Solução de problemas de um ponto de acesso leve que não se junta a um Wireless LAN Controller

Índice

Introdução

Este documento fornece uma visão geral do processo de junção e detecção do Wireless LAN Controller (WLC). Este documento também fornece informações sobre alguns dos problemas porque um ponto de acesso leve (LAP) falha ao se juntar ao WLC e como solucionar esses problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração dos LAPs e dos WLCs da Cisco
- Conhecimento básico do protocolo de ponto de acesso leve (LWAPP)

Convenções

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

Visão geral do processo de junção e de detecção do Wireless LAN Controller (WLC)

Em uma rede sem fio unificada da Cisco, os LAPs devem primeiro detectar e se juntarem ao WLC para poderem atender os clientes sem fio.

Originalmente, os controladores apenas funcionavam no modo de camada 2. No modo de camada 2, os LAPs precisam estar na mesma sub-rede que a interface de gerenciamento, e a interface do gerenciador AP no modo de camada 3 não está presente no controlador. Os LAPs comunicam-se com o controlador usando apenas um encapsulamento da camada 2 (encapsulamento de ethernet) e não utilizam Dynamic Host Configuration Protocol (DHCP) para um endereço IP.

Quando o modo de camada 3 no controlador foi desenvolvido, uma nova interface de camada 3 chamada gerenciador AP foi introduzida. No modo de camada 3, os LAPS utilizam DHCP para um endereço IP primeiro e, depois, enviam a solicitação de detecção para a interface de gerenciamento usando os endereços IP (Camada 3). Isso permitiu que o LAPs ficassem em uma sub-rede diferente do que a interface de gerenciamento do controlador. O modo de camada 3 é o modo atual predominante. Alguns controladores e LAPs apenas podem ser executados no modo de camada 3.

Contudo, isso apresentou um problema novo: como os LAPs encontraram o endereço IP de

gerenciamento do controlador quando estavam em uma sub-rede diferente?

No modo de camada 2, eles precisavam ficar na mesma sub-rede. No modo de camada 3, o controlador e o LAP estão essencialmente em um jogo de ocultar/exibir na rede. Se você não informar o LAP onde o controlador está através da opção 43 do DHCP, a resolução de DNS do “Cisco-lwapp-controller@local_domain”, ou não configurá-lo estaticamente, o LAP não saberá onde encontrar na rede a interface de gerenciamento do controlador.

Além desses métodos, o LAP procura automaticamente na sub-rede local os controladores com um broadcast local de 255.255.255.255. Também, o LAP recorda o endereço IP de gerenciamento de qualquer controlador que tenha se juntado através de reinicializações. Portanto, se você colocar o LAP primeiro na sub-rede local da interface de gerenciamento, ele encontrará a interface de gerenciamento do controlador e lembrará o endereço. Isso é chamado de fornecimento. Isso não ajudará a encontrar o controlador se você substituir um LAP posteriormente. Portanto, a Cisco recomenda usar a opção 43 do DHCP ou os métodos DNS.

Quando os LAPs detectam o controlador, eles sabem se o controlador está no modo de camada 2 ou no modo de camada 3. Portanto, os LAPs sempre conectam-se ao endereço da interface de gerenciamento do controlador com uma solicitação de detecção primeiro. O controlador informa então o LAP em que modo ele está na resposta da detecção. Se o controlador estiver no modo de camada 3, a resposta da detecção conterá o endereço IP do gerenciador AP da camada 3, de forma que o LAP poderá enviar uma solicitação de junção para interface do gerenciador AP em seguida.

Nota: Por padrão, as interfaces do gerenciador AP e de gerenciamento são deixadas sem etiquetas em suas VLAN durante a configuração. Caso elas tenham uma etiqueta, verifique se elas estão etiquetadas para a mesma VLAN para receberem corretamente a resposta da junção e da detecção do WLC.

O AP do LWAPP passa por esse processo na inicialização para o modo de camada 3:

1. O LAP inicializa e usa DHCPs em um endereço IP se ele não tiver sido atribuído anteriormente como um endereço IP estático.
2. O LAP envia uma solicitação de detecção para os controladores através de vários algoritmos de detecção e cria uma lista de controladores. Essencialmente, o LAP informa o máximo de endereços de interface de gerenciamento que for possível para a lista de controladores através do seguinte:Opção 43 de DHCP (boa para empresas globais em que os escritórios e os controladores estão em continentes diferentes)Entrada de DNS para cisco-capwap-controller (boa para empresas locais - também pode ser usada para localizar onde os APs totalmente novos se juntam)**Nota:** Se você usa CAPWAP, verifique se há uma entrada de DNS para cisco-capwap-controller.Endereços IP de gerenciamento dos controladores que o LAP recorda previamenteUm broadcast da camada 3 na sub-redeProvisionamento via OTAInformações configuradas estaticamenteDesta lista, o método o mais fácil a usar-se para o desenvolvimento é ter os regaços na mesma sub-rede como a interface de gerenciamento do controlador e permitir que a transmissão da camada 3 do s do de LAPâ encontre o controlador. Esse método deve ser usado para empresas que possuem uma rede pequena e não possuem um servidor DNS local.O próximo método de implantação mais fácil é usar uma entrada de DNS com DHCP. Você pode ter entradas múltiplas do mesmo nome de DNS. Isso permite que o LAP detecte vários controladores. Esse método deve ser usado pelas empresas que têm todos os seus controladores em um único local e possuem um servidor DNS local. Ou, se a empresa tiver vários sufixos DNS e os

controladores estiverem segregados por sufixo.A opção 43 de DHCP é usada por grandes empresas para localizar as informações através do DHCP. Esse método é usado por grandes empresas que possuem um sufixo DNS único. Por exemplo, a Cisco possui edifícios na Europa, na Austrália e nos Estados Unidos. Para garantir que os LAPS se juntem apenas a controladores localmente, a Cisco não pode usar uma entrada de DNS e deve usar as informações da opção 43 de DCHP para informar os LAPs qual é o endereço IP de gerenciamento de seu controlador local.Finalmente, a configuração estática é usada para uma rede que não tenha um servidor DHCP. Você pode estaticamente configurar a informação necessária juntar-se a um controlador através da porta de Console e do s CLI do de APâ. Para obter informações sobre como configurar estaticamente as informações do controlador usando a CLI do AP, consulte Manually Configuring Controller Information Using the Access Point CLI.Para obter uma explicação detalhada sobre os diferentes algoritmos de detecção que os LAPs usam para localizar controladores, consulte LAP Registration with WLC.Para obter informações sobre a configuração da opção 43 de DHCP em um servidor DHCP, consulte DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example.

3. Envie uma solicitação de detecção para cada controlador na lista e aguarde a resposta de detecção do controlador que contém o nome do sistema, os endereços IP do gerenciador AP, o número de APs já anexados a cada interface do gerenciador AP e a capacidade excedente total para o controlador.
4. Veja a lista de controladores e envie uma solicitação de junção a um controlador nessa ordem (apenas se o AP recebeu uma resposta de detecção dele):Nome do sistema do controlador principal (configurado previamente no LAP)Nome do sistema do controlador secundário (configurado previamente no LAP)Nome do sistema do controlador terciário (configurado previamente no LAP)Controlador mestre (se o LAP não tiver sido configurado previamente com os nomes de controlador principal, secundário ou terciário. Usado sempre para saber a qual controlador totalmente novo que os LAPs se junta)Se nenhuma opção acima for visualizada, equilibre a carga entre os controladores usando o valor de capacidade excedente na resposta da detecção.Se dois controladores tiverem a mesma capacidade excedente, envie a solicitação de junção para o primeiro controlador que respondeu à solicitação de detecção com uma resposta de detecção. Se um único controlador tiver vários gerenciadores AP em várias interfaces, escolha a interface do gerenciador AP com o menor número de APs.O controlador responderá a todas as solicitações de detecção sem verificar os certificados ou as credenciais AP. Contudo, as solicitações de junção precisam ter um certificado válido para obter uma resposta de junção do controlador. Se o LAP não receber uma resposta de junção de sua escolha, ele tentará o próximo controlador na lista, exceto se o controlador for um controlador configurado (Principal/Secundário/Terciário).
5. Quando recebe a resposta da junção, o AP verifica se possui a mesma imagem que a do controlador. Se não tiver, o AP faz o download da imagem a partir do controlador e reinicializa para carregar a nova imagem e inicia o processo novamente a partir da etapa 1.
6. Se tiver a mesma imagem do software, ele pedirá a configuração ao controlador e mudará para o estado registrado no controlador.Depois que você fizer o download da configuração, o AP poderá ser recarregado novamente para aplicar a nova configuração. Portanto, um recarregamento extra poderá ocorrer. Isso é um comportamento normal.

Depurar do controlador

Existem alguns comandos de **depuração** no controlador que você pode usar para ver o processo completo na CLI.

- **debugar** pacotes de descoberta das mostras do do do **enableâ dos eventos do lwapp** e junte-se a pacotes.
- **debugar a** informação do nível do pacote das mostras do do do **enableâ do pacote lwapp da** descoberta e junte-se a pacotes.
- **debugar o** processo de validação certificada das mostras do do do **enableâ do pki pm**.
- **debugar o** do do **desabilitação-allâ** gerencie debuga fora.

Com um aplicativo de terminal que possa capturar a saída para um arquivo de registro, acesse o console ou secure shell (SSH)/Telnet para o controlador e insira estes comandos:

config session timeout 120 config serial timeout 120 show run-config (and spacebar thru to collect all) **debug mac addr** <*ap-mac-address*> (in xx:xx:xx:xx:xx format) **debug client** <*ap-mac-address*> **debug lwapp events enable debug lwapp errors enable debug pm pki enable**

Após a captura das depurações, use o comando **debug disable-all** para desligar todas as depurações.

As próximas seções mostram a saída desses comandos de **depuração** quando o LAP se registra com o controlador.

debug lwapp events enable

Esse comando fornece informações sobre os eventos e erros do LWAPP que ocorrem durante o processo de detecção e junção do LWAPP.

Essa é a saída do **comando debug lwapp events enable** para um LAP que tem a mesma imagem que a do WLC:

Nota: Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.

debug lwapp events enable Wed Oct 24 16:59:35 2007: 00:0b:85:5b: fb:d0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b: fb:d0 to 00:0b:85:33:52:80 on port '2' *!--- LWAPP discovery request sent to the WLC by the LAP.* Wed Oct 24 16:59:35 2007: 00:0b:85:5b:fb:d0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2 *!--- WLC responds to the discovery request from the LAP.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2' *!--- LAP sends a join request to the WLC.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 AP ap:5b:fb:d0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:5B:FB:D0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 LWAPP Join-Request MTU path from AP 00:0b:85:5b:fb:d0 is 1500, remote debug mode is 0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully added NPU Entry for AP 00:0b:85:5b:fb:d0 (index 55) Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0 AP IP: 10.77.244.219, AP Port: 49085, next hop MAC: 00:0b:85:5b:fb:d0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:5b:fb:d0 *!--- WLC responds with a join reply to the LAP.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Register LWAPP event for AP 00:0b:85:5b:fb:d0 slot 0 -- LAP registers with the WLC Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 *!--- LAP requests for the configuration information from the WLC.* Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Updating IP info for AP 00:0b:85:5b:fb:d0 -- static 1, 10.77.244.219/255.255.255.224, gtw 10.77.244.220 Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: Send AP Timesync of 1193245188 source MANUAL Wed Oct 24 16:59:48 2007:

```
spamEncodeDomainSecretPayload:Send domain secret
TSWEBRET<0d,59,aa,b3,7a,fb,dd,b4,e2,bd,b5,e7,d0,b2,52,4d,ad,21,1a,12> to AP 00:0b:85:5b:fb:d0
Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:5b:fb:d0 !--- WLC responds by providing all the necessary configuration information
to the LAP. Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'eap fast' Wed
Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48
2007: Running spamEncodeCreateVapPayload for SSID 'webauth' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'eap fast' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'webauth' . . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0
Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5b:fb:d0 . . Wed
Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP Up event for AP 00:0b:85:5b:fb:d0 slot 0!
!--- LAP is up and ready to service wireless clients. Wed Oct 24 16:59:48 2007:
00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5b:fb:d0 . . . Wed Oct
24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP RRM_CONTROL_RES from AP 00:0b:85:5b:fb:d0 !--
- WLC sends all the RRM and other configuration parameters to the LAP.
```

Como mencionado na seção anterior, quando um LAP tiver se registrado com um WLC, ele verificará para saber se tem a mesma imagem que o controlador. Se as imagens no LAP e no WLC forem diferentes, os LAPs farão o download da nova imagem a partir do WLC primeiro. Se o LAP tiver a mesma imagem, ele continuará a fazer o download da configuração e de outros parâmetros a partir do WLC.

Você verá essas mensagens na saída do **comando debug lwapp events enable** se o LAP fizer o download de uma imagem a partir do controlador como parte do processo de registro:

```
Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from AP
00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from
AP 00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES
from AP 00:0b:85:5b:fb:d0
```

Uma vez que o download de imagem estiver concluído, o LAP será reinicializado e executará a detecção e se juntará ao algoritmo novamente.

debug pm pki enable

Como parte do processo de junção, o WLC autentica cada LAP verificando se o seu certificado é válido.

Quando o AP envia a solicitação de junção do LWAPP para o WLC, ele integra o seu certificado X.509 na mensagem do LWAPP. O AP também gera um ID de sessão aleatório que também é incluído na solicitação de junção do LWAPP. Quando o WLC recebe a solicitação de junção do LWAPP, ele valida a assinatura do certificado X.509 usando a chave pública do AP e verifica se o certificado foi emitido por uma autoridade de certificado confiável.

Igualmente olha a data de início e o momento para o intervalo da validez do certificado AP e compara a aquela data e o tempo a sua própria data e hora (daqui o pulso de disparo do do do controllerâ s precisa de ser ajustado perto da data atual e hora). Se o certificado X.509 for validado, o WLC gerará uma chave de criptografia AES aleatória. O WLC coloca a chave AES em seu mecanismo de criptografia de modo que ele possa criptografar e descriptografar mensagens futuras de controle que serão trocadas com o AP. Observe que os pacotes de dados são enviados no túnel do LWAPP entre o LAP e o controlador.

O **comando debug pm pki enable** mostra o processo de validação de certificado que ocorre durante a fase de junção no controlador. O **comando debug pm pki enable** também exibirá a chave hash do AP durante o processo de junção se o AP tiver um certificado autoassinado (SSC) criado pelo programa de conversão do LWAPP. Se o AP tiver um certificado instalado pelo

fabricante (MIC), você não verá uma chave hash.

Nota: Todos os APs que foram fabricados após junho de 2006 possuem um MIC.

Aqui está a saída do **comando debug pm pki enable**quando o LAP com um MIC junta-se ao controlador:

Nota: Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.

```
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: locking ca cert table
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b8591c3c0, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <issuer>  C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:91:c3:c0
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 2d812f0c
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 20f00bf3
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: user cert verfied using >bsnOldDefaultCaCert< Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: ValidityString (current): 2007/10/25/13:52:59 Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: AP version is 0x400d900, sending Cisco ID cert...
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <cscoDefaultIdCert> Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59
2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 2, ID cert >bsnSslWebadminCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 3, ID cert >bsnSslWebauthCert< Thu Oct 25 13:52:59 2007:
sshpmGetIssuerHandles: Airespace ID cert ok; sending it... Thu Oct 25 13:52:59 2007:
sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing
to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row
4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 5,
CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCID: comparing to row 0, ID
cert >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromHandle: calling
sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: called
```

```
to get cert for CID 156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 0,
certname >bsnOldDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
1, certname >bsnDefaultRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 2, certname >bsnDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 3, certname >bsnDefaultBuildCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing
to row 4, certname >cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID:
comparing to row 5, certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007:
sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03
2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: called to get cert for CID 156af135 Thu Oct 25 13:53:03
2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 3, certname >bsnDefaultBuildCert< Thu
Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 4, certname
>cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 5,
certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: called to
encrypt 16 bytes Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: successfully encrypted, out is
192 bytes Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for CID 156af135 Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: match in row 0
Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 172 bytes Thu
Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 24 bytes Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25 13:53:03
2007: sshpmPrivateKeyEncrypt: encrypted bytes: 384 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: called with 0xae0c358 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: freeing public key
```

Para um LAP com um SSC, o **comando debug pm pki enable** terá esta aparência. Observe que o hash SSC também é visto nessa saída.

Nota: Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.

```
(Cisco Controller) > debug pm pki enable Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate
<bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
cscoDefaultMfgCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert< Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on
Public Key Data Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122
300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003
82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd
7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0
39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3
9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce
cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e
c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e
c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db
251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc
1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490
881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b
d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693
f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f
76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3
```

```
b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f
de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8
eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301
0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This is the actual SSC key-hash value. Mon May 22
06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode
is 0
```

Depurar do LAP

Se o depurador do controlador não indicar uma solicitação de junção, você poderá depurar o processo a partir do LAP contanto que o LAP tenha uma porte de console. Você pode ver o processo de inicialização do LAP com esses comandos, mas primeiro você precisa entrar no modo de ativação (a senha padrão é Cisco):

- **debugar a** informação da opção de DHCP 43 das mostras do do do **detailâ DHCP**.
- **debugar o** do do **udpâ IP** mostra a junta/pacotes de descoberta ao controlador assim como às perguntas DHCP e DNS (toda a estes é pacotes de UDP. A porta 12223 é a porta de origem do s do do controllerâ).
- **debugar** eventos das mostras LWAPP do do do **eventâ do cliente do lwapp** para o AP.
- as inutilizações do do do **allâ do undebug** debugam no AP.

Aqui está um exemplo da saída do comando **debug ip udp**. Essa saída parcial dá uma ideia dos pacotes que são enviados pelo LAP durante o processo de inicialização para detectar e juntar-se a um controlador.

```
UDP: sent src=10.77.244.199(20679), dst=10.77.244.208(12223)
!--- LWAPP Discovery Request sent to a controller to which !--- the AP was previously registered
to. UDP: sent src=10.77.244.199(20679), dst=172.16.1.50(12223) !--- LWAPP Discovery Request
using the statically configured controller information. UDP: sent src=10.77.244.199(20679),
dst=255.255.255.255(12223) !--- LWAPP Discovery Request sent using subnet broadcast. UDP: sent
src=10.77.244.199(20679), dst=172.16.1.51(12223) !--- LWAPP Join Request sent to AP-Manager
interface on statically configured controller.
```

Evitar problemas relacionados ao DHCP

Os LAPs que usam DHCP para encontrar um endereço IP antes que eles comecem o processo de detecção do WLC podem ter problemas no recebimento de um endereço DHCP devido a um erro de configuração dos parâmetros relacionados ao DHCP. Esta seção explica como o DHCP funciona com WLCs e fornece algumas instruções recomendadas para evitar problemas relacionados ao DHCP.

Para o DHCP, o controlador comporta-se como um roteador com um endereço IP auxiliar. Isto é, ele preenche o endereço IP do gateway e encaminha a solicitação através de um pacote unicast diretamente para o servidor DHCP.

Quando a oferta do DHCP retorna ao controlador, ele altera o endereço IP do servidor DHCP para o seu endereço IP virtual. A razão para ele fazer isso é porque quando o Windows move-se entre APs, a primeira coisa que ele faz é tentar contatar o servidor DHCP e renovar o endereço.

Se o endereço do servidor DHCP for 1.1.1.1 (endereço IP virtual típico em um controlador), o controlador poderá interceptar esse pacote e rapidamente responder ao Windows.

Isso é também porque o endereço IP virtual é o mesmo em todos os controladores. Se um laptop com o Windows mover para um AP em um outro controlador, ele tentará contatar a interface

virtual no controlador. Devido ao evento de mobilidade e à transferência do contexto, o controlador novo para o qual o cliente do Windows moveu-se possui todas as informações para responder ao Windows novamente.

Se você quiser usar o servidor DHCP interno no controlador, tudo que você tem que fazer é colocar o endereço IP de gerenciamento como o servidor DHCP na interface dinâmica que você criou na sub-rede. Depois, atribua essa interface à WLAN.

A razão pela qual o controlador precisa de um endereço IP em cada sub-rede é para que ele possa preencher o endereço do gateway DHCP na solicitação do DHCP.

Estes são alguns pontos a serem lembrados quando você for configurar servidores DHCP para a WLAN:

1. O endereço IP do servidor DHCP não deve estar dentro de nenhuma sub-rede dinâmica que estiver no controlador. Ele será bloqueado, mas poderá ser substituído por este comando: **`config network mgmt-via-dynamic-interface`** `on version 4.0 only (command not available in version 3.2)`
2. O controlador enviará o DHCP através do unicast de sua interface dinâmica (no código mais recente) usando o seu endereço IP nessa interface. Certifique-se de que qualquer firewall permita que esse endereço acesse o servidor DHCP.
3. Certifique-se de que a resposta do servidor DHCP possa alcançar o endereço dinâmico do controlador nessa VLAN através de todos firewalls. Execute ping no endereço da interface dinâmica a partir do servidor DHCP. Execute ping no servidor DHCP com um endereço IP de origem do endereço de gateway da interface dinâmica.
4. Certifique-se de que a VLAN do AP seja permitida nos switches e roteadores e que as suas portas estejam configuradas como troncos de forma que os pacotes (incluindo o DHCP) etiquetados com a VLAN sejam permitidos através da rede com fio.
5. Assegure-se de que o servidor DHCP esteja configurado para atribuir um endereço IP na VLAN do AP. Você também pode configurar o WLC como um servidor DHCP. Para obter mais informações sobre como configurar o servidor DHCP no WLC, consulte Using the GUI to Configure DHCP section of Cisco Wireless LAN Controller Configuration Guide, Release 5.0.
6. Verifique se o endereço IP do controlador em sua interface dinâmica estará dentro de um dos escopos de DHCP no servidor DHCP.
7. Finalmente, verifique se você não está usando um servidor DHCP que não responde a solicitações DHCP do unicast, como o PIX.

Se você não pode resolver o problema de DHCP, existem duas soluções:

- Tente um servidor DHCP interno. Configure o endereço do servidor DHCP na interface dinâmica para ser o endereço IP de gerenciamento e, depois, o pool interno DHCP. Se o escopo de DHCP for permitido, isso deverá funcionar.
- Verifique se não há nenhuma resposta à solicitação DHCP enviando a saída para a CLI (console ou SSH) a partir dessas depurações:`0. debug mac addr <mac address>`
  `1. debug dhcp message enable`
  `2. debug dhcp packet enable` Isso deve indicar que o pacote DHCP foi enviado, mas que o controlador não recebeu uma resposta.

Finalmente, devido à segurança no controlador, não é recomendado colocar uma VLAN ou uma sub-rede no controlador que também contenha os LAPs, exceto se ele estiver na sub-rede da interface de gerenciamento.

Nota: O servidor RADIUS ou servidor DHCP não deve ficar em nenhuma das sub-redes da interface dinâmica do controlador. A segurança bloqueará os pacotes de retorno que tentarem se comunicar com o controlador.

Usar servidores de syslog para solucionar problemas do processo de junção do LAP

O software do controlador versão 5.2 permite que você configure os APs para enviar todos os erros relacionados ao CAPWAP ao servidor de syslog. Você não precisa ativar nenhum comando de depuração no controlador porque todas as mensagens de erro do CAPWAP podem ser visualizadas no servidor de syslog. Para obter mais informações sobre esse recurso e os comandos usados para ativá-lo, leia a seção Troubleshooting the Access Point Join Process of the configuration guide Cisco Wireless LAN Controller Configuration Guide, Release 5.2.

O LAP não se junta ao controlador, por quê?

Verifique os princípios básicos primeiro

- O AP e o WLC podem se comunicar?
- Certifique-se que o AP está obtendo um endereço do DHCP (verifique os alugueres do servidor DHCP para ver se há o MAC address do s do de APâ).
- Tente executar ping no AP a partir do controlador.
- Verifique se a configuração STP no switch está correta de modo que os pacotes para as VLANs não sejam bloqueados.
- Se os pings forem bem sucedidos, assegure-se de que o AP tenha pelo menos um método pelo qual detectar pelo menos um console WLC único ou use telnet/ssh no controlador para executar a depuração.
- Cada vez que as repartições AP, ele iniciam a sequência da descoberta de WLC e a tentam encontrar o AP. Repartição o AP e a verificação se se junta ao WLC.

Aqui estão alguns dos problemas mais comuns encontrados devido aos quais os LAPs não se juntarão ao WLC.

Problema 1: A hora do controlador está fora do intervalo de validade do certificado

Conclua estas etapas para solucionar esse problema:

1. Problemas dos comandos **debug lwapp errors enable** e debug pm pki enable.A saída do **comando debug lwapp event enable** mostra a depuração de mensagens certificadas que são passadas entre o AP e o WLC. A saída mostra claramente uma mensagem de que o certificado foi rejeitado.**Nota:** Certifique-se de levar em conta o deslocamento do Tempo Universal Coordenado (UTC).Esta é a saída do **comando debug lwapp events enable** no controlador:**Nota:** Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.
```
Thu Jan  1 00:09:46 1970: 00:0b:85:5b:fb:d0 Received LWAPP DISCOVERY
REQUEST
from AP 00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Jan 1 00:09:46 1970: 00:0b:85:5b:fb:d0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2
Thu Jan  1 00:09:57 1970: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST
```

from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2'
Thu Jan 1 00:09:57 1970: 00:0b:85:5b:fb:d0 **LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:5b:fb:d0.** Thu Jan 1 00:09:57 1970: 00:0b:85:5b:fb:d0 **Unable to free public key for AP 00:0B:85:5B:FB:D0** Thu Jan 1 00:09:57 1970: spamProcessJoinRequest : spamDecodeJoinReq failed Essa é a saída do **comando debug pm pki enable** no controlador. Essa saída segue o processo para a validação do certificado.**Nota:** Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California, L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e, MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer> O=Cisco Systems, CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is 00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
 ....
 ....
 ....
 ....
 Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
 Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using >cscoDefaultMfgCaCert<
 Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current): 2005/04/15/07:55:03
 Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: **Current time outside AP cert validity interval: make sure the controller time is set.** Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil) Essas informações mostram claramente que a hora do controlador está fora do intervalo de validade do certificado do LAP. Portanto, o LAP não pode se registrar com o controlador. Os certificados instalados no LAP têm um intervalo predefinido de validade. O tempo do controlador deve ser ajustado de tal maneira que está dentro do intervalo da validade de certificado do certificado do s do de LAPâ.

2. Emita o comando **show time** a partir da CLI do controlador para verificar se a data e a hora definidas no controlador estão dentro desse intervalo de validade. Se a hora do controlador for maior ou menor do que esse intervalo de validade do certificado, altere a hora do controlador para que fique dentro desse intervalo.**Nota:** Se a hora não estiver definida corretamente no controlador, escolha **Commands > Set Time** no modo GUI do controlador ou emita o comando config time na CLI do controlador para ajustar a hora do controlador.
3. Em LAPs com acesso a CLI, verifique os certificados com o comando **show crypto ca certificates** a partir da CLI do AP.Esse comando permite que você verifique o intervalo de validade do certificado definido no AP. Este é um exemplo:AP0015.63e5.0c7e#**show crypto ca certificates** .....
.... Certificate Status: Available Certificate Serial Number: 4BC6DAB80000000517AF Certificate Usage: General Purpose Issuer: cn=Cisco Manufacturing CA o=Cisco Systems Subject: Name: **C1200-001563e50c7e** ea=support@cisco.com cn=C1200-001563e50c7e o=Cisco Systems l=San Jose st=California c=US CRL Distribution Point: http://www.cisco.com/security/pki/crl/cmca.crl Validity Date: start date: 17:22:04 UTC Nov 30 2005 end date: 17:32:04 UTC Nov 30 2015 renew date: 00:00:00 UTC Jan 1 1970 Associated Trustpoints: Cisco_IOS_MIC_cert .....
.... A saída inteira não é listada já que podem existir muitos intervalos de validade associados à saída desse comando. Você precisa considerar somente o intervalo de validade especificado pelo ponto de confiança associado: Cisco_IOS_MIC_cert com o nome do AP relevante no campo de nome. Nessa saída de exemplo, é Nome: C1200-001563e50c7e. Esse é o intervalo de validade

do certificado real a ser considerado.

Problema 2: Incompatibilidade no domínio regulatório

Você vê esta mensagem na saída do **comando debug lwapp events enable**:

Nota: Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.

```
Wed Oct 24 17:13:20 2007: 00:0b:85:91:c3:c0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:80 on port '2'
Wed Oct 24 17:13:20 2007: 00:0e:83:4e:67:00 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:91:c3:c0 on Port 2
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:81 on  port '2'
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 AP ap:91:c3:c0:
txNonce  00:0B:85:33:52:80 rxNonce  00:0B:85:91:C3:C0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 LWAPP Join-Request MTU path
from AP 00:0b:85:91:c3:c0 is 1500, remote debug mode is 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully added NPU Entry
for AP 00:0b:85:91:c3:c0 (index 48)
Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0
AP IP: 10.77.246.18, AP Port: 7228, next hop MAC: 00:17:94:06:62:88
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully transmission
of LWAPP Join-Reply to AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:91:c3:c0 to  00:0b:85:33:52:81
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP info for AP 00:0b:85:91:c3:c0 --
static 0, 10.77.246.18/255.255.255.224, gtw 10.77.246.1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP 10.77.246.18 ===> 10.77.246.18
for AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 0 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211a Regulatory Domain
(-N) does not match with country (US )  reg. domain -AB for the slot 0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 1 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211bg Regulatory Domain (-N)
does not match with country (US ) reg. domain -AB for the slot 1 Wed Oct 24 17:13:47 2007:
spamVerifyRegDomain AP RegDomain check for the country US failed Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: Regulatory Domain check Completely FAILED The AP will
not be allowed to join Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 apfSpamProcessStateChangeInSpamContext: Deregister
LWAPP event for AP 00:0b:85:91:c3:c0 slot 1 Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0 Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 1
```

A mensagem indica claramente que há uma incompatibilidade no domínio regulatório do LAP e do WLC. O WLC suporta vários domínios regulatórios, mas cada domínio regulatório deve ser selecionado antes que um LAP possa juntar-se a partir desse domínio. Por exemplo, o WLC que usa o domínio regulatório -A somente pode ser usado com APs que usam o domínio regulatório -A (e assim por diante). Ao comprar APs e WLCs, certifique-se de que eles compartilhem o mesmo domínio regulatório. Só então os LAPS poderão se registrados com o WLC.

Nota: Os rádios 802.1b/g e 802.11a devem estar no mesmo domínio regulatório para um LAP

único.

Problema 3: Mensagem de erro AP cannot join because the maximum number of APs on interface 2 is reached

Você poderá ver essa mensagem de erro quando a AP tentar juntar-se ao controlador:

```
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 4498: AP cannot join because the maximum number of
APs on interface 2 is reached.
```

Por padrão, os controladores da série 4400 podem suportar até 48 APs por porta. Quando você tentar conectar mais que 48 APs no controlador, você receberá essa mensagem de erro. Contudo, você pode configurar seu controlador da série 4400 para suportar mais APs em uma interface única (por porta) usando um desses métodos:

- Agregação do link (para controladores no modo de camada 3)
- Várias interfaces do gerenciador AP (para controladores no modo de camada 3)
- Conexão de portas adicionais (para controladores no modo de camada 2)

Para obter mais informações, consulte Configuring a 4400 Series Controller to Support More Than 48 Access Points.

Nota: A Cisco introduziu os WLCs da série 5500 para usuários corporativos com recursos adicionais. Eles não têm restrições quanto ao número de APs por porta. Consulte o Choosing Between Link Aggregation and Multiple AP-Manager Interfaces section of Cisco Wireless LAN Controller Configuration Guide Release 6.0 para obter mais informações.

Problema 4: Com APs do SSC, a política de AP do SSC fica desativada

Se a política de SSC estiver desativada no controlador, você verá essas mensagens de erro no controlador das saídas dos comandos **debug lwapp events enable** e debug pm pki enable:

```
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Wed Aug 9 17:20:21 2006 [ERROR] spam_crypto.c 1509: Unable to free public key for
AP 00:12:44:B3:E5:60
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include valid
certificate in CERTIFICATE_PAYLOAD from AP 00:12:44:b3:e5:60. Wed Aug 9 17:20:21 2006 [CRITICAL]
sshpmPkiApi.c 1493: Not configured to accept Self-signed AP cert
```

Conclua estas etapas para solucionar esse problema:

Execute uma destas duas ações:

- Emita o comando **show auth-list** na CLI do controlador para verificar se o controlador está configurado para aceitar APs com SSCs.Esta é uma saída de exemplo:`#show auth-list`
  `Authorize APs against AAA ..... disabled Allow APs with Self-signed Certificate (SSC) .... enabled Mac Addr Cert Type Key Hash ---------- --------- ---------- 00:09:12:2a:2b:2c SSC 12345678901234567890123456789012345678901234567890`
- Escolha **Security > AP Policies** na GUI.Verifique se a caixa de seleção **Accept Self Signed Certificate** está ativada. Se não estiver, ative-a.Escolha **SSC** como o tipo de certificado.Adicione o AP à lista de autorização com o endereço MAC e a chave hash.Essa chave hash pode ser obtida da saída do **comando debug pm pki enable**. Consulte o Problema

6 para obter informações sobre a obtenção do valor da chave hash.

Problema 5: Lista de autorização de AP ativada no WLC; LAP não está na lista de autorização

Nesses casos, você verá esta mensagem no controlador na saída do **comando debug lwapp events enable**:

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:51:5a:e0
```

Se você estiver usando um LAP que tenha uma porta de console, você verá esta mensagem quando emitir o comando **debug lwapp client error**:

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: No more AP manager IP addresses remain.
```

Isso novamente é uma indicação clara que o LAP não faz parte da lista de autorização de AP no controlador.

Você pode ver o status da lista de autorização de AP usando este comando:

```
(Cisco Controller) >show auth-list Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Para adicionar um LAP à lista de autorização de AP, use o comando **config auth-list add mic <AP MAC Address>** . Para obter mais informações sobre como configurar a autorização do LAP, consulte Lightweight Access Point (LAP) Authorization in a Cisco Unified Wireless Network Configuration Example.

Problema 6: Chave hash pública SSC está errada ou ausente

Conclua estas etapas para solucionar esse problema:

1. Emita o **comando debug lwapp events enable**.Isso verifica se o AP tenta juntar-se.
2. Emita o comando **show auth-list** .Esse comando mostra a chave hash pública que o controlador tem em armazenamento.
3. Emita o **comando debug pm pki enable**.Esse comando mostra a chave hash pública real. A chave hash pública real deve corresponder à chave hash pública que o controlador tem em armazenamento. Uma discrepância causa o problema. Esta é uma saída de exemplo dessa mensagem de depuração:**Nota:** Algumas linhas da saída foram movidas para a segunda

linha devido a limitações de espaço.`(Cisco Controller) >` **`debug pm pki enable`** `Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert cscoDefaultMfgCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122 300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb 058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8 eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301 0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles:` **`SSC Key Hash is 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9`** *`!--- This is the actual SSC key-hash value.`* `Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14 2006: spamRadiusProcessResponse:` **`AP Authorization failure for 00:0e:84:32:04:f0`**

Conclua estas etapas para solucionar o problema:

1. Copie a chave hash pública da saída do **comando debug pm pki enable** e use-a para substituir a chave hash pública na lista de autenticação.
2. Emita o comando **config auth-list add ssc AP_MAC AP_key** para adicionar o endereço MAC do AP e a chave hash à lista de autorização.Aqui está um exemplo deste comando:**Nota:** Este comando foi movido para a segunda linha devido a limitações de espaço.`(Cisco Controller)>`**`config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9`**

Problema 7: Há uma corrupção do certificado ou da chave pública no AP

O LAP não se junta a um controlador por causa de um problema de certificado.

Problemas dos comandos **debug lwapp errors enable** e debug pm pki enable. Você vê mensagens que indicam os certificados ou as chaves que estão corrompidos.

Nota: Algumas linhas da saída foram movidas para a segunda linha devido a limitações de espaço.

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 LWAPP Join Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP
```

```
00:0f:24:a9:52:e0. Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Deleting and removing AP
00:0f:24:a9:52:e0 from fast path Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free
public key for AP
```

Use uma destas duas opções para resolver o problema:

- Pedido do do MIC APâ um Return Materials Authorization (RMA).
- Downgrade do do de SSC APâ ao Cisco IOS? Software Release 12.3(7)JA.Se for um AP com um SSC, converta-o novamente para IOS usando o botão MODE. Depois use a ferramenta de atualização lwapp para converter de volta para o LWAPP. Isso deve criar um certificado novamente.

Conclua estas etapas para fazer o downgrade:

1. Use a opção do botão de redefinição.
2. Limpe as configurações do controlador.
3. Execute a atualização novamente.

Para obter mais informações sobre como fazer o downgrade de um LAP, consulte Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.

Se você tiver um WCS, você poderá enviar os SSCs para o novo WLC. Para obter mais informações sobre como configurar APs usando o WCS, consulte Configuring Access Points section of *Cisco Wireless Control System Configuration Guide, Release 5.1*.

Problema 8: O controlador pode estar trabalhando no modo de camada 2

Conclua esta etapa para solucionar esse problema:

Verifique o modo de operação do controlador. Os APs convertidos apenas suportam detecção na camada 3. Os AP convertidos não suportam detecção na camada 2.

Conclua estas etapas para solucionar o problema:

1. Defina o WLC para o modo de camada 3.
2. Reinicialize e configure a interface do gerenciador AP.Se você tiver uma porta de serviço, como a porta de serviço em um 4402 ou em um 4404, ela deverá estar em uma super-rede diferente das interfaces de gerenciamento e do gerenciador AP.

Problema 9: Você recebe esta mensagem de erro no AP após a conversão para o LWAPP

Você verá esta mensagem de erro:

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs
no certs in the  SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

O AP é recarregado após 30 segundos e inicia o processo novamente.

Conclua estas etapas para resolver o problema:

1. Você tem um AP com SSC. Converta-o novamente para uma imagem IOS autônoma.
2. Limpe a configuração emitindo o comando **write erase** e recarregue. Não salve a configuração quando estiver recarregando.

Problema 10: O controlador recebe uma mensagem de detecção do AP na VLAN errada (você vê a depuração da mensagem de detecção, mas não a resposta)

Você vê esta mensagem na saída do **comando debug lwapp events enable**:

`Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!`
Essa mensagem significa que o controlador recebeu uma solicitação de detecção através de um endereço IP de broadcast que tem um endereço IP de origem que não está em nenhuma sub-rede configurada no controlador. Isso também significa que o controlador está descartando o pacote.

O problema é que o AP não está enviando a solicitação de detecção para o endereço IP de gerenciamento. O controlador está relatando uma solicitação de detecção de broadcast de uma VLAN que não está configurada no controlador. Isso geralmente ocorre quando os troncos do cliente permitiram VLANS em vez de restringi-las a VLANS sem fio.

Conclua estas etapas para resolver o problema:

1. Se o controlador estiver em outra sub-rede, os APs devem ser **desobstruídos** para o endereço IP do controlador ou os APs devem receber o endereço IP dos controladores usando qualquer um dos métodos de detecção.
2. O switch é configurado para permitir algumas VLANs que não estão no controlador. Restrinja as VLANs permitidas nos troncos.

Problema 11: O LAP 1250 não é capaz de se juntar ao WLC

A instalação consiste em um WLC 2106 que executa a versão 4.1.185.0. Um AP Cisco 1250 não pode se juntar ao controlador.

O registro no WLC mostra o seguinte:

```
Mon Jun 2 21:19:37 2008AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2
21:19:37 2008 AP Associated. Base Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:26 2008 AP
Disassociated. Base Radio MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:20 2008 AP with MAC
f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2 21:19:20 2008 AP Associated. Base
Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:09 2008 AP Disassociated. Base Radio
MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:03 2008 AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x)
is unknown.
```

Solução: Isso é porque o LAP do Cisco 1250 series não é suportado na versão 4.1. O AP do Cisco Aironet 1250 Series é suportado a partir das versões 4.2.61 e posteriores do controlador. Para corrigir esse problema, atualize o software do controlador para 4.2.61.0 ou posterior.

Problema 12: AP não é capaz de se juntar ao WLC, o Firewall está bloqueando as portas necessárias

Se um firewall for usado na rede empresarial, verifique se as seguintes portas estão ativadas no

firewall para que o LAP possa juntar-se e comunicar-se com o controlador.

Você deve ativar estas portas:

- Ative essas portas UDP para o tráfego LWAPP:Dados - 12222Controle - 12223
- Ative estas portas UDP para o tráfego de mobilidade:16666 - 1666616667 - 16667
- Ative as portas UDP 5246 e 5247 para o tráfego CAPWAP.
- TCP 161 e 162 para o SNMP (para o Wireless Control System [WCS])

Estas portas são opcionais (dependendo de seus requisitos):

- UDP 69 para o TFTP
- TCP 80 e/ou 443 para o HTTP ou o HTTPS para o acesso a GUI
- TCP 23 e/ou 22 para o Telnet ou o SSH para o acesso a CLI

Problema 13: Endereço IP duplicado na rede

Esse é um outro problema comum que é visto quando o AP tenta se juntar ao WLC. Você poderá ver essa mensagem de erro quando o AP tentar juntar-se ao controlador.

```
No more AP manager IP addresses remain
```

Uma das razões para essa mensagem de erro é quando há um endereço IP duplicado na rede que corresponde ao endereço IP do gerenciador AP. Nesse caso, o LAP mantém o ciclo de energia e não pode se juntar ao controlador.

Os depuradores mostrarão que o WLC recebe as solicitações de detecção do LWAPP a partir dos APs e transmite uma resposta de detecção do LWAPP para os APs. Contudo, os WLC não recebem solicitações de junção do LWAPP a partir dos APs.

Para solucionar esse problema, execute ping no gerenciador AP de um host com fio na mesma sub-rede IP que o gerenciador AP. Depois, verifique o cachê ARP. Se um endereço IP duplicado for encontrado, remova o dispositivo com o endereço IP duplicado ou troque o endereço IP no dispositivo de modo que tenha um endereço IP exclusivo na rede.

O AP poderá então juntar-se ao WLC.

Problema 14: Os APs do LWAPP não se juntarão ao WLC se a MTU da rede tiver menos de 1500 bytes

Isso é devido à identificação de bug Cisco **CSCsd94967**. Os APs do LWAPP podem não se juntar a um WLC. Se a solicitação de junção do LWAPP for maior que 1500 bytes, o LWAPP deverá fragmentar a solicitação de junção do LWAPP. A lógica para todos APs do LWAPP é que o tamanho do primeiro fragmento é 1500 bytes (incluindo o cabeçalho IP e UDP) e o segundo fragmento é 54 bytes (incluindo o cabeçalho IP e UDP). Se a rede entre os APs do LWAPP e o WLC tiver um tamanho de MTU menor que 1500 (como pode ser encontrado ao usar um protocolo de encapsulamento como IPSec, VPN, GRE, MPLS etc.), o WLC não poderá suportar a solicitação de junção do LWAPP.

Você encontrará esse problema sob estas condições:

- WLC que executa a versão 3.2 ou anterior

- O caminho de rede MTU entre o AP e o WLC é menor que 1500 bytes

Para resolver esse problema, use uma destas opções:

- Atualize para o software WLC 4.0, se ele for compatível com a plataforma. Na versão 4.0 do WLC, esse problema foi resolvido permitindo que o túnel LWAPP remonte até 4 fragmentos.
- Aumente o caminho de rede MTU para 1500 bytes.
- Use REAPs 1030 para o locais alcançáveis através dos caminhos MTU baixos. As conexões LWAPP do REAP aos APs 1030 foram modificadas para suportar essa situação através da redução do MTU usado para o modo REAP.

Problema 15: O LAP da série 1142 não se junta ao WLC, mensagem de erro no WLC: lwapp_image_proc: unable to open tar file

Os LAPs da série 1142 são suportados apenas com a versão 5.2 ou posterior do WLC. Se você executa as versões do WLC anteriores a 5.2, você não poderá registrar o LAP para o controlador e verá uma mensagem de erro semelhante ao seguinte:

```
*Mar 27 15:04:38.596: %LWAPP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.597: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.606: %LWAPP-3-CLIENTERRORLOG: not receive read response(3)
*Mar 27 15:04:38.609: lwapp_image_proc: unable to open tar fileMar 12 15:47:27.237
spam_lrad.c:8317 LWAPP-3-IMAGE_DOWNLOAD_ERR3:
Refusing image download request from AP 0X:2X:D0:FG:a7:XX - unable to open
image file /bsn/ap//c1140
```

Para registrar os LAPs 1140 para o WLC, atualize o firmware no WLC para 5.2 ou versões posteriores.

Problema 16: Os LAPs da série 1000 não podem se juntar ao Wireless LAN controller, o WLC executa a versão 5.0

Isso é porque a versão 5.0.148.0 ou posterior do software WLC não é compatível com os APs do Cisco Aironet 1000 series. Se você tem um Cisco 1000 Series DOBRA em uma rede, que execute versões 5.0.48.0 WLC, o REGAÇO do 1000 Series não se junta ao controlador e você vê este mensagem de armadilha no WLC.

```
"AP with MAC xx:xx:xx:xx:xx:xx is unkown"
```

Problema 17: Regaços com a imagem da malha não capaz de juntar-se ao WLC

O Access point de pouco peso não se registra com o WLC. O log indica este o Mensagem de Erro

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
 Type: WLAN USER
```

Isto pode acontecer se o Access point de pouco peso foi enviado com uma imagem da malha e reage do modo de Bridge. Se o REGAÇO foi pedido com software da malha nele, você precisa de adicionar o REGAÇO à lista da autorização AP. Escolha a **Segurança > as políticas AP** e adicionar o **AP à** lista da autorização. O AP deve então juntar-se, transferir à imagem do controlador, a seguir do registro com o WLC no modo de Bridge. Então você precisa de mudar o AP ao modo local. O REGAÇO transfere a imagem, as repartições e os registros de volta ao controlador no modo local.

Problema 18: Mensagem de erro - Dropping primary discovery request from AP XX:

AA: BB: XX: DD: DD - maximum APs joined 6/6

Há um limite para o número de LAPs que podem ser suportados por um WLC. Cada WLC suporta um determinado número de LAPs, o que depende do modelo e da plataforma. Essa mensagem de erro é vista no WLC quando ele recebe uma solicitação de detecção após ter alcançado a sua capacidade de AP máxima.

Aqui está o número de LAPs suportados nos diferentes modelos e plataformas do WLC:

- O controlador da série 2100 suporta até 6, 12 ou 25 LAPs. Isso depende do modelo do WLC.
- O 4402 suporta até 50 LAPs, enquanto o 4404 suporta até 100. Isso torna-o ideal para empresas grandes e aplicativos com alta densidade.
- O Catalyst 6500 Series Wireless Services Module (WiSM) é um switch Catalyst 6500 integrado e dois controladores Cisco 4404 que suporta até 300 LAPs.
- O Cisco 7600 Series Router WiSM é um roteador Cisco 7600 integrado e dois controladores Cisco 4404 que suporta até 300 LAPs.
- O Cisco 28/37/38xx Series Integrated Services Router é um roteador 28/37/38xx integrado e um módulo de rede de controlador Cisco que suporta até 6, 8, 12 ou 25 LAPs, dependendo da versão do módulo de rede. As versões que suportam 8, 12 ou 25 APs e a versão NME-AIR-WLC6-K9 6-access-point possuem um processador de alta velocidade e mais memória integrada que a versão NM-AIR-WLC6-K9 6-access-point.
- O Catalyst 3750G Integrated WLC Switch é um switch Catalyst 3750 integrado e um controlador Cisco 4400 series que suporta até 25 ou 50 LAPs.

Informações Relacionadas

- Exemplo de configuração de autorização de um ponto de acesso leve (LAP) em uma rede sem fio unificada da Cisco
- Registro de AP leve (LAP) em um Wireless LAN Controller (WLC)
- Guia de configuração do Cisco Wireless LAN Controller, versão 4.1
- Suporte Técnico e Documentação - Cisco Systems