Dépanner un point d'accès léger ne pouvant pas se joindre à un contrôleur LAN sans fil

Contenu

Introduction

Ce document donne une présentation du processus de détection et de jointure d'un contrôleur de réseau local sans fil (WLC). Il fournit également des informations sur certains des problèmes en raison desquels un point d'accès léger (LAP) ne parvient pas à joindre un WLC et sur la façon de dépanner ces problèmes.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration des LAP et des WLC Cisco
- Connaissance de base du protocole LWAPP (Lightweight Access Point Protocol)

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Présentation du processus de détection et de jointure d'un contrôleur de réseau local sans fil (WLC)

Dans un réseau sans fil unifié Cisco, les LAP doivent d'abord détecter et joindre un WLC avant de pouvoir prendre en charge des clients sans fil.

Initialement, les contrôleurs fonctionnaient seulement en mode de couche 2. En mode de couche 2, les LAP doivent obligatoirement être sur le même sous-réseau car l'interface de gestion et l'interface du gestionnaire d'AP en mode de couche 3 ne sont pas présentes sur le contrôleur. Les LAP communiquent avec le contrôleur en utilisant uniquement l'encapsulation de couche 2 (encapsulation Ethernet) et n'applique pas DHCP (protocole de configuration dynamique d'hôte) à une adresse IP.

Quand le mode de couche 3 sur le contrôleur a été développé, la nouvelle interface de couche 3 appelée « interface de gestionnaire d'AP » a été introduite. En mode de couche 3, les LAP appliquaient tout d'abord DHCP à une adresse IP, puis envoyaient leur demande de détection à l'interface de gestion en utilisant des adresses IP (couche 3). Cela permettait aux LAP de ne pas se trouver sur le même sous-réseau que l'interface de gestion du contrôleur. Le mode de couche 3 est le mode dominant aujourd'hui. Certains contrôleurs et LAP peuvent seulement exécuter le mode de couche 3.

Cependant, cela a présenté un nouveau problème : comment les LAP trouvaient-ils l'adresse IP de gestion du contrôleur quand il se trouvait sur un sous-réseau différent ?

En mode de couche 2, ils devaient nécessairement se trouver sur le même sous-réseau. En mode de couche 3, le contrôleur et le LAP jouent essentiellement à cache-cache dans le réseau. Si vous ne dites pas au LAP où se trouve le contrôleur via l'option DHCP 43, la résolution DNS de « Cisco-lwapp-controller@local_domain », ou si vous ne la configurez pas statiquement, le LAP ne sait pas où trouver, dans le réseau, l'interface de gestion du contrôleur.

En plus de ces méthodes, le LAP recherche automatiquement sur le sous-réseau local les contrôleurs ayant la diffusion locale 255.255.255.255. En outre, le LAP se souvient, après les redémarrages, de l'adresse IP de gestion de tout contrôleur qu'il joint. Par conséquent, si vous mettez d'abord le LAP sur le sous-réseau local de l'interface de gestion, il recherchera l'interface de gestion du contrôleur et se souviendra de l'adresse. Cela est appelé « priming ». Cela ne permet pas de trouver le contrôleur si vous remplacez un LAP par la suite. Par conséquent, Cisco recommande d'utiliser l'option DHCP 43 ou des méthodes DNS.

Quand les LAP détectent le contrôleur, ils ne savent pas si le contrôleur est en mode de couche 2 ou en mode de couche 3. Par conséquent, les LAP se connectent toujours à l'adresse d'interface de gestion du contrôleur d'abord avec une demande de détection. Le contrôleur indique alors au LAP dans quel mode il est dans la réponse de détection. Si le contrôleur est en mode de couche 3, la réponse de détection contient l'adresse IP du gestionnaire d'AP de couche 3, de sorte que le LAP peut ensuite envoyer une demande de jointure à l'interface du gestionnaire d'AP.

Remarque: Par défaut, l'interface de gestion et l'interface du gestionnaire d'AP sont toutes les deux laissées sans balises sur leur VLAN pendant la configuration. Dans le cas où elles seraient balisées, assurez-vous qu'elles sont balisées sur le même VLAN afin de recevoir correctement la réponse de détection et de jointure du WLC.

L'AP LWAPP passe par le processus suivant lors du démarrage pour le mode de couche 3 :

1. Le LAP démarre et applique DHCP à une adresse IP si aucune adresse IP statique ne lui a été précédemment assignée.
2. Le LAP envoie des demandes de détection aux contrôleurs via les divers algorithmes de détection et établit une liste de contrôleurs. En fait, le LAP apprend autant d'adresses d'interface de gestion que possible pour la liste de contrôleurs via :L'option DHCP 43 (appropriée pour les sociétés mondiales dont les bureaux et les contrôleurs se trouvent sur des continents différents)L'entrée DNS pour cisco-capwap-controller (appropriée pour les entreprises locales - peut également être utilisée pour rechercher où les tout nouveaux AP établissent une jointure)**Remarque:** Si vous utilisez CAPWAP, assurez-vous qu'il y a une entrée DNS pour cisco-capwap-controller.Les adresses IP de gestion des contrôleurs dont le LAP se souvient précédemmentUne diffusion de couche 3 sur le sous-réseauL'approvisionnement sans filLes informations configurées statiquementDe cette liste, la méthode facile à l'utiliser pour le déploiement est d'avoir les recouvrements sur le même sous-réseau que l'interface de gestion du contrôleur et de permettre à l'émission de la couche 3 du s de de LAPâ pour trouver le contrôleur. Cette méthode doit être utilisée pour les sociétés qui ont un petit réseau et ne possèdent pas un serveur DNS local.La méthode la plus facile suivante du déploiement consiste à utiliser une entrée DNS avec DHCP. Vous pouvez avoir plusieurs entrées du même nom DNS. Cela permet au LAP de détecter plusieurs contrôleurs. Cette méthode doit être utilisée par les sociétés qui ont tous leurs contrôleurs dans un emplacement unique et qui possèdent un serveur DNS local. Elle doit être utilisée également si la société a plusieurs suffixes DNS et que les contrôleurs sont isolés par suffixe.L'option DHCP 43 est utilisée par les grandes sociétés pour localiser les

informations via DHCP. Cette méthode est utilisée par les grandes entreprises qui ont un suffixe DNS unique. Par exemple, Cisco possède des locaux en l'Europe, en Australie et aux États-Unis. Afin de garantir que les LAP joignent les contrôleurs uniquement localement, Cisco ne peut pas utiliser une entrée DNS et doit utiliser les informations de l'option DHCP 43 pour indiquer aux LAP quelle est l'adresse IP de gestion de leur contrôleur local.Enfin, la configuration statique est utilisée pour un réseau qui n'a pas de serveur DHCP. Vous pouvez statiquement configurer les informations nécessaires pour joindre un contrôleur par l'intermédiaire du port de console et du s CLI de d'APâ. Pour obtenir des informations sur la façon de configurer statiquement les informations de contrôleur à l'aide de la CLI de l'AP, consultez Configuration manuelle des informations de contrôleur à l'aide de la CLI du point d'accès.Pour obtenir une explication détaillée sur les différents algorithmes de détection que les LAP utilisent pour rechercher des contrôleurs, consultez Enregistrement du LAP avec le WLC.Pour obtenir des informations sur la configuration de l'option DHCP 43 sur un serveur DHCP, consultez Exemple de configuration de l'option DHCP 43 pour les points d'accès légers Cisco Aironet.

3. Envoyez une demande de détection à chaque contrôleur de la liste et attendez la réponse de détection du contrôleur qui contient le nom du système, les adresses IP du gestionnaire d'AP, le nombre d'AP déjà attachés à chaque interface de gestionnaire d'AP et la surcapacité globale pour le contrôleur.
4. Consultez la liste de contrôleurs et envoyez une demande de jointure à un contrôleur, dans l'ordre suivant (seulement si l'AP a reçu une réponse de détection de lui) :Nom du système du contrôleur primaire (précédemment configuré sur le LAP)Nom du système du contrôleur secondaire (précédemment configuré sur le LAP)Nom du système du contrôleur tertiaire (précédemment configuré sur le LAP)Contrôleur principal (si le LAP n'a pas été précédemment configuré avec des noms de contrôleurs primaires, secondaires ou tertiaires. Utilisé pour toujours savoir à quel contrôleur les tout nouveaux LAP se joignent)Si aucune des options ci-dessus n'apparaît, équilibrez la charge entre les contrôleurs en utilisant la valeur de surcapacité dans la réponse de détection.Si deux contrôleurs ont la même surcapacité, envoyez la demande de jointure au premier contrôleur qui a répondu à la demande de détection avec une réponse de détection. Si un seul contrôleur a plusieurs gestionnaires d'AP sur plusieurs interfaces, choisissez l'interface de gestionnaire d'AP ayant avec le plus petit nombre d'AP.Le contrôleur répondra à toutes les demandes de détection sans vérifier les certificats ou des informations d'identification des AP. Cependant, les demandes de jointure doivent avoir un certificat valide pour obtenir une réponse de jointure du contrôleur. Si le LAP ne reçoit pas une réponse de jointure de son choix, il essayera le contrôleur suivant dans la liste, à moins que le contrôleur ne soit un contrôleur configuré (primaire/secondaire/tertiaire).
5. Quand il reçoit la réponse de jointure, l'AP vérifie qu'il a la même image que celle du contrôleur. Si ce n'est pas le cas, l'AP télécharge l'image à partir du contrôleur et redémarre pour charger la nouvelle image, puis recommence tout le processus depuis l'étape 1.
6. S'il a la même image logicielle, il demande la configuration à partir du contrôleur et passe dans l'état enregistré sur le contrôleur.Une fois la configuration téléchargée, l'AP peut se recharger de nouveau pour appliquer la nouvelle configuration. Par conséquent, un rechargement supplémentaire peut se produire, ce qui constitue un comportement normal.

Déboguer à partir du contrôleur

Il y a certaines commandes **debug** sur le contrôleur que vous pouvez utiliser pour afficher la totalité de ce processus sur la CLI.

- le de d'**enableâ d'événements de debug lwapp** affiche des paquets de détection et joint des paquets.
- le de d'**enableâ de paquet de debug lwapp** affiche à paquet les informations de niveau de la détection et joint des paquets.
- les expositions de de d'**enableâ de PKI de debug pm** délivrent un certificat le processus de validation.
- **mettez au point le** de de **débronchement-allâ** arrête met au point.

Avec une application du terminal qui peut capturer la sortie dans un fichier journal, connectez la console à votre contrôleur ou appliquez-lui Secure Shell (SSH)/Telnet, puis entrez les commandes suivantes :

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**

Après avoir capturé les débogages, utilisez la commande **debug disable-all** pour désactiver tous les débogages.

Les sections suivantes montrent la sortie de ces commandes **debug** quand le LAP s'enregistre auprès du contrôleur.

debug lwapp events enable

Cette commande fournit des informations sur les événements et les erreurs LWAPP qui se produisent pendant le processus de détection et de jointure LWAPP.

Voici la sortie de la commande **debug lwapp events enable** pour un LAP qui a la même image que celle du WLC :

Remarque: Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.

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.
```

Comme mentionné dans la section précédente, une fois qu'un LAP s'enregistre auprès du WLC, il vérifie s'il a la même image que le contrôleur. Si les images sur le LAP et le WLC sont différentes, les LAP commencent par télécharger la nouvelle image à partir du WLC. Si le LAP a la même image, il continue à télécharger la configuration et d'autres paramètres à partir du WLC.

Vous verrez les messages suivant dans la sortie de la commande **debug lwapp events enable** si le LAP télécharge une image à partir du contrôleur dans le cadre de la procédure d'enregistrement :

```
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
```

Une fois le téléchargement de l'image terminé, le LAP redémarrera et exécutera de nouveau l'algorithme de détection et de jointure.

debug pm pki enable

Dans le cadre du processus de jointure, le WLC authentifie chaque LAP en vérifiant que son certificat est valide.

Quand l'AP envoie la demande de jointure LWAPP au WLC, il inclut son certificat X.509 dans le message LWAPP. L'AP génère également un ID de session aléatoire qui est également inclus dans la demande de jointure LWAPP. Quand le WLC reçoit la demande de jointure LWAPP, il valide la signature du certificat X.509 en utilisant la clé publique de l'AP et vérifie que le certificat a été émis par une autorité de certification de confiance.

Il également regarde la date et l'heure commençantes pour l'intervalle de la validité du certificat AP et compare que date et temps à sa propre date et temps (par conséquent l'horloge de de de controllerâ s doit être placé à près de la date et heure actuelles). Si le certificat X.509 est validé, le WLC génère une clé de chiffrement AES aléatoire. Le WLC analyse la clé AES dans son moteur de chiffrement de sorte qu'il puisse chiffrer et déchiffrer de futurs messages de contrôle LWAPP échangés avec l'AP. Notez que les paquets de données sont envoyés en clair dans le tunnel LWAPP entre le LAP et le contrôleur.

La commande **debug pm pki enable** présente le processus de validation de la certification qui se produit pendant la phase de jointure sur le contrôleur. La commande **debug pm pki enable** affichera également la clé de hachage de l'AP pendant le processus de jointure si l'AP a un

certificat auto-signé (SSC) créé par le programme de conversion LWAPP. Si l'AP a un certificat installé manufacturé (MIC), vous ne verrez pas de clé de hachage.

Remarque: Tous les AP fabriqués après juin 2006 ont un certificat MIC.

Voici la sortie de la commande **debug pm pki enable** quand le LAP ayant un certificat MIC joint le contrôleur :

Remarque: Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.

```
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
```

Pour un LAP ayant un certificat SSC, la sortie de la commande **debug pm pki enable** ressemblera à ceci. Notez que le hachage SSC est également présenté dans cette sortie.

Remarque: Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.

```
(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
```

Déboguer à partir du LAP

Si les débogages du contrôleur n'indiquent pas une demande de jointure, vous pouvez déboguer le processus à partir du LAP à condition que le LAP ait un port de console. Vous pouvez voir le processus de démarrage du LAP avec les commandes suivantes, mais vous devez d'abord passer en mode enable (le mot de passe par défaut est Cisco) :

- le de de **detailâ de debug dhcp** affiche les informations de l'option 43 DHCP.
- **mettez au point le** de d'**udpâ d'IP** affiche les paquets de joindre/détection au contrôleur aussi bien que le DHCP et les requêtes DNS (toute la ces derniers est des paquets UDP. Le port 12223 est le port de source du s de de controllerâ).
- le de d'**eventâ de client de debug lwapp** affiche des événements LWAPP pour AP.
- les débronchements de de d'**allâ d'undebug** met au point sur AP.

Voici un exemple de la sortie de la commande **debug ip udp**. Cette sortie partielle donne une idée des paquets qui sont envoyés par le LAP pendant le processus de démarrage pour détecter et joindre un contrôleur.

```
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.
```

Éviter les problèmes liés à DHCP

Les LAP qui utilisent DHCP pour rechercher une adresse IP avant de commencer le processus de détection des WLC pourraient avoir des difficultés à recevoir une adresse DHCP en raison de la configuration incorrecte des paramètres relatifs à DHCP. Cette section explique comment DHCP fonctionne avec des WLC et fournit certaines des meilleures pratiques pour éviter des problèmes liés à DHCP.

Pour DHCP, le contrôleur se comporte comme un routeur avec une adresse d'assistance IP. En d'autres termes, il remplit l'adresse IP de la passerelle et transfère la demande par l'intermédiaire d'un paquet de monodiffusion directement au serveur DHCP.

Quand l'offre DHCP revient au contrôleur, il remplace l'adresse IP du serveur DHCP par son adresse IP virtuelle. En effet, quand Windows est en itinérance entre des AP, la première chose qu'il fait est d'essayer de contacter le serveur DHCP et de renouveler l'adresse.

Lorsque l'adresse du serveur DHCP est 1.1.1.1 (adresse IP virtuelle par défaut sur un contrôleur), le contrôleur peut intercepter ce paquet et répondre rapidement à Windows.

C'est également pourquoi l'adresse IP virtuelle est la même sur tous les contrôleurs. Si un

ordinateur portable Windows est en itinérance vers un AP sur un autre contrôleur, il essayera de contacter l'interface virtuelle sur le contrôleur. En raison de l'événement de mobilité et du transfert de contexte, le nouveau contrôleur vers lequel le client Windows est en itinérance a déjà toutes les informations pour répondre de nouveau à Windows.

Si vous voulez utiliser le serveur DHCP interne sur le contrôleur, vous devez simplement mettre l'adresse IP de gestion comme serveur DHCP sur l'interface dynamique que vous créez pour le sous-réseau. Attribuez ensuite cette interface au WLAN.

Le contrôleur a besoin d'une adresse IP sur chaque sous-réseau car il peut ainsi remplir l'adresse de la passerelle DHCP dans la requête DHCP.

Voici certains des points à retenir quand vous configurez des serveurs DHCP pour le WLAN :

1. L'adresse IP du serveur DHCP ne doit pas faire partie d'un sous-réseau dynamique qui est sur le contrôleur. Elle sera bloquée mais peut être remplacée à l'aide de la commande suivante :
   `config network mgmt-via-dynamic-interface` `on version 4.0 only (command not available in version 3.2)`
2. Le contrôleur transférera le DHCP par monodiffusion à partir de son interface dynamique (en code plus récent) en utilisant son adresse IP sur cette interface. Assurez-vous que tous les pare-feu autorisent cette adresse à atteindre le serveur DHCP.
3. Assurez-vous que la réponse du serveur DHCP peut accéder à l'adresse dynamique du contrôleur sur ce VLAN à travers tous les pare-feu. Effectuez un test Ping sur l'adresse de l'interface dynamique à partir du serveur DHCP. Effectuez un test Ping sur le serveur DHCP avec une adresse IP source de l'adresse de passerelle de l'interface dynamique.
4. Assurez-vous que le VLAN de l'AP est autorisé sur les commutateurs et les routeurs et que leurs ports sont configurés en tant que liaisons agrégées de sorte que les paquets (y compris DHCP) balisés avec le VLAN sont autorisés sur le réseau câblé.
5. Assurez-vous que le serveur DHCP est configuré pour attribuer une adresse IP sur le VLAN de l'AP. Vous pouvez également configurer le WLC comme serveur DHCP. Pour plus d'informations sur la façon de configurer le serveur DHCP sur le WLC, consultez la section Utilisation de la GUI pour configurer DHCP du Guide de configuration du contrôleur LAN sans fil Cisco, Version 5.0.
6. Vérifiez que l'adresse IP du contrôleur sur son interface dynamique fera partie d'une des portées DHCP sur le serveur DHCP.
7. Enfin, vérifiez que vous n'utilisez pas un serveur DHCP qui ne répond pas aux requêtes DHCP de monodiffusion telles que PIX.

Si vous ne pouvez pas résoudre votre problème lié à DHCP, il y a 2 solutions :

- Essayez un serveur DHCP interne. Configurez l'adresse du serveur DHCP sur l'interface dynamique pour qu'elle soit l'adresse IP de gestion, puis le pool interne DHCP. Si la portée DHCP est activée, cela devrait fonctionner.
- Vérifiez qu'il n'y a aucune réponse à la requête DHCP en envoyant la sortie sur la CLI (console ou SSH) de ces débogages :`0. debug mac addr <mac address>`
  `1. debug dhcp message enable`
  `2. debug dhcp packet enable` Cela doit indiquer que le paquet DHCP a été transféré mais que le contrôleur n'a pas reçu de réponse.

Enfin, en raison de la sécurité sur le contrôleur, il est déconseillé de mettre un VLAN ou un sous-réseau sur le contrôleur qui contient également les LAP, à moins qu'il soit sur le sous-réseau

d'interface de gestion.

Remarque: Le serveur RADIUS ou le serveur DHCP ne doivent être sur aucun des sous-réseaux de l'interface dynamique du contrôleur. La sécurité bloquera les paquets de retour qui essayent de communiquer avec le contrôleur.

Utilisation de serveurs syslog pour dépanner le processus de jointure du LAP

La version 5.2 du logiciel de contrôleur vous permet de configurer les AP pour envoyer à un serveur syslog toutes les erreurs liées à CAPWAP. Vous n'avez pas besoin d'activer des commandes de débogage sur le contrôleur car tous les messages d'erreur CAPWAP peuvent être affichés à partir du serveur syslog lui-même. Pour plus d'informations sur cette fonction et les commandes utilisées pour l'activer, lisez la section Dépannage du processus de jointure du point d'accès du Guide de configuration du contrôleur LAN sans fil Cisco, Version 5.2.

Raisons pour lesquelles le LAP ne joint pas le contrôleur

Effectuer tout d'abord les vérifications de base

- L'AP et le WLC peuvent-ils communiquer ?
- Assurez-vous qu'AP obtient une adresse de DHCP (vérifiez les baux de serveur DHCP pour l'adresse MAC du s de d'APâ).
- Essayez d'effectuer un test Ping sur l'AP à partir du contrôleur.
- Vérifiez si la configuration STP sur le commutateur est faite convenablement de sorte que des paquets vers les VLAN ne soient pas bloqués.
- Si les tests Ping sont effectués avec succès, vérifiez que l'AP a au moins une méthode permettant de détecter au moins une console de WLC ou d'appliquer Telnet/SSH dans le contrôleur pour exécuter les débogages.
- Chaque fois que l'AP redémarre, il lance la séquence de détection des WLC et essaie de localiser l'AP. Redémarrez l'AP et vérifiez s'il joint le WLC.

Voici certains des problèmes couramment rencontrés en raison de quoi les LAP ne joignent pas le WLC.

Problème 1 : L'heure du contrôleur est en dehors de l'intervalle de validité du certificat

Effectuez les étapes suivantes afin de résoudre ce problème :

1. Émettez les commandes **debug lwapp errors enable** et **debug pm pki enable**.La sortie de la commande **debug lwapp event enable** montre le débogage de messages de certificat qui sont passés entre l'AP et le WLC. La sortie affiche clairement un message indiquant que le certificat est rejeté.**Remarque:** Veillez à prendre en compte le décalage du Coordinated Universal Time (UTC).Voici la sortie de la commande **debug lwapp events enable** sur le contrôleur :**Remarque:** Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.
```
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 Voici la sortie de la commande **debug pm pki enable** sur le contrôleur. Cette sortie suit le processus de validation du certificat.**Remarque:** Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.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) Ces informations montrent clairement que l'heure du contrôleur est en dehors de l'intervalle de validité du certificat du LAP.
Par conséquent, le LAP ne peut pas s'enregistrer auprès du contrôleur. Les certificats installés dans le LAP ont un intervalle de validité prédéfini. Le temps de contrôleur devrait être placé de telle manière qu'il soit dans l'intervalle de validité de certificat du certificat du s de de LAPâ.

2. Émettez la commande **show time** du contrôleur CLI afin de vérifier que la date et l'heure définis sur votre contrôleur tombent dans cet intervalle de validité. Si l'heure du contrôleur est ultérieure ou antérieure à cet intervalle de validité du certificat, modifiez l'heure du contrôleur pour qu'elle soit dans cet intervalle.**Remarque:** Si l'heure n'est pas définie correctement sur le contrôleur, choisissez **Commands > Set Time** en mode GUI du contrôleur, ou émettez la commande **config time** dans la CLI du contrôleur afin de définir l'heure du contrôleur.
3. Sur les LAP ayant un accès à la CLI, vérifiez les certificats avec la commande **show crypto ca certificates** à partir de la CLI de l'AP.Cette commande vous permet de vérifier l'intervalle de validité du certificat défini dans l'AP. Voici un exemple :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 .....
.... La sortie entière

n'est pas listée car il peut y avoir beaucoup d'intervalles de validité associés avec la sortie de cette commande. Vous devez considérer seulement l'intervalle de validité spécifié par le point de confiance associé : Cisco_IOS_MIC_cert avec le nom d'AP pertinent dans le champ de nom. Dans cet exemple de sortie, c'est Name: `C1200-001563e50c7e`. **C'est l'intervalle réel de validité du certificat à considérer.**

Problème 2 : Non-correspondance dans le domaine réglementaire

Le message suivant s'affiche dans la sortie de la commande **debug lwapp events enable** :

Remarque: Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.

```
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
```

Le message indique clairement qu'il y a une non-correspondance dans le domaine réglementaire du LAP et du WLC. Le WLC prend en charge plusieurs domaines réglementaires, mais chaque domaine réglementaire doit être sélectionné avant qu'un LAP puisse joindre ce domaine.
Par exemple, le WLC qui utilise le domaine réglementaire -A peut uniquement être utilisé avec les

AP qui utilisent le domaine réglementaire -A (etc.). Quand vous achetez des AP et WLC, assurez-vous qu'ils partagent le même domaine réglementaire. C'est la condition nécessaire pour que les LAP puissent s'enregistrer auprès du WLC.

Remarque: Les radios 802.1b/g et radios 802.11a doivent toutes les deux être dans le même domaine réglementaire pour un LAP unique.

Problème 3 : Message d'erreur « AP cannot join because the maximum number of APs on interface 2 is reached »

Le message d'erreur suivant peut s'afficher quand l'AP essaie de joindre le contrôleur :

```
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.
```

Par défaut, les contrôleurs de gamme 4400 peuvent prendre en charge jusqu'à 48 AP par port. Quand vous essayez de connecter plus de 48 AP sur le contrôleur, vous recevez ce message d'erreur. Cependant, vous pouvez configurer votre contrôleur de la gamme 4400 pour prendre en charge plus d'AP sur une interface unique (par port) en utilisant l'une des méthodes suivantes :

- Agrégation de liaisons (pour les contrôleurs en mode de couche 3)
- Plusieurs interfaces de gestionnaire d'AP (pour des contrôleurs en mode de couche 3)
- Connexion à des ports supplémentaires (pour les contrôleurs en mode de couche 2)

Pour plus d'informations, consultez Configuration d'un contrôleur de la gamme 4400 pour prendre en charge plus de 48 points d'accès.

Remarque: Cisco a introduit les WLC de la gamme 5500 pour les utilisateurs en entreprise disposant de fonctionnalités supplémentaires. Ils n'ont aucune restriction sur le nombre d'AP par port. Consultez la section Choix entre l'agrégation de liaisons et plusieurs interfaces de gestionnaire d'AP du Guide de configuration du contrôleur LAN sans fil Cisco, Version 6.0 pour plus d'informations.

Problème 4 : Avec les AP SSC, la politique des AP SSC est désactivée.

Si la politique des SSC est désactivée sur le contrôleur, les messages d'erreur suivant s'affichent sur le contrôleur dans les sorties des commandes **debug lwapp events enable** et **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
```

Effectuez les étapes suivantes afin de résoudre ce problème :

Exécutez l'une de ces deux actions :

- Émettez la commande **show auth-list** sur la CLI du contrôleur afin de vérifier si le contrôleur est configuré pour accepter les AP avec SSC.Voici est un exemple de sortie :`#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
```

- Choisissez **Security > AP Policies** dans le GUI.Vérifiez si la case à cocher **Accept Self Signed Certificate** est activée. Sinon, activez-la.Choisissez **SSC** en tant que type de certificat.Ajoutez AP à la liste des autorisations avec adresse MAC et hachage de clé.Ce hachage de clé peut être obtenu à partir de la sortie de la commande **debug pm pki enable**. Consultez le Problème 6 pour obtenir des informations sur l'obtention de la valeur de hachage de clé.

Problème 5 : Liste des autorisations d'AP activée sur le WLC ; LAP non présent dans la liste des autorisations

En pareil cas, le message suivant s'affichera sur le contrôleur dans la sortie de la commande **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
```

Si vous utilisez un LAP qui a un port de console, le message suivant s'affichera quand vous émettrez la commande **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.
```

Cela indique à nouveau clairement que le LAP ne fait pas partie de la liste des autorisations d'AP sur le contrôleur.

Vous pouvez afficher l'état de la liste des autorisations d'AP à l'aide de la commande suivante :

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

Afin d'ajouter un LAP à la liste des autorisations d'AP, utilisez la commande **config auth-list add mic <AP MAC Address>**. Pour plus d'informations sur la façon de configurer l'autorisation d'AP, consultez l'Exemple de configuration de l'autorisation de points d'accès légers (LAP) dans un réseau sans fil unifié Cisco.

Problème 6 : Le hachage de clé publique SSC est erroné ou manquant

Effectuez les étapes suivantes afin de résoudre ce problème :

1. Émettez la commande **debug lwapp events enable**.Cela vérifie que l'AP essaie d'effectuer

une jointure.

2. Émettez la commande **show auth-list**.Cette commande montre le hachage de clé publique que le contrôleur a dans la mémoire.
3. Émettez la commande **debug pm pki enable**.Cette commande montre le hachage de clé publique réel. Le hachage de clé publique réel doit correspondre au hachage de clé publique que le contrôleur a dans la mémoire. Une différence cause le problème. C'est un exemple de sortie de ce message de débogage :**Remarque:** Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.`(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`**

Effectuez les étapes suivantes pour résoudre le problème :

1. Copiez le hachage de la clé publique situé dans la sortie de la commande **debug pm pki enable** et employez-le pour substituer le hachage de la clé publique dans la liste d'authentification.
2. Émettez la commande **config auth-list add ssc AP_MAC AP_key** afin d'ajouter l'adresse MAC de l'AP et le hachage de clé à la liste des autorisations :C'est un exemple de cette commande :**Remarque:** Cette commande a été déplacée sur la deuxième ligne en raison de contraintes d'espace.`(Cisco Controller)>` **`config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9`**

Problème 7 : Il y a corruption d'un certificat ou d'une clé publique sur l'AP

Le LAP ne joint pas de contrôleur en raison d'un problème de certificat.

Émettez les commandes **debug lwapp errors enable** et **debug pm pki enable**. Vous voyez des messages qui indiquent que des certificats ou des clés sont altérés.

Remarque: Certaines lignes de la sortie ont été déplacées sur la deuxième ligne en raison de contraintes d'espace.

```
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
```

Employez l'une de ces deux options afin de résoudre le problème :

- Demande de de MIC APâ une autorisation de matériaux de retour (RMA).
- Downgrade de de de SSC APâ au Cisco IOS ? Version de logiciel 12.3(7)JA.Si c'est un AP avec un SSC, reconvertissez-le à IOS à l'aide du bouton MODE. Ensuite, utilisez à nouveau l'outil de mise à niveau LWAPP pour reconvertir vers LWAPP. Cela devrait recréer le certificat.

Accomplissez ces étapes afin de rétrograder :

1. Utilisez le bouton de réinitialisation.
2. Effacez les paramètres du contrôleur.
3. Réexécutez la mise à niveau.

Pour plus d'informations sur la mise à niveau d'un LAP vers une version antérieure, consultez Mise à niveau des points d'accès autonomes Cisco Aironet vers le mode léger.

Si vous avez un WCS, vous pouvez émettre les SSC sur le nouveau WLC. Pour plus d'informations sur la façon de configurer des AP en utilisant le WCS, consultez la section Configuration des points d'accès du *Guide de configuration du système de contrôle sans fil Cisco, Version 5.1*.

Problème 8 : Le contrôleur pourrait fonctionner en mode de couche 2

Effectuez l'étape suivante afin de résoudre ce problème :

Vérifiez le mode de fonctionnement du contrôleur. Les AP convertis supportent seulement la découverte de la couche 3. Les AP convertis ne supportent pas la découverte de la couche 2.

Effectuez les étapes suivantes pour résoudre le problème :

1. Définissez le WLC pour être en mode couche 3.
2. Redémarrez et configurez l'interface de gestionnaire d'AP.Si vous avez un port de service, comme le service port sur 4402 ou 4404, il doit se trouver dans un super-réseau différent du gestionnaire d'AP et des interfaces de gestion.

Problème 9 : Vous recevez un message d'erreur sur l'AP après la conversion vers le LWAPP

Vous voyez le message d'erreur suivant :

```
*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
```

L'AP se recharge après 30 secondes et recommence le processus.

Complétez les étapes suivantes pour résoudre ce problème :

1. Vous avez un SSC AP. Effectuez une reconversion vers une image IOS autonome.
2. Effacez la configuration en émettant la commande **write erase** et rechargez. N'enregistrez pas la configuration lors du rechargement.

Problème 10 : Le contrôleur reçoit le message de détection de l'AP sur le VLAN incorrect (vous voyez le débogage de message de détection, mais pas de réponse)

Le message suivant s'affiche dans la sortie de la commande **debug lwapp events enable** :

```
Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!
```

Ce message signifie que le contrôleur a reçu une demande de détection via une adresse IP de diffusion qui a une adresse IP source, laquelle n'est dans aucun sous-réseau configuré sur le contrôleur. Cela signifie également que le contrôleur supprime le paquet.

Le problème est que l'AP n'envoie pas la demande de détection à l'adresse IP de gestion. Le contrôleur signale une demande de détection de diffusion à partir d'un VLAN qui n'est pas configuré sur le contrôleur. Cela se produit généralement quand le client effectue une agrégation de tous les VLAN autorisés au lieu de les restreindre aux VLAN sans fil.

Complétez les étapes suivantes pour résoudre ce problème :

1. Si le contrôleur se trouve sur un autre sous-réseau, les AP doivent faire l'objet d'un **priming** pour l'adresse IP des contrôleurs, ou les AP doivent recevoir l'adresse IP des contrôleurs en utilisant n'importe laquelle des méthodes de détection.
2. Le commutateur est configuré pour autorisé certains VLAN qui ne se trouvent pas sur le contrôleur. Restreignez les VLAN autorisés sur les agrégations.

Problème 11 : Le LAP 1250 ne peut pas joindre le WLC

La configuration se compose d'un WLC 2106 qui exécute la version 4.1.185.0. Un AP Cisco 1250 ne peut pas joindre le contrôleur.

Le journal sur le WLC indique ceci :

```
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.
```

Solution : Cela est dû au fait que le LAP de la gamme Cisco 1250 n'est pas pris en charge sur la version 4.1. Le LAP de la gamme Cisco Aironet 1250 est pris en charge à partir des versions de contrôleur 4.2.61. Afin de résoudre ce problème, mettez à niveau le logiciel du contrôleur vers la version 4.2.61.0 ou une version ultérieure.

Problème 12 : L'AP ne peut pas joindre le WLC, car le pare-feu bloque des ports nécessaires

Si un pare-feu est utilisé dans le réseau d'entreprise, assurez-vous que les ports suivants sont activés sur le pare-feu pour que le LAP puisse joindre le contrôleur et communiquer avec lui.

Vous devez activer les ports suivants :

- Activez les ports UDP suivants pour le trafic LWAPP :Données - 12222Contrôle - 12223
- Activez les ports UDP suivants pour le trafic de mobilité :16666 - 1666616667 - 16667
- Activez les ports UDP 5246 et 5247 pour le trafic CAPWAP.
- TCP 161 et 162 pour SNMP (pour le système de contrôle sans fil [WCS])

Les ports suivants sont facultatifs (selon vos besoins) :

- UDP 69 pour TFTP
- TCP 80 et/ou 443 pour le HTTP ou HTTPS pour l'accès à la GUI
- TCP 23 et/ou 22 pour Telnet ou SSH pour l'accès à la CLI

Problème 13 : Adresse IP en double dans le réseau

C'est un autre problème fréquent qui est constaté quand l'AP essaye de joindre le WLC. Le message d'erreur suivant peut s'afficher quand l'AP essaie de joindre le contrôleur.

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

Une des raisons pour lesquelles ce message d'erreur apparaît est qu'il y a une adresse IP en double sur le réseau qui correspond à l'adresse IP du gestionnaire d'AP. En pareil cas, le LAP se met sans cesse hors tension et ne peut pas joindre le contrôleur.

Les débogages montreront que le WLC reçoit des demandes de détection LWAPP des AP et qu'il transmet une réponse de détection LWAPP aux AP. Cependant, les WLC ne reçoivent pas les demandes de jointure LWAPP en provenance des AP.

Afin de résoudre ce problème, effectuez un test Ping sur le gestionnaire d'AP à partir d'un hôte câblé sur le même sous-réseau IP que le gestionnaire d'AP. Vérifiez ensuite le cache ARP. Si une adresse IP en double est trouvée, supprimez le périphérique avec l'adresse IP en double ou modifiez l'adresse IP sur le périphérique de sorte qu'il ait une adresse IP unique sur le réseau.

L'AP peut alors joindre le WLC.

Problème 14 : Les AP LWAPP ne joignent pas le WLC si la MTU du réseau est inférieure à 1 500 octets

Cela est dû au bogue Cisco ayant l'ID **CSCsd94967**. La jointure des AP LWAPP à un WLC pourrait échouer. Si la demande de jointure LWAPP est supérieure à 1 500 octets, LWAPP

doivent la fragmenter. La logique pour tous les AP LWAPP est que la taille du premier fragment est de 1 500 octets (y compris l'en-tête IP et UDP) et celle du second fragment est de 54 octets (y compris l'en-tête IP et UDP). Si le réseau entre les AP LWAPP et le WLC a une taille de MTU inférieure à 1 500 (comme ce pourrait être le cas lors de l'utilisation d'un protocole de transmission tunnel tel qu'IPsec VPN, GRE, MPLS, etc.), le WLC ne peut pas gérer la demande de jointure LWAPP.

Vous rencontrerez ce problème dans les conditions suivantes :

- WLC qui exécute la version 3.2 ou antérieure du logiciel
- MTU de chemin d'accès réseau entre l'AP et le WLC inférieure à 1 500 octets

Pour résoudre ce problème, utilisez l'une des options suivantes :

- Effectuez une mise à niveau vers la version 4.0 du logiciel du WLC, si la plate-forme la prend en charge. Dans la version 4.0 du WLC, ce problème est résolu en permettant au tunnel LWAPP pour réassembler jusqu'à 4 fragments.
- Augmentez la MTU de chemin d'accès réseau à 1 500 octets.
- Utilisez des REAP 1030 pour les emplacements accessibles via des chemins d'accès à faibles MTU. Les connexions LWAPP REAP à 1 030 AP ont été modifiées pour traiter cette situation en réduisant la MTU utilisée pour le mode REAP.

Problème 15 : Le LAP de la gamme 1142 ne joint pas le WLC ; message d'erreur sur le WLC : lwapp_image_proc: unable to open tar file

Les MAP de la gamme 1142 sont prises en charge uniquement avec le WLC version 5.2 et ultérieures. Si vous exécutez des versions du WLC antérieures à 5.2, vous ne pouvez pas enregistrer le LAP auprès du contrôleur et un message d'erreur semblable à celui-ci s'affichera :

```
*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
```

Afin d'enregistrer les LAP 1140 auprès du WLC, mettez à niveau le firmware sur le WLC vers la version 5.2 ou ultérieures.

Problème 16 : Les LAP de la gamme 1000 ne peuvent pas joindre le contrôleur de réseau local sans fil ; le WLC exécute la version 5.0

Cela est dû au fait que la version 5.0.148.0 ou ultérieures du logiciel du WLC n'est pas compatible avec les AP de la gamme Cisco Aironet 1000. Si vous avez une gamme Cisco 1000 ENROULEZ dans un réseau, qui exécute des versions 5.0.48.0 WLC, le RECOUVREMENT de gamme 1000 ne joint pas le contrôleur et vous voyez ce message dérouté sur le WLC.

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

Problème 17 : Recouvrements avec l'image de maille non capable joindre WLC

Le point d'accès léger ne s'inscrit pas au WLC. Le log affiche ceci le message d'erreur

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

Ceci peut se produire si le point d'accès léger était expédié avec une image de maille et est en mode de passerelle. Si le RECOUVREMENT était commandé avec le logiciel de maille là-dessus, vous devez ajouter le RECOUVREMENT à la liste d'autorisation AP. Choisissez le **Security > AP Policies** et ajoutez **AP à la** liste d'autorisation. AP devrait alors joindre, télécharger l'image à partir du contrôleur, puis de l'inscription au WLC en mode de passerelle. Alors vous devez changer AP au mode local. Le RECOUVREMENT télécharge l'image, les réinitialisations et les registres de nouveau au contrôleur en mode local.

Problème 18 : Message d'erreur - Dropping primary discovery request from AP XX:Aa : BB : XX : Densité double : DD - maximum APs joined 6/6

Il y a une limite au nombre de LAP qui peuvent être pris en charge par un WLC. Chaque WLC prend en charge un certain nombre de LAP, lequel dépend du modèle et de la plate-forme. Ce message d'erreur s'affiche sur le WLC quand il reçoit une demande de détection après avoir atteint sa capacité d'AP maximale.

Voici le nombre de LAP pris en charge sur les différentes plates-formes et les différents modèles de WLC :

- Le contrôleur de la gamme 2100 prend en charge jusqu'à 6, 12 ou 25 LAP. Cela dépend du modèle du WLC.
- Le 4402 prend en charge jusqu'à 50 LAP, tandis que le 4404 en prend en charge jusqu'à 100. Il est donc idéal pour les grandes entreprises et les applications à haute densité.
- Le module Wireless Services Module (WiSM) de la gamme Catalyst 6500 est un commutateur Catalyst 6500 intégré et deux contrôleurs Cisco 4404 qui prennent en charge jusqu'à 300 LAP.
- Le WiSM du routeur de la gamme Cisco 7600 est un routeur Cisco 7600 intégré et deux contrôleurs Cisco 4404 qui prennent en charge jusqu'à 300 LAP.
- Le routeur à services intégrés de la gamme Cisco 28/37/38xx est un routeur 28/37/38xx intégré et un module de réseau de contrôleur Cisco qui prend en charge jusqu'à 6, 8, 12 ou 25 LAP, en fonction de la version du module de réseau. Les versions qui prennent en charge 8, 12 ou 25 AP et la version à 6 points d'accès NME-AIR-WLC6-K9 proposent un processeur à grande vitesse et davantage de mémoire intégrée que la version à 6 points d'accès NM-AIR-WLC6-K9.
- Le commutateur du WLC intégré Catalyst 3750G est un commutateur Catalyst 3750 intégré et un contrôleur de la gamme Cisco 4400 qui prennent en charge jusqu'à 25 ou 50 LAP.

Informations connexes

- Exemple de configuration de l'autorisation des points d'accès légers (LAP) dans un réseau sans fil unifié Cisco
- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.1
- Support et documentation techniques - Cisco Systems