. Se nenhum túnel for estabelecido, os pacotes não podem ir em qualquer lugar.
- O AP configurado como um dispositivo WDS não funciona como esperado, e a configuração WDS não funciona.

Q. Quantos identificadores do conjunto de serviço (SSID) podem existir pelo VLAN?

A. Você pode ter somente um SSID pelo VLAN. O uso de múltiplos SSID sobre um único VLAN não é apoiado no Aironet AP.

Q. Que é o valor BSSID quando ESSIDs múltiplos são atribuídos aos APs?

A. Se o AP está sendo executado no modo leve, a seguir cada ESSID em um AP será tratado através de um BSSID diferente (onde cada BSSID é baseado na base de rádio MAC, e difere somente no low-order-nibble.)

Se o AP for ser executado em IO, a seguir todo o ESSIDs no AP será tratado através do mesmo BSSID (a menos que MBSSID seja configurado, neste caso será tratado através de BSSIDs diferente).

Q. É possível estabelecer meu rádio A para a ponte e o rádio G para a funcionalidade AP? Se sim, como posso eu fazer isto?

A. Sim, é possível estabelecer cada rádio em seu AP para a funcionalidade diferente. Em seu cenário, isto pode ser feito se você estabelecer identificadores diferentes do conjunto de serviço (SSID) para o rádio G e A. Então, estabeleça o papel em um parâmetro da rede de rádio para o rádio G ao AP e para o rádio A à ponte-raiz.

Q. Quando dois clientes se associam a dois AP diferentes que são conectados na mesma sub-rede, a comunicação acontece através da rede ligada com fio ou acontece sem fio?

A. Para este cenário, se os dois AP são ajustados ao modo de raiz, a comunicação entre os dois AP é feita através da rede cabeada. Se um dos AP está ajustado ao modo repetição e o outro AP está ajustado ao modo raiz, a comunicação entre os APs acontece sem fio.

Q. Você pode permitir o roteamento ou a tradução de endereço de rede (NAT) no Cisco AP?

A. Não, a distribuição e os recursos NAT não são suportados em AP.

Q. Há uma maneira de programar um horário em que o Cisco IOS AP com base no software está disponível? Eu quero fornecer o acesso baseado em tempo aos clientes que se conectam ao AP.

A. Você pode configurar as lista de controle de acesso com base no período (ACL) com uso dos intervalos de tempo. Os ACL com base no período ajudam-no a certificar-se de que os usuários podem alcançar a rede Wireless dentro de um período de tempo particular, por exemplo, 9:00 A M. a 5:00 P.m. (0900 1700). O uso de ACL com base no período não fecha o AP ou o rádio. Os ACL com base no período param a passagem do tráfego no AP de modo que os usuários não possam acessar a rede. Para obter informações sobre de como configurar esta característica, refira os *ACL com base no período usando a seção de intervalos de tempo de* Listas de acesso de ConfiguringIP.

Q. Podem os AP ter conjuntos de DHCP múltiplos através das sub-redes diferentes?

A. Quando você configura o AP como um servidor DHCP, os endereços IP estão atribuídos aos dispositivos que estão na mesma sub-rede como o servidor DHCP. Os dispositivos comunicam-se com os outros dispositivos na sub-rede, mas não se comunicam além da sub-rede. Se você precisa de passar dados além da sub-rede, você deve atribuir um roteador padrão. O endereço IP do roteador padrão deve estar na mesma sub-rede como o AP que você configurou como o servidor DHCP.

Q. Qual é a medida do dBm? Como eu determino os valores equivalentes do dBm para a intensidade de sinal (no mW) listada em meu ponto de acesso Aironet (AP)?

A. O DB da unidade mede a potência de um sinal em função de sua relação a um outro valor padrão. Esta abreviatura dB é combinado frequentemente com outras abreviaturas a fim de

representar os valores que são comparados. Portanto, o dBm é o valor que resulta de comparar o DB com um valor de referência padrão de 1 mW.

A fórmula para calcular este valor do dBm da intensidade de sinal dada no mW é:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Esta lista define os termos na fórmula. o log10 é a base 10 do logaritmo.

- O sinal é a potência do sinal (por exemplo, 50 pés mW).
- A referência é a potência da referência (por exemplo, 1 mW).

Exemplo:

Se você quer calcular a potência da intensidade em dB de força de sinal 50 mW, aplique esta fórmula:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Esta fórmula conduz a uma regra comum que diga:

- Para cada aumento de 3dB (dBm aqui), esta leva a um aumento no dobro na potência de transmissão atual (mW). Para cada diminuição de 3 dB, isto reduz a potência de transmissão à metade do seu valor atual.
- Para cada aumento de 10 dB (dBm), conduz aos dez tempos um aumento na potência de transmissão atual (mW). Para cada diminuição de 10 dB, isto reduz a potência de transmissão a dez vezes seu valor atual.
- Para cada aumento de 30 dB(dBm), isto leva a um aumento de 1000 vezes na potência de transmissão atual. Para cada diminuição de DB 30, isto reduz a potência de transmissão a 1000 vezes seu valor atual.

Esta tabela fornece o dBm aproximado aos valores mW:

dBm	mW
0	1
1	1.25
2	1.56
3	2
4	2.5
5	3.12
6	4
7	5
8	6.25
9	8
10	10
11	12.5
12	16
13	20
14	25
15	32
16	40
17	50
18	64
19	80
20	100
21	128
22	160
23	200
24	256
25	320
26	400
27	512
28	640
29	800
30	1000 or 1 W

Refira aos valores da potência RF para mais informação.

Q. Como eu mudo os ajustes da data e hora em Cisco 1231 AP?

A. Vá para a interface da WEB (GUI), escolha **Services > SNTP**, Selecione as **configurações de tempo** e mude o tempo.

Q. Se o CCKM não for configurado no cliente, mas for configurado em APs, o cliente será capaz de se associar ao AP? Podem os clientes fazer roaming normal?

A. O comportamento depende da configuração do AP. Se o CCKM não for configurado/suportado no cliente, o cliente não se associa com um AP que seja ajustado ao CCKM “obrigatório.” Se a infra-estrutura (AP) é ajustada ao CCKM “opcional,” o cliente associa e faz seu aperto de mão do NON-CCKM.

Dependente do cliente atribuído, recomenda-se ajustar tipicamente o CCKM a “opcional” na infra-estrutura que permite a associação de todos os dispositivos mas de vaguear rápido dos apoios SOMENTE para dispositivos capazes/associados CCKM.

Q. Qual é a diferença na capacidade de memória entre AP 1240 e 1230?

A. Estas são as capacidades de memória do AP 1240 e 1230:

- O AP 1240 é uma plataforma AP 32-MB.
- O AP1230 é uma plataforma AP 16-MB.

Q. Eu tenho dois AP 1240s que suportam esse link de flexibilidade do papel. Eu gostaria de construir uma ponte entre eles com 802.11a, com os clientes juntados nas faixas 802.11b/g. Há alguma limitação para fazer isto?

A. A flexibilidade do papel do link do ponto de acesso fornece o apoio da funcionalidade do modo de Bridge para os pontos de acesso que têm a capacidade da dupla-faixa (1200, 1230, e a série 1240AG). Na configuração de destino, o rádio 802.11a é executado no modo de Bridge, quando o rádio 802.11g estiver no modo de ponto de acesso.

A exigência é que quando você configura um AP com flexibilidade do papel do link, um dos rádios do AP deve ser configurado como uma raiz AP, e o segundo AP que as pontes traseiras devem estar no repetidor ou no modo WGB à raiz AP.

Q. Quantos aparelhos de telefonia IP Wireless são recomendados por AP?

A. O tamanho da rede de telefonia do IP é essencial para garantir a largura de banda adequada e que os recursos estejam disponíveis para levar o tráfego de voz crítico. Além das diretrizes usuais do design de telefonia IP para componentes sob medida, tais como portas do gateway PSTN, transcodificadores, largura de banda de WAN, e assim por diante, igualmente consideram estas edições 802.11b ao fazer sob medida sua rede de telefonia do IP Wireless:

- Número dos dispositivos 802.11b por AP: Cisco recomenda que você não tenha mais de 15 a 25.
- Número dos telefones 802.11b por AP

Antes que toda a discussão sobre planos da rede possa ocorrer, isto ajuda a compreender os princípios da capacidade geral de rede. Estas diretrizes da capacidade de rede aplicam-se a fazer sob medida a rede de telefonia do IP Wireless:

- Não mais de sete atendimentos concorrentes G.711 pelo AP
- Não mais de oito atendimentos concorrentes G.729 pelo AP

Nota: Estas recomendações de design assumem que a detecção de atividade da voz (VAD) foi desabilitada no Cisco 7920 Wireless IP Phones.

O uso do VAD nos telefones Cisco 7920 pode conservar a largura de banda, mas a Cisco

recomenda que você desabilita o VAD em todos os servidores do Cisco CallManager para fornecer a melhor qualidade geral de voz. Além da determinação do quanto largura de faixa é necessário para uma chamada VoIP 802.11b, você também deve considerar a contenção global de rádio para um canal RF específico. A regra geral é que você não deve distribuir mais do que 20 a 25 802.11b endpoints por AP. Quanto mais endpoints você adicionar a um AP, mais você reduz a quantidade de largura de banda total e potencialmente aumenta o atraso de transmissão. O número máximo de telefones por AP depende dos padrões de chamada dos usuários individuais (baseado nas proporções de Erlang). A Cisco recomenda que não mais de sete chamadas simultâneas usem o G.711 ou oito chamadas simultâneas usem o G.729. Além desse número de atendimentos, quando os dados de background excessivos estão presentes, a qualidade de voz de todos os atendimentos torna-se inaceitável. As taxas do empacotamento para estas recomendações são baseadas nos exemplos de taxa 20-ms com VAD desabilitada. Esta taxa gera 50 pacotes por segundo (pps) em cada sentido. Um tamanho de amostra maior (tal como 40 ms) pode gerar um maior número de chamadas simultâneas, mas a ele igualmente aumenta o atraso de ponta a ponta das chamadas VoIP.

O número de telefones 802.11b que você pode distribuir por Camada-2 sub-rede ou o VLAN depende destes fatores:

- Use não mais de sete G.711 ou oito G.729 chamadas ativas por AP.
- A relação de chamadas é usada para determinar o número de chamadas ativos e não-ativas. Esta relação é frequentemente determinada com calculadoras Erlang. Baseado nestes fatores e proporções de Erlang normais da negócio-classe (entre 3:1 e 5:1), a Cisco recomenda que você distribua não mais de 450 a 600 telefones Cisco 7920 por camada-2 sub-redes ou VLAN.

Refere-se à seção do *Tamanho de Rede* da seção de Infra-estrutura de Rede Wireless, bem como a WLAN está pronta para Voz? para informações detalhadas.

Q. Como posso parar um AP1200 de processar pedidos de autenticação após um determinado número de tentativas?

A. Você pode usar a opção das novas tentativas máxima no servidor AAA para limitar o número de vezes que os clientes podem tentar acessar uma rede. O valor das tentativas máxima pode ser configurado manualmente no servidor AAA, ou você pode usar o número padrão de novas tentativas, o qual depende do servidor AAA usado.

Q. Onde posso encontrar informação sobre as diferenças nas várias plataformas de APs e LAPs?

A. Refira às perguntas mais frequentes do Cisco Wireless Hardware. Este documento contém informações úteis que compara os diferentes modelos AP e LAP.

Q. O Point-to-Point-Protocol over Ethernet (PPPoE) é suportado no Cisco Aironet Access Points?

A. Não, o PPPoE não é suportado no Cisco Aironet Access Points.

Q. O VLAN Trunking Protocol (VTP) é suportado no Cisco Aironet Access Points?

A. Não, VTP não é suportado no Cisco Aironet Access Points.

Q. O Cisco Aironet AP suporta o 802.11f padrão Inter-Access Point Protocol (IAPP)?

A. Não, o Cisco Aironet AP não suporta o IAPP baseado 802.11f. O Cisco Access Points oferece seu próprio protocolo inter-Access Point robusto, cheio de características e comprovado.

Q. Qual é o uso do comando grupo-ponte 1 block-unknown-sourcee grupo-ponte 1 source-learning em um AP?

A. Use o comando de interface de configuração **grupo-ponte block-unknown-source** para bloquear o tráfego de de endereços MAC desconhecidos na interface específica. Use a forma **no** do comando para desabilitar a fonte de bloqueio desconhecido na interface específica.

Para que o STP funcione corretamente, **block-unknown-source** deve esta desabilitada para as interfaces que participam no STP.

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Quando você permite o STP em uma interface, **block-unknown-source**está desabilitado por padrão.

O comando **grupo-ponte 1 source-learning** faz o AP aprender o endereço de origem do cliente. Use a forma **no** do comando para desabilitar o AP de aprender o endereço de origem do cliente.

Q. Há uma maneira de dar a prioridade ao tráfego que flui através do AP de modo que o tráfego de um SSID particular configurado no AP utilize uma largura de banda mais alta do que os outros SSID no mesmo AP?

A. Isto pode ser conseguido com aplicação do Qualidade de Serviço (QoS) no AP.

- Crie políticas de QoS e aplique as políticas aos VLAN configurados em seu ponto de acesso. Estes originais explicam o QoS e como configurar políticas de QoS no AP.Qualidade--Serviço WirelessConfigurando QoS no Aironet Access Points
- Então, mapeie os SSID configurados no AP aos VLANs individuais mencionados. Desta maneira, se você dá a prioridade ao tráfego baseado no VLAN, você pode, por sua vez, dar a prioridade ao tráfego baseado no SSID.

Q. Há uma maneira de limitar o número máximo de dispositivos do cliente que podem conectar a um único ponto de acesso autônomo?

A. O comportamento padrão de um dispositivo do cliente Cisco é que conecta ao AP que tem a melhor intensidade de sinal disponível. Mas você pode limitar os clientes que podem conectar a

todo o AP particular com a autenticação de MAC. Você precisa de fornecer o MAC address do cliente ao AP de modo que o AP possa permitir somente aqueles clientes e restringir todos os clientes restantes que não são parte da lista permitida do MAC address da conexão a esse AP particular.

Q. De onde você pode transferir o software mais recente?

A. O equipamento de Cisco Aironet opera melhor quando você carrega todos os componentes com a versão mais recente do software. Refira ao Cisco Wireless Software Center (somente clientes registrados) a fim de fazer o download do software e drivers mais recentes.

Q. É necessário desligar todos os laptops e outros dispositivos wireless durante um upgrade AP?

A. Não, não é necessário desligar os dispositivos. Uma upgrade AP é um processo seguro, e tudo pode ficar ligado. Certifique-se de que você esteja conectado a um servidor TFTP.

Q. Onde posso encontrar instruções sobre como promover o Cisco IOS® no Cisco Aironet AP?

A. Refira ao trabalho com imagens do software para instruções sobre como promover o Cisco IOS no AP.

Nota: Use a opção **force-reload** com o **comando archive download-sw**.

Nota: Quando você fizer o upgrade do AP ou o sistema de ponte do software digitando o **comando archive download-sw** no CLI, você deve usar a opção **force-reload**. Se o AP ou a ponte não recarregam a memória Flash após o upgrade, as páginas da interface do web browser podem não refletir o upgrade. Este exemplo mostra como fazer o upgrade do software do sistema usando o **comando archive download-sw**:

```
AP#archive download-sw /force-reload /
overwrite tftp://10.0.0.1/image-name
```

Q. Eu tenho uns 1100 AP. Eu quero promover o rádio AP do IEEE 802.11B a IEEE 802.11g. Se eu promover o rádio no AP, posso usar os PC cards existentes? Ou eu preciso de fazer o upgrade dos PC cards também? Os cartões são atualmente cartões 802.11b.

A. Um upgrade do rádio 802.11b a 802.11g não resulta em uma melhora no desempenho se você usar somente os clientes 802.11b. Uma vantagem do upgrade de rádio 802.11g é que você pode conectar os clientes 802.11b e 802.11g com o AP. Com o upgrade, os clientes 802.11b se conectam a 11 Mbps e os clientes 802.11g conectam a 54 Mbps.

Q. Como você ajusta o AP de volta a suas configurações padrão de fábrica?

A. Refira ao procedimento de recuperação de senha para o equipamento Cisco Aironet.

Perguntas Frequentes de Troubleshooting

Q. Eu fiz algumas alterações de configuração ao AP. Quando eu tento salvar as mudanças, eu recebo esta mensagem no AP: **"Erro escrevendo as novas configurações do arquivo "flash: /config.txt.new" nv_done: incapaz de abrir o "flash: /config.txt.new" nv_done: incapaz de abrir o "flash: /private-multiple-fs.new" [OK]". O que significa a mensagem?**

A. Esta Mensagem de Erro indica que não há nenhum espaço no flash para armazenar a configuração nova. Tente apagar todos os arquivos velhos que existirem. Ou, se há mais de uma versão do Cisco IOS Software, apague a versão que você não usa. Isto pode liberar algum espaço no flash. Emita o **comando dir flash** a fim determinar se há algum arquivo velho da exceção de informação de travamento que você pode apagar ou imagens antigas que não são mais utilizadas. Emita o **comando write memory** a fim de liberar espaço de modo que você possa escrever a configuração na memória.

Q. Eu uso o Aironet Client Utility (ACU) 6,3 e Cisco 1200 Access Points (APs) que roda o Cisco IOS Software versão 12.3(8)JA. Quando o cliente Wireless é associado ao AP, o nome AP não aparece no ACU. Por que?

A. **O nome AP** é o hostname para o AP. Se as extensões Aironet são habilitadas no AP, então o nome AP é indicado no ACU.

Se você não deseja ver o nome AP, você pode desabilitar extensões do Cisco Aironet ao padrão IEEE 802.11B (**nenhuma extensão aironet no dot11** sob a interface de rádio). As extensões do Cisco Aironet são habilitadas por padrão no AP.

Se previamente desabilitado, você pode habilitar as extensões do Cisco Aironet com este comando:

```
AP(config-if)#dot11 extension aironet
```

Em uma baliza, o AP inclui um elemento de informação que é propriedade da Cisco que contem o nome AP. Se você desativar as extensões Aironet no AP, o AP não ilumina seu nome. Refira à Desabilitação e a Habilitação de extensões Aironet para obter mais informações sobre as extensões Aironet.

Q. Meu Access Point (AP) aceita e conecta a somente um cliente de cada vez. Qual pode ser o motivo?

A. Uma razão possível poderia ser que o parâmetro **max-associations** está ajustado para **1** sob a configuração do service-set identifier (SSID). Use a configuração do comando **max-associations** SSID a fim configurar o número máximo de associações suportadas pela interface de rádio (para o SSID especificado). Use a forma **no** do comando a fim restaurar o parâmetro ao valor padrão. Este padrão máximo é 255.

Q. Como é possível recuperar senhas perdidas?

A. Refira ao procedimento de recuperação de senha para o equipamento Cisco Aironet.

Q. Os números de série não aparecem em nenhum dos BR350 ou dos AP350 que nós temos por comandos. Estes são VxWorks e não foram convertidos ao IO. Como eu recupero esta informação dos dispositivos?

A. O 350 Series AP e as pontes que executam VxWorks não indicam o número de série no software. A única maneira de identificar o número de série nestas unidades é inspecionar fisicamente a etiqueta no hardware.

Q. Quais são as possíveis fontes de interferência para o link da freqüência de rádio (FR) do AP?

A. A interferência pode vir de um número de fontes, como:

- Telefones sem fio 2.4 gigahertz
- Fornos de microondas com proteção imprópria
- Equipamento Wireless produzidos por outras empresas

Motores elétricos e partes de metal móveis de máquinas podem igualmente causar interferência. Consulte estes documentos para obter outras informações:

- Troubleshooting Problemas que Afetam a Comunicação de Freqüência de Rádio
- Problemas de conectividade intermitente nas pontes Wireless

Q. Eu vejo a Mensagem de Erro: %C4K_EBM-4-HOSTFLAPPING:Host [mca-addr] no [num] vlan está batendo entre a porta [num] e a porta [num] conectados aos pontos de acesso. Como nós resolvemos isto?

A. Esta Mensagem de Erro ocorre quando o interruptor aprende o mesmo endereço MAC através das portas múltiplas. Isto pode ser devido a uma destas razões

1. Quando um cliente faz o roaming de um AP a um outro AP, o AP novo informa o cliente do MAC address ao interruptor. Se ambos os AP são conectados ao mesmo interruptor, o MAC address do cliente está associado a ambas as portas de switch conectadas aos AP. Isto cria uma entrada duplicada para o cliente e gera esta Mensagem de Erro até o tempo que o interruptor sincroniza sua tabela CAM. Este Mensagem de Erro é bastante normal em um ambiente Wireless, mas, se houver muito roaming, este pode sobrecarregar a CPU do interruptor. Verifique o driver e o firmware do cliente. Além disso, assegure-se de que a cobertura seja boa de modo que o cliente não vagueie frequentemente.
2. Quando há um loop, o interruptor pode aprender o mesmo MAC address através das portas múltiplas conectadas a outros interruptores. Assegure-se de que o TP esteja habilitado no interruptor.

Q. Por que é que o cartão do cliente não se associa ao AP o mais próximo?

A. Se há AP múltiplos em sua topologia Wireless, seu cliente mantem uma associação com o AP com que o cliente se associou originalmente, até que o cliente perca o keepalive beacon desse AP. Se o contato é perdido e se as tentativas de recuperar o contato com o AP original continuam a falhar, o cliente irá procurar um outro AP. O cliente tenta se associar a este AP novo se o cliente tem direitos e autorização suficientes no AP novo.

Q. Eu tenho um Cisco AP e Cisco Secure Access Control Server (ACS) 3.2. Eu tenho o Extensible Authentication Protocol (EAP) implementado na rede. Os usuários não são autenticados pelo servidor RADIUS. Quando eu emito comandos debug no AP, eu obtenho esta saída: **"Jun 2 15:58:13.553: %RADIUS-4-RADIUS_DEAD: O RADIUS server 10.10.1.172:1645,1646 não está respondendo. Jun 2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.10.1.172:1645,1646 retornou. Jun 2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758 Authentication failed."** Por que eu vejo estas Mensagens de Erro no AP?

A. Uma das razões pelas quais estes Mensagens de Erro aparecem é que o segredo compartilhado não é o mesmo no AP e no ACS. Este erro é comum quando você configura o EAP. Se há uma má combinação do segredo compartilhado entre o AP e o ACS 3.2, o EAP não funciona. O servidor RADIUS não aceita os pacotes que o AP encaminha. Assegure-se de que o segredo compartilhado no AP combine com o aquele configurado no servidor ACS. Para obter informações sobre de como debugar, consulte Debug Authentications.

Q. Quando eu vi os logs no AP, encontrei o erro: **"Mar 9 11:05:26.225 Information Group rad_acct: O servidor Radius 10.10.1.172:1645,1646 está respondendo outra vez (não estava respondendo antes). Mar 9 11:03:09.361 Error Group rad_acct: Nenhum servidor Radius ativo encontrado."** Quais são as causas deste erro e como posso resolver o problema?

A. É normal ver este registro quando a configuração **radius-server deadtime** está configurada no AP. É um registro da informação e não um problema principal. Use o **comando radius-server deadtime** a fim ajustar um intervalo no qual o AP não tente usar os servidores que não respondem, evitando a espera para que um pedido tenha o time out antes de tentar o servidor seguinte. Um server marcado como inativo é deixado de lado para pedidos adicionais pela duração em minutos que você especificar, até 1440 (24 horas).

Q. Eu tenho um AP1230 com Cisco IOS Software Versão 12.3(4)JA. Quando eu atualizar a lista de controle de acesso (ACL), eu recebo a mensagem: **"% Atenção: Salvar esta configuração no nvram pode corromper todos os arquivos do gerenciamento de rede ou da segurança armazenados na extremidade do nvram. Continue? [não]: "**

A. Este é um mensagem de advertência e não um erro. Se você selecionar [no] então não será salvo no ponto de acesso (AP). As configurações não foram salvas no RAM não-volátil (NVRAM), elas foram salvas em Flash.

Mesmo que seja um aviso, você tem uma edição da memória neste AP. Você tem diversos arquivos .rcore que ocupam muito espaço em sua memória. Esta saída mostra um exemplo:

```
AP(config-if)#dot11 extension aironet
```

Para limpar a memória, apague todos os arquivos .rcore do flash.

Este é um exemplo do comando que você precisa de incorporar ao modo habilitar:

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

Nota: Emita este **delete flash:** comando para cada arquivo .rcore em seu Flash.

Q. Eu tenho um módulo de serviços do Wireless LAN (WLSM) com o Cisco IOS Software Versão 12.4(4)T1 instalado. As conexões aos clientes estão caindo. Depois que eu olhar os registros, eu vejo um número de mensagens tais como “a autenticação precedente já não é mais válida " e “dissociado porque a estação de envio está saindo (ou saiu) de BSS”. Que é o problema?

A. Ambas estas mensagens apontam para um problema RF. Atribua os canais diferentes no AP a fim fixar este problema.

Q. O Cisco Aironet AP em minha rede de WLAN não transmite os identificadores do conjunto de serviço (SSID). Qual pode ser o motivo? Eu preciso de permitir uns recursos particulares no AP?

A. Enquanto você não permite o modo Guest sob o gerenciador SSID, o AP não transmite o SSID em suas balizas. Você pode verificar com um cliente e a varredura para SSID a fim certificar-se não estar listada.

A fim permitir o modo guest em um SSID, digite este comando no AP no modo de configuração global:

```
Ap<config>#dot11 ssid ssid-string
Ap<config-ssid>#guest-mode
```

Q. Eu tenho meu AIR-AP1231G-A-K9 AP. Por que eu não vejo a opção para ligar o rádio A neste AP e consigo ver somente a opção para rádios G? Não posso associar os clientes 802.11b à ele?

A. O AIR-AP1231G-A-K9 AP tem um rádio G. O número da peça AP1231G implica que ele tenha somente rádio G. Os rádios G são compatíveis com rádios B porque trabalham na mesma freqüência. Não há nenhum rádio A nesta unidade e é por isso você não pode ligá-lo. Você pôde precisar de adicionar o módulo do rádio A. O rádio A funciona em uma freqüência diferente (em 5 gigahertz) do que os rádios G e B (em 2,4 gigahertz).

Q. Eu tenho um Cisco Wireless IP Phone 7920 que está conectado ao Cisco AP. Eu vejo que o 7920 está associado ao AP, mas nenhum endereço IP foi atribuído. Eu uso o Extensible Authentication Protocol (EAP). Eu vejo a mensagem Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated , a qual é seguida por “Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated”, e “ Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4". Então eu vejo “Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ”. Que é o problema?

A. O motivo pelo qual você recebe estas mensagens é que o segredo compartilhado no AP é diferente do que o segredo compartilhado do servidor Radius. Certifique-se de que as chaves de segredo compartilhado para o EAP são idênticas em ambos. Você deve redigitar a chave de segredo compartilhado no AP e no servidor Radius.

Q. Eu tenho um problema com meu AP. Ele continua a enviar mensagens RTS demais nas explosões que causam a dissociação inesperada de clientes associados. Estes clientes foram associados com este AP em um nível de sinal entre o -91 e -95 dBm. Que é a razão para esta dissociação inesperada? É isto um comportamento esperado do AP?

A. Sim, este é um comportamento esperado. Seu cliente está na margem da célula 1 Mbps. Uma vez que você a vê em -91 a -95 dBm, o comportamento anormal é esperado.

Instale mais APs a fim solucionar este problema. Ou, se sua cobertura desejada está em uma área focalizada um pouco do que Omni-direcional, use antenas direcionais.

O RTS é causado pelos novos mecanismos ativados. O cliente deve responder a um RTS com um CTS, mas se o cliente os vê em um sniffer como um grupo de ao redor oito quadros RTS sem o CTS correspondente, a seguir o cliente não ouve o AP, ou o cliente está até agora ausente que o AP não pode o ouvir. Ambos os dispositivos têm que ouvir-se, não apenas seu AP ouvindo o cliente. Assim, se a antena no cliente não é do grande projeto (provável), ou seu transmissor não transmite em 100 mW (muito provável), ou seu receptor está em nenhuma parte perto da sensibilidade do dBm -90 a -95 (quase garantido se não é um cliente Cisco), a seguir você obtém a operação que você descreve.

Q. Nós usamos a Tecnologia Cisco LWAPP Wireless APs. Embora eu tenha visto muitas retransmissões de TCP e duplicata ACK em clientes, eu não vejo estes em nosso ambiente cabeado. É isso normal para a Tecnologia Wireless?

A. Os pacotes corruptos e os pacotes retransmitidos são dois de métrica fundamental de 802,11 WLAN. A análise de pacotes corrompidos e retransmitidos em 802.11 difere da análise em um LAN cabeado por três motivos:

- Primeiramente, 802.11 WLAN possui tipicamente muito mais pacotes corruptos do que os LAN cabeados, assim a importância de quadros corrompidos no 802.11 WLAN é aumentada.
- Em segundo, o 802,.11 define uma camada de link de dados segura, assim que significa que cada pacote corrupto deve conduzir a uma retransmissão. Os LAN cabeados tipicamente não definem uma camada de link de dados segura, assim que a retransmissão ocorre somente se um protocolo de camada superior seguro está em uso.
- Finalmente, a confiança da camada superior é tipicamente end-to-end, o que significa que um pacote corrupto em qualquer lugar entre a fonte e o destino causa uma retransmissão. Uma retransmissão 802.11, desde que ocorre na camada 2, é executada entre relações Wireless, assim a retransmissão 802.11 pode somente ser causada pela corrupção no “segmento local.” Isto facilita muito a identificação do lugar da corrupção em um 802.11 WLAN do que em um LAN ligado com fio tradicional. Deixe-nos explorar as implicações destas diferenças.

Um dos desafios de um ambiente Wireless é que é difícil determinar se o analisador vê as mesmas coisas que fazem os clientes. As diferenças entre o analisador e o cliente - rádios, antenas, ou locais físicos diferentes - podem fazer com que o analisador considere coisas diferentes do que faz o cliente. Por exemplo, se o analisador estiver longe do AP, mas o cliente Wireless estiver próximo ao AP, o analisador pode ver um quadro corrompido, enquanto a estação considera um quadro não corrompido. Desde que nós sabemos que cada quadro corrompido gera uma retransmissão, nós podemos usar os números relativos de retransmissões e de quadros corrompidos para avaliar o grau a que o analisador vê o que as estações na rede consideram.

Q. Nós vemos esta mensagem do syslog ser transmitido em toda a nossa rede. Por que isto ocorre, e como nós podemos parar isto?

```
Ap<config>#dot11 ssid ssid-string
Ap<config-ssid>#guest-mode
```

A. Estas mensagens são mensagens de advertência e nós as vemos quando a transgressão WLAN é permitida e o ID de WLAN particular não está selecionado nem está anunciado em um slot/rádio.

Q. Eu tenho problemas quando eu atualizo meu AP usando o servidor TFTP. Cada vez que eu tento atualizar, ele adiciona uma extensão do .tar ao arquivo c1200-k9w7-tar.default da imagem de upgrade, que fazem com que o AP não reconheça o arquivo. Eu não pude encontrar uma maneira de me livrar da extensão adicional do .tar. (Eu fiz o download e tentei ambos o solarwind e o tftpd32.) O que devo fazer para eliminar este problema?

A. O problema poderia ser que o Sistema Operacional está escondendo o tipo de arquivo conhecido. Vá ao **Meu Computador**. Clique em**Tools > Folder Options > View**, role para baixo até que você encontre o parâmetro **Hide extensions for known file types**, e desmarcar a caixa. Isto deve eliminar o problema.

Q. Meus pontos de acesso encontram frequentemente um mensagem de alarme “utilização elevada da CPU”. Nesses casos, reiniciar o hardware levar o Ponto de Acesso em condição de trabalho. Como posso superar este problema?

A. Há diversas razões para que os Pontos de Acesso tenham “utilização elevada da CPU.”

- Se o Ponto de Acesso da Cisco (AP) for conectado à rede através de um interruptor, as vezes pode-se observar “utilização elevada da CPU” no AP. Isto é porque, por padrão, todos os VLANs são permitidos no AP do interruptor onde o AP está conectado. Isto pode criar um problema, especialmente quando aplicado a uma rede enorme. Se todos os VLANs são permitidos no AP, isto pode resultar em **utilização elevada da CPU**, e a conectividade pode ser afetada. Os clientes associados aos problemas de Ponto de Acesso, e as vezes a utilização elevada da CPU pode também derrubar a rede Wireless.A fim evitar este problema, remova os VLANs do interruptor de modo que somente o tráfego de VLAN em que o AP é interessado passe pelo AP.
- Se os Pontos de Acesso forem configurados com interfaces loopback, as vezes a “utilização elevada da CPU” será observada no AP. Embora as interfaces de loopback possam ser configuradas no Cisco AP, elas não são suportadas no AP, portanto elas não devem ser configuradas. Recomenda-se remover as interfaces de loopback se são configurados no AP.**Nota:** Os APs e as pontes não suportam o comando de interface loopback.

O primeiro passo para troubleshooting este problema, emita o **comando show process cpu** no AP. Isto dá-lhe uma ideia de quais processos usam a CPU.

Igualmente, se o AP executa uma primeira versão do 12.3(2)JA2, faça o upgrade para a versão 12.3(2)JA2 porque existe um problema conhecido nas versões anteriores onde os pedidos do serviço mataram o CPU.

Q. O 871W Wi-Fi Router deixa derruba sessões estabelecidas wi-fi de modo que a sessão de VPN do usuário precisa de ser restabelecida todo o tempo. Qual é a razão?

A. Há diversas razões possíveis que podem causar este problema. Conecte ambas as antenas ao 871W Router. Mude o canal para 1, 6 ou 11 e verifique que canal possui o melhor desempenho. Também, você pôde ter outros AP no ambiente que podem estar causando interferência. Esta é apenas uma razão possível.

Informações Relacionadas

- Cisco Downloads for Wireless Products (somente clientes registrados)
- Cisco Aironet 1240 AG Series Q&A
- Cisco Aironet 1230 AG séries Q&A
- Guia de Configuração do Software Cisco Aironet Access Point para VxWorks
- Manual de configuração do Cisco IOS Software para pontos de acesso do Cisco Aironet, 12.2(13)JA
- Cisco Aironet 350 Series Troubleshooting TechNotes
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems