Erro do controlador do Wireless LAN (WLC) e mensagens de sistema FAQ

Índice

Introdução

Este documento contém informações sobre as perguntas mais frequentes (FAQ) sobre mensagens de erro e mensagens de sistema relacionadas às controladoras Cisco Wireless LAN (WLAN) (WLC).

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

Perguntas Frequentes sobre Mensagens de Erro

Q. Iniciamos a conversão de mais de 200 pontos de acesso (APs) do Cisco IOS® Software para o Lightweight AP Protocol (LWAPP) com um Cisco 4404 WLC. Terminamos a conversão de 48 APs e recebemos uma mensagem no WLC que indica: **[ERROR] spam_lrad.c 4212: O AP não pode se unir porque o número máximo de APs na interface 1 foi atingido.** Por que o erro ocorre?

A. Você deve criar interfaces adicionais do gerenciador de AP para oferecer suporte a 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 do gerenciador de AP para ativar APs adicionais. Mas, certifique-se de que suas configurações da porta principal e do porto de backup para cada gerente não sobrepõem. 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.

Q. Eu tenho uma controladora de Wireless LAN (WLC) 4402 e uso pontos de acesso lightweight (LAPs) 1240. Eu estou tentando habilitar a criptografia de 128 bits na WLC. Quando eu seleciono a criptografia WEP de 128 bits na WLC, eu recebo um erro que diz que não há suporte a 128 bits no 1240s: **[ERROR] spam_lrad.c 12839: Not creating SSID mde on CISCO AP xx: xx: xx: xx: xx: xx because WEP128 bit is not**

supported. Por que eu recebo este erro?

A. Os comprimentos de chaves mostrados nas WLCs são realmente o número de bits que existem no segredo compartilhado e não incluem o 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 escolhe o tamanho chave do 128-bit no WLC, é realmente uma criptografia da chave de WEP do 152-bit (128 + 24 IV). Somente os regaços do Cisco 1000 Series (AP1010, AP1020, AP1030) apoiam o uso do ajuste da chave de WEP do bit WLC 128.

Q. Por que eu recebo a mensagem de erro WEP key size of 128 bits is not supported on 11xx, 12xx and 13xx model APs. **Wlan will not be pushed to these Access Points.** quando tento configurar a WEP em uma WLC?

A. Em uma controladora Wireless LAN, quando você escolhe WEP estático como o método de segurança da camada 2, as opções de tamanho da chave WEP disponíveis são:

- 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 a WEP de 64 bits, você precisa de escolher **40 bits** como o tamanho da chave WEP. A controladora adiciona o IV de 24 bits para formar uma chave WEP de 64 bits. Similarmente, 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.

Q. Os clientes não podem autenticar a um WLAN que seja configurado para o WPA2 e o controlador indique o **apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Could not process the RSN and WARP IE's. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:00:0c:f1:0c:51:22, SSID:** <>. Por que eu recebo este erro?

A. Isto ocorre na maior parte 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 você instalou o patch de WPA2 da Microsoft para oferecer suporte à WPA2.
- Atualize o driver e o firmware do cliente.
- Desative as extensões Aironet na WLAN.

Q. Uma vez que eu recarrego o WLC, eu obtenho **segunda-feira o 17 de julho 15:23:28 uma anomalia 2006 MFP detectada - 3023 eventos inválidos MIC encontrados como violados pelo rádio 00:XX:XX:XX:XX e detectados pela relação do dot11 no slot 0 de AP 00:XX:XX:XX:XX em 300 segundos ao observar respostas da ponta de prova,** Mensagem de Erro dos **beacon frame.** Por que este erro ocorre e como eu obtenho livrado dele?

A. Este Mensagem de Erro é considerado quando os quadros com valores incorretos MIC são detectados por regaços permitidos MFP. Refira a proteção do quadro do Gerenciamento da infraestrutura (MFP) com WLC e DOBRE o exemplo de configuração para obter mais informações sobre de MFP. Termine uma destas quatro etapas:

1. Verifique e remova todo o rogue ou AP inválidos ou clientes em sua rede, que gerarem quadros inválidos.
2. Desabilite a infraestrutura MFP, se MFP não é permitido em outros membros do grupo da mobilidade como os regaços podem ouvir quadros do Gerenciamento dos regaços de outros WLC no grupo que não têm MFP permitido. Refira os Grupos de mobilidade FAQ do controlador do Wireless LAN (WLC) para obter mais informações sobre do grupo da mobilidade.
3. O reparo para este Mensagem de Erro está disponível nas liberações 4.2.112.0 e 5.0.148.2 WLC. Promova os WLC a qualquer uma destas liberações.
4. Como uma última opção, tente recarregar o REGAÇO que gerencie este Mensagem de Erro.

Q. O cliente AIR-PI21AG-E-K9 associa com sucesso com um Access Point (AP) usando a autenticação Protocolo flexível da autenticação extensível através do Tunelamento seguro (EAP-FAST). No entanto, quando o AP associado é desligado, o cliente não migra para outro AP. Esta mensagem é mostrada continuamente no log de mensagens da controladora: **"Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - perhaps the user is already logged onto the system? Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4".** Por quê?

A. 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/controladora, não responde a re-autenticações).

Isso é documentado no bug da Cisco ID CSCsd02837 (somente clientes registrados). 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 mobile também pode ocorrer devido a qualquer uma das seguintes razões:

- 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.

Q. Quando instalo o novo blade do Wireless Services Module (WiSM) no 6509 Switch e implemento o Protected Extensible Authentication Protocol (PEAP) no Microsoft IAS Server, eu recebo o seguinte erro: **`*Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.Reload Reason: FAILED CRYPTO INIT. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPP changed state to DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs no certs in the SSC Private File *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00:23.557: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD:`** Reload requested by LWAPP CLIENT. . Por quê?

A. O RAIO e o dot1x debugam a mostra que o WLC envia um pedido do acesso, mas não há nenhuma resposta do servidor de IAS. 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.

Q. Os pontos de acesso lightweight (LAPs) não se registram na controladora. O que pode ser o problema? Recebo as seguintes mensagens de erro na controladora: **`Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0. Thu Feb 3 03:20:47 2028:`** Unable to free public key for AP 00:0B:85:68:F4:F0.

A. Quando o ponto de acesso (AP) envia a solicitação de união do Lightweight Access Point Protocol (LWAPP) à WLC, ele inclui 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 usando a chave pública dos APs e verifica se certificado foi emitido por uma autoridade de certificação confiável. Ela também observa a data e hora de início do intervalo de validade do certificado do AP e compara a aquela data e o tempo às suas próprias data e hora.

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

Q. Um AP Lightweight Access Point Protocol (LWAPP) não é capaz de se unir à sua controladora. O log da controladora Wireless LAN (WLC) exibe uma mensagem similar a esta: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01. Por quê?

A. Você poderá receber esta mensagem de erro se o túnel LWAPP entre o AP e a WLC atravessar um caminho de rede com uma MTU inferior a 1500 bytes. Isto causa a fragmentação dos pacotes LWAPP. Este é um bug conhecido da controladora. Consulte o bug da Cisco ID CSCsd39911 (somente clientes registrados).

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

Q. Estou tentando estabelecer um tunelamento de convidado entre minha

controladora interna e a controladora 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 similar a esta: **Security Policy Mismatch for WLAN <Wlan ID>. Anchor Export Request from Switch IP:** <controller Ip address> Ignored. Qual é o problema?

A. O Tunelamento do convidado fornece a segurança adicional para o acesso de usuário convidado à rede Wireless 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 causado por uma inconsistência em qualquer uma das políticas de segurança configuradas para essa WLAN específica nas controladoras internas e da DMZ. Verifique se as políticas de segurança, bem como outras configurações como timeout da sessão, são atendidas.

Um outro motivo comum para esse problema é a controladora da DMZ não estar 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.

Q. Recebo várias 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?

A. Como o multicast é desabilitado nas controladoras, as mensagens que causam este alarme podem ser mensagens do 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.

Q. Recebo a mensagem de erro "[SECURITY] apf_foreignap.c 763: **STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port." Mensagem de Erro em** um de meus controladores. O que esse erro significa e que passos devo executar para resolvê-lo?

A. Esta mensagem é exibida quando a controladora recebe uma solicitação de DHCP para um endereço MAC para o qual não há 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. Algo que pode ser feito para ajudar a mitigar essa mensagem é permitir somente as VLAN que são usadas na controladora no tronco que vai para a controladora com o comando **switchport vlan allow** no switch.

Q. Porque eu recebo esta mensagem de erro no console: Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc?

A. Isto pode ser devido à carga elevada de utilização 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.

Isso é documentado na seção CPU da Controladora Sobrecarregada dos Release Notes dos Cisco Wireless LAN Controllers e Lightweight Access Points para Release 3.2.116.21.

Q. Eu recebo estas mensagens de erro de chaves da Wired Equivalent Privacy (WEP) em meu sistema de controle Wireless (WCS): `The WEP Key configured at the station may be wrong. Station MAC Address is 'xx: xx: xx: xx: xx: xx', AP base radio MAC is 'xx: xx: xx: xx: xx:` xx' and Slot ID is '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?

A. Se todas suas configurações relativas à segurança estão perfeitas, as mensagens que você recebe agora são causadas por bugs. Há alguns bug conhecidos na controladora. Consulte os bug da Cisco IDs CSCse17260 (clientes registrados somente) e CSCse11202 (clientes registrados somente), que indicam que “A chave WEP configurada na estação pode estar incorreta com os **clientes WPA e TKIP, respectivamente**”. Na realidade, o bug **CSCse17260** é uma duplicata de **CSCse11202**. A correção do bug **CSCse11202** já está disponível na WLC release 3.2.171.5.

Nota: Os releases de WLC mais recentes contêm uma correção para esses bugs.

Q. Usamos um servidor RADIUS externo para autenticar clientes Wireless através da controladora. A controladora envia esta mensagem de erro regularmente: no radius servers are responding. Por que nós vemos estas mensagens de erro?

A. Quando uma solicitação sai da WLC para o servidor Radius, cada pacote possui um número de sequência para o qual a WLC espera uma resposta. Se não há nenhuma 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. Isso é configurado na GUI da WLC em **Security > authentication-server**. O máximo é 30 segundos. Assim, talvez seja útil ajustar este valor de tempo limite para o máximo a fim de resolver o problema.

Às vezes, os servidores RADIUS executam **“descartes silenciosos”** do pacote de solicitação proveniente 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 marcará o servidor RADIUS como não respondendo.

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

Se o recurso **failover agressivo** estiver habilitado na WLC, a WLC será muito agressiva para marcar o servidor AAA como não respondendo. Contudo, isso não deveria ser feito porque o servidor AAA poderia não estar respondendo somente àquele cliente específico (ao fazer o descarte silencioso). Isso pode ser uma resposta a outros clientes válidos (com certificados válidos). No entanto, a WLC ainda poderia marcar o servidor AAA como não respondendo e não funcional.

Para resolver isso, desabilite o recurso de **failover agressivo**. Emita o **comando disable do agressivo-Failover do raio da configuração do** controlador CLI a fim executar isto. 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.

Q. Vários clientes são incapazes de se associar a um LWAPP e a controladora registra a mensagem de erro IAPP-3-MSGTAG015: `iappSocketTask:` iappRecvPkt returned error. Por que isso acontece?

A. Isto acontece na maior parte das vezes devido a um problema com os adaptadores Intel que oferecem suporte ao CCX v4, mas que executam uma versão do Client Bundle 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 ID CSCsi91347 (somente clientes registrados) para obter mais informações sobre esta mensagem de erro.

Q. Recebo esta mensagem de erro na Wireless LAN Controller (WLC): Reached Max EAP-Identity Request retries (21) for STA 00:05:4e:42:ad:c5. Por quê?

A. Esta mensagem de erro ocorre quando o usuário tenta se conectar a uma rede WLAN protegida por EAP e atinge o número máximo de tentativas de EAP pré-configurado. Quando o usuário falhar ao se autenticar, a controladora eliminará o cliente e o cliente não poderá se conectar à rede até que o temporizador da exclusão expire ou seja cancelado manualmente 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.

Q. Recebo esta mensagem de erro na Wireless LAN Controller (WLC): **Um alerta de switch da categoria é gerado com severidade 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?

A. Isso pode ocorrer devido ao bug da Cisco ID 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.

Q. Recebo uma mensagem de falha de perfil do ruído em Monitor > 802.11b/g Radios. Eu quero entender por que recebo essa mensagem de falha?

A. O status do perfil de ruído FAILED/PASSED é definido após o resultado do teste feito pela WLC e em comparação com o limite atual definido. 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 recomenda-se alterar as configurações depois de compreender claramente o design da rede e como ele afetará o desempenho da rede.

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

Q. Eu não consigo definir a porta 2 como a porta de backup na 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?

A. Um gerenciador de AP não possui 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. De forma geral, 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.

Q. Eu recebo a seguinte mensagem de erro: **The AP '00:0b:85:67:6b:b0' received a WPA MIC error on protocol '1' from Station '00:13:02:8d:f6:41'.** Counter measures have been activated and traffic has been suspended for 60 seconds. Por quê?

A. A Verificação de Integridade das Mensagens (MIC) incorporada no Wi-Fi Protected Access (WPA) inclui um contador de quadros que impede um ataque com o envolvimento de pessoas. Esse erro significa que alguém na rede está tentando reproduzir a mensagem que foi enviada

pelo cliente original ou pode significar que o cliente está com defeito.

Se um cliente falha repetidamente a verificação MIC, o controlador desabilita o WLAN na relação AP onde os erros são detectados por 60 segundos. A primeira falha MIC é registrada, e um temporizador é iniciado a fim permitir a aplicação das contramedidas. Se uma falha subsequente MIC ocorre dentro de 60 segundos da falha precedente a mais recente, a seguir um STA cuja a entidade do IEEE 802.1X atue como um suplicante deve o deauthenticate próprio ou o deauthenticate todos os STA com uma associação de segurança se sua entidade do IEEE 802.1X atuou como um autenticador.

Além disso, o dispositivo não recebe nem transmite nenhuns frames de dados TKIP-cifrada, e não recebe nem transmite nenhuns frames de dados unencrypted diferentes das mensagens do IEEE 802.1X, a ou de todo o par por um período de pelo menos 60 segundos depois que detecta a segunda falha. Se o dispositivo é um AP, recusa associações novas com o TKIP durante um este período de 60 segundos; no fim do período de 60 segundos, o AP recomeça operações normal e permite STA (com referência a) ao associado.

Isso impede um possível ataque no esquema de criptografia. Estes erros MIC não podem ser desligados em versões WLC antes de 4.1. Com versão 4.1 e mais recente do controlador do Wireless LAN, há um comando mudar o momento da varredura para erros MIC. O comando é **tkip da Segurança de WLAN da configuração mantém o id> <wlan do seconds> <0-60**. Use o valor 0 a fim desabilitar a detecção de falha MIC para contramedidas.

Q. A seguinte mensagem de erro pode ser vista nos logs da minha controladora: **[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed.** Por quê?

A. Essas mensagens de erro são vistas com mais frequência quando a porta do serviço da controladora está com 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 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.

Q. Meus clientes Wireless não conseguem se conectar à rede Wireless LAN (WLAN). O WiSM ao qual o ponto de acesso (AP) está conectado informa a seguinte mensagem: Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00. O que isso significa?

A. Como uma condição para acessar a mídia, a camada de MAC verifica o valor de seu vetor de atribuição 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 enviá-lo com base no comprimento e na taxa de dados do quadro. 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 está sendo falsificado (um ataque real em potencial) e você deverá confirmar se isso é verdade com uma captura de pacote.

Q. Depois que configuramos a controladora e a reinicializamos, não podemos mais acessá-la no modo seguro da Web (https). A seguinte mensagem de erro é recebido quando tento acessar a controladora no modo seguro da Web: **`Secure Web: Web Authentication Certificate not found (error)`**. Qual é a causa deste problema?

A. Pode haver diversas razões associadas 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 deste comando, você deve ver esta mensagem: Web Authentication certificate has been generated.

Agora, você deverá poder acessar o modo seguro da Web da controladora após a reinicialização.

Q. Os controladores relatam às vezes este mensagem de alerta do ataque da assinatura da inundação da desassociação IDS contra os clientes válidos em que o MAC address do atacante é aquele de um Access Point (AP) juntado a esse controlador: **`Alerta: IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'. The Signature description is 'Disassociation flood', with precedence 'x'. The attacker's mac address is 'hh: HH: HH: HH: HH: hh', channel number is 'x', and the number of detections is 'x'.`** Por que isso ocorre?

A. Isso ocorre devido ao bug da Cisco ID CSCsg81953 (somente clientes registrados).

Os ataques de Inundação de Desassociação de IDS contra clientes válidos são algumas vezes relatados em situações em que o endereço MAC do agressor é o mesmo endereço de um AP associado a essa controladora.

Quando um cliente está associado ao AP mas para de se comunicar com ele devido à remoção da placa, a sair do alcance, etc., o AP espera por ele até o timeout de ociosidade. 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.

Q. Eu recebo esta mensagem de erro no syslog da controladora: **[WARNING] apf_80211.c 2408: Received a message with an invalid supported rate from station <xx: xx: xx: xx: xx: xx: xx> [ERROR] apf_utils.c 198: Missing Supported Rate.** Por quê?

A. Na realidade, as mensagens de ausência de taxa com suporte indicam que a WLC está configurada para determinadas taxas de dados obrigatórios nas opções de Wireless, mas a placa NIC não possui 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. Este Syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Descodifique Msg: não podia combinar o** Mensagem de Erro do **<id> do ID de WLAN** é a transmissão em nossa rede. Por que isto ocorre e como eu paro-o?

A. Esta mensagem é transmissão pelos regaços. Isto está visto quando você configurou a característica da ultrapassagem WLAN para um WLAN e esse WLAN particular não está anunciado.

Configurar o `syslog host 0.0.0.0 global ap da configuração` a fim pará-lo ou você pode pôr um endereço IP de Um ou Mais Servidores Cisco ICM NT específico se você tem um servidor de SYSLOG de modo que a mensagem seja transmissão ao server apenas.

Q. Eu recebo a seguinte mensagem de erro em minha controladora Wireless LAN (WLC): **[ERROR] File: apf_mm.c : Linha: 581 : Announce collision for mobile 00:90:7a:05:56:8a, deleting.** Por quê?

A. Geralmente, essa mensagem de erro indica que a controladora anunciou colisões para um cliente Wireless (isto é, APs separados anunciam que possuem o cliente), mas ela não recebeu uma entrega 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

haver uma anomalia relacionada a um cliente ou a uma condição específica.

Q. Minha controladora gera esta mensagem de alarme: Coverage threshold of '12' violated. O que é esse erro e como posso resolvê-lo?

A. Essa mensagem de alarme é gerada quando uma razão sinal-ruído (SNR) do cliente cai abaixo do 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 um furo de cobertura existe quando os níveis de SNR dos clientes caem abaixo de um determinado limite de SNR. Esse limite de SNR varia com base em dois valores: A potência de transmissão do AP e o valor do perfil de cobertura da controladora.

Em 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 de SNR do cliente (|dB|) = [Potência de transmissão do 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.

Q. Estou usando o ACS v 4.1 e uma controladora Wireless LAN (WLC) 4402. Quando a WLC tenta autenticar o MAC de um cliente Wireless como ACS 4.1, o ACS não responde com o ACS e relata esta mensagem de erro: O "*erro interno ocorreu*". Todas as minhas configurações estão corretas. Por que este erro interno ocorre?

A. O bug da Cisco ID CSCsh62641 relativo à autenticação (somente clientes registrados) no ACS 4.1 refere-se à mensagem de erro de erro interno do ACS.

Este erro pode ser o problema. Há um patch disponível para este bug na página Downloads do ACS 4.1 (somente clientes registrados) que deve resolver o problema.

Q. A Cisco 4400 Series Wireless LAN Controller (WLC) não inicializa. Esta mensagem de erro é recebida na controladora: `** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg:` 10 ** Can't read from device 0. Por quê?

A. 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.

Q. 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. As seguintes mensagens de erro são adicionadas ao log de mensagens: `Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Cannot allocate new Mbuf. Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbufs.` Por quê?

A. Isso ocorre devido ao bug da Cisco ID CSCsh93980 (somente clientes registrados). Esse bug foi resolvido na versão 4.1.185.0 da WLC. Promova seu controlador a fim superar a esta versão de software ou a mais tarde esta mensagem.

Q. Atualizamos nossa controladora Wireless LAN (WLC) 4400 para o código 4.1, mas nosso syslog foi bombardeado por mensagens como: `May 03 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) received with invalid SPA 192.168.1.233/TPA 192.168.1.233. Que essas mensagens indicam?

A. Isso pode ocorrer quando a WLAN é marcada como DHCP obrigatório. Nesses casos, somente as estações que recebem o endereço IP via DHCP podem se associar. Não são permitidos aos clientes estáticos associar a este 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.

Q. Quando você usa o recurso de Power over Ethernet (PoE) na Cisco 2106 Wireless LAN Controller , os rádios AP não são habilitados. O AP é incapaz de verificar alimentação in-line suficiente. `A mensagem de erro Radio slot disabled.` é exibida a mensagem de erro. Como posso corrigir isso?

A. Essa mensagem de erro ocorre quando o switch que alimenta o ponto de acesso é um switch pré-padrão, mas o AP não oferece suporte ao modo pré-padrão de alimentação 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 habilitar o modo **pré-padrão de** potência no AP que está sujeito a essa mensagem de erro. Isso pode ser feito na CLI da controladora 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 o software release 4.1 de um release 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

Q. A controlador gera uma mensagem do syslog dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: `Unable to add an ARP entry for xx: xx. - xxx.x ao processador de rede. entry does not exist.` semelhante a esta. O que essa mensagem do syslog significa?

A. Enquanto alguns clientes wireless enviam respostas ARP, a unidade de processador de rede (NPU) precisa conhecer essas respostas. Assim, 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 sobre a funcionalidade da WLC devido a isso, mas a WLC gera essa mensagem do syslog.

Q. Instalei e configurei uma nova 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.

A. A falha do sensor de temperatura interna é cosmética e pode ser resolvida com uma atualização para a versão 4.2.61.0 da WLC.

As WLCs 2106 e 526 **produzidas a partir de 01/07/2007** podem usar chips de sensor de temperatura de outros fabricantes. Esse novo sensor funciona muito bem, mas não é compatível com o software posterior ao release 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.

O bug da Cisco ID CSCsk97299 (somente clientes registrados) refere-se a esse problema. Esse erro é mencionado nos Release Notes da versão 4.2 da WLC.

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

A. Essa mensagem de erro significa que a controladora não foi capaz de entrar em contato com o servidor RADIUS padrão ou que não havia um servidor definido.

Uma possível razão para esse comportamento é o bug da Cisco ID CSCsk08181 (somente clientes registrados), o qual 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: Interface 1 source MAC address is not found.` é mostrada na controladora Wireless LAN (WLC). Que ela significa?

A. Ela significa que a controladora encontrou um erro ao enviar um pacote proveniente da CPU.

Q. As seguintes mensagens de erro são exibidas na controladora Wireless LAN (WLC):

- `Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'cliWebInitParms.cfg'`
- `Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'rfidInitParms.cfg'`
- `Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'dhcpParms.cfg'`
- `Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'bcastInitParms.cfg'`
- `18 de março 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Não suprimem do arquivo: remoção do arquivo sshpmInitParms.cfg falhada. - Processo: Nome: fp_main_task, Id:11ca7618`
- `18 de março 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Não suprimem do arquivo: remoção do arquivo bcastInitParms.cfg falhada. - Processo: Nome: fp_main_task, Id:11ca7618`

O que essas mensagens de erro indicam?

A. Estas mensagens são mensagens informativa e são parte do procedimento normal da bota. Estas mensagens aparecem devido a uma falha ler ou suprimir de diversos arquivos de configuração diferentes. Quando os arquivos de configuração específica não são encontrados ou se o arquivo de configuração não pode ser lido, a sequência da configuração para cada processo manda esta mensagem, por exemplo, nenhuma configuração do servidor DHCP, nenhuma configuração das etiquetas (RF ID), e assim por diante. Estas são as mensagens da baixo-severidade que podem com segurança ser ignoradas. Essas mensagens não interrompem a operação da controladora.

Q. A mensagem 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 00:14:XX:02:XX:XX in contained state - no available AP to contain. é exibida.` é exibida a mensagem de erro. Que ela significa?

A. Isto significa que o AP que executou a função desonesto da retenção está já não disponível, e o controlador não pode encontrar nenhum AP apropriado para executar a retenção desonesto.

Q. `O DTL-1-ARP_POISON_DETECTED: O STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (1 op) recebido com` mensagem de sistema `inválido dos TERMAS 192.168.1.152/TPA 192.168.0.206` aparece no controlador do Wireless LAN. Que esta mensagem implica?

A. É possível que o sistema detectou a falsificação ou o envenenamento ARP. Mas, esta mensagem não implica necessariamente que toda a falsificação maliciosa ARP ocorreu. A mensagem aparece quando estas circunstâncias são verdadeiras:

- Um WLAN é configurado com o DHCP exigido, e um dispositivo do cliente, após a associação nesse WLAN, transmite um mensagem ARP sem o primeiro DHCP de terminação. Este pode ser comportamento normal; pode acontecer, por exemplo, quando o cliente está endereçado estaticamente, ou quando o cliente guarda um aluguel de DHCP

válido de uma associação prévia. O Mensagem de Erro pode olhar como 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 desta circunstância é que o cliente é incapaz de enviar ou receber todo o tráfego de dados, até que ele DHCPs com o WLC.Refira a seção das mensagens DTL do Guia de Mensagens do Sistema do controlador de LAN do Cisco Wireless para mais informação.

Q. Os regaços não usam a potência sobre os Ethernet (PoE) pôr acima. Eu ver que entra o controlador do 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`** Que é o problema?

A. Isto pode acontecer se a potência sobre ajustes dos Ethernet (PoE) não é configurada corretamente. Quando um Access point que esteja convertido ao modo leve, por exemplo, um AP1131 ou um AP1242, ou um Access point do 1250 Series é posto por um injetor de energia que esteja conectado a um interruptor PRE-inteligente do gerenciamento de energia de Cisco (PRE-IPM), você precisa de configurar a potência sobre os Ethernet (PoE), igualmente conhecidos como a potência em linha.

Refira configurar a potência sobre Ethernet para obter mais informações sobre de como configurar a potência sobre os Ethernet (PoE).

Q. Você vê esta mensagem no controlador do 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`** Que ela significa?

A. O Lightweight Access Points segue um determinado algoritmo para encontrar um controlador. A descoberta e junta-se ao processo é explicada em detalhe no registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (o WLC)

Este Mensagem de Erro está considerado no WLC, quando recebe um pedido da descoberta depois que alcançou sua capacidade do máximo AP.

Se o controlador principal para um REGAÇO não é configurado ou se seu um novo fora do REGAÇO da caixa, manda pedidos da descoberta LWAPP a todos os controladores alcançáveis. Se a descoberta pede alcances um controlador que seja executado em sua capacidade completa AP, o WLC obtém os pedidos e realiza que está em sua capacidade do máximo AP, e não responde ao pedido e dá este erro.

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

A. Consulte o Guia de Mensagens do Sistema da Cisco Wireless LAN Controller 4.2 para obter mais informações sobre as mensagens de sistema do LWAPP.

Q. **`o erro que extrai o`** Mensagem de Erro dos **`arquivos do webauth`** aparece no controlador do Wireless LAN (WLC). Que ela significa?

A. O WLC não carrega um pacote feito sob encomenda da autenticação da Web/transmissão se qualquer dos arquivos empacotados tem maior de 30 caráteres no nome de arquivo, que inclui a

extensão de arquivo. O pacote personalizado do AUTH da Web tem um limite de até 30 caráteres para nomes de arquivo. Assegure-se de que nenhum nome de arquivo dentro do pacote esteja maior de 30 caráteres.

Q. Os controladores do Wireless LAN (WLC), executando o código 5.2 ou 6.0 com um grande número grupos AP, a Web GUI não podem indicar todos os grupos configurados AP. Que é o problema?

A. Os grupos faltantes AP podem ser considerados se você usa a **mostra que** CLI os ap-**grupos wlan** comandam.

Tente adicionar um grupo adicional AP à lista. Por exemplo, 51 grupos AP distribuídos, e os 51st faltam (página 3). Adicionar o 52nd grupo, e a página 3 deve publicar-se na Web GUI.

A fim resolver esta edição, elevação à versão 7.0.220.0 WLC.

Informações Relacionadas

- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Perguntas Frequentes de Troubleshooting de WiSM
- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems