WLC に接続できない Lightweight AP のトラブルシューティング

内容

はじめに

このドキュメントでは、AireOS ワイヤレス LAN コントローラ（WLC）のディスカバリと参加プロセスについて説明します。

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。

- Lightweightアクセスポイント(LAP)およびCisco AireOS WLCの設定に関する基礎知識
- Lightweight Access Point プロトコル（CAPWAP）に関する基礎知識

使用するコンポーネント

このドキュメントではAireOS WLCを中心に説明し、Catalyst 9800については説明しません。ただし、参加プロセスはほとんど同じです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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。

WLC ディスカバリと参加プロセスの概要

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。

しかし、これには次の疑問があります。コントローラが異なるサブネットに属している場合、LAP はそのコントローラの管理 IP アドレスをどのように見つけたのでしょうか。

LAPに対して、DHCPオプション43、Cisco-capwap-controller.local_domainのDomain Name System（DNS；ドメインネームシステム）解決、またはスタティックな設定を介してコントローラの場所を通知しない場合、LAPでは、ネットワーク内のどこでコントローラの管理インターフェイスを検索すればよいかが認識されません。

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はコントローラの管理IPアドレスを記憶し、リブート後もモビリティピアとして存在するコントローラを保持します。ただし、APは別のWLCに加入するとすぐに、その新しいWLCとそのモビリティピアのIPだけを記憶し、以前のWLCのIPは記憶しません。そのため、管理インターフェイスのローカルサブネット上に LAP を最初に配置すると、コントローラの管理インターフェイスが検出され、アドレスが記憶されます。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 方式の使用を推奨します。

LAP は必ず、ディスカバリ要求によって最初にコントローラの管理インターフェイスのアドレスに接続します。その後コントローラは LAP にレイヤ 3 AP マネージャインターフェイス（デフォルトで管理用にすることも可能）の IP アドレスを通知し、LAP が次に AP マネージャインターフェイスに参加要求を送信できるようにします。

AP は起動時に次のプロセスを実行します。

- 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。
- 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。

a. DHCP オプション 43 (オフィスとコントローラが異なる大陸にあるグローバル企業に適しています) 。

cisco-capwap-controller

- のDNSエントリ (ローカルビジネスに適している。新規のAPが参加する場所を見つけるためにも使用できます) 。CAPWAPを使用する場合、 cisco-capwap-controllerのDNSエントリがあることを確認します。
- 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.
- 静的に設定された情報.
- AP が最後に参加した WLC のモビリティグループにあるコントローラ.

上記の中でも特に簡単なのは、コントローラの管理インターフェイスと同じサブネットに LAP を配置し、LAP のレイヤ 3 ブロードキャストを使用してコントローラを検出する方法です。小規模なネットワークがあり、ローカル DNS サーバーを所有していない企業は、この方法を使用する必要があります。

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。すべてのコントローラが 1 ヵ所に置かれ、ローカル DNS サーバーを所有している企業は、この方法を使用する必要があります。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、大企業が DHCP によって情報をローカライズするために使用されます。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。

最後に、DHCP サーバーがないネットワークには、静的設定が使用されます。コンソールポートおよび AP CLI を使用して、コントローラに接続するために必要な情報を静的に設定できます。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を確認するには、次のコマンドを使用します。

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

DHCP サーバーでの DHCP オプション 43 の設定方法については、DHCP オプション 43 の設定の例を参照してください。

- リスト上のすべてのコントローラにディスカバリリクエストを送信し、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されている AP の数、およびコントローラの全体的な過剰容量を含むコントローラのディスカバリ応答を待ちます。
- 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）。

a. プライマリコントローラのシステム名（以前に LAP で設定済み）。

b. セカンダリコントローラのシステム名（以前に LAP で設定済み）。

c. ターシャリコントローラのシステム名（以前に LAP で設定済み）。

d. プライマリコントローラ（LAP が以前にプライマリ、セカンダリ、またはターシャリコントローラ名で設定されていない場合。新しい LAP が参加するコントローラを常に把握しておくために使用されます）。

e. 上記の条件のいずれにも当てはまらない場合、ディスカバリ応答の過剰容量値を使用することで、コントローラ間のロードバランシングを行います。

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、証明書のチェックまたは AP クレデンシャルなしですべてのディスカバリ要求に応答します。ただし、コントローラから参加応答を取得するには、参加要求に有効な証明書が必要です。LAP は、選択したコントローラから参加応答を受信しない場合、コントローラが設定済みのコントローラ（プライマリ/セカンダリ/ターシャリ）でないかぎり、リスト内の次のコントローラを試行します。

• 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。

• 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。

設定のダウンロード後、新しい設定を有効にするために AP がもう一度リロードされることがあります。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でプロセス全体を表示するために使用できる**debug** コマンドがいくつかあります。

•

debug capwap events enable:検出パケットと参加パケットを表示します。

- **debug capwap packet enable**:検出パケットと参加パケットの情報をパケットレベルで表示します。

- **debug pm pki enable**:証明書の検証プロセスを表示します。

- **debug disable-all**:デバッグをオフにします。

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。

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

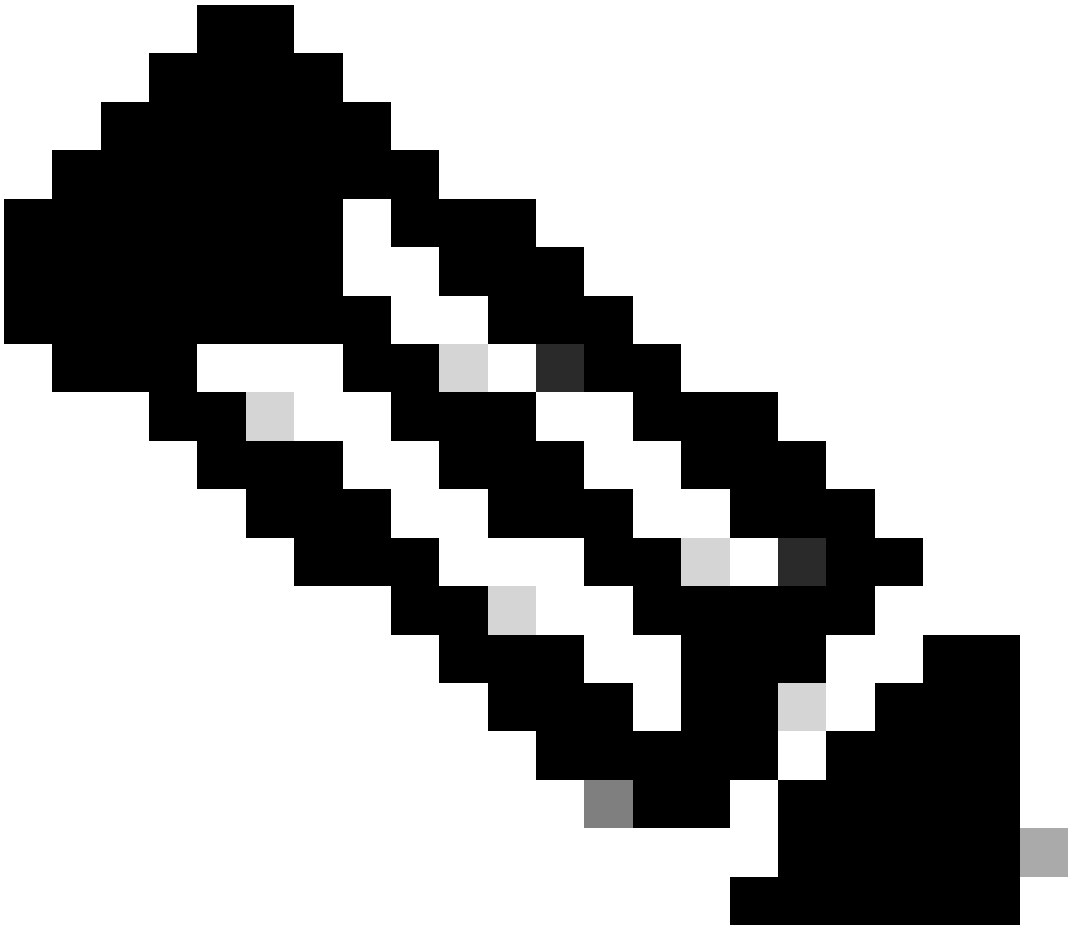
デバッグをキャプチャした後、debug disable-allコマンドを使用して、すべてのデバッグを無効にします。

以降のセクションでは、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 capwap events enable

このコマンドを使用すると、CAPWAP ディスカバリプロセスと参加プロセス中に起きる CAPWAP イベントとエラーに関する情報を確認できます。

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



注：出力された行の一部は、スペースの制約により 2 行目に移動しています。

---

debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317

!--- CAPWAP discovery request sent to the WLC by the LAP.

*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317

!--- WLC responds to the discovery request from the LAP.

*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

!--- LAP sends a join request to the WLC.

*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join

!--- WLC responds with a join reply to the LAP.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure

!--- LAP requests for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99

!--- WLC responds by providing all the necessary configuration information to the LAP.

*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.

!--- LAP is up and ready to service wireless clients.

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- 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 capwap events enable** コマンド出力に次のメッセージが表示されます。

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

イメージのダウンロードが完了すると、LAP がリブートして検出を実行し、アルゴリズムに再度参加します。

debug pm pki enable

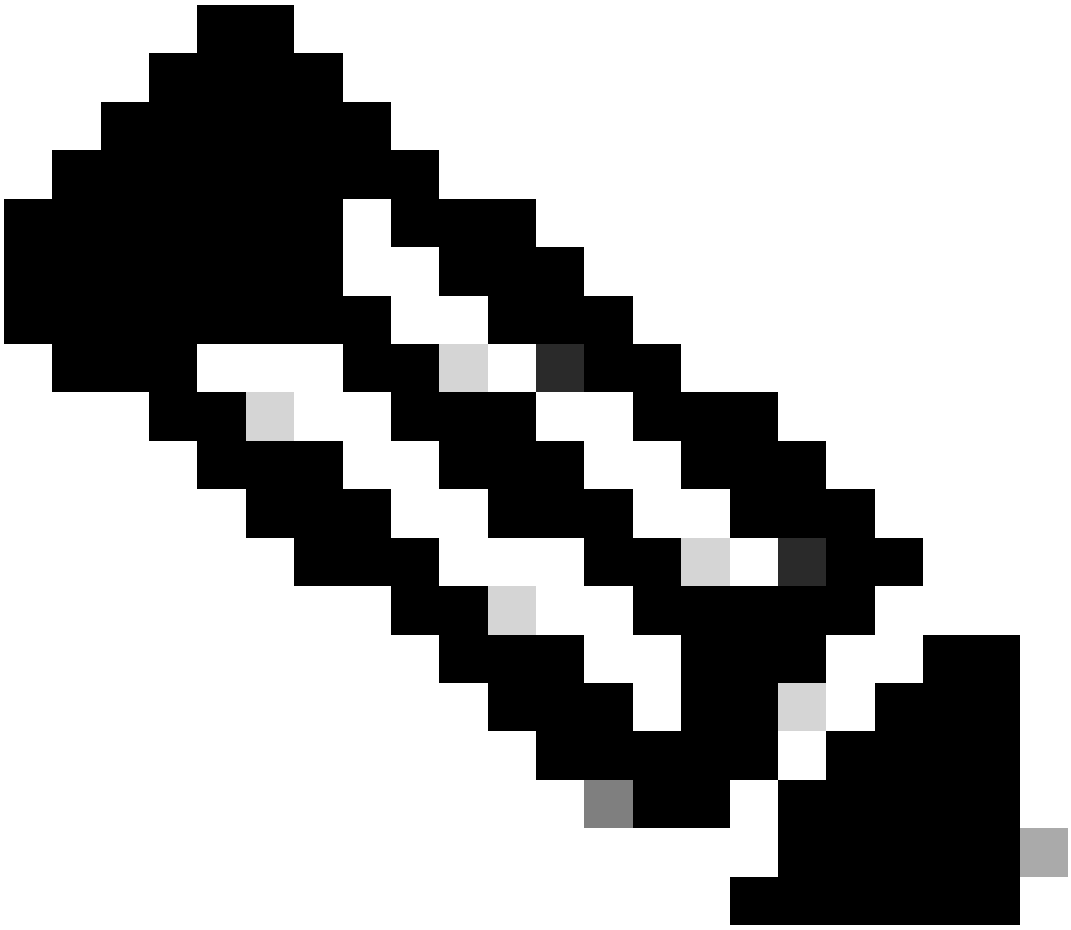
参加プロセスの一環として、WLC は証明書の有効性を確認して各 LAP を認証します。

AP は、CAPWAP 参加要求を WLC に送信するときに、X.509 証明書を CAPWAP メッセージに埋め込みます。AP はランダムセッション ID も生成します。これも CAPWAP 参加要求に含まれます。WLC は CAPWAP 参加要求を受信すると、AP の公開キーを使用して X.509 証明書の署名を検証し、信頼された証明機関によって証明書が発行されていることを確認します。

また、AP の証明書の有効性間隔の開始日時を確認し、その日付および時刻を、自身の日付および時刻と比較します (したがって

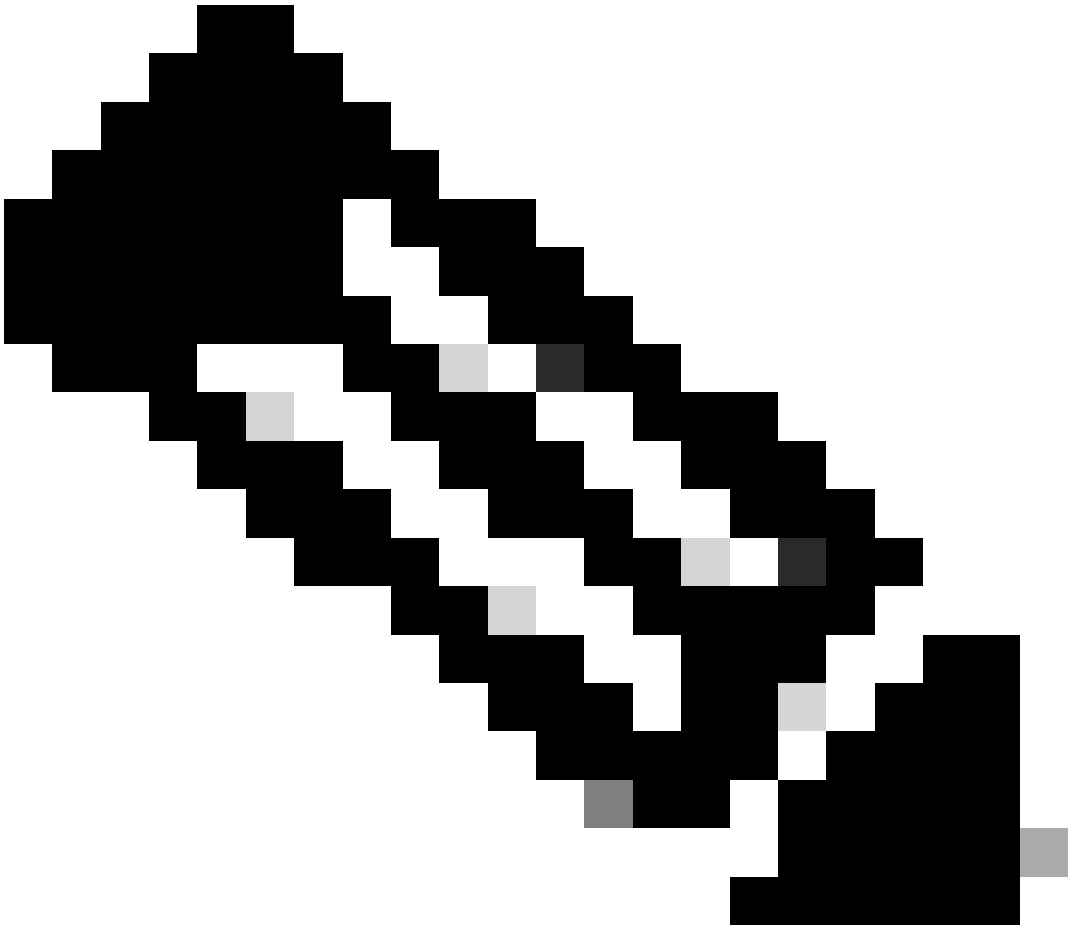
、コントローラのクロックは現在の日時近くに設定する必要があります）。X.509 証明書が確認されたら、WLC はランダム AES 暗号化キーを生成します。WLC は、この AES キーを暗号化エンジンに配置するので、今後 AP と交換する CAPWAP 制御メッセージの暗号化と復号を行うことができます。データパケットは、LAP とコントローラの間の CAPWAP トンネルではクリアテキストで送信されることに注意してください。

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。また、LWAPP変換プログラムによって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** コマンドを使用すると、joinプロセスでのAPハッシュキーも表示されます。AP に製造元でインストールされる証明書（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 AP には必ず MIC が付いています。

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：出力された行の一部は、スペースの制約により 2 行目に移動しています。

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

AP からのデバッグ

コントローラのデバッグで参加要求が示されない場合、AP にコンソールポートがあれば AP からプロセスをデバッグできます。次の各コマンドで AP の起動プロセスを確認できますが、最初にイネーブルモードに入る必要があります (デフォルトのパスワードは「Cisco」) 。

- **debug dhcp detail** :DHCP オプション 43 の情報を表示します。
- **debug ip udp**:APが送受信したすべてのUDPパケットを表示します。
- debug capwap client event :AP の capwap イベントを表示します。

- **debug capwap client error**:AP の capwap エラーを表示します。

- **debug dtls client event**:AP の DTLS イベントを表示します。

- **debug dtls error enable**:AP の DTLS エラーを表示します。

-

undebug all:AP でのデバッグを無効にします。

debug capwap

コマンドの出力例を次に示します。この部分的な出力から、AP がコントローラを検出し参加するために起動プロセス中に送信するパケットの内容がわかります。

<#root>

AP can discover the WLC via one of these options :

!--- AP discovers the WLC via option 43

*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set

!--- capwap Discovery Request using the statically configured controller information.

*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set

!--- Capwap Discovery Request sent using subnet broadcast.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

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認します (AP の MAC アドレスに対する DHCP サーバーリースを確認します) 。
- コントローラから AP に ping を実行します。
- VLAN へのパケットがブロックされないように、スイッチの STP 設定が正しいかどうかを確認します。
- 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。

Field Notice：証明書の期限切れ - FN63942

ハードウェアに組み込まれた証明書は、製造後 10 年間有効です。AP または WLC が 10 年以上前のものである場合、期限切れの証明書が原因で AP の接続に問題が生じるおそれがあります。この問題の詳細については、このField Notice(Field Notice:FN63942)を参照してください。

調査を要する潜在的な問題：例

問題 1：コントローラの時刻が証明書の有効期間外である

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。

- APでdebug dtls client error + debug dtls client eventコマンドを発行します。

<#root>

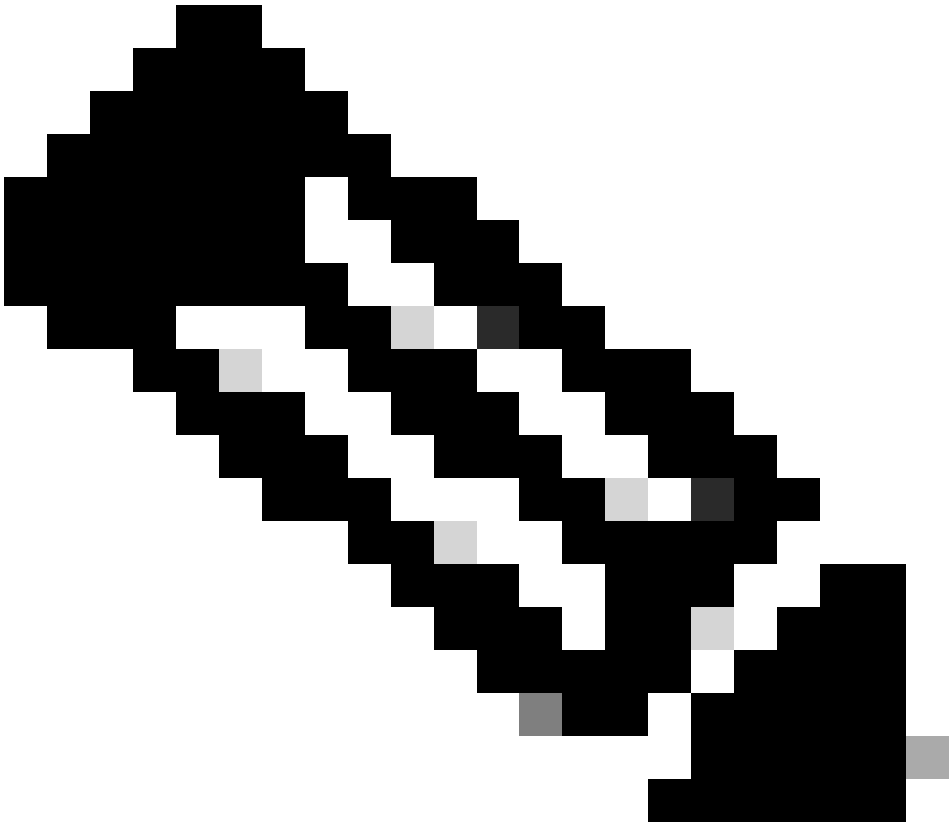
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

この情報は、コントローラの時刻が AP の証明書有効期間外であることを明確に示しています。そのため、AP はコントローラに登録できません。AP 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。コントローラの時刻は、AP の証明書の証明書有効期間内で設定する必要があります。

- 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に、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：コントローラで時刻が正しく設定されていない場合、コントローラのGUIモードでCommands > Set Timeを選択するか、コントローラのCLIでconfig timeコマンドを発行してコントローラの時刻を設定します。

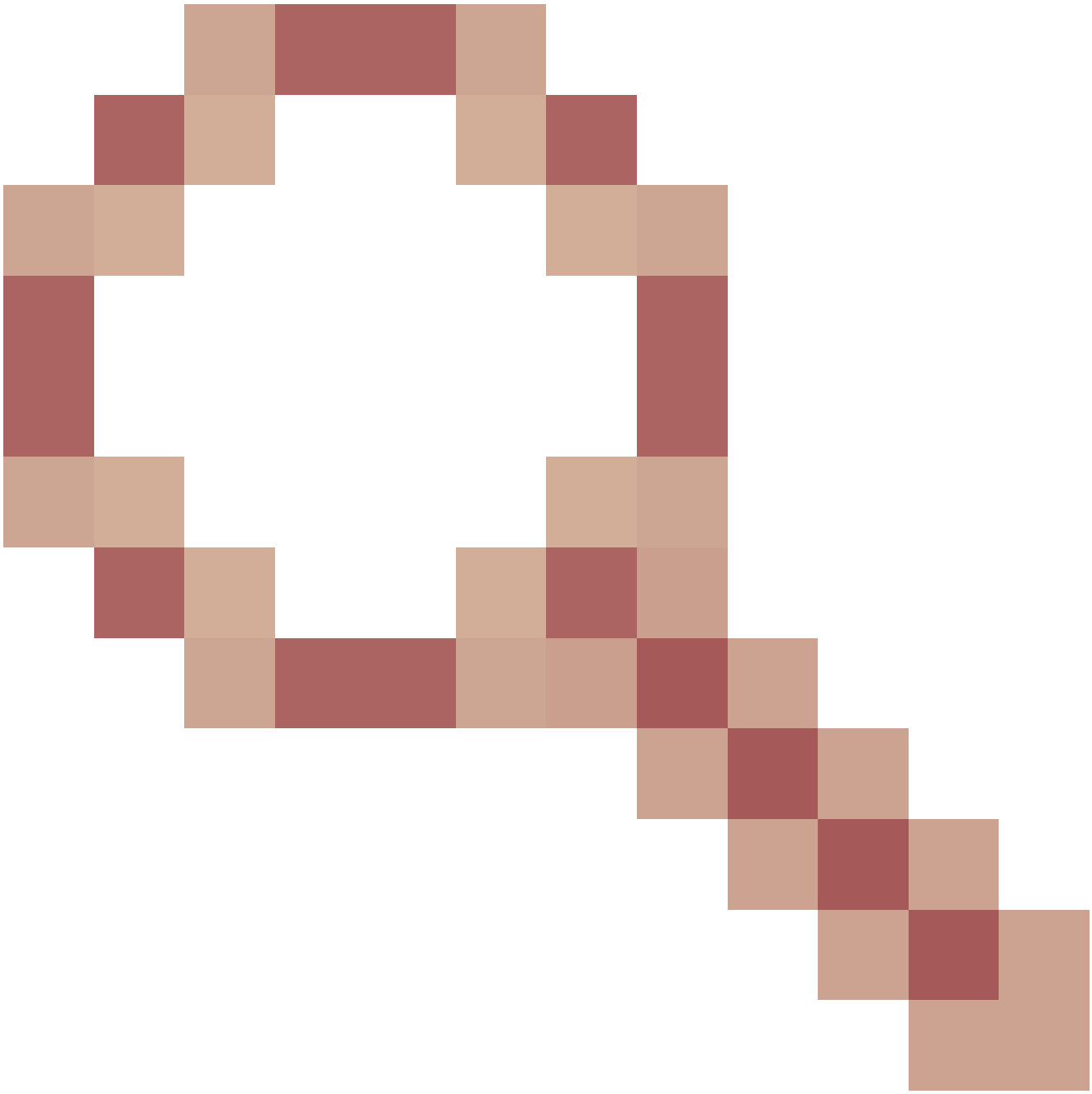
- CLIにアクセス可能なAPで、AP CLIから**show crypto ca certificates** コマンドを実行して証明書を確認します。

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。

```
AP00c1.649a.be5c#show crypto ca cert
.....................................
.....................................
.....................................
.....................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
.................................
.................................
.................................
```

このコマンドの出力には多数の有効期間が関連付けられている可能性があるため、出力全体が表示されているわけではありません。Associated Trustpoint: Cisco_IOS_MIC_cert で指定され、名前フィールドに関連する AP 名が入力されている有効期間のみを考慮します。この出力例では、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。

- Cisco Bug ID CSCuq19142



LAP/WLCのMICまたはSSCのライフタイム期限切れによるDTLS障害の詳細は、「Cisco Bug ID CSCuq19142」を参照してください。

問題 2：規制ドメインの不一致

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

<#root>

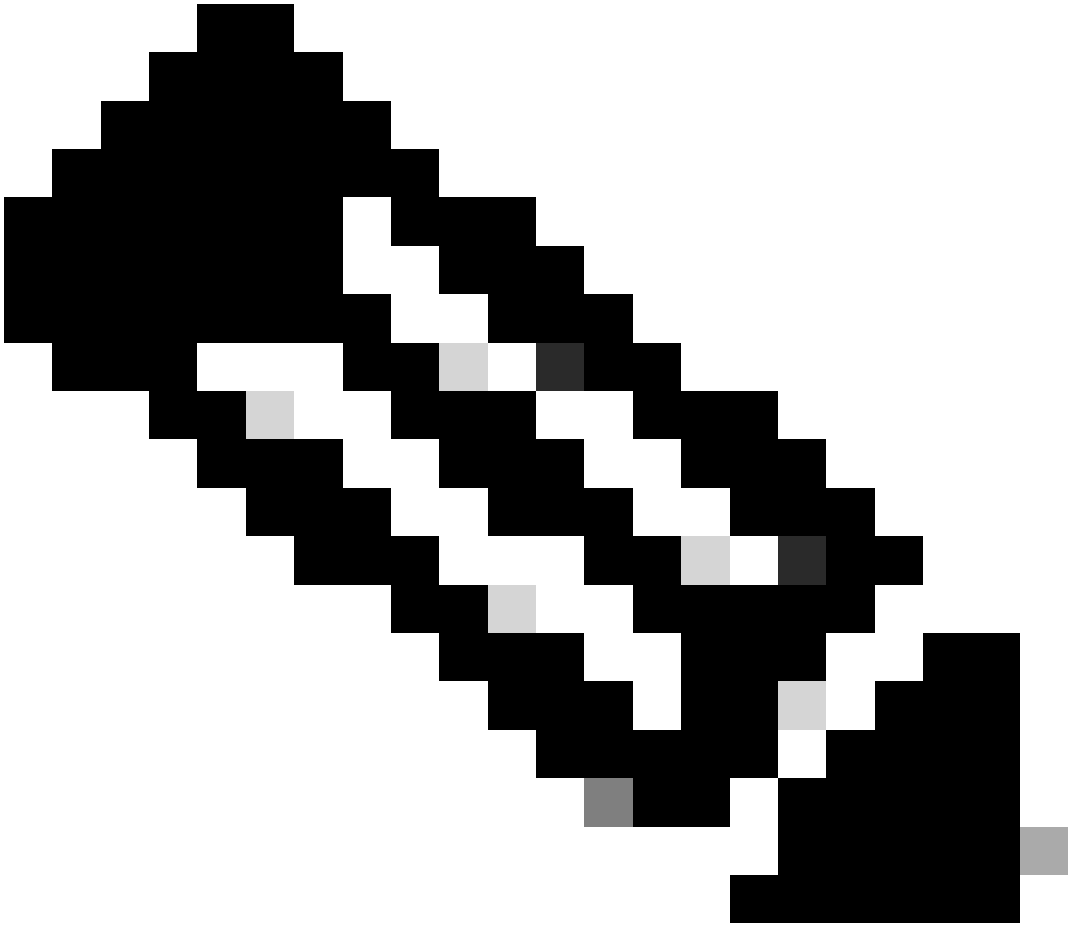
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

このメッセージは、LAP と WLC の規制ドメインに不一致があることを明確に示しています。WLC は複数の規制ドメインをサポートしていますが、AP がそのドメインから参加するには、それぞれの規制ドメインをあらかじめ選択しておく必要があります。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) 。複数の AP を購入する際は、AP の規制ドメインが共通していることを確認してください。それ以外の場合は、AP は WLC に登録できません。



注：単一の AP に対し、802.1b/g と 802.11a 両方の無線が同じ規制ドメインに属している必要があります。

問題 3：WLC で AP 認証リストが有効になっている。LAP が許可リストにない

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

```
<#root>

Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP 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
CAPWAP 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
CAPWAP 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 CAPWAP 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 CAPWAP 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を使用する場合は、debug capwap client errorコマンドを発行すると次のメッセージが表示されます。

<#root>

```
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.

これも、LAP がコントローラの AP 許可リストに含まれていないことを明確に示しています。

次のコマンドを使用して、AP 許可リストのステータスを表示できます。

<#root>

```
(Cisco Controller) >
```

show auth-list

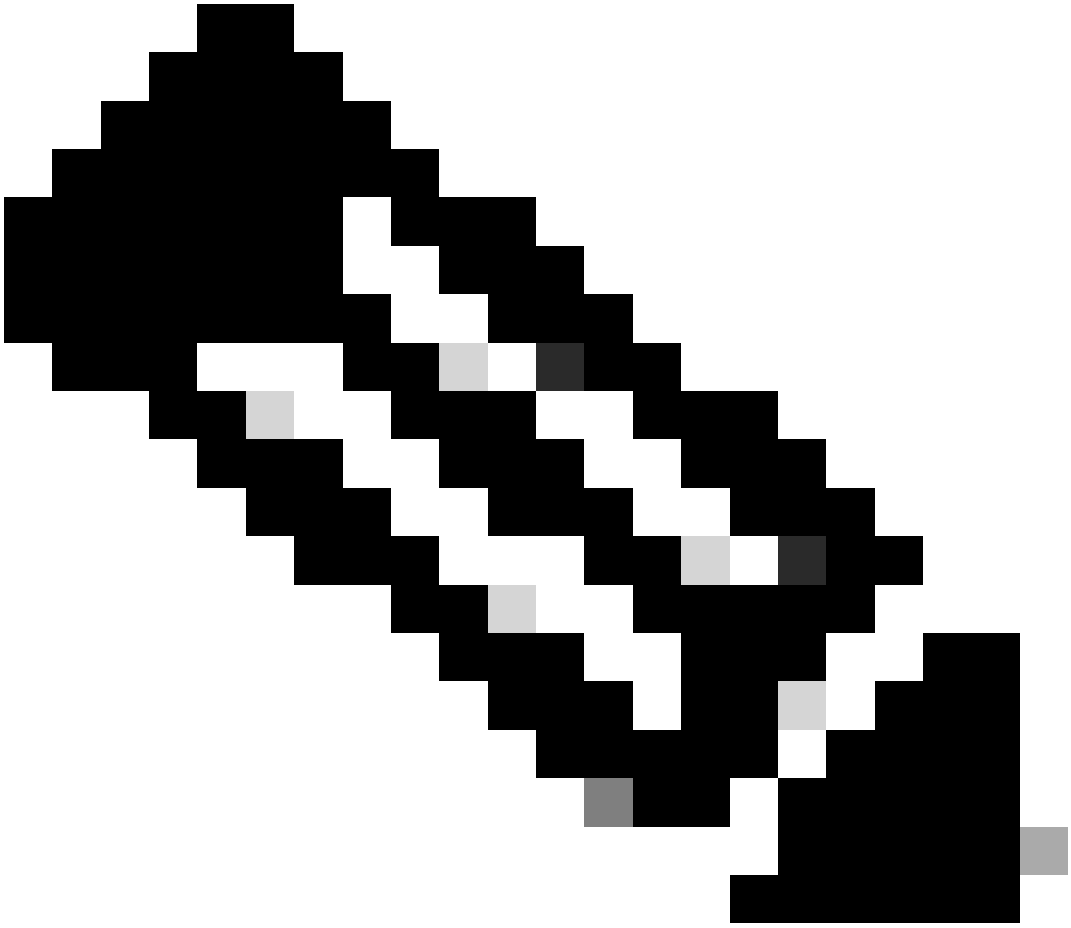
```
Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

LAPをAP認証リストに追加するには、config auth-list add mic <AP MAC Address> コマンドを使用します。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 4：AP に証明書または公開キーの破損がある

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 capwap errors enableコマンドと**debug pm pki enable** コマンドを発行します。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：出力された行の一部は、スペースの制約により 2 行目に移動しています。

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

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 AP - 返品許可（RMA）をリクエストする
- LSC AP - LSC 証明書を再プロビジョニングする.

問題 5：コントローラが誤った VLAN で AP ディスカバリメッセージを受信している（ディスカバリメッセージのデバッグは表示されるが、応答は表示されない）

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

<#root>

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

このメッセージは、コントローラが、コントローラのサブネット設定に含まれていない送信元 IP アドレスを持つブロードキャスト IP アドレスによってディスカバリ要求を受信したことを示します。これは、コントローラがパケットをドロップすることも意味します。

問題は、AP が管理 IP アドレスにディスカバリ要求を送信したのではないということです。コントローラは、コントローラに設定されていない VLAN からのブロードキャスト ディスカバリ要求を報告します。これは通常、トランクが VLAN を許可し、それらをワイヤレス VLAN に制限しなかった場合に発生します。

この問題を解決するには、次の手順を実行します。

- コントローラが別のサブネット上にある場合、AP はコントローラの IP アドレスをプライミングするか、または AP はいずれかのディスカバリ方法を使用してコントローラの IP アドレスを受信する必要があります。

- スイッチは、コントローラ上にない一部の 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 6：AP が WLC に参加できず、ファイアウォールが必要なポートをブロックしている

エンタープライズ 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、ファイアウォールでこれらのポートが有効になっていることを確認します。

次のポートをイネーブルにする必要があります。

- 次の UDP ポート（CAPWAP トラフィック）をイネーブルにします。
  - データ：5247
  - 制御：5246
- 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 ~ 16666
  - 16667 ~ 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）。

以下のポートはオプションです（要件によって異なります）。

- 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 7：ネットワーク内の IP アドレスの重複

これは、AP が WLC に参加しようとするときに見られるもう 1 つの一般的な問題です。このエラーメッセージは、AP がコントローラに参加しようとしたときに表示されます。

<#root>

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 は電源の再投入を開始し続け、コントローラに参加できません。

デバッグでは、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ています。

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 アドレスが見つかった場合は、重複する IP アドレスを持つデバイスを削除するか、ネットワーク上で一意の IP アドレスを持つようにデバイスの IP アドレスを変更します。

その後 AP は WLC に接続できます。

問題 8：メッシュイメージを持つ LAP が WLC に参加できない

Lightweight アクセス ポイントが WLC に登録されません。ログには、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。その後、AP は参加し、コントローラからイメージをダウンロードしてから、ブリッジモードで WLC に登録する必要があります。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てリブートし、ローカルモードでコントローラに登録し直します。

問題9:Microsoft DHCPのアドレスが正しくない

アクセスポイントは、WLCへの加入を試みたときにIPアドレスを迅速に更新できます。これにより、Windows DHCPサーバはこれらのを BAD_ADDRESSとしてマークし、DHCPプールがすぐに枯渇する可能性があります。 詳細については、『Ciscoワイヤレスコントローラコンフィギュレーションガイド、リリース8.2』の「クライアントローミング」の章を参照してください。

関連情報

- シスコのテクニカルサポートとダウンロード

- **Catalyst 9800でのAP加入プロセス**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。