Wireless LAN Controller に接続しない Lightweight アクセス ポイントのトラブルシューティング

目次

XX: DD: DD -最大 AP 6/6 に加入しました
関連情報

概要

このドキュメントは、Wireless LAN Controller（WLC）のディスカバリと接続のプロセスについて概説します。 また、Lightweight アクセス ポイント（LAP）が WLC に接続できない問題とそのトラブルシューティング手順も説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LAP および Cisco WLC の設定に関する基本的な知識
- Lightweight アクセス ポイント プロトコル（LWAPP）に関する基礎知識

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Wireless LAN Controller（WLC）の検出および接続プロセスの概要

Cisco Unified Wireless Network では LAP はワイヤレス クライアントに対してサービスを提供する前に WLC を検出して接続する必要があります。

当初コントローラはレイヤ 2 モードでのみ動作していました。 レイヤ 2 モードでは LAP は管理インターフェイスと同じサブネット上にあり、レイヤ 3 モードの AP マネージャ インターフェイスはコントローラにありません。 LAP はレイヤ 2 カプセル化（イーサネット カプセル化）のみを使用してコントローラと通信し、IP アドレスに対して Dynamic Host Configuration Protocol（DHCP）を使用しません。

コントローラのレイヤ 3 モードの開発時に、新たなレイヤ 3 インターフェイスである AP マネージャが導入されました。 レイヤ 3 モードでは LAP は最初に IP アドレスに対して DHCP を使用してから、IP アドレス（レイヤ 3）を使用して管理インターフェイスにディスカバリ要求を送信します。 これによりコントローラの管理インターフェイスとは異なるサブネットに LAP を配置できます。 現在ではレイヤ 3 モードは占有モードです。 一部のコントローラと LAP ではレイヤ 3 モードだけが実行可能です。

ただしこれにより、 LAP が異なるサブネット内にあるコントローラの管理 IP アドレスをどのように検出するのかという新たな問題が生じます。

レイヤ 2 モードではこれらは同一サブネット内に存在している必要があります。 レイヤ 3 モードではコントローラと LAP は実質的にはネットワーク上でかくれんぼをしているようなものです。 LAP に対し DHCP オプション 43 または DNS 解決（「Cisco-lwapp-controller@local_domain」）を使用してコントローラの位置を通知しない場合、あるいは LAP を静的に設定していない場合

、LAP はネットワーク内でコントローラの管理インターフェイスを検出する場所を認識しません。

これらの方法以外にも、LAP は 255.255.255.255 ローカル ブロードキャストを使用してコントローラのローカルサブネットを自動的に検索します。 また LAP は接続したコントローラの管理 IP アドレスをリブート後にも記憶しています。 したがって最初に管理インターフェイスのローカルサブネットに LAP を配置すると、LAP はコントローラの管理インターフェイスを検出し、そのアドレスを記憶します。 これはプライミングと呼ばれます。 LAP を後で置き換える場合、コントローラは検出されなくなります。 したがって、DHCP オプション 43 または DNS を使用した方法を使用することを推奨します。

LAP はコントローラの検出時に、そのコントローラがレイヤ 2 モードとレイヤ 3 モードのいずれであるかを認識しません。 したがって LAP は常に最初にディスカバリ要求を使用してコントローラの管理インターフェイス アドレスに接続します。 次にコントローラが LAP に対し、コントローラのモードをディスカバリ応答で通知します。 コントローラがレイヤ 3 モードの場合、ディスカバリ応答にはレイヤ 3 AP マネージャ IP アドレスが含まれているため、LAP は次に AP マネージャ インターフェイスに対して接続要求を送信できます。

注: デフォルトでは、設定時に管理インターフェイスおよび AP マネージャ インターフェイスの両方が VLAN 上でタグなしのままになります。 タグが付けられる場合は、WLC からのディスカバリおよび接続応答を適切に受信できるように、同じ VLAN にタグ付けされていることを確認してください。

LWAPP AP ではレイヤ 3 モードでの起動時に次の処理が行われます。

1. LAP に対して以前に静的 IP アドレス割り当てられていない場合には、LAP はブートすると IP アドレスに DHCP を使用します。
2. LAP が各種ディスカバリ アルゴリズムを使用してコントローラにディスカバリ要求を送信し、コントローラ リストを作成します。 実質的には、LAP は次の方法で可能な限り多くのコントローラの管理インターフェイス アドレスを取得します。DHCP オプション 43 (オフィスとコントローラが複数の地域に散在しているグローバル企業で最適です) cisco-capwap-controller の DNS エントリ (ローカル ビジネスに最適です。新たな AP が接続した位置を検出する場合にも使用できます。) **注:** CAPWAP を使用する場合は、cisco-capwap-controller の DNS エントリがあることを確認してください。LAP が以前に記憶したコントローラの管理 IP アドレスサブネットでのレイヤ 3 ブロードキャストOver-the-Air Provisioning静的に設定された情報このリストから、配備のために使用するべき最も容易な方式は同じ サブネットの LAPs をコントローラのマネージメントインターフェイスとして持つことおよびコントローラを見つける LAPâ s レイヤ3 ブロードキャストを許可することです。 この方法は小規模ネットワークを導入しておりローカル DNS サーバを所有していない企業で使用します。次に簡単な展開方法は、DHCP で DNS エントリを使用する方法です。同一 DNS 名のエントリを複数使用できます。 これにより LAP が複数のコントローラを検出できます。 この方法は、複数コントローラを一カ所に配置しており、ローカル DNS サーバを所有する企業で使用します。 また、複数の DNS サフィクスを使用しており、コントローラがサフィクスによって分離されている場合にもこの方法を使用します。DHCP オプション 43 は、DHCP を使用して情報をローカライズする大企業で使用されます。 この方法は、1 つの DNS サフィクスを使用する大企業が使用します。 たとえばシスコは欧州、オーストラリア、米国にビルを所有しています。 LAP がコントローラにローカルでのみ接続するようにする場合、シスコでは DNS エントリを使用できないため、DHCP オプション 43 情報を使用して LAP に対しローカル コントローラの管理 IP アドレスを通知する必要があります。最終的には、静的 な 設定は DHCPサーバがないネットワークのために使用されます。コ

ンソールポートおよび APâ s CLI によってコントローラに加入するのに静的に必要な情報を設定できます。 AP CLI を使用してコントローラ情報を静的に設定する方法については、『アクセス ポイント CLI を使用したコントローラ情報の手動設定』を参照してください。 LAP がコントローラの検出に使用する各種ディスカバリ アルゴリズムの詳細については、『WLC への LAP の登録』を参照してください。DHCP サーバでの DHCP オプション 43 の設定については、『Lightweight Cisco Aironet アクセス ポイント用 DHCP オプション 43 の設定例』を参照してください。

3. リスト内のすべてのコントローラにディスカバリ要求を送信し、ディスカバリ応答がコントローラから返されるまで待機します。ディスカバリ応答には、システム名、AP マネージャの IP アドレス、各 AP マネージャ インターフェイスにすでに接続している AP の数、コントローラの総余剰キャパシティが含まれています。
4. コントローラ リストを参照し、次のリストの順序に従ってコントローラに接続要求を送信します（AP がコントローラからのディスカバリ応答を受信した場合のみ）。プライマリ コントローラのシステム名（LAP で以前に設定された名前）セカンダリ コントローラのシステム名（LAP で以前に設定された名前）ターシャリ コントローラのシステム名（LAP で以前に設定された名前）マスター コントローラ（以前にプライマリ、セカンダリ、またはターシャリ コントローラ名を使用して LAP が設定されていない場合。 新しい LAP が接続するコントローラを常に認識しておくために使用されます。 ）上記のいずれも不明な場合は、ディスカバリ応答の余剰キャパシティ値を使用してコントローラ間でロード バランスを行います。2 つのコントローラの余剰キャパシティが同一の場合、ディスカバリ要求に対してディスカバリ応答で最初に応答したコントローラに接続要求を送信します。 1 つのコントローラで複数のインターフェイスに複数の AP マネージャがある場合は、AP の数が最も少ない AP マネージャ インターフェイスを選択してください。コントローラは、証明書や AP クレデンシャルを検査せずにすべてのディスカバリ要求に応答します。 ただし、コントローラから接続応答を受信できるようにするため、接続要求には有効な証明書が必要です。 LAP が選択したコントローラから接続応答を受信しない場合、LAP はリスト内の次のコントローラ（設定済みコントローラ（プライマリ/セカンダリ/ターシャリ）以外）を試します。
5. AP は接続応答を受信すると、AP に含まれているイメージがコントローラと同じであることを確認します。 コントローラと同じイメージが含まれていない場合、AP はコントローラからイメージをダウンロードしてリブートし、新しいイメージをロードし、このプロセスをステップ 1 から再び実行します。
6. 同じソフトウェア イメージが含まれている場合、コントローラに対して設定を要求し、コントローラで登録状態に移行します。AP は設定をダウンロードした後に、新しい設定を適用するために再度リロードすることがあります。 したがってリロードが 1 回余分に実行されることがありますが、これは通常の動作です。

コントローラからのデバッグ

コントローラには、CLI でプロセス全体を確認するために使用できる **debug** コマンドがいくつかあります。

- **デバッグ lwapp イベント enableâ** はディスカバリ パケットおよび加入パケットを示します。
- **デバッグ lwapp パケット enableâ** はパケットがディスカバリの情報を水平にし、パケットに加入することを示します。
- **デバッグ pm PKI enableâ** は認証の検証 プロセスを表示します。
- **デバッグ ディセーブルallâ** はデバッグを消します。

ログ ファイルに出力をキャプチャできるターミナル アプリケーションを使用して、コントローラにコンソール インまたはコントローラへの安全なシェル (SSH) /tenet 接続し、次のコマンドを入力します。

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**

デバッグのキャプチャ後に、**debug disable-all** コマンドを使用してすべてのデバッグをオフにします。

以降の項では、LAP がコントローラに登録している場合のこれらの **debug** コマンドの出力を示します。

debug lwapp events enable

このコマンドは、LWAPP ディスカバリおよび接続プロセスで発生した LWAPP イベントとエラーに関する情報を提供します。

WLC と同じイメージが含まれている LAP に対する **debug lwapp events enable** コマンドの出力を次に示します。

注: 以下の出力では、スペースの制約上 2 行に分割されている行があります。

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.*

前の項で説明したように、WLC に登録された LAP は、コントローラと同じイメージが LAP にあるかどうかを確認します。 LAP と WLC のイメージが異なる場合、LAP は最初に WLC から新しいイメージをダウンロードします。 LAP に同じイメージがある場合は、設定とその他のパラメータを WLC からダウンロードします。

LAP が登録プロセスの一部としてコントローラからイメージをダウンロードする場合は、**debug lwapp events enable** コマンド出力に次のメッセージが表示されます。

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

イメージのダウンロードが完了すると、LAP がリブートし、ディスカバリおよび接続アルゴリズムが再度実行されます。

debug pm pki enable

接続プロセスにおいて WLC は各 LAP の証明書が有効であることを確認し、各 LAP を認証します。

AP は WLC に LWAPP 接続要求を送信するときに、その X.509 証明書を LWAPP メッセージに組み込みます。 また、AP はランダムなセッション ID を生成し、LWAPP 接続要求に付加します。 WLC は LWAPP 接続要求を受信すると、AP の公開キーを使用して X.509 証明書のシグニチャを検証し、その証明書が信頼できる認証局から発行されたものであるかを確認します。

それはまた AP 認証の有効期間の開始日および時間を検知 し、自身の日時 (それ故に controllerâ s はクロック 現在の日付と時間の近くでに設定 される必要があります) とこと日時比較します。 X.509 証明書が確認されたら、WLC はランダム AES 暗号化キーを生成します。 WLC は AES キーを暗号化エンジンに送ります。これにより、AP との間で今後交換される LWAPP 制御メッセージを暗号化および復号化できます。 LAP とコントローラ間の LWAPP トンネルではデータパケットは暗号化されていない状態で送信される点に注意してください。

debug pm pki enable コマンドは、コントローラの接続フェーズで実行される証明書検証プロセスを表示します。 LWAPP 変換プログラムにより作成された自己署名証明書 (SSC) が AP にある場合には、**debug pm pki enable** コマンドは接続処理中に AP ハッシュ キーも表示します。 AP に Manufactured Installed Certificate (MIC) がある場合、ハッシュ キーは表示されません。

注: 2006 年 6 月以降に製造されたすべての AP には MIC があります。

MIC のある LAP がコントローラに接続する場合の **debug pm pki enable** コマンドの出力を次に示します。

注: 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
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
```

SSC が格納されている LAP での **debug pm pki enable** コマンドの出力は次のようになります。この出力には SSC ハッシュも含まれている点に注意してください。

注: 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
(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
```

LAP からのデバッグ

コントローラ デバッグで接続要求が示されなかった場合、LAP にコンソール ポートが組み込まれていれば LAP からプロセスをデバッグできます。 次に示すコマンドでは LAP ブートアップ プロセスを確認できますが、最初にイネーブル モードに切り替える必要があります (デフォルト パスワードは Cisco です) 。

- **デバッグ dhcp detailâ** は DHCP オプション 43 情報を示します。
- **debug ip udpâ** はコントローラ、また DHCP および DNS クエリ (これらすべては UDP パ

ケットに加入/ディスカバリ パケットをです示します。 ポート 12223 は controllerâ s 送信元ポートです) 。
- **デバッグ lwapp クライアント eventâ** は AP のための LWAPP イベントを示します。
- **undebug allâ** は AP のデバッグをディセーブルにします。

debug ip udp コマンドの出力例を次に示します。 次に示す部分的な出力から、コントローラを検出してコントローラに接続するためにブート プロセス中に LAP により送信されるパケットがわかります。

```
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.
```

DHCP 関連の問題の回避

WLC ディスカバリ プロセス開始前に DHCP を使用して IP アドレスを検出する LAP では、DHCP 関連パラメータの設定の誤りが原因で DHCP アドレスの受信で問題が発生することがあります。 この項では、WLC での DHCP の機能と、DHCP 関連の問題を回避するためのベスト プラクティスを説明します。

DHCP では、コントローラは IP ヘルパー アドレスが設定されたルータのように動作します。 つまり、ゲートウェイ IP アドレスを入力し、ユニキャスト パケットによって DHCP サーバに要求を直接転送します。

DHCP オファーがコントローラに戻ると、DHCP サーバ IP アドレスが仮想 IP アドレスに変換されます。 これは、Windows が AP 間でローミングするときに、最初に DHCP サーバへの接続とアドレスの更新が試行されるために行われます。

DHCP サーバ アドレスが 1.1.1.1 (コントローラの一般的な仮想 IP アドレス) の場合、コントローラはそのパケットを代行受信し、Windows に対して迅速に応答できます。

これは、仮想 IP アドレスがすべてのコントローラで同一である理由の 1 つです。 Windows ラップトップは、別のコントローラの AP にローミングするときにはコントローラの仮想インターフェイスへの接続を試行します。 モビリティ イベントとコンテキスト転送により、Windows クライアントのローミング先の新しいコントローラには Windows に再度応答するための情報がすでにすべて準備されています。

コントローラの内部 DHCP サーバを使用する場合に必要な操作は、サブネットに作成するダイナミック インターフェイスで DHCP サーバとして管理 IP アドレスを指定するだけです。 これによりそのインターフェイスが WLAN に割り当てられます。

コントローラに各サブネット内の IP アドレスが必要な理由として、このようにすることで、DHCP 要求に DHCP ゲートウェイ アドレスを指定できることがあります。

WLAN の DHCP サーバを設定する際に留意すべき点がいくつかあります。

1. DHCP サーバの IP アドレスは、コントローラの動的サブネット内のアドレスであってはなりません。 これはブロックされますが、次のコマンドでオーバライドできます。
   config network mgmt-via-dynamic-interface on version 4.0 only (command not available in version 3.2)

2. コントローラは、ダイナミック インターフェイスで IP アドレスを使用して、ダイナミック インターフェイスからユニキャストによって DHCP を転送します。 すべてのファイアウォールでこのアドレスが DHCP サーバに到達できるように許可されていることを確認します。
3. DHCP サーバからの応答が、ファイアウォールを通過してその VLAN 上のコントローラのダイナミック アドレスに到達できることを確認します。 DHCP サーバからダイナミック インターフェイス アドレスに対して ping を実行します。 ダイナミック インターフェイスのゲートウェイ アドレスの発信元 IP アドレスを使用して DHCP サーバに対して ping を実行します。
4. スイッチとルータで AP の VLAN が許可されている場合、そのスイッチとルータのポートをトランクとして設定します。これにより、VLAN でタグ付けされているパケット（DHCP を含む）が有線ネットワークで許可されます。
5. AP の VLAN 上の IP アドレスを割り当てるように DHCP サーバが設定されていることを確認します。 また、WLC を DHCP サーバとして設定することもできます。 WLC での DHCP の設定方法については、『Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 5.0』の『GUI を使用した DHCP の設定』を参照してください。
6. コントローラのダイナミック インターフェイスの IP アドレスが、DHCP サーバの DHCP 範囲の 1 つに属していることを確認します。
7. 最後に、ユニキャスト DHCP 要求に応答しない DHCP サーバ（PIX など）を使用していないことを確認します。

DHCP の問題を解決できない場合の解決策が 2 つあります。

- 内部 DHCP サーバを使用してみます。 ダイナミック インターフェイスで管理 IP アドレスとして使用する DHCP サーバ アドレスを設定し、次に DHCP 内部プールを設定します。 DHCP スコープが有効な場合、この解決策で解決できるはずです。
- CLI（コンソールまたは SSH）での以下のデバッグからの出力を送信して、DHCP 要求に対する応答がないことを確認します。`0. debug mac addr <mac address>`
  `1. debug dhcp message enable`
  `2. debug dhcp packet enable` これは、DHCP パケットが転送されるがコントローラが応答を受信していないことを示します。

最後に、コントローラのセキュリティのため、LAP も含むコントローラが管理インターフェイス サブネット内にない場合は、このコントローラに VLAN またはサブネットを指定することは推奨されません。

注: RADIUS サーバまたは DHCP サーバをコントローラのダイナミック インターフェイス サブネットに含めないでください。 セキュリティにより、コントローラとの通信を試行する戻りパケットがブロックされます。

syslog サーバを使用した LAP 接続プロセスのトラブルシューティング

コントローラ ソフトウェア リリース 5.2 では、すべての CAPWAP 関連エラーを syslog サーバに送信するよう AP を設定できます。 すべての CAPWAP エラー メッセージは syslog サーバ自体から表示できるので、コントローラでデバッグ コマンドを有効にする必要はありません。 この機能と、この機能を有効にするコマンドの詳細については、『Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 5.2』の『アクセス ポイントの接続プロセスのトラブルシューティング』を参照してください。

LAP がコントローラに接続しない原因について

基本事項の確認

- AP と WLC が通信できるかどうかを確認します。
- AP が DHCP からアドレスを取得していることを確かめて下さい（APâ s MAC アドレスがあるように DHCPサーバ リースを確認して下さい）。
- コントローラから AP に対して ping を実行します。
- スイッチの STP 設定が正しく、VLAN へのパケットがブロックされないことを確認します。
- ping が正常に実行される場合は、1 つ以上の WLC コンソールを検出する手段、およびコントローラに telnet/ssh 接続してデバッグを実行できる手段が AP に 1 つ以上あることを確認します。
- AP はリブート時に毎回 WLC ディスカバリ シーケンスを開始し、AP の検出を試行します。AP をリブートし、AP が WLC に接続するかどうかを確認します。

LAP が WLC に接続しない原因となるよくある問題について説明します。

問題 1： コントローラの時刻が、証明書の有効期間内ではない

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. **debug lwapp errors enable** コマンドと **debug pm pki enable** コマンドを実行します。**debug lwapp event enable** コマンドの出力は、AP と WLC の間で渡される証明書メッセージのデバッグを示します。 この出力に、証明書が拒否されたことを示すメッセージが明示されます。**注:** 協定世界時（UTC）のオフセットを必ず考慮に入れてください。次に、コントローラでの **debug lwapp events enable** コマンドの出力を次に示します。**注:** 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
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
```

次に、コントローラでの **debug pm pki enable** コマンドの出力を示します。 この出力は、証明書検証プロセスの後に出力されます。**注:** 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
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)
```

この情報では、コントローラの時刻が LAP の証明書の有効期間内ではないことが明示されています。 そのため、LAP はコントローラに登録できません。 LAP にインストールされている証明書には有効期間が事前に定義されています。 コントローラ時間は LAPâ s 認証の認証の妥当性 間隔の内にあるように設定 する必要があります。

2. コントローラに設定されている日付と時刻が有効期間内であることを確認するため、コントローラの CLI から **show time** コマンドを発行します。 コントローラの時刻がこの証明書の有効期間の前後になっている場合は、期間内になるようにコントローラの時刻を変更します。**注:** コントローラの時刻が正しく設定されていない場合は、コントローラ GUI モードで [Commands] > [Set Time] を選択するか、またはコントローラ CLI から **config time** コマンドを実行してコントローラの時刻を設定します。
3. CLI にアクセス可能な LAP で、AP CLI から **show crypto ca certificates** コマンドを実行して証明書を検証します。このコマンドでは、AP で設定されている証明書の有効期間を確認できます。 次に例を示します。

```
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 ..............................
..................................... ..................................... 
```

このコマンドの出力に関連する有効期間は多数になる場合があるので、出力全体は示していません。 考慮する必要があるのは、関連する AP の名前が名前フィールドに 指定されている Associated Trustpoint: Cisco_IOS_MIC_cert によって指定されている有効期間だけです（ この出力例では名前フィールドは Name: C1200-001563e50c7e です ）。 考慮する必要がある実際の証明書の有効期間はこの部分です。

問題 2： 規制ドメインでの不一致

debug lwapp events enable コマンド出力に次のメッセージが表示されます。

注: 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
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
```

このメッセージは、LAP と WLC の規制ドメインで不一致があることを明示しています。 WLC では複数の規制ドメインがサポートされていますが、規制ドメインから LAP が接続する前に、各規制ドメインを選択する必要があります。 たとえば規制ドメイン -A を使用する WLC では、規制ドメイン -A を使用する AP しか使用できません (他の場合も同様)。 AP および WLC を購入するときには、それらが同一の規制ドメインのものかどうかを確認してください。 それ以外の場合は、LAP を WLC に登録できません。

注: 無線 802.1b/g と 802.11a は 1 つの LAP の同一規制ドメインに属している必要があります。

問題 3： エラー メッセージ：AP cannot join because the maximum number of APs on interface 2 is reached

AP がコントローラに接続しようとすると次のエラー メッセージが表示されることがあります。

```
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.
```

4400 シリーズ コントローラでは、デフォルトでポートあたり最大 48 の AP に対応できます。 コントローラに 48 を超える AP を接続しようとするとこのエラー メッセージが表示されます。 ただし、次のいずれかの方法で (ポートあたり) 1 つのインターフェイスでこれよりも多くの AP に対応できるように 4400 シリーズ コントローラを設定できます。

- リンク集約 (レイヤ 3 モードのコントローラの場合)
- 複数の AP マネージャ インターフェイス (レイヤ 3 モードのコントローラの場合)
- 追加ポートの接続 (レイヤ 2 モードのコントローラの場合)

詳細については、『4400 シリーズ コントローラでの 48 を超えるアクセス ポイントへの対応の設定』を参照してください。

注: シスコは、企業ユーザを対象に追加機能を搭載した 5500 シリーズ WLC を導入しました。 この WLC ではポートあたりの AP の数に制限はありません。 詳細については、『Cisco Wireless LAN Controller コンフィギュレーション ガイド リリース 6.0』の『リンク集約と複数 AP 管理インターフェイスの選択』を参照してください。

問題 4： SSC AP で SSC AP のポリシーが無効になっている

コントローラで SSC ポリシーが無効になっている場合、コントローラで **debug lwapp events enable** コマンドと **debug pm pki enable** コマンドの出力に次のエラー メッセージが示されます。

```
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
```

この問題のトラブルシューティングを行うには、次の手順を実行します。

次のいずれかの操作を行います。

- SSC が格納されている AP を受け入れるようにコントローラが設定されているかどうかを調べるために、コントローラの CLI で **show auth-list** コマンドを実行します。次に出力例を示します。`#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`
- GUI で [Security] > [AP Policies] を選択します。[Accept Self Signed Certificate] チェックボックスにチェックマークが付いているかどうかを確認します。 チェックマークが付いていない場合は、チェックマークを付けます。証明書の種類として [SSC] を選択します。MAC アドレスとキー ハッシュを指定して、AP を認証リストに追加します。このキー ハッシュは、**debug pm pki enable** コマンドの出力から取得できます。 キーハッシュ値の取得については、「問題 6」を参照してください。

問題 5： AP 認証リストが WLC で有効になっているが LAP が認証リストにない

このような場合、コントローラで **debug lwapp events enable** コマンドの出力に次のメッセージが示されます。

```
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
```

コンソール ポートを備えた LAP を使用している場合は、**debug lwapp client error** コマンドを実行すると次のメッセージが表示されます。

```
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.
```

このメッセージにも、LAP がコントローラの AP 認証リストにないことが明示されています。

AP 認証リストのステータスを確認するには、次のコマンドを使用します。

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

LAP を AP 許可リストに追加するために、**構成 auth リストを追加します** mic *<AP MAC アドレス>* コマンドを使用して下さい。 LAP 認証の設定方法の詳細については、『Cisco Unified Wireless Network での Lightweight アクセス ポイント（LAP）認証の設定例』を参照してください。

問題 6： SSC の公開キー ハッシュが間違っているか存在しない

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. **debug lwapp events enable** コマンドを実行します。これにより AP が接続を試行しているかどうかが確認されます。
2. **show auth-list** コマンドを実行します。このコマンドは、コントローラに保存されている公開キー ハッシュを表示します。
3. **debug pm pki enable** コマンドを実行します。このコマンドは、実際の公開キー ハッシュを表示します。 実際の公開キー ハッシュは、コントローラに保存されている公開キー ハッシュと一致している必要があります。 不一致があると問題が発生します。 このデバッグ メッセージの出力例を次に示します。**注:** 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
(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
```

この問題を解決するには、次の手順を実行します。

1. **debug pm pki enable** コマンドの出力から公開キー ハッシュをコピーして、認証リストの公開キー ハッシュを置き換えます。
2. AP の MAC アドレスとキー ハッシュを認証リストに追加するため、**config auth-list add ssc AP_MAC AP_key** コマンドを発行します。このコマンドの例を次に示します。**注:** このコマンドは、スペースの制約上 2 行に分割されています。`(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9`

問題 7： AP の証明書または公開キーが破損している

証明書の問題が原因で LAP がコントローラに接続しません。

debug lwapp errors enable コマンドと **debug pm pki enable** コマンドを実行します。 破損している証明書またはキーを示すメッセージが表示されます。

注: 以下の出力では、スペースの制約上 2 行に分割されている行があります。

```
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
```

次の 2 つのオプションのどちらかを使用して、問題を解決してください。

- MIC APâ 要求 Return Materials Authorization（ RMA ）。
- Cisco IOS への SSC APâ ダウングレードか。 ソフトウェア リリース 12.3(7)JA。SSC が格納されている AP の場合、[MODE] ボタンを使用して IOS に変換します。 次に lwapp アップグレード ツールを再度使用して LWAPP に変換します。 これにより証明書が再作成されます。

ダウングレードするには、次の手順を実行します。

1. リセット ボタンのオプションを使用します。
2. コントローラの設定をクリアします。
3. アップグレードを再び実行します。

LAP のダウンロードの詳細については、『自律型 Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード』を参照してください。

WCS を使用している場合は、新しい WLC に SSC をプッシュできます。 WCS を使用する AP の設定方法の詳細については、『Cisco Wireless Control System コンフィギュレーション ガイド、リリース 5.1』の『アクセス ポイントの設定』を参照してください。

問題 8： コントローラがレイヤ 2 モードで動作している可能性がある

この問題のトラブルシューティングを行うには、次の手順を実行します。

コントローラの動作モードを確認します。 変換後の AP ではレイヤ 3 のディスカバリだけがサポートされます。 変換後の AP ではレイヤ 2 のディスカバリはサポートされません。

この問題を解決するには、次の手順を実行します。

1. WLC がレイヤ 3 モードになるように設定します。
2. リブートして AP マネージャ インターフェイスを設定します。4402 または 4404 のサービス ポートのようなサービス ポートがある場合は、AP マネージャ インターフェイスおよび管理インターフェイスとは別のスーパーネットに設定する必要があります。

問題 9： LWAPP への変換後に AP でエラー メッセージを受け取る

次のエラー メッセージが表示されます。

```
*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
```

AP は 30 秒後にリロードし、プロセスをもう一度開始します。

この問題を解決するには、次の手順を実行します。

1. SSC AP を用意します。 自律型 IOS イメージに変換します。
2. **write erase** コマンドを実行して設定をクリアし、リロードします。 リロードの時点で設定を保存しないでください。

問題 10： コントローラが誤った VLAN に関する AP ディスカバリ メッセージを受け取る（応答ではなくディスカバリ メッセージ デバッグが表示される）

debug lwapp events enable コマンド出力に次のメッセージが表示されます。

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

このエラー メッセージは、コントローラの設定済みサブネット内にない発信元 IP アドレスを持つブロードキャスト IP アドレスからのディスカバリ要求をコントローラが受信したことを意味しています。 つまり、コントローラがパケットをドロップします。

ここでは AP がディスカバリ要求を管理 IP アドレスに送信しないことが問題となります。 コントローラは、コントローラで設定されていない VLAN からのブロードキャスト要求を報告します。 通常、このようになるのは、ユーザがすべての使用可能な VLAN を無線 VLAN に制限するのではなく、それらをトランキングする場合です。

この問題を解決するには、次の手順を実行します。

1. コントローラが別のサブネットにある場合、AP はコントローラ IP アドレスについて**プライミング**されているか、または次のいずれかの検出方法を使用してコントローラ IP アドレス

を受信する必要があります。
2. スイッチが、コントローラにない一部の VLAN を許可するように設定されています。 このように許可されている VLAN をトランクで制限します。

問題 11: 1250 LAP が WLC に接続できない

このセットアップは、バージョン 4.1.185.0 が稼働する 2106 WLC で構成されています。 Cisco 1250 AP はコントローラに接続できません。

WLC のログに次の情報が出力されます。

```
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.
```

解決策： これは、バージョン 4.1 では Cisco 1250 シリーズ LAP がサポートされていないために発生します。 Cisco Aironet 1250 シリーズ AP は、バージョン 4.2.61 以降のコントローラでサポートされています。 この問題を解決するには、ソフトウェアを 4.2.61.0 以降にアップグレードします。

問題 12: AP が WLC に接続できない（ファイアウォールにより必要なポートがブロックされている）

企業ネットワークでファイアウォールが使用されている場合は、LAP がコントローラに接続して通信できるようにするため、ファイアウォールで次のポートが有効になっていることを確認します。

次のポートを有効にする必要があります。

- LWAPP トラフィックのために次の UDP ポートを有効にします。データ トラフィック：12222制御トラフィック：12223
- モビリティ トラフィックのために次の UDP ポートを有効にします。16666 - 1666616667 - 16667
- CAPWAP トラフィックのために UDP ポート 5246 と 5247 を有効にします。
- SNMP のために TCP 161 および 162 を有効にします（Wireless Control System（WCS）の場合）。

次のポートはオプションです（必要に応じて有効にしてください）。

- UDP 69（TFTP）
- TCP 80 および 443（HTTP または HTTPS。GUI アクセスで使用）
- TCP 23 および 22（Telnet または SSH。CLI アクセスで使用）

問題 13: ネットワーク上で重複 IP アドレスが存在する

AP が WLC に接続するときに発生するもう 1 つの一般的な問題です。 AP がコントローラに接続しようとすると次のエラー メッセージが表示されることがあります。

No more AP manager IP addresses remain
このエラー メッセージが表示される理由の 1 つに、ネットワーク上で AP マネージャ IP アドレスと一致する重複 IP アドレスが存在することがあります。 このような場合、LAP は電源のオン/オフを繰り返すためコントローラに接続できません。

デバッグにより WLC が AP から LWAPP ディスカバリ要求を受信し、LWAPP ディスカバリ応答を AP に送信することが示されます。 ただし WLC は LWAPP 接続要求を AP から受信しません。

この問題のトラブルシューティングを行うには、AP マネージャと同じ IP サブネット内の有線ホストから AP マネージャに対して ping を実行します。 次に ARP キャッシュを調べます。 重複する IP アドレスが検出されたら、その重複 IP アドレスのデバイスを削除するか、そのデバイスの IP アドレスを変更します。これにより、デバイスにネットワーク上で一意の IP アドレスが割り当てられます。

その後 AP は WLC に接続できます。

問題 14: ネットワーク MTU が 1500 バイト未満の場合 LWAPP AP が WLC に接続しない

これは、Cisco Bug ID **CSCsd94967** が原因で発生します。 LWAPP AP が WLC に接続できない可能性があります。 LWAPP 接続要求が 1500 バイトを超えている場合、LWAPP は LWAPP 接続要求を分割する必要があります。 すべての LWAPP AP でのロジックは、最初のフラグメント サイズは 1500 バイト（IP および UDP ヘッダーを含む）であり、2 番目のフラグメント サイズが 54 バイト（IP および UDP ヘッダーを含む）というものです。 LWAPP AP と WLC 間のネットワークの MTU サイズが 1500 未満の場合（IPsec VPN、GRE、MPLS などのトネリング プロトコルの使用時に発生する可能性があります）、WLC は LWAPP 接続要求を処理できません。

この問題が発生する状況を次に示します。

- WLC でバージョン 3.2 以前のソフトウェアが稼働している場合
- AP と WLC 間のネットワーク パス MTU が 1500 バイト未満の場合

この問題を解決するには、次のいずれかの手順を実行します。

- プラットフォームで WLC ソフトウェア 4.0 がサポートされている場合はこのソフトウェアにアップグレードする。 WLC バージョン 4.0 では、LWAPP トンネルを 4 フラグメントまで再アセンブル可能にすることで問題が修正されました。
- ネットワーク パス MTU を 1500 バイトに増加する。
- 小さい MTU パスで到達可能な口ケーションに 1030 REAP を使用する。 1030 AP への REAP LWAPP 接続が変更され、REAP モードで使用される MTU を減らすことでこの状態に対応できるようになりました。

問題 15: 1142 シリーズ LAP が WLC に接続せず WLC にエラー メッセージが表示される： lwapp_image_proc: unable to open tar file

1142 シリーズ LAP は WLC リリース 5.2 以降でのみサポートされています。 5.2 より古いバージョンの WLC を実行している場合、LAP をコントローラに登録できず、次のようなエラー メッセージが表示されます。

```
*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
```

1140 LAP を WLC に登録するには、WLC のファームウェアを 5.2 以降のバージョンにアップグレードしてください。

問題 16: 1000 シリーズ LAP が Wireless LAN Controller (WLC バージョン 5.0) に接続できない

これは、WLC ソフトウェア リリース 5.0.148.0 以降には Cisco Aironet 1000 シリーズ AP と互換性がないことが原因で発生します。 WLC バージョン 5.0.48.0 が稼働するネットワークに Cisco 1000 シリーズ LAP が接続している場合、1000 シリーズ LAP はコントローラに接続せず、WLC で次のトラップ メッセージが表示されます。

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

問題 17: メッシュ イメージが搭載されている LAP が WLC に接続できない

Lightweight アクセス ポイントが WLC に登録されません。 ログに次のエラー メッセージが表示されます。

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

これは、Lightweight アクセス ポイントにメッシュ イメージが搭載されており、このアクセス ポイントがブリッジ モードの場合に発生します。 LAP とメッシュ ソフトウェアを併せて発注した場合は、LAP を AP 認証リストに追加する必要があります。 [Security] > [AP Policies] を選択して AP を認証リストに追加します。 AP はコントローラに接続し、コントローラからイメージをダウンロードし、ブリッジ モードで WLC に登録します。 次に、AP をローカル モードに変更します。 LAP はイメージをダウンロードし、リブートしてローカル モードでコントローラに再び登録します。

問題 18: エラーメッセージ-プライマリ ディスカバリ 要求を AP XX から廃棄します: AA: BB: XX: DD: DD -最大 AP 6/6 に加入しました

WLC でサポートできる LAP の数は制限されています。 各 WLC でサポートされる LAP の数は限定されており、この数はモデルとプラットフォームによって異なります。 このエラー メッセージは、WLC の AP 最大数に達した後で WLC がディスカバリ要求を受け取ると WLC 上で表示されます。

各種 WLC プラットフォームおよびモデルでサポートされている LAP の数を次に示します。

- 2100 シリーズ コントローラでは 6、12、または 25 個の LAP がサポートされています。 この数は WLC のモデルによって異なります。
- 4402 では最大 50 個の LAP、4404 では最大 100 個の LAP がサポートされています。 このため、大企業や密度が高い大規模アプリケーションに理想的です。
- Catalyst 6500 シリーズ Wireless Services Module (WiSM) は、Catalyst 6500 スイッチと 2 つの Cisco 4404 コントローラが統合されたもので、最大 300 個の LAP をサポートします。
- Cisco 7600 シリーズ ルータ WiSM は、Cisco 7600 ルータと 2 つの Cisco 4404 コントローラが統合されたもので、最大 300 個の LAP をサポートします。
- Cisco 28/37/38xx シリーズ サービス統合型ルータは、28/37/38xx ルータと Cisco コントロー

ラ ネットワーク モジュールを統合したもので、ネットワーク モジュールのバージョンに応じて最大 6 個、8 個、12 個、または 25 個の LAP をサポートします。 8 個、12 個、または 25 個の AP をサポート可能なバージョンおよび NME-AIR-WLC6-K9 6 アクセス ポイント バージョンは、高速プロセッサと、NM-AIR-WLC6-K9 6 アクセス ポイント バージョンよりも大容量のオンボード メモリを搭載しています。
- Catalyst 3750G 統合型 WLC スイッチは、Catalyst 3750 スイッチと Cisco 4400 シリーズ コントローラが統合されたもので、最大 25 個または 50 個の LAP をサポートします。

関連情報

- Cisco Unified Wireless Network での Lightweight アクセス ポイント（LAP）の認可設定の例
- Wireless LAN Controller（WLC）への Lightweight AP（LAP）の登録
- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 4.1
- テクニカルサポートとドキュメント - Cisco Systems