Consulte Perguntas frequentes sobre mensagens de sistema e erros da controladora Wireless LAN (WLC)

Contents

Introduction

Este documento descreve as perguntas frequentes (FAQ) sobre mensagens de erro e mensagens de sistema para as Controladoras Cisco Wireless LAN (WLAN) (WLCs).

Conventions

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

Perguntas Frequentes sobre Mensagens de Erro

Q. A conversão de mais de 200 access points (APs) do Cisco IOS® Software para o Lightweight AP Protocol (LWAPP) com um Cisco 4404 WLC foi iniciada. A conversão de 48 APs foi concluída, e a mensagem recebida no WLC declarou: `[ERROR] spam_lrad.c 4212: o AP não pode ingressar porque o número máximo de APs na interface 1 foi atingido.` Por que o erro ocorre?

R.Você deve criar interfaces adicionais do gerenciador de AP para suportar mais de 48 APs. Caso contrário, você receberá um erro semelhante a este:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Configure múltiplas interfaces do gerenciador de AP e configure portas principais ou de backup que outras interfaces do gerenciador de AP não usam. Você deve criar uma segunda interface de gerenciador de AP para ativar APs adicionais. Mas certifique-se de que suas configurações de porta primária e porta de backup para cada gerenciador não se sobreponham. Em outras palavras, se o gerenciador de AP 1 usa a porta 1 como principal e a porta 2 como backup, o gerenciador de AP 2 deve usar a porta 3 como principal e a porta 4 como backup.

P. Eu tenho uma controladora Wireless LAN (WLC) 4402 e uso 1240 pontos de acesso lightweight (LAPs). Habilitei a criptografia de 128 bits na WLC. Quando seleciono a criptografia WEP de 128 bits na WLC, recebo um erro que diz que não há suporte para 128 bits no 1240s: `[ERROR] spam_lrad.c 12839: Não criando o modo SSID no AP CISCO xx:xx:xx:xx:xx:xx:xx porque não há suporte para WEP128 bits.` Por que eu recebo este erro?

R.Os comprimentos de chave mostrados nas WLCs são, na verdade, o número de bits que estão no segredo compartilhado e não incluem os 24 bits do Vetor de Inicialização (IV). Muitos produtos, inclusive os produtos Aironet, os chamam de chave WEP de 128 bits. Na realidade, trata-se de uma chave de 104 bits com um IV de 24 bits. O tamanho da chave de 104 bits é o que deve ser habilitado na WLC para possibilitar a criptografia WEP de 128 bits.

Se você escolher o tamanho de chave de 128 bits na WLC, na verdade é uma criptografia de chave WEP de 152 bits (128 + 24 IV). Somente os LAPs Cisco 1000 Series (AP1010, AP1020, AP1030) suportam o uso da configuração de chave WEP de 128 bits da WLC.

P. Por que recebo o `tamanho de chave WEP de 128 bits sem suporte nos APs dos modelos 11xx, 12xx e 13xx. A WLAN não pode ser enviada para esses pontos de acesso.` Mensagem de erro quando tento configurar a WEP em uma WLC?

R.Em uma controladora Wireless LAN, quando você escolhe a WEP estática como o método de segurança da camada 2, você tem essas opções para o tamanho da chave WEP.

- não definido
- 40 bits
- 104 bits
- 128 bits

Estes valores do tamanho da chave não incluem o vetor de inicialização (IV) de 24 bits que é concatenado com a chave WEP. Assim, para uma WEP de 64 bits, você precisa escolher**40** bits como tamanho da chave WEP. A controladora adiciona o IV de 24 bits para formar uma chave WEP de 64 bits. Da mesma forma, para uma chave WEP de 128 bits, escolha**104 bits**.

As controladoras também oferecem suporte a chaves WEP de 152 bits (128 bits + IV de 24 bits). Esta configuração não é válida nos APs modelos 11xx, 12xx e 13xx. Assim, quando você tenta configurar o WEP com 144 bits, a controladora envia uma mensagem para informar que esta configuração WEP não é enviada para os APs modelos 11xx, 12xx e 13xx.

P. Os clientes não podem se autenticar em uma WLAN configurada para WPA2, e a controladora exibe a mensagem de erro `apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Não foi possível processar a estação RSN e WARP IE. que não usa RSN (WPA2) em WLAN que requer RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>`. Por que eu recebo este erro?

R.Isso ocorre principalmente devido à incompatibilidade no lado do cliente. Execute estes passos para corrigir este problema:

- Verifique se o cliente é certificado Wi-fi para WPA2 e verifique a configuração do cliente para ver se a WPA2 está habilitada.
- Verifique a folha de dados para ver se o utilitário cliente oferece suporte à WPA2. Instale quaisquer patches de suporte a WPA2 lançados pelo fornecedor. Se você usa o Utilitário do Windows, certifique-se de que instalou o patch WPA2 da Microsoft para oferecer suporte à WPA2. Consulte o suporte da Microsoft para obter mais informações.
- Atualize o driver e o firmware do cliente.
- Desative as extensões Aironet na WLAN.

P. Assim que reinicializo a WLC, recebo o `evento MFP Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event encontrado como violado pelo rádio 00:XX:XX:XX:XX:XX e detectado pela interface dot11 no slot 0 do AP 00:XX:XX:XX:XX:XX em 300 segundos ao observar respostas de sondagem, mensagem de` erro `Beacon Frames`. Por que esse erro ocorre e como posso eliminá-lo?

R.Essa mensagem de erro é vista quando quadros com valores de MIC incorretos são detectados por LAPs ativados por MFP. Consulte Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example para obter mais informações sobre MFP. Conclua uma destas quatro etapas:

1. Verifique e remova todos os APs ou clientes invasores ou inválidos em sua rede, que geram quadros inválidos.
2. Desative a infraestrutura MFP, se a MFP não estiver habilitada em outros membros do grupo de mobilidade, pois os LAPs podem ouvir quadros de gerenciamento dos LAPs de outras WLCs do grupo que não têm a MFP habilitada. Consulte Perguntas frequentes sobre grupos de mobilidade da controladora Wireless LAN (WLC)para obter mais informações sobre o grupo de mobilidade.
3. A correção dessa mensagem de erro está disponível nas versões 4.2.112.0 e 5.0.148.2 da WLC. Atualize as WLCs para qualquer uma dessas versões.
4. Como última opção, tente recarregar o LAP que gera essa mensagem de erro.

P. O cliente AIR-PI21AG-E-K9 associa-se com êxito a um ponto de acesso (AP) com Autenticação Flexível do Extensible Authentication Protocol via Secure Tunneling (EAP-FAST). No entanto, quando o AP associado é desligado, o cliente não migra para outro AP. Esta mensagem aparece continuamente no registro de mensagens do controlador: "Sex Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - Maybe the user is already logged into the system? (Sex Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Não é possível permitir que o usuário entre no sistema - talvez o usuário já esteja conectado ao sistema?) Sex Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Não é possível excluir o nome de usuário para o celular 00:40:96:ad:75:f4". Por quê?

R.Quando a placa do cliente precisa fazer roaming, ela envia uma solicitação de autenticação, mas não lida corretamente com as chaves (não informa o AP/controlador, não responde à reautenticação).

Isso está documentado no bug Cisco IDCSCsd02837. Esse bug foi corrigido no Cisco Aironet 802.11a/b/g Client Adapters Install Wizard 3.5.

Em geral, `a mensagem Unable to delete username for` mobilemtambém ocorre devido a qualquer um destes motivos:

- O nome de usuário específico é usado em mais de um dispositivo cliente.
- O método de autenticação usado para esta WLAN possui uma identidade anônima externa. Por exemplo, no PEAP-GTC ou EAP-FAST, é possível definir um nome de usuário genérico como a identidade externa (visível), enquanto que o nome de usuário real é ocultado dentro do túnel TLS entre o cliente e o servidor Radius. Dessa forma, a controladora não pode vê-lo nem usá-lo. Nesses casos, esta mensagem pode ser exibida. Este problema é mais comumente observado com alguns clientes de terceiros ou com firmware antigo.

  Observação: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bugs da Cisco.

P. Quando eu instalo o novo blade Wireless Services Module (WiSM) no switch 6509 e implemento o Protected Extensible Authentication Protocol (PEAP) com o servidor Microsoft IAS, recebo este erro: *Mar 1 00:00:23.526: %LWAPP-5-CHANGED: o LWAPP alterou o estado para DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Recarregar solicitado pelo LWAPP LIENT.Reload Motivo: FALHA NA INICIALIZAÇÃO DE CRIPTOGRAFIA. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPP alterou estado para DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP alterou estado para DISCOVERY *Mar 1

00:00:23.557: LWAPP_R_CLIENT_ERROUPER_DEBUG:lwapp_crypto_init_ssc_keys_and_certs nenhum certificado no arquivo privado SSC *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00:23.557: lwapp_crypto_init: PKI_StartSession falhou *Mar 1 00:00:23.706: %SYS-5-1 CARREGAMENTO: recarregamento solicitado pelo CLIENTE LWAPP. . Por quê?

R.As depurações RADIUS e dot1x mostram que a WLC envia uma solicitação de acesso, mas não há resposta do IAS Server. Conclua estes passos para fazer o troubleshooting do problema:

1. Verifique a configuração do IAS Server.
2. Verifique o arquivo de log.
3. Instale software, como o Ethereal, capazes de informar detalhes da autenticação.
4. Pare e reinicie o serviço IAS.

P. Os pontos de acesso lightweight (LAPs) não são registrados com a controladora. Qual pode ser o problema? Eu vejo estas mensagens de erro na controladora: Thu Feb 3 03:20:47 2028: LWAPP Join-Request não inclui certificado válido em CERTIFICATE_PAYLOAD do AP 00:0b:85:68:f4:f0. Quinta, 3 de fevereiro 03:20:47 2028: Não foi possível liberar a chave pública para AP 00:0B:85:68:F4:F0.

R.Quando o ponto de acesso (AP) envia a solicitação de união do Lightweight Access Point Protocol (LWAPP) à WLC, ele incorpora seu certificado X.509 na mensagem LWAPP. Isso também gera um ID de sessão aleatório que é incluído na solicitação de união do LWAPP. Quando a WLC recebe a solicitação de união do LWAPP, ela valida a assinatura do certificado X.509 com a chave pública dos APs e verifica se o certificado foi emitido por uma autoridade de certificação confiável. Ele também examina a data e a hora de início do intervalo de validade do certificado AP e compara essa data e hora com sua própria data e hora.

Este problema pode ocorrer devido a uma configuração de relógio incorreta na WLC. Para ajustar o relógio na WLC, execute o comando **show time** e **config time** comandos.

P. Um AP Lightweight Access Point Protocol (LWAPP) não é capaz de se unir à sua controladora. O registro da controladora Wireless LAN (WLC) exibe uma mensagem semelhante a esta: LWAPP Join-Request não inclui um certificado válido em CERTIFICATE_PAYLOAD do AP 00:0b:85:68:ab:01. Por quê?

R.Você pode receber essa mensagem de erro se o túnel LWAPP entre o AP e a WLC atravessar um caminho de rede com uma MTU abaixo de 1500 bytes. Isto causa a fragmentação dos pacotes LWAPP. Este é um bug conhecido da controladora. Consulte o bug da Cisco IDCSCsd39911.

A solução é atualizar o firmware da controladora para a versão 4.0(155).

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bugs da Cisco.

P. Desejo estabelecer o tunelamento de convidado entre meu controlador interno e o controlador âncora virtual na zona desmilitarizada (DMZ). No entanto, quando um usuário tenta se associar a um SSID convidado, ele é incapaz de receber o endereço IP da DMZ, como esperado. Consequentemente, o tráfego de usuário não é tunelado para a controladora na DMZ. A saída do comando debug mobile handoff exibe uma mensagem semelhante a esta: Security Policy Mismatch for WLAN <Wlan ID>. Solicitação de exportação de âncora do IP do switch: <endereço IP do controlador> ignorado. Qual é o problema?

R.O tunelamento de convidados fornece segurança adicional para o acesso de usuários convidados à rede sem fio corporativa. Isso ajuda a garantir que os usuários convidados sejam incapazes de acessar a rede corporativa sem passar primeiro pelo firewall corporativo. Quando um usuário se associa a uma WLAN que está designada como a WLAN convidada, o tráfego de usuário é tunelado para a controladora de WLAN localizada na DMZ fora do firewall corporativo.

Agora, considerando esse cenário, pode haver diversas razões para este tunelamento de convidado não funcionar da forma esperada. Como a saída do comando debug implica, o problema pode ser com a incompatibilidade em qualquer uma das políticas de segurança configuradas para essa WLAN específica nos controladores internos e DMZ. Verifique se as políticas de segurança, bem como outras configurações como timeout da sessão, são atendidas.

Outro motivo comum para esse problema é que a controladora DMZ não está ancorada nela mesma para essa WLAN específica. Para um tunelamento de convidado funcionar corretamente e para que a DMZ administre o endereço IP do usuário (usuário que pertence a uma WLAN convidada), é essencial que a ancoragem apropriada seja feita para essa WLAN específica.

P. Eu vejo muitas mensagens **"CPU Receive Multicast Queue is full on Controller"** na controladora Wireless LAN (WLC) 2006, mas não nas WLCs 4400. Por quê? Desabilitei o multicast nas controladoras. Qual é a diferença do limite da fila de multicast entre as plataformas WLC 2006 e 4400?

R.Como o multicast está desativado nos controladores, as mensagens que causam esse alarme podem ser mensagens Address Resolution Protocol (ARP). Não há nenhuma diferença na profundidade da fila (512 pacotes) entre as WLCs 2000 e as WLCs 4400. A diferença é que o NPU 4400 filtra os pacotes ARP, enquanto que tudo é feito via software no 2006. Isso explica porque as WLCs 2600 enxergam as mensagens, mas não as WLCs 4400. Uma WLC 44xx processa pacotes de multicast via hardware (através da CPU). Uma WLC 2000 processa pacotes de multicast via software. O processamento na CPU é mais eficiente do que o via software. Consequentemente, a fila da 4400 é esvaziada mais rápido, enquanto que a WLC 2006 se esforça um pouco ao ver muitas destas mensagens.

P. Vejo a mensagem de erro **"[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Recebeu um pacote na porta 1, mas nenhum AP Estrangeiro configurado para essa porta."** em um de meus controladores. O que esse erro significa e que etapas devo executar para resolvê-lo?

R.Essa mensagem é vista quando a controladora recebe uma solicitação DHCP para um endereço MAC para o qual não tem uma máquina de estado. Isto é observado frequentemente em bridges ou sistemas que executam máquinas virtuais como o VMware. A controladora escuta as solicitações de DHCP porque executa o snooping de DHCP. Assim, ela sabe quais endereços estão associados aos clientes conectados aos seus pontos de acesso (APs). Todo o tráfego para os clientes Wireless passa através da controladora. Quando o destino de um pacote é um cliente Wireless, ele vai para a controladora e atravessa o túnel Lightweight Access Point Protocol (LWAPP) para o AP e então para o cliente. Uma coisa que pode ser feita para ajudar a mitigar essa mensagem é permitir somente as VLANs que são usadas no controlador no tronco que vai para o controlador com o comando **switchport vlan** allowno switch.

P. Por que vejo esta mensagem de erro no console: **Falha na mensagem 'Set Default Gateway' da tabela do sistema, Id = 0x0050b986 valor do erro = 0xfffffc**?

R.Isso pode ocorrer devido à alta carga da CPU. Quando a CPU da controladora está sobrecarregada, por exemplo, ao executar cópias de arquivo ou outras tarefas, ela não tem tempo para processar todos os ACKs que o NPU envia em resposta às mensagens de configuração.

Quando isso ocorre, a CPU gera mensagens de erro. No entanto, as mensagens de erro não afetam o serviço ou a funcionalidade.

Para obter mais informações, consulte Cisco Wireless LAN Controllers.

P. Recebo estas mensagens de erro de chave WEP (Wired Equivalent Privacy) no meu sistema de controle sem fio (WCS): `A chave WEP configurada na estação pode estar incorreta. O endereço MAC da estação é 'xx:xx:xx:xx:xx:xx', o MAC do rádio base do AP é 'xx:xx:xx:xx:xx:xx' e o ID do slot é '1'.` Contudo, eu não uso a WEP como o parâmetro de segurança em minha rede. Uso somente o Wi-Fi Protected Access (WPA). Por que eu recebo estas mensagens de erro de WEP?

R.Se todas as suas configurações relacionadas à segurança forem perfeitas, as mensagens que você recebe agora são causadas por bugs. Há alguns bug conhecidos na controladora. Consulte os bugs da Cisco IDCSCse17260 e Cisco, mas ID CSCse11202, que declaram "A chave WEP configurada na estação pode estar errada **com clientes WPA e TKIP, respectivamente**". Na verdade, o bug da Cisco ID **CSCse17260**é uma duplicata do **bug da Cisco ID** CSCse11202. A correção para a Cisco, mas a ID **CSCse11202**, já está disponível com a versão 3.2.171.5 da WLC.

> **Observação**: as versões mais recentes do WLC têm uma correção para esses bugs.

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

P. Eu uso um servidor RADIUS externo para autenticar clientes sem fio através da controladora. O controlador envia esta mensagem de erro regularmente: `nenhum servidor radius está respondendo`. Por que eu vejo essas mensagens de erro?

R.Quando uma solicitação sai da WLC para o servidor RADIUS, cada pacote tem um número de sequência para o qual a WLC espera uma resposta. Se não houver resposta, há uma mensagem que `mostra radius-server not responding`.

O tempo padrão para que a WLC ouça de volta do servidor Radius é 2 segundos. Ele é definido na GUI da WLC **emSecurity > authentication-server**. O máximo é 30 segundos. Portanto, pode ser útil definir esse valor de tempo limite ao máximo para resolver esse problema.

Às vezes, os servidores RADIUS executam**'descartes silenciosos'**do pacote de solicitação que vem da WLC. O servidor RADIUS pode rejeitar esses pacotes devido a inconsistências de certificado e diversas outras razões. Esta é uma ação válida pelo servidor. Além disso, nesses casos, a controladora pode marcar o servidor RADIUS como não respondendo

Para resolver o problema dos descartes silenciosos, desabilite o recurso **agressivo de** failover na WLC.

Se o recurso de failover **assertivo** estiver habilitado na WLC, a WLC será muito agressiva para marcar o servidor AAA como não respondendo. No entanto, isso não deve ser feito porque o servidor AAA não pode responder somente àquele cliente específico (ele faz descarte silencioso). Isso pode ser uma resposta a outros clientes válidos (com certificados válidos). No entanto, a WLC ainda pode marcar o servidor AAA como não respondendo e não funcional.

Para superar isso, desabilite o recurso **de** failover **agressivo**. Execute **o comando config radius**

aggressive-failover disableda CLI do controlador para fazer isso. Se ele estiver desabilitado, a controladora executará o failover para o próximo servidor AAA somente se houver 3 clientes consecutivos que falharam ao receber uma resposta do servidor RADIUS.

P. Vários clientes não podem se associar a um LWAPP e o controlador registra a mensagem de erro `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt returns`. Por que isso acontece?

R.Isso acontece principalmente devido a um problema com os adaptadores Intel que suportam CCX v4, mas que executam uma versão de pacote de cliente anterior à 10.5.1.0. Se você atualizar o software para a versão 10.5.1.0 ou posterior, o problema será resolvido. Consulte o bug da Cisco IDCSCsi91347 para obter mais informações sobre essa mensagem de erro.

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

P. Eu vejo esta mensagem de erro na controladora Wireless LAN (WLC): `Alcançado o máximo de novas tentativas de solicitação de identidade EAP (21) para STA 00:05:4e:42:ad:c5`. Por quê?

R.Essa mensagem de erro ocorre quando o usuário tenta se conectar a uma rede WLAN protegida por EAP e falha no número pré-configurado de tentativas de EAP. Quando o usuário falha na autenticação, a controladora exclui o cliente e o cliente não pode se conectar à rede até que o temporizador de exclusão expire ou seja manualmente substituído pelo administrador.

A exclusão detecta as tentativas de autenticação feitas por um dispositivo único. Quando esse dispositivo exceder um número máximo de falhas, seu endereço MAC não poderá mais se associar.

A exclusão ocorre:

- Após 5 falhas de autenticação consecutivas para autenticações compartilhadas (a 6ª tentativa é eliminada)
- Após 5 falhas de associação consecutivas para autenticações de MAC (a 6ª tentativa é eliminada)
- Após 3 falhas de autenticação EAP/802.1X consecutivas (a 4ª tentativa é eliminada)
- Qualquer falha externa do servidor de políticas (NAC)
- Qualquer instância de duplicação de endereço IP
- Após 3 falhas consecutivas da autenticação da Web (a 4ª tentativa é eliminada)

O temporizador que define quanto tempo um cliente é excluído pode ser configurado, e exclusão pode ser habilitada ou desabilitada na controladora ou no nível de WLAN.

P. Eu vejo esta mensagem de erro na controladora Wireless LAN (WLC): `Um alerta do switch de categoria é gerado com gravidade 1 pelo switch WLCSCH01/10.0.16.5 A mensagem do alerta é Controller '10.0.16.5'. Os servidores RADIUS não estão respondendo às solicitações de autenticação.` Que é o problema?

R.Isso pode ocorrer devido à ID de bug da Cisco CSCsc05495. Devido a este bug, a controladora injeta periodicamente um par AV incorreto (atributo 24, “estado”) nas mensagens de solicitação de autenticação que violam um RFP do RADIUS e causam problemas para alguns servidores de autenticação. Este foi corrigido na versão 3.2.179.6.

> **Observação**: somente usuários registrados da Cisco podem acessar informações e

ferramentas internas de bug da Cisco.

P. Recebo uma mensagem Noise Profile failure (Falha no perfil de ruído) em Monitor > 802.11b/g Radios. Eu quero entender por que recebo essa mensagem de falha?

R.O status do perfil de ruído FAILED/PASSED é definido após o resultado do teste feito pela WLC e em comparação com o limite definido atual. Por padrão, o valor do ruído é ajustado para -70. O estado FAILED indica que o valor de limite para esse parâmetro específico ou ponto de acesso (AP) foi excedido. Você pode ajustar os parâmetros no perfil, mas é recomendável alterar as configurações depois de compreender claramente o projeto de rede e como ele pode afetar o desempenho da rede.

Os limites PASSED/FAILED do Radio Resource Management (RRM) são definidos globalmente para todos os APs nas páginas **802.11a Global Parameters > Auto** RF **e802.11b/g Global Parameters > Auto** RF. Os limites de PASSED/FAILED do RRM são definidos individualmente para este AP na página**Interfaces do AP 802.11 > Performance**Profile.

P. Não consigo definir a porta 2 como a porta de backup para a interface do gerenciador de AP. A mensagem de erro retornada é Could not set port configuration. Eu consigo definir a porta 2 como a porta de backup na interface de gerenciamento. A porta ativa atual para ambas as interfaces é a porta 1. Por quê?

R.Um gerenciador de AP não tem uma porta de backup. No entanto, havia suporte nas versões anteriores. Desde a versão 4.0, não há suporte a portas de backup na interface do gerenciador de AP. Como regra, um único gerenciador de AP deve ser configurado em cada porta (sem backups). Se você usa a agregação de link (LAG), há somente um gerenciador de AP.

A interface estática (ou permanente) do gerenciador de AP deve ser atribuída à porta 1 do sistema de distribuição e deve possui um endereço IP exclusivo. Ela não pode ser mapeada em uma porta de backup. Ela é configurada geralmente na mesma sub-rede de VLAN ou IP que a interface de gerenciamento, mas isso não é obrigatório.

P. Vejo esta mensagem de erro: o `AP '00:0b:85:67:6b:b0' recebeu um erro de MIC WPA no protocolo '1' da Estação '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds.` Por quê?

R.A Verificação de Integridade da Mensagem (MIC) incorporada no Acesso Protegido Wi-Fi (WPA) inclui um contador de quadros que evita um ataque de intermediários. Esse erro significa que alguém na rede deseja reproduzir a mensagem que foi enviada pelo cliente original ou pode significar que o cliente está com defeito.

Se um cliente falhar repetidamente na verificação do MIC, o controlador desabilita a WLAN na interface do AP onde os erros são detectados por 60 segundos. A primeira falha de MIC é registrada e um temporizador é iniciado para permitir a aplicação das contramedidas. Se uma falha subsequente de MIC ocorrer dentro de 60 segundos da falha anterior mais recente, um STA cuja entidade IEEE 802.1X tenha atuado como um solicitante deverá invalidar a si mesmo ou invalidar todos os STAs com uma associação de segurança se sua entidade IEEE 802.1X tiver atuado como um autenticador.*

Além disso, o dispositivo não recebe nem transmite quadros de dados criptografados por TKIP e não recebe nem transmite quadros de dados não criptografados diferentes de mensagens IEEE 802.1X, para ou de qualquer peer por um período de pelo menos 60 segundos após detectar a segunda falha. Se o dispositivo for um AP, ele não permitirá novas associações com o TKIP

durante esse período de 60 segundos; no final do período de 60 segundos, o AP retomará as operações normais e permitirá que os STAs (re)se associem.

Isso impede um possível ataque no esquema de criptografia. Esses erros de MIC não podem ser desativados nas versões de WLC anteriores à 4.1. Com o Wireless LAN Controller versão 4.1 e posterior, há um comando para alterar o tempo de verificação para erros de MIC. O comando **isconfig wlan security tkip hold-down <0-60 seconds> <wlan id>**. Use o valor 0 para desativar a detecção de falha de MIC para contramedidas.

*Invalidar: Finalizar autenticação.

P. Esta mensagem de erro é vista nos logs do meu controlador: `[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed.` Por quê?

R.Essas mensagens de erro são vistas principalmente quando a porta de serviço do controlador tem o DHCP habilitado, mas não recebe um endereço IP de um servidor DHCP.

Por padrão, a interface da porta de serviço física tem um cliente DHCP instalado e procura por um endereço via DHCP. A WLC tenta solicitar um endereço DHCP para a porta de serviço. Se nenhum servidor DHCP estiver disponível, a solicitação de DHCP para a porta de serviço falhará. Assim, as mensagens de erro são geradas.

A solução alternativa é configurar um endereço IP estático para porta de serviço (mesmo se a porta de serviço estiver desconectada) ou ter um servidor DHCP disponível para atribuir um endereço IP à porta de serviço. Em seguida, recarregue a controladora, se necessário.

Na realidade, a porta de serviço é reservada para o gerenciamento out-of-band da controladora e da recuperação do sistema, além de para a manutenção no caso de uma falha de rede. Ela é também a única porta que permanece ativa quando a controladora está no modo de inicialização. A porta de serviço não pode ter marcas 802.1Q. Consequentemente, ela deve ser conectada a uma porta de acesso no switch vizinho. O uso da porta de serviço é opcional.

A interface da porta de serviço controla rigorosamente as comunicações e é mapeada estaticamente pelo sistema à porta de serviço. Ela deve possuir um endereço IP em uma sub-rede diferente das sub-redes de gerenciamento, do gerenciador de AP e de quaisquer interfaces dinâmicas. Ela também não pode ser mapeada em uma porta de backup. A porta de serviço pode usar o DHCP para obter um endereço IP ou receber um endereço IP estático. No entanto, não é possível atribuir um gateway padrão à interface da porta de serviço. As rotas estáticas podem ser definidas através da controladora para o acesso de rede remota à porta de serviço.

P. Meus clientes sem fio não conseguem se conectar à rede LAN sem fio (WLAN). O WiSM ao qual o ponto de acesso (AP) está conectado relata esta mensagem: `Ataque do Big NAV Dos do AP com o rádio base MAC 00:0g:23:05:7d:d0, Slot ID 0 e MAC origem 00:00:00:00:00:00.` O que isso significa?

R.Como condição para acessar o meio, a camada MAC verifica o valor do seu vetor de alocação de rede (NAV). O NAV é um contador residente em cada estação que representa a quantidade de tempo que o quadro anterior precisa para enviar seu quadro. O NAV deverá ser zero para que uma estação possa tentar enviar um quadro. Antes da transmissão de um quadro, uma estação calcula a quantidade de tempo necessária para enviar o quadro com base no comprimento do quadro e na taxa de dados. A estação coloca um valor que representa esse tempo no campo de duração no cabeçalho do quadro. Quando as estações recebem o quadro, elas examinam o valor do campo de duração e o usam como base para ajustar seu NAVs correspondentes. Esse

processo reserva a mídia para a estação de envio.

Uma NAV alto indica a presença de um valor inflado de NAV (mecanismo de detecção de portadora virtual do 802.11). Se o endereço MAC relatado for 00:00:00:00:00:00, ele provavelmente será falsificado (possivelmente um ataque real) e você precisará confirmar isso com uma captura de pacote.

P. Após configurar o controlador e reinicializá-lo, não consigo acessá-lo no modo seguro da Web (https). Esta mensagem de erro é recebida enquanto eu tento acessar o modo seguro da Web do controlador: `Web Segura: Certificado de Autenticação da Web não encontrado (erro).` Qual é a causa deste problema?

R.Pode haver vários motivos associados a esse problema. Um motivo comum pode estar relacionado à configuração da interface virtual da controladora. Para resolver este problema, remova a interface virtual e gere-a novamente com este comando:

```
WLC>config interface address virtual 1.1.1.1
```

Em seguida, reinicialize-a. Após a controladora reinicializar, gere localmente outra vez o certificado de webauth na controladora com este comando:

```
WLC>config certificate generate webauth
```

Na saída desse comando, você pode ver esta mensagem:`O certificado de autenticação da Web foi gerado.`

Agora você pode acessar o modo seguro da Web do controlador na reinicialização.

P. As controladoras às vezes relatam esta mensagem de alerta de ataque de Assinatura de Inundação de Desassociação de IDS para clientes válidos nos quais o endereço MAC do invasor é o de um ponto de acesso (AP) associado a essa controladora: `Alerta: Ataque de assinatura de 'inundação de desassociação' de IDS detectado no protocolo '802.11b/g' do AP '<AP name>' no Controlador 'x.x.x.x'. The Signature description is 'Disassociation flood', with precedence 'x'. O endereço mac do invasor é 'hh:hh:hh:hh:hh:hh', o número do canal é 'x' e o número de detecções é 'x'`. Por que isso ocorre?

R.Isso se deve ao bug da Cisco IDCSCsg81953 .

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

Os ataques de Inundação de Desassociação de IDS contra clientes válidos são, às vezes, reportados onde o endereço MAC do invasor é o de um AP associado a essa controladora.

Quando um cliente é associado ao AP, mas interrompe as comunicações devido à remoção da placa, ele se movimenta fora do intervalo e assim por diante, para o AP, o AP espera até o timeout ocioso. Uma vez que o timeout de ociosidade seja alcançado, o AP enviará a esse cliente um quadro de desassociação. Quando o cliente não confirma o quadro de desassociação, o AP retransmite os quadros várias vezes (ao redor de 60 quadros). O subsistema IDS da controladora ouve essas retransmissões e alerta com esta mensagem.

Este bug foi resolvido na versão 4.0.217.0. Atualize a sua controladora para esta versão para resolver esta mensagem de alerta exibida para clientes e APs válidos.

P. Recebo esta mensagem de erro no syslog do controlador: **[WARNING] apf_80211.c 2408: recebeu uma mensagem com uma taxa suportada inválida da estação <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Ausência de taxa suportada.** Por quê?

R.Na verdade, `as mensagens Missing Supported Rate` indicam que a WLC está configurada para determinadas taxas de dados exigidas nas configurações sem fio, mas a placa de rede não tem a taxa necessária.

Se você possui taxas de dados como 1 e 2M definidas como exigidas na controladora, mas a placa NIC não se comunica nessas taxas de dados, você pode receber esse tipo de mensagem. Trata-se de um comportamento inadequado da placa NIC. Por outro lado, se sua controladora oferecer suporte a 802.11g e o cliente for uma placa 802.11b (somente), a mensagem será legítima. Se essas mensagens não causam nenhum problema e as placas ainda podem se conectar, basta ignorá-las. Se as mensagens forem específicas da placa, certifique-se de que o driver da placa esteja atualizado.

Q. Esta **mensagem de erro** syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN ID <id>** é transmitida em nossa rede. Por que isso ocorre e como faço para interrompê-lo?

R.Essa mensagem é transmitida pelos LAPs. Isso é visto quando você configura o recurso de substituição de WLAN para uma WLAN e essa WLAN específica não é anunciada.

`Configureconfig ap syslog host global 0.0.0.0`para interrompê-lo ou você pode colocar um endereço IP específico se tiver um Servidor syslog para que a mensagem seja transmitida somente para o servidor.

P. Recebo esta mensagem de erro em minha controladora Wireless LAN (WLC): **[ERROR] Arquivo: apf_mm.c : Linha: 581 : Anunciar colisão para mobile 00:90:7a:05:56:8a, excluindo.** Por quê?

R.Geralmente, essa mensagem de erro indica que a controladora anunciou colisões para um cliente sem fio (isto é, APs separados anunciam que têm o cliente) e a controladora não recebeu uma transferência de um AP para o próximo. Não há nenhum estado de rede para manter. Elimine o cliente Wireless e faça com que o cliente tente outra vez. Se este problema ocorre com frequência, pode haver um problema com a configuração da mobilidade. Caso contrário, pode ser uma anomalia relacionada a um cliente ou condição específica.

P. Meu controlador gera esta mensagem de alarme: **Limite de cobertura de '12' violado.** O que é esse erro e como posso resolvê-lo?

R.Essa mensagem de alarme é gerada quando a razão sinal-ruído (SNR) de um cliente cai para um valor menor que o valor limite de SNR para o rádio específico. 12 é o valor limite de SNR para a detecção de furos da cobertura.

O algoritmo de detecção e correção de furos de cobertura determina se existe um buraco de cobertura quando os níveis de SNR dos clientes são menores que um determinado limite de SNR. Esse limite de SNR varia com base em dois valores: potência de transmissão de AP e o valor do perfil de cobertura do controlador.

Em detalhes, o limite de SNR do cliente é definido pela potência de transmissão de cada AP

(representada em dBm), menos o valor constante de 17 dBm, menos o valor configurável pelo usuário do perfil de cobertura (o padrão é 12 dB).

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

Este valor configurável pelo usuário do perfil de cobertura pode ser acessado desta forma:

1. Na GUI da WLC, vá para o título principal de Wireless e selecione a opção de rede para o padrão de WLAN à escolha no lado esquerdo (802.11a ou 802.11b/g). Em seguida, selecione Auto RF no canto superior direito da janela.
2. Na página Auto RF Global parameters, vá para a seção Profile Thresholds. Nessa seção, você pode encontrar o valor da cobertura (3 a 50 dBm). Esse valor é o valor configurável pelo usuário do perfil de cobertura.
3. Esse valor pode ser editado para influenciar o valor limite de SNR do cliente. A outra forma de influenciar o limite de SNR é aumentar a potência de transmissão e compensar a detecção de furos de cobertura.

P. Uso o ACS v 4.1 e uma controladora Wireless LAN (WLC) 4402. Quando a WLC tenta autenticar um cliente sem fio com o MAC para o ACS 4.1, o ACS não responde com o ACS e relata esta mensagem de erro: "*Erro interno* ". Todas as minhas configurações estão corretas. Por que este erro interno ocorre?

R.Há um bug da Cisco relacionado à autenticação IDCSCsh62641 no ACS 4.1, em que o ACS fornece **a mensagem de erro interno** occurederror.

Esse erro pode ser o problema. Há um patch disponível para esse bug no site de downloads do ACS 4.1 que pode corrigir o problema.

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

Q. O Cisco 4400 Series Wireless LAN Controller (WLC) não pode ser inicializado. Esta mensagem de erro é recebida no controlador: `** Não é possível usar ide 0:4 para fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Erro reg: 10 ** Não é possível ler do dispositivo 0.` Por quê?

R.O motivo desse erro pode ser um problema de hardware. Abra uma ocorrência do TAC para fazer troubleshooting adicional deste problema. Para abrir uma ocorrência do TAC, você precisa de um contrato válido com Cisco. Consulte o Suporte Técnico para saber como entrar em contato com o TAC Cisco.

P. A controladora Wireless LAN (WLC) apresenta problemas de buffer de memória. Quando os buffers de memória encherem, a controladora causará um crash e precisará ser reinicializada para voltar a funcionar. Essas mensagens de erro são vistas no registro de mensagens: `Seg Abr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Seg 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Cannot allocate new Mbuf. Seg 9 10:41:03 2007 [ERRO] sysapi_if_net.c 219: MbufGet: sem Mbufs livres.` Por quê?

R.Isso se deve ao bug da Cisco IDCSCsh93980. Esse bug foi resolvido na versão 4.1.185.0 da WLC. Atualize seu Controlador para esta versão de software ou posterior para superar esta mensagem.

Observação: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

P. Executei a atualização de nosso código 4400s para 4.1 da controladora Wireless LAN (WLC) e nosso syslog foi bombardeado por mensagens como esta: `May03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op 1) recebido com SPA 192.168.1.233/TPA 192.168.1.233 inválido.` Que essas mensagens indicam?

R.Isso pode ocorrer quando a WLAN é marcada como DHCP necessário . Nesses casos, somente as estações que recebem o endereço IP via DHCP podem se associar. Os clientes estáticos não podem se associar a esta WLAN. A WLC atua como um agente de repetição de DHCP e grava o endereço IP de todas as estações. Essa mensagem de erro é gerada quando a WLC recebe uma solicitação de ARP de uma estação antes que a WLC receba pacotes DHCP da estação e grave seu endereço IP.

P. Quando você usa o Power over Ethernet (PoE) no Cisco 2106 Wireless LAN Controller, os rádios AP não são habilitados. O AP é incapaz de verificar alimentação in-line suficiente. `Slot de rádio desativado.` É exibida uma mensagem de erro. Como posso corrigir isso?

R.Esta mensagem de erro ocorre quando o switch, que liga o Ponto de acesso, é um switch pré-padrão, mas o AP não suporta o modo pré-padrão de potência de entrada.

Um switch pré-padrão da Cisco é aquele que não oferece suporte ao gerenciamento de energia inteligente (IPM), mas tem potência suficiente para um ponto de acesso padrão.

Você deve ativar oModo pré-padrão de alimentação no AP que está sujeito a esta mensagem de erro. Isso pode ser feito a partir da CLI do controlador com o comando config ap power pre-standard {enable | disable} {all | Cisco_AP}.

Esse comando já deverá estar configurado, se necessário, se você atualizar para a versão 4.1 do software a partir de uma versão anterior. No entanto, talvez seja necessário inserir esse comando para instalações novas ou se você restaurar o AP para os padrões de fábrica.

Os seguintes switches de 15 watts pré-padrão de Cisco estão disponíveis:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

P. O controlador gera um `dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: não é possível adicionar uma entrada ARP para xx:xx.-xxx.x ao processador de rede. a entrada não existe.` mensagem de syslog semelhante a esta. O que essa mensagem de syslog significa?

R.Enquanto alguns clientes sem fio enviam uma resposta ARP, a NPU (Network Processor Unit) precisa saber essa resposta. Assim, a resposta ARP é encaminhada para a NPU, mas o software da WLC não deve tentar adicionar essa entrada ao processador de rede. Se ele o fizer, essas

mensagens serão geradas. Não há nenhum impacto na funcionalidade da WLC devido a isso, mas a WLC gera essa mensagem de syslog.

P. Instalei e configurei um novo Cisco 2106 WLC. A WLC indica que o sensor de temperatura falhou. Quando você inicia sessão na interface da Web sob "controller summary", a mensagem "sensor failed" é mostrada ao lado da temperatura interna. Todo o resto parece funcionar normalmente.

R.A falha interna do sensor de temperatura é superficial e pode ser resolvida com um upgrade para a versão 4.2.61.0 da WLC.

A WLC 2106 e a WLC 526**construídas em ou após 01/07/2007** podem usar o chip sensor de temperatura de outro fornecedor. Esse novo sensor funciona bem, mas não é compatível com software posterior à versão 4.2. Assim, um software mais antigo não pode ler a temperatura e mostra esse erro. As demais funcionalidades da controladora não são afetadas por esse defeito.

Há um bug Cisco IDCSCsk97299 conhecido relacionado a esse problema. Esse erro é mencionado nos Release Notes da versão 4.2 da WLC.

> **Observação**: somente usuários registrados da Cisco podem acessar informações e ferramentas internas de bug da Cisco.

P. Recebo a mensagem `radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Could not find applicable RADIUS server for WLAN <WLAN ID> - cannot find a default server"` para TODOS os SSIDs. A mensagem é exibida até mesmo para os SSID que não usam servidores AAA.

R.Essa mensagem de erro significa que o controlador não conseguiu entrar em contato com o servidor radius padrão ou que não foi definido.

Um motivo possível para esse comportamento é o bug da Cisco IDCSCsk08181, que foi resolvido na versão 4.2. Atualize sua controladora para a versão 4.2.

Q. A `mensagem: Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: O endereço MAC de origem da interface 1 não foi encontrado.` Uma mensagem de erro é exibida na controladora Wireless LAN (WLC). Que ela significa?

R.Isso significa que o controlador apresentou um erro ao enviar um pacote originado na CPU.

P. Essas mensagens de erro são exibidas na controladora Wireless LAN (WLC):

- `Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Falha ao ler o arquivo de configuração 'cliWebInitParms.cfg'`
- `Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Falha ao ler o arquivo de configuração 'rfidInitParms.cfg'`
- `Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Falha ao ler o arquivo de configuração 'dhcpParms.cfg'`
- `Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Falha ao ler o arquivo de configuração 'bcastInitParms.cfg'`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Falha ao excluir o arquivo: sshpmInitParms.cfg. Falha na remoção do arquivo. -Process: Name:fp_main_task, Id:11ca7618`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Falha ao excluir o arquivo: bcastInitParms.cfg. Falha na remoção do arquivo. -Process: Name:fp_main_task, Id:11ca7618`

P. O que essas mensagens de erro indicam?

R.Essas mensagens são informativas e fazem parte do procedimento normal de inicialização. Essas mensagens aparecem devido a uma falha na leitura ou exclusão de vários arquivos de configuração diferentes. Quando determinados arquivos de configuração não são encontrados ou se o arquivo de configuração não puder ser lido, a sequência de configuração de cada processo envia essa mensagem, por exemplo, no DHCP server config, no tags (RF ID) config e assim por diante. Essas são mensagens de baixa gravidade que podem ser ignoradas com segurança. Essas mensagens não interrompem a operação da controladora.

P. A mensagem de erro **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN: Unable to keep rogue 0:14:XX:02:XX:XX in contained state - no available AP to contains (Não há AP disponível para conter)** é exibida. Que ela significa?

R.Isso significa que o AP que executou a função de contenção de invasor não está mais disponível, e a controladora não pode encontrar nenhum AP adequado para executar a contenção de invasor.

P. A mensagem do **sistema DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) recebida com SPA 192.168.1.152/TPA 192.168.0.206** é exibida no Wireless LAN Controller. O que essa mensagem implica?

R.É possível que o sistema tenha detectado falsificação ou envenenamento ARP. Mas essa mensagem não implica necessariamente que ocorreu qualquer falsificação ARP mal-intencionada. A mensagem aparece quando estas condições são verdadeiras:

- Uma WLAN é configurada com DHCP necessário e um dispositivo cliente, depois de se associar a essa WLAN, transmite uma mensagem ARP sem antes completar o DHCP. Esse pode ser um comportamento normal; pode acontecer, por exemplo, quando o cliente é endereçado estaticamente ou quando o cliente mantém um aluguel de DHCP válido de uma associação anterior. A mensagem de erro pode ser semelhante a este exemplo:

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206
```

O efeito dessa condição é que o cliente é incapaz de enviar ou receber qualquer tráfego de dados, até que faça DHCPs através da WLC.

Consulte a seção Mensagens DTL do Guia de Mensagens do Sistema do Cisco Wireless LAN Controller para obter mais informações.

P. Os LAPs não usam Power over Ethernet (POE) para ligar. Eu vejo os registros na controladora Wireless LAN:

AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power

P. Que é o problema?

R.Isso pode acontecer se as configurações de Power over Ethernet (POE) não estiverem configuradas corretamente. Quando um access point que foi convertido para o modo lightweight, por exemplo, um AP1131 ou AP1242, ou um access point 1250 series é alimentado por um injetor de energia conectado a um switch Cisco pre-Intelligent Power Management (pré-IPM), você precisa configurar o Power over Ethernet (PoE), também conhecido como inline power.

Consulte Configurar o Suporte a Power over Ethernet, Ethernet para obter mais informações.

P. Você vê esta mensagem na controladora Wireless LAN (WLC):

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery
request from
AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

P. O que isso indica?

R.Os Pontos de Acesso Lightweight rastreiam um certo algoritmo para encontrar um controlador. O processo de descoberta e junção é explicado em detalhes no Registro de APs Lightweight (LAP) em uma controladora Wireless LAN (WLC).

Essa mensagem de erro é vista na WLC quando ela recebe uma solicitação de descoberta depois de ter atingido sua capacidade máxima de AP.

Se a controladora primária de um LAP não estiver configurada ou se for um novo LAP pronto para uso, ele enviará solicitações de descoberta LWAPP a todas as controladoras acessíveis. Se as solicitações de descoberta atingirem um controlador que é executado em sua capacidade total de AP, a WLC obterá as solicitações e perceberá que está em sua capacidade máxima de AP e não responderá à solicitação e emitirá esse erro.

P. Onde posso encontrar mais informações sobre as mensagens do sistema LWAPP?

R.Consulte o Guia de Mensagens do Sistema do Cisco Wireless LAN Controller, 4.2 (Desativado)para obter mais informações sobre as mensagens do Sistema LWAPP.

P. A mensagem de erro `Error extraindo webauth files` (Erro ao extrair arquivos webauth) é exibida na controladora Wireless LAN (WLC). Que ela significa?

R.O WLC falha ao carregar um pacote Custom Web Authentication/Passthrough se qualquer um dos arquivos do pacote tiver mais de 30 caracteres no nome do arquivo, o que inclui a extensão do arquivo. O pacote de autenticação da Web personalizado tem um limite de até 30 caracteres para nomes de arquivo. Certifique-se de que nenhum nome de arquivo dentro do pacote tenha mais de 30 caracteres.

P. As controladoras de LAN sem fio (WLCs), que executam o código 5.2 ou 6.0 com um grande número de grupos de APs, a GUI da Web não exibe todos os grupos de APs configurados. Que é o problema?

R.Os grupos de AP ausentes podem ser vistos se você usar o CLI **show wlan ap-groups**comando.

Tente adicionar mais um grupo AP à lista. Por exemplo, 51 grupos AP foram implantados e o 51º está faltando (página 3). Adicione o 52º grupo e a Página 3 deverá ser exibida na GUI da Web.

Para resolver esse problema, atualize para a versão 7.0.220.0 da WLC.

Informações Relacionadas

- Perguntas Frequentes de Troubleshooting de WiSM

- Página de Suporte Wireless
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.