Cisco WLC への AP 接続

CAPWAP

アクセス ポイント通信プロトコルについて

Cisco Lightweight アクセス ポイントは、IETF 標準 Control and Provisioning of Wireless Access Points Protocol（CAPWAP）を使用してネットワーク上のコントローラおよび他の Lightweight アクセス ポイントと通信します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、コントローラによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次の理由でコントローラに実装されます。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- コントローラにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

LWAPP を使用可能なアクセス ポイントは CAPWAP コントローラを検出して join することができ、CAPWAP コントローラへの変換はシームレスです。たとえば、CAPWAP 使用時のコントローラ ディスカバリ プロセスおよびファームウェア ダウンロード プロセスは、LWAPP 使用時のものと同じです。例外として、レイヤ 2 の展開は CAPWAP ではサポートされません。

CAPWAP コントローラおよびLWAPP コントローラは、同じネットワークで展開が可能です。CAPWAP を使用可能なソフトウェアでは、アクセス ポイントは CAPWAP を実行するコントローラでも LWAPP を実行するコントローラでも join できます。Cisco Aironet 1040、1140、1260、3500、および3600 シリーズアクセス ポイントは唯一の例外であり、これらはCAPWAP のみをサポートし、CAPWAP を実行するコントローラにのみ join します。たとえば、1130 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにも LWAPP を実行するコントローラにも join できますが、1140 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにのみ join できます。

次に、アクセス ポイント通信プロトコルについて従う必要がある注意事項を示します。

- LWAPPを使用するアクセスポイントからのトラフィックのみ許可するようファイアウォールが設定されている場合は、ファイアウォールのルールを変更して CAPWAP を使用するアクセス ポイントからのトラフィックを許可する必要があります。
- CAPWAP UDP ポート 5246 および 5247（LWAPP UDP ポート 12222 および 12223 と同等のポート）が有効になっており、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト（ACL）がコントローラとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。

アクセス ポイント通信プロトコルの制約事項

- 仮想コントローラ プラットフォームでは、クライアントごとのダウンストリーム レート制限は FlexConnect 中央スイッチングでサポートされません。
- レート制限は、どの方向からでも CPU 宛てのすべてのトラフィックに適用されます（無線または有線）。コントローラは常にデフォルトの **config advanced rate enable** コマンドで実行して、コントローラに対するトラフィックのレート制限を有効にし、サービス妨害（DoS）攻撃から保護することをお勧めします。Internet Control Message Protocol（ICMP）エコー応答のレート制限をテスト目的で停止するためには、**config advanced rate disable** コマンドを使用できます。ただし、テスト完了後に **config advanced rate enable** コマンドを再適用することをお勧めします。
- コントローラが適切な日時で設定されていることを確認してください。コントローラに設定されている日時がアクセスポイントの証明書の作成日とインストール日に先行すると、アクセス ポイントはコントローラに join しません。

CAPWAP の最大伝送単位情報の表示

コントローラ上の CAPWAP パスの最大伝送単位（MTU）を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1f:ca:bd:bc:7c
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.193
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU.................................. 1485
```

CAPWAP のデバッグ

次のコマンドを使用して、CAPWAP デバッグ情報を取得します。

- **debug capwap events** {**enable** | **disable**}：CAPWAP イベントのデバッグを有効または無効にします。
- **debug capwap errors** {**enable** | **disable**}：CAPWAP エラーのデバッグを有効または無効にします。
- **debug capwap detail** {**enable** | **disable**}：CAPWAP 詳細のデバッグを有効または無効にします。
- **debug capwap info** {**enable** | **disable**}：CAPWAP 情報のデバッグを有効または無効にします。
- **debug capwap packet** {**enable** | **disable**}：CAPWAP パケットのデバッグを有効または無効にします。
- **debug capwap payload** {**enable** | **disable**}：CAPWAP ペイロードのデバッグを有効または無効にします。
- **debug capwap hexdump** {**enable** | **disable**}：CAPWAP 16 進数ダンプのデバッグを有効または無効にします。
- **debug capwap dtls-keepalive** {**enable** | **disable**}：CAPWAP DTLS データ キープアライブ パケットのデバッグを有効または無効にします。

優先モード

優先モードについて

優先モードでは、アクセス ポイントが WLC に join するときに使用する CAPWAP L3 トランスポート（IPv4 と IPv6）を（プライマリ/セカンダリ/ターシャリ設定に基づいて）管理者が設定できます。

優先モードには次の 2 つのレベルがあります。

- AP グループ別
- グローバル設定

優先モードの設定のガイドライン

次の優先モードの設定を使用できます。

- AP グループ特有の有線モードは、AP グループの有線モードが設定されており、AP がそのグループに属している場合のみ、AP に適用されます。
- グローバル優先モードは、デフォルト グループ の AP、およびと優先モードが設定されていない AP グループに適用されます。
- デフォルトでは、AP グループの優先モードの値は設定されず、グローバルの優先モードの値は IPv4 に設定されます。
- 優先モードが設定されている AP がコントローラに join しようとして失敗すると、他のトランスポートの AP マネージャの選択に戻り、同じコントローラに join します。両方のトランスポートが失敗すると、AP は次のディスカバリ応答に移動します。
- このようなシナリオでは、スタティック IP の設定は、優先モードよりも優先されます。次に例を示します。
  - コントローラでは、優先モードは IPv4 アドレスで設定されます。
  - AP では、スタティック IPv6 は CLI または GUI を使用して設定されます。
  - AP は、IPv6 トランスポート モードを使用してコントローラに join します。
- コントローラ CLI は、優先モードの XML サポートを提供します。

CAPWAP 設定の望ましいモード（GUI）

手順

ステップ 1 **[Controller]** > **[General]** を選択して、[Global Configuration] ページを開きます。 [CAPWAP Preferred Mode] リスト ボックスを選択し、グローバルな CAPWAP 優先モードして、IPv4 または IPv6 のどちらかを選択します。

（注） デフォルトでは、コントローラは CAPWAP 優先モード IPv4 アドレスで設定されます。

ステップ 2 **[WLAN]** > **[Advanced]** > **[APGroup]** > **[General]** タブの順に選択し、[CAPWAP Preferred Mode] チェックボックスをオンにして、IPv4 または IPv6 CAPWAP 優先モードで AP グループを設定します。

ステップ 3 **[Wireless]** > **[ALL APs]** > **[General]** タブの順に選択して、[APs CAPWAP] 設定を確認します。[IP Config] セクションを参照して、AP の CAPWAP 優先モードの適用先がグローバルか、AP グループかを確認します。

ステップ 4 **[Monitor]** > **[Statistics]** > **[Preferred Mode]** の順に選択すると、ユーザは優先モード コマンドが AP に正常にプッシュされるかどうかを確認できます。

- [Prefer Mode of Global/AP Groups]：IPv4、IPv6、またはグローバルで設定した AP の名前。
- [Total]：優先モードで設定された AP の総数。
- [Success]：AP が優先モードで正常に設定された回数をカウントします。
- [Unsupporte]：IPv6 CAPWAP で join できない AP。
- [Already Configured]：すでに設定済みの AP を設定しようとした試行回数をカウントします。
- [Per AP Group Configured]：AP グループごとに設定された優先モード。
- [Failure]：AP が優先モード設定に失敗した回数をカウントします。

CAPWAP 優先モードの設定（CLI）

手順

ステップ 1 次のコマンドを使用して、AP グループおよびすべての AP の優先モードを設定します。グローバルな優先モードは、AP グループの優先モードがすでに設定されている AP には適用されません。設定が正常終了すると、AP は CAPWAP を再起動して、プライマリ/セカンダリ/ターシャリ設定に基づいてコントローラを選択した後、設定された優先モードで join します。

config ap preferred-mode {IPv4|IPv6}*{ <apgroup>|<all>}*

ステップ 2 （設定解除する） AP の優先モードをディセーブルにするには、このコマンドを使用します。

config ap preferred-mode disable *<apgroup>*

（注） <apgroup> に属する AP は CAPWAP を再起動し、グローバルな優先モードでコントローラに再 join します。

ステップ 3 次のコマンドを使用して、優先モード設定の統計情報を表示します。統計情報は累積されませんが、最後に実行された優先モードの設定 CLI に対して更新されます。

show ap prefer-mode stats

ステップ 4 次のコマンドを使用して、すべての AP グループ用に設定された優先モードを表示します。

show wlan apgroups

ステップ 5 次のコマンドを使用して、設定されているグローバルな優先モードを表示します。

show network summary

ステップ 6 次のコマンドを使用して、AP にプッシュされる優先モード コマンドがグローバル コンフィギュレーションからなのか、AP グループ固有の設定からなのかを表示して確認します。

show ap config general <Cisco AP>

```
(Cisco Controller) >show ap config general AP-3702E

Cisco AP Identifier.............................. 2
Cisco AP Name.................................... AP-3702E
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... bc:16:65:09:4e:fc
IPv6 Address Configuration....................... SLAAC
IPv6 Address..................................... 2001:9:2:35:be16:65ff:fe09:4efc
IPv6 Prefix Length............................... 64
Gateway IPv6 Addr................................ fe80::a2cf:5bff:fe51:c4ce
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Enabled
Ssh State........................................ Globally Enabled
Cisco AP Location................................ default location
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ amb
Primary Cisco Switch IP Address.................. 9.2.35.25
.....................................
.....................................
.....................................
.....................................
.....................................
Ethernet Port Speed.............................. Auto
AP Link Latency.................................. Disabled
Rogue Detection.................................. Enabled
AP TCP MSS Adjust................................ Disabled
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (Global Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................... Not Available
```

（注） コマンド出力の **Capwap Prefer Mode** を確認します。

UDP Lite

UDP Lite について

リリース 8.0 の CAPWAP 機能は IPv4 と IPv6 の両方をカバーします。CAPWAP の変更はコントローラと AP に及びます。IPv6 に対応していない古いイメージを実行している AP は、IPv4 アドレスとダウンロード イメージを持っていれば、IPv6 対応コントローラに接続できます。その逆も同様です。

IPv6 の実装には、AP とコントローラのパフォーマンスを低下させる User Datagram Protocol（UDP）の完全なペイロードチェックサムが必須です。パフォーマンスの影響を最小限に抑え

る目的で、コントローラと AP は、データグラムのヘッダー チェックサムのみが必須の UDP Lite をサポートしているため、パケット全体のチェックサムが回避されます。UDP Lite を有効にすると、パケット処理時間が短縮されます。

UDP Lite プロトコルは、IP プロトコル ID 136 を使用して、UDP で使用されるものと同じ CAPWAP ポートを使用します。UDP Lite を有効にする場合は、ネットワーク ファイアウォールでプロトコル 136 を許可する必要があります。UDP と UDP Lite を切り替えると、AP が接続解除されてから、再接続されます。UDP Lite はデータ トラフィックに使用され、UDP は制御トラフィックに使用されます。

UDP Lite が有効になっているコントローラは、IPv4 しかサポートしない既存の AP とともに IPv6 対応 AP とメッセージを交換できます。

（注） デュアル スタック コントローラは、IPv4 AP マネージャと IPv6 AP マネージャの両方を使用してディスカバリ要求に応答します。

AP ディスカバリ メカニズムは、AP に割り当てられた IPv4 アドレスと IPv6 アドレスの両方を使用します。AP は、送信元アドレス選択を使用して、IPv6 コントローラに到達するためのアドレスを決定します。

UDP Lite のグローバル設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[Global Configuration]** を選択して、[Global Configuration] ページを開きます。

ステップ 2 [Global UDP Lite] セクションで、[UDP Lite] チェックボックスをオンにして、UDP Lite をグローバルに有効にします。

（注） IPv6 UDP Lite は CAPWAPv4 トンネルを使用して接続された AP には適用されません。これらは CAPWAPv6 トンネルを使用してコントローラに接続している AP にのみ適用されます。

ステップ 3 [Apply] をクリックして、グローバル UDP Lite 構成を設定します。

ステップ 4 必要に応じて、ステップ 2 で説明したグローバル IPv6 UDP Lite を選択解除することによって、グローバル UDP Lite 構成をオーバーライドすることができます。

（注） UDP と UDP Lite を切り替えると、AP が接続解除されてから、再接続されます。

ステップ 5 [Save Configuration] をクリックして、変更を保存します。

AP 上での UDP Lite の設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points] > [All APs]** の順に選択して、[All APs] ページを開きます。

ステップ 2 IPv6 アドレスを含む [AP Name] を選択してクリックし、選択した AP の [Details] ページを開きます。

ステップ 3 [Advanced] タブで、[UDP Lite] チェックボックスをオンにして、選択した AP の UDP Lite を有効にします。

（注） このフィールドは CAPWAPv6 トンネル経由でコントローラに join している AP の場合にのみ表示されます。Web UI ページでは、CAPWAPv4 トンネル経由でコントローラに join している AP のこのフィールドが表示されません。

ステップ 4 [Apply] をクリックして、変更を確定します。

ステップ 5 [Save Configuration] をクリックして、変更を保存します。

UDP Lite の設定（CLI）

手順

ステップ 1 UDP Lite をグローバルに有効にするには、次のコマンドを使用します。
config ipv6 capwap udplite enable *all*

ステップ 2 選択した AP 上で UDP Lite を有効にするには、次のコマンドを使用します。
config ipv6 capwap udplite enable <*Cisco AP*>

ステップ 3 UDP Lite をグローバルに無効にするには、次のコマンドを使用します。
config ipv6 capwap udplite disable *all*

ステップ 4 選択した AP 上で UDP Lite を無効にするには、次のコマンドを使用します。
config ipv6 capwap udplite disable <*Cisco AP*>

ステップ 5 コントローラ上の UDP Lite のステータスを表示するには、次のコマンドを使用します。
show ipv6 summary

```
(Cisco Controller) >show ipv6 summary

Global Config.............................. Disabled
Reachable-lifetime value..................... 300
Stale-lifetime value......................... 86400
Down-lifetime value.......................... 30
RA Throttling.............................. Disabled
RA Throttling allow at-least................. 1
RA Throttling allow at-most.................. 1
RA Throttling max-through.................... 10
RA Throttling throttle-period................ 600
RA Throttling interval-option............... passthrough
```

```
NS Mulitcast CacheMiss Forwarding.......... Disabled
NA Mulitcast Forwarding..................... Enabled
IPv6 Capwap UDP Lite....................... Enabled
Operating System IPv6 state ............... Disabled

(Cisco Controller) >
```

データ DTLS

データ暗号化の設定

Cisco WLC を使用すると、Datagram Transport Layer Security（DTLS）を使用して AP と Cisco WLC 間で送信される CAPWAP コントロール パケット（および、オプションで CAPWAP データ パケット）を暗号化できます。DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。CAPWAP コントロール パケットとはコントローラとアクセス ポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロール プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

表 *1 : CAPWAP* サポート情報の *DTLSv1.2*

リリース	サポート情報
8.2	サポート対象外
8.3.11x.0 または以降のリリース	Cisco WLC および Cisco Wave 2 AP でサポート
すべてのリリース	Cisco Wave 1 AP ではサポートされていません

Web 認証と WebAdmin 向けに、以下のプロトコルを、設定に基づいてサポートしています。

- TLSv1.2
- TLSv1.0
- SSLv3
- SSLv2

（注） Cisco WLC は、ゲートウェイのスタディック設定のみをサポートします。そのため、ゲートウェイの IP アドレスを変更する ICMP リダイレクトは考慮されません。

データ暗号化の制約事項

- Cisco 1130 および 1240 シリーズのアクセス ポイントはソフトウェアベースの暗号化で DTLS データ暗号化をサポートしています。
- 1040、1140、1250、1260、1550、1600、1540、1560、1570、1700、1815、2600、2700、2800、3500、3600、3700、3800 のアクセス ポイントはハードウェア ベースの暗号化で DTLS データ暗号化をサポートします。
- Cisco Aironet 1552 および 1522 屋外アクセス ポイントはデータ DTLS をサポートしています。
- DTLS データ暗号化は、Cisco Aironet 700、800、1530、1810、1830、および 1850 シリーズ アクセス ポイントではサポートされていません。
- DTLS データ暗号化は OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。ほとんどのアクセス ポイントは会社のビルディング内の安全なネットワークにおいて展開されるため、データの暗号化は必要ありません。反対に、OfficeExtend アクセス ポイントとコントローラの間のトラフィックは安全でないパブリック ネットワークを経由するため、これらのアクセス ポイントではデータの暗号化はより重要です。データの暗号化が有効な場合、トラフィックはアクセス ポイントで暗号化されてからコントローラに送信され、また、コントローラで暗号化されてからクライアントに送信されます。
- 暗号化はコントローラおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- シスコのユニファイド ローカル ワイヤレス ネットワーク環境では、Cisco 1130 および 1240 アクセス ポイントで DTLS を有効にしないでください。有効にすると、重大なスループットの低下が発生し、AP が使用できなくなるおそれがあります。

  OfficeExtend アクセス ポイントの詳細は、『OfficeExtend Access Points』を参照してください。
- コントローラを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- データ DTLS のアベイラビリティは次のとおりです。
  - Cisco 5508 WLC は、2 つのライセンス オプションで使用可能です。ライセンス要件なしでデータ DTLS を使用可能なイメージと、データ DTLS を使用するためにライセンスを必要とする別のイメージ。「Cisco 5508 WLC 用 DTLS イメージのアップグレードまたはダウングレード」の項を参照してください。DTLS のイメージとライセンス付き DTLS のイメージは、次のとおりです。

    ライセンス付きの DTLS：AS_5500_LDPE_x_x_x_x.aes

    ライセンスなしの DTLS—AS_5500_x_x_x_x.aes
  - Cisco 2504 WLC、Cisco WiSM2、Cisco Virtual Wireless Controller：デフォルトでは、DTLS は含まれていません。データ DTLS をオンにするには、ライセンスをインストー

ルする必要があります。これらのプラットフォームには、データ DTLS を無効にした 1 つのイメージがあります。データ DTLS を使用するには、ライセンスが必要です。

データ DTLS が含まれていない Cisco 仮想ワイヤレス コントローラの場合、コントローラの平均スループットは約 200 Mbps です。データ DTLS を使用するすべての AP を使用すると、コントローラの平均スループットは約 100 Mbps になります。

- コントローラにデータ DTLS のライセンスがなく、コントローラに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- Cisco 5508 シリーズ コントローラを使用しているロシア以外のお客様はデータ DTLS ライセンスを必要としません。ただし、Cisco 2504 WLC、 Cisco 8510 WLC、Cisco WiSM2、および Cisco Virtual Wireless Controller を使用しているすべてのお客様は、データ DTLS 機能をオンにするためにはデータ DTLS ライセンスが必要です。

Cisco 5508 WLC 用 DTLS イメージのアップグレードまたはダウングレード

手順

ステップ 1 アップグレード操作は、最初の試みで失敗し、警告はライセンス付きの DTLS イメージへのアップグレードを行うと元に戻せないことを示します。

（注） ステップ 1 の後にコントローラをリブートしないでください。

ステップ 2 次のアップデートでは、ライセンスが適用され、イメージが正常に更新します。

DTLS イメージへまたは DTLS イメージからのアップグレード時のガイドライン

- ライセンス付きのデータ DTLS イメージがインストールされると、通常のイメージ（ライセンスなしのデータ DTLS）をインストールできません。
- ライセンス付き DTLS イメージから別のライセンス付き DTLS イメージにアップグレードできます。
- 通常のイメージ（DTLS）からライセンス付きの DTLS イメージへのアップグレードは、2 ステップ プロセスで行います。
- **show sysinfo** コマンドを使用して、イメージのアップグレードの前後に LDPE イメージを確認できます。

データ暗号化の設定（GUI）

Cisco WLC に基本ライセンスがインストールされていることを確認します。ライセンスがインストールされると、アクセス ポイントのデータ暗号化を有効化できます。

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[All APs]** の順に選択して、[All APs] ページを開きます。

ステップ 2 データ暗号化を有効にする AP の名前をクリックします。

ステップ 3 [Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます。

ステップ 4 このアクセス ポイントでデータ暗号化を有効にする場合は [Data Encryption] チェックボックスをオンにします。この機能を無効にする場合はオフにします。デフォルト値はオフです。

（注） データ暗号化モードに変更するには、アクセス ポイントをコントローラに再 join する必要があります。

ステップ 5 設定を保存します。

データ暗号化の設定（CLI）

（注） DTLS ライセンスがないイメージでは、**config** または **show** コマンドは使用できません。

コントローラの CLI を使用してコントローラ上のアクセス ポイントの DTLS データ暗号化を有効にする手順は、次のとおりです。

手順

ステップ 1 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ暗号化を有効または無効にします。

config ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

デフォルト値は [disabled] です。

（注） データ暗号化モードに変更するには、アクセス ポイントをコントローラに再 join する必要があります。

ステップ 2 アクセスポイントおよび接続しているクライアントの切断を確認するよう求めるプロンプトが表示されたら、**Y** と入力します。

ステップ 3 **save config** コマンドを入力して、設定を保存します。

ステップ 4 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示します。

show ap link-encryption {**all** | *Cisco_AP*}

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセス ポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。

ステップ 5 すべてのアクティブな DTLS 接続の概要を表示するには、次のコマンドを入力します。

show dtls connections

（注） DTLS データ暗号化で問題が発生した場合は、**debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} コマンドを入力して、すべての DTLS メッセージ、イベント、トレース、またはパケットをデバッグします。

ステップ 6 次のコマンドを入力して、AP とコントローラの間の DTLS 接続用の新しい暗号スイートを有効にします。

config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

ステップ 7 次のコマンドを入力して、DTLS 暗号スイートの概要を表示します。

show ap dtls-cipher-suite

アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定

アクセス ポイントからの CAPWAP フレームの VLAN タギングについて

AP コンソールのまたはコントローラから直接イーサネット インターフェイスで VLAN タギングを設定できます。設定はフラッシュ メモリに保存され、ローカルにスイッチングされるすべてのトラフィックとともに、すべての CAPWAP フレームは設定されるように VLAN タグを使用し、VLAN にはマッピングされていません。

AP からの CAPWAP フレームの VLAN タギングの制約事項

- この機能は、ブリッジ モードのメッシュ アクセス ポイントではサポートされません。
- CAPWAP VLAN タギングは、 802.11 ac Wave 2 AP：18xx、2800、3800、および 1560 に対する 8.5 以降のリリースでサポートされています。

アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[All APs]** の順に選択して、[All APs] ページを開きます。

ステップ 2 AP の [Details] ページを開くには、AP 名のリストから AP 名をクリックします。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 VLAN タギングの領域で、[VLAN Tagging] チェックボックスを選択します。

ステップ 5 [Trunk VLAN ID] テキスト ボックスに、ID を入力します。

約 10 分後に、アクセス ポイントが指定したトランク VLAN を経由してトラフィックをルーティングできない場合、リブートおよびタグなしモードで CAPWAP フレームの送信により、

アクセスポイントは回復手順を実行し、コントローラに再アソシエートします。コントローラは Cisco Prime Infrastructure などトラップ サーバにトランク VLAN の失敗を示すトラップを送信します。

アクセス ポイントが指定トランク VLAN を経由してトラフィックをルーティングできない場合、パケットのタグ付けが解除され、コントローラに再アソシエートされます。コントローラは Cisco Prime Infrastructure などトラップ サーバにトランク VLAN の失敗を示すトラップを送信します。

トランク VLAN ID が 0 の場合、アクセス ポイントは CAPWAP フレームのタグ付けを解除します。

AP が CAPWAP フレームにタグ付けするかタグ付けを解除するかを示す VLAN タグのステータスが表示されます。

ステップ 6 [Apply] をクリックします。

ステップ 7 設定するとアクセス ポイントがリブートされることを通知する警告メッセージが表示されます。[OK] をクリックして作業を続行します。

ステップ 8 [Save Configuration] をクリックします。

次のタスク

設定後にタグ付きイーサネット フレームをサポートするには、AP のイーサネット インターフェイスに接続されているスイッチまたは他の機器も設定する必要があります。

アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、アクセス ポイントからの CAPWAP フレームの VLAN タギングを設定します。

config ap ethernet tag {**disable** | **id** *vlan-id*} {*ap-name* | **all**}

ステップ 2 次のコマンドを入力して、AP またはすべての AP についての VLAN タギング情報を表示できます。

show ap ethernet tag {**summary** | *ap-name*}

Cisco WLC の検出と join

コントローラ ディスカバリ プロセス

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してコントローラを検知してから、コントローラに CAPWAP join request を送信します。これに対し、コントローラはアクセス ポイントに CAPWAP join response を返し、アクセス ポイントはコントローラに join できるようになります。アクセス ポイントがコントローラに join すると、コントローラによってアクセス ポイントの構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

次に、コントローラ ディスカバリ プロセスの注意事項を示します。

- LWAPP から CAPWAP へのアップグレード パスおよび CAPWAP から LWAPP へのダウングレード パスがサポートされます。LWAPP イメージを持つアクセス ポイントは、LWAPP でディスカバリ プロセスを開始します。LWAPP コントローラを検出すると、LWAPP ディスカバリ プロセスを開始してコントローラに join します。LWAPP コントローラが見つからない場合は、CAPWAP でディスカバリを開始します。1 つのディスカバリ タイプ（CAPWAP または LWAPP）でディスカバリ プロセスを開始した回数が最大ディスカバリ カウントを超えてもアクセス ポイントが discovery response を受信しない場合は、ディスカバリ タイプはもう一方のタイプに変更されます。たとえば、アクセス ポイントが LWAPP でコントローラを検出できない場合、CAPWAP でディスカバリ プロセスを開始します。
- アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してコントローラに再 join します。
- コントローラが CAPWAP ディスカバリ応答で送信する IP アドレスを設定するには、**config network ap-discovery nat-ip-only** {**enable** | **disable**} コマンドを使用します。
- アクセス ポイントをネットワークでアクティブにするには、コントローラがそのアクセス ポイントを検出する必要があります。Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。
  - Layer 3 CAPWAP または LWAPP ディスカバリ：この機能は、アクセス ポイントとは異なるサブネット上で有効化でき、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IPv4 アドレスと IPv6 アドレスのどちらかと UDP パケットが使用されます。
  - CAPWAP マルチキャスト ディスカバリ：ブロードキャストが IPv6 アドレス内に存在しません。アクセス ポイントは、すべてのコントローラのマルチキャスト アドレス（FF01::18C）に CAPWAP ディスカバリ メッセージを送信します。コントローラは、同じ L2 セグメント上に存在する AP のみから IPv6 ディスカバリ要求を受け取り、IPv6 ディスカバリ応答を返します。
  - ローカルに保存されているコントローラの IPv4 または IPv6 アドレス ディスカバリ：アクセス ポイントがすでにコントローラにアソシエートされている場合は、プライマ

リ、セカンダリ、およびターシャリ コントローラの IPv4 または IPv6 アドレスがアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセス ポイントにコントローラの IPv4 または IPv6 アドレスを保存するこのプロセスは、「アクセス ポイントのプライミング」と呼ばれます。

- オプション 43 を使用した DHCP サーバ ディスカバリ：この機能では、DHCP オプション 43 を使用して、コントローラの IPv4 アドレスをアクセス ポイントに提供します。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。
- オプション 52 を使用した DHCP サーバ ディスカバリ：この機能は、DHCP オプション 52 を使用して、AP が接続先のコントローラの IPv6 アドレスを検出できるようにします。DHCPv6 メッセージの一部として、DHCP サーバは IPv6 アドレスをコントローラ管理に提供します。
- DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してコントローラを検出できます。CISCO-LWAPP-CONTROLLER.*localdomain* または CISCO-CAPWAP-CONTROLLER.*localdomain* への応答としてコントローラの IPv4 アドレスと IPv6 アドレスを返すように DNS を設定する必要があります。ここで、*localdomain* はアクセス ポイント ドメイン名です。

  アクセス ポイントは、DHCPv4/DHCPv6 サーバから IPv4/IPv6 アドレスと DNSv4/DNSv6 の情報を受信すると、DNS に接続して CISCO-LWAPP-CONTROLLER.*localdomain* または CISCO-CAPWAP-CONTROLLER.*localdomain* を解決します。DNS がコントローラの IP アドレス（IPv4 アドレスと IPv6 アドレスのどちらかまたはその両方）のリストを送信すると、アクセス ポイントがコントローラにディスカバリ要求を送信します。

コントローラ ディスカバリ プロセスのガイドラインと制約事項

- ディスカバリ プロセスでは、1040、1140、1260、3500、および 3600 シリーズ アクセス ポイントはシスコの CAPWAP コントローラのみをクエリーします。LWAPP コントローラに関するクエリーは送信されません。これらのアクセス ポイントで LWAPP と CAPWAP コントローラの両方に対するクエリーを送信する場合は、DNS を更新する必要があります。
- コントローラが現在の時刻に設定されていることを確認してください。コントローラをすでに経過した時刻に設定すると、その時刻には証明書が無効である可能性があり、アクセス ポイントがコントローラに join できない場合があります。
- ダウンタイムを回避するため、グローバル HA を設定しながら AP で CAPWAP を再起動すると、AP が戻り、バックアップ プライマリ コントローラに参加します。これにより、バックグラウンドでプライマリ コントローラによる検出が開始されます。プライマリによる検出に成功すると、AP が戻り、プライマリに再度参加します。

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセス ポイントの DHCP ベンダー クラス ID（VCI）文字列に基づいてオプションを返すようにプログラムする必要があります（DHCP オプション 60）。

TLV ブロックの形式は、次のとおりです。

- 型：0xf1（十進数では 241）
- 長さ：コントローラの IP アドレス数 * 4
- 値：コントローラの管理インターフェイスの IP アドレス リスト

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセス ポイントの VCI ストリングは上記の VCI ストリングと異なります。VCI ストリングには、「ServiceProvider」が含まれます。たとえば、このオプション付きの 3600 は、VCI ストリング「Cisco AP c3600-ServiceProvider」を返します。

（注） DHCP サーバから取得するコントローラの IP アドレスは、ユニキャスト IP アドレスになります。DHCP オプション 43 を設定する場合は、マルチキャスト アドレスとしてコントローラの IP アドレスを設定しないでください。

アクセス ポイントのコントローラへの join の確認

コントローラを交換する場合、アクセス ポイントが新しいコントローラに join していることを確認する必要があります。

アクセス ポイントのコントローラへの join の確認（GUI）

手順

ステップ 1 次の手順で、新しいコントローラをマスター コントローラとして設定します。

a) [Controller] > [Advanced] > [Master Controller Mode] の順に選択し、[Master Controller Configuration] ページを開きます。
b) [Master Controller Mode] チェックボックスをオンにします。
c) [Apply] をクリックして、変更を確定します。
d) [Save Configuration] をクリックして、変更を保存します。

ステップ 2 （任意）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。

ステップ 3 アクセス ポイントを再起動します。

ステップ 4 すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定するには、[Master Controller Configuration] ページで [Master Controller Mode] チェックボックスをオフにします。

アクセス ポイントのコントローラへの join の確認（CLI）

手順

ステップ 1 次のコマンドを入力して、新しいコントローラをマスター コントローラとして設定します。

config network master-base enable

ステップ 2 （任意）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。

ステップ 3 アクセス ポイントを再起動します。

ステップ 4 次のコマンドを入力して、すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定します。

config network master-base disable

Cisco WLC のバックアップ

バックアップ コントローラの設定について

中央のロケーションにある単一のコントローラは、アクセス ポイントでローカルのプライマリ コントローラとの接続を失った場合にバックアップとして機能できます。中央および地方のコントローラは、同じモビリティ グループに存在する必要はありません。ネットワーク上の特定のアクセス ポイントに対してプライマリ、セカンダリ、およびターシャリ コントローラを指定できます。コントローラ GUI または CLI を使用して、バックアップ コントローラの IP アドレスを指定できます。これにより、アクセス ポイントはモビリティ グループ外のコントローラをフェールオーバーできます。

次に、バックアップ コントローラの設定に関する注意事項を示します。

- コントローラに接続されているすべてのアクセス ポイントに対してプライマリとセカンダリのバックアップ コントローラ（プライマリ、セカンダリ、ターシャリのコントローラが指定されていないか応答がない場合に使用される）や、ハートビート タイマーおよびディスカバリ要求タイマーなどの各種タイマーを設定できます。コントローラの障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビー

ト間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。

- アクセス ポイントはバックアップ コントローラのリストを維持し、リスト上の各エントリに対して定期的に Primary discovery request を送信します。アクセス ポイントがコントローラから新しい discovery response を受信すると、バックアップ コントローラのリストが更新されます。Primary discovery request に 2 回連続で応答できなかったコントローラはすべて、リストから削除されます。アクセス ポイントのローカル コントローラに障害が発生した場合、プライマリ、セカンダリ、ターシャリ、プライマリ バックアップ、セカンダリ バックアップの順に、バックアップ コントローラ リストから使用可能なコントローラが選択されます。アクセス ポイントはバックアップ リストで使用可能な最初のコントローラからの discovery response を待機し、プライマリ ディスカバリ要求タイマーで設定された時間内に応答を受信した場合は、このコントローラに join します。制限時間に達すると、アクセス ポイントはコントローラを join できないものと見なし、リストで次に使用可能なコントローラからの discovery response を待ちます。
- アクセス ポイントのプライマリ コントローラが再度オンラインになると、アクセス ポイントはバックアップ コントローラからアソシエート解除してプライマリ コントローラに再接続します。アクセス ポイントはプライマリ コントローラにのみフォールバックします。設定されている使用可能なセカンダリ コントローラにはフォールバックしません。たとえば、アクセス ポイントがプライマリ、セカンダリ、およびターシャリ コントローラで設定されている場合、プライマリおよびセカンダリ コントローラが応答しなくなるとターシャリ コントローラにフェールオーバーします。プライマリ コントローラがダウンしている間、セカンダリ コントローラがオンラインに戻ると、アクセス ポイントはセカンダリ コントローラにフォール バックせず、ターシャリ コントローラへの接続が維持されます。アクセス ポイントは、プライマリ コントローラがオンラインに戻り、ターシャリ コントローラからプライマリ コントローラにフォールバックするまで待機します。ターシャリ コントローラに障害が発生し、プライマリ コントローラがまだダウンしている場合、アクセス ポイントは使用可能なセカンダリ コントローラにフォール バックします。

バックアップ コントローラの設定に関する制約事項

- 高速ハートビート タイマーは、ローカル モードまたは FlexConnect モードのアクセス ポイントにのみ設定できます。

バックアップ コントローラの設定（GUI）

手順

ステップ 1 [Wireless] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。

ステップ 2 [Local Mode AP Fast Heartbeat Timer State] ドロップダウン リストから [Enable] を選択してローカル モードのアクセス ポイントの高速ハートビート タイマーを有効にするか、または [Disable] を選択してタイマーを無効にします。デフォルト値は [Disable] です。

ステップ 3 ステップ 2 で [Enable] を選択した場合は、[Local Mode AP Fast Heartbeat Timeout] テキスト ボックスに入力して、ローカル モードのアクセス ポイントに高速ハートビート タイマーを設定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。

Cisco Flex 7510/8510/8540 コントローラに対する AP 高速ハートビート タイムアウト値の範囲は、10 ～ 15（両端の値を含む）であり、他のコントローラの場合は 1 ～ 10（両端の値を含む）になります。Cisco Flex 7510/8510/8540 コントローラに対するハートビート タイムアウトのデフォルト値は 10 です。他のコントローラに対するデフォルト値は 1 秒です。

ステップ 4 [FlexConnect Mode AP Fast Heartbeat Timer State] ドロップダウン リストから [Enable] を選択して FlexConnect アクセス ポイントの高速ハートビート タイマーを有効にするか、または [Disable] を選択してこのタイマーを無効にします。デフォルト値は [Disable] です。

ステップ 5 FlexConnect 高速ハートビートを有効にする場合は、[FlexConnect Mode AP Fast Heartbeat Timeout] テキスト ボックスに FlexConnect モード AP 高速ハートビート タイムアウト値を入力します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。

Cisco Flex 7510/8510/8540 コントローラに対する FlexConnect モード AP 高速ハートビート タイムアウト値の範囲は 10 ～ 15（両端の値を含む）であり、他のコントローラの場合は 1 ～ 10 になります。Cisco Flex 7510/8510/8540 コントローラに対するハートビート タイムアウトのデフォルト値は 10 です。他のコントローラに対するデフォルト値は 1 秒です。

ステップ 6 [AP Primary Discovery Timeout] テキスト ボックスに 30 ～ 3600 秒（両端の値を含む）の値を入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。デフォルト値は 120 秒です。

ステップ 7 すべてのアクセス ポイントにプライマリ バックアップ コントローラを指定する場合は、プライマリ バックアップ コントローラの IPv4/IPv6 アドレスを [Back-up Primary Controller IP Address] テキスト ボックスに、コントローラの名前を [Back-up Primary Controller Name] テキスト ボックスに入力します。

（注） IP アドレスのデフォルト値は 0.0.0.0 であり、プライマリ バックアップ コントローラをは無効です。

ステップ 8 すべてのアクセス ポイントにセカンダリ バックアップ コントローラを指定する場合は、セカンダリ バックアップ コントローラの IPv4/IPv6 アドレスを [Back-up Secondary Controller IP Address] テキスト ボックスに、コントローラの名前を [Back-up Secondary Controller Name] テキスト ボックスに入力します。

（注） IP アドレスのデフォルト値は 0.0.0.0 であり、セカンダリ バックアップ コントローラを無効にします。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 次の手順で、特定のアクセス ポイントにプライマリ、セカンダリ、およびターシャリ バックアップ コントローラを設定します。

a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
b) プライマリ、セカンダリ、およびターシャリ バックアップ コントローラを設定するアクセス ポイントの名前をクリックします。
c) [High Availability] タブを選択して、[All APs > Details for]（High Availability）ページを開きます。
d) 必要に応じて、このアクセス ポイントのプライマリ コントローラの名前と IP アドレスを [Primary Controller] テキスト ボックスに入力します。

（注） この手順および次の 2 つの手順におけるバックアップ コントローラの IP アドレスの入力はオプションです。バックアップ コントローラが、アクセス ポイントが接続されている（プライマリ コントローラ）モビリティ グループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。コントローラ名および IP アドレスは、同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうでない場合、アクセス ポイントはバックアップ コントローラに join できません。

e) 必要に応じて、このアクセス ポイントのセカンダリ コントローラの名前と IP アドレスを [Secondary Controller] テキスト ボックスに入力します。
f) 必要に応じて、このアクセス ポイントのターシャリ コントローラの名前と IP アドレスを [Tertiary Controller] テキスト ボックスに入力します。
g) [Apply] をクリックして、変更を確定します。

ステップ 11 [Save Configuration] をクリックして、変更を保存します。

バックアップ コントローラの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、特定のアクセス ポイントのプライマリ コントローラを設定します。

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

（注） このコマンドの *controller_ip_address* パラメータおよびそれに続く 2 つのコマンドはオプションです。バックアップ コントローラが、アクセス ポイントが接続されている（プライマリ コントローラ）モビリティ グループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。各コマンドで、*controller_name* および *controller_ip_address* は同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうでない場合、アクセス ポイントはバックアップ コントローラに join できません。

ステップ 2 次のコマンドを入力して、特定のアクセス ポイントのセカンダリ コントローラを設定します。

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 3 次のコマンドを入力して、特定のアクセス ポイントのターシャリ コントローラを設定します。

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 4 次のコマンドを入力して、すべてのアクセス ポイントのプライマリ バックアップ コントローラを設定します。

config advanced backup-controller primary *system name ip_addr*

（注） このコマンドは、IPv4 と IPv6 の両方で有効です。

ステップ 5 次のコマンドを入力して、すべてのアクセス ポイントのセカンダリ バックアップ コントローラを設定します。

config advanced backup-controller secondary *system name ip_addr*

（注） プライマリまたはセカンダリ バックアップ コントローラ エントリを削除するには、コントローラの IPv4/IPv6 アドレスとして *0.0.0.0* を入力します。

（注） このコマンドは、IPv4 と IPv6 の両方で有効です。

ステップ 6 次のコマンドを入力して、ローカルまたは FlexConnect アクセス ポイントに対する高速ハートビート タイマーを有効または無効にします。

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable** | **disable**} *interval*

ここで、**all** はローカルと FlexConnect の両方のアクセス ポイントです。*interval* の値は、Cisco Flex 7510、8510、3504、5520、および 8540 コントローラの場合は 10 ～ 15 秒、Cisco 2504、5508、WiSM2、および vWLC コントローラの場合は 1 ～ 10 秒です。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。次のコマンドを入力して、デフォルト値では無効になっています。アクセス ポイントのハートビート タイマーを設定します。

config advanced timers ap-heartbeat-timeout *interval*

interval の値は、1 ～ 30 秒です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。デフォルト値は 30 秒です。

注意 高遅延リンクと一緒に高速ハートビート タイマーを有効にしないでください。高速ハートビート タイマーを有効にする必要がある場合、タイマー値を遅延よりも大きくする必要があります。

ステップ 7 次のコマンドを入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。

config advanced timers ap-primary-discovery-timeout *interval*

interval の値は、30 ～ 3600 秒です。デフォルト値は 120 秒です。

ステップ 8 次のコマンドを入力して、アクセス ポイントのディスカバリ タイマーを設定します。

config advanced timers ap-discovery-timeout *interval*

interval の値は、1 ～ 10 秒です。デフォルト値は 10 秒です。

ステップ 9 次のコマンドを入力して、802.11 認証応答タイマーを設定します。

config advanced timers auth-timeout *interval*

interval の値は、5 ～ 600 秒です。デフォルト値は 10 秒です。

ステップ 10 次のコマンドを入力して、変更を保存します。

save config

ステップ 11 次のコマンドを入力して、アクセス ポイントの設定を表示します。

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

IPv4 を使用しているプライマリ シスコ スイッチの IP アドレスに対して **show ap config general** *Cisco_AP* コマンドを実行すると、次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name........................ 1-5520
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-8540
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-8540
Tertiary Cisco Switch IP Address................. 1.1.1.4
...
```

IPv6 を使用するプライマリ Cisco スイッチの IP アドレスに対する **show ap config general** *Cisco_AP* コマンドでは、次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP6
Country code..................................... US - United States
Regulatory Domain allowed by Country.............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 13
MAC Address...................................... 44:2b:03:9a:9d:30
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:5:96:295d:3b2:2db2:9b47
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::6abd:abff:fe8c:764a
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Disabled
Ssh State........................................ Globally Disabled
Cisco AP Location................................ _5500
Cisco AP Floor Label............................. 0
```

```
Cisco AP Group Name.............................. IPv6-Same_VLAN
Primary Cisco Switch Name....................... Maulik_WLC_5500-HA
Primary Cisco Switch IP Address................. 2001:9:5:95::11
```

IPv4 を使用して設定されている場合、**show advanced backup-controller** コマンドでは、次のような情報が表示されます。

```
AP primary Backup Controller ..................... controller1 10.10.10.10
AP secondary Backup Controller ..............  0.0.0.0
```

IPv6 を使用して設定されている場合、**show advanced backup-controller** コマンドでは、次のような情報が表示されます。

```
AP primary Backup Controller ..................... WLC_5500-2 fd09:9:5:94::11
AP secondary Backup Controller .................. vWLC 9.5.92.11
```

show advanced timers コマンドの場合は、次のような情報が表示されます。

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)............ disable
AP Primary Discovery Timeout (seconds)........... 120
```

AP のフェールオーバー プライオリティ

アクセス ポイントに対するフェールオーバー プライオリティの設定について

各コントローラには、定義された数のアクセス ポイント用通信ポートが装備されています。未使用のアクセス ポイント ポートがある複数のコントローラが同じネットワーク上に展開されている場合、1つのコントローラが故障すると、ドロップしたアクセス ポイントは、自動的に未使用のコントローラ ポートをポーリングして、そのポートにアソシエートします。

次に、アクセス ポイントのフェールオーバー プライオリティを設定する際の注意事項を示します。

- バックアップ コントローラがプライオリティ レベルの高いアクセス ポイントからの join 要求を認識できるよう、また、プライオリティ レベルの低いアクセス ポイントを必要に応じて関連付け解除してポートを使用可能にできるようにワイヤレス ネットワークを設定できます。
- フェールオーバーのプライオリティ レベルは、通常の無線ネットワークの運用中は無効です。コントローラ障害後に使用できるバックアップ コントローラ ポートよりも多くのアソシエーション要求が発生する場合のみ有効となります。

- ネットワークのフェールオーバー プライオリティを有効にして、個別のアクセス ポイントにプライオリティを割り当てることができます。
- デフォルトでは、すべてのアクセス ポイントはプライオリティ レベル 1 に設定されています。これは、最も低いプライオリティ レベルです。このため、これよりも高いプライオリティ レベルを必要とするアクセス ポイントにのみ、プライオリティ レベルを割り当てる必要があります。

アクセス ポイントのフェールオーバー プライオリティの設定（GUI）

手順

ステップ 1 [Wireless] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。

ステップ 2 [Global AP Failover Priority] ドロップダウン リストから [Enable] を選択してアクセス ポイント フェールオーバー プライオリティを有効にするか、または [Disable] を選択してこの機能を無効にし、アクセス ポイント プライオリティの割り当てをすべて無視します。デフォルト値は [Disable] です。

ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ステップ 5 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 6 フェールオーバー プライオリティを有効にするアクセス ポイントの名前をクリックします。

ステップ 7 [High Availability] タブを選択します。[All APs > Details for]（[High Availability]）ページが表示されます。

ステップ 8 [AP Failover Priority] ドロップダウン リストで次のオプションのいずれかを選択して、アクセス ポイントのプライオリティを指定します。

- [Low]：アクセス ポイントにプライオリティ レベル 1 を割り当てます。これは最も低いプライオリティ レベルです。これはデフォルト値です。
- [Medium]：アクセス ポイントにプライオリティ レベル 2 を割り当てます。
- [High]：アクセス ポイントにプライオリティ レベル 3 を割り当てます。
- [Critical]：アクセス ポイントにプライオリティ レベル 4 を割り当てます。これは最も高いプライオリティ レベルです。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

アクセス ポイントのフェールオーバー プライオリティの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、アクセス ポイント フェールオーバー プライオリティを有効または無効にします。

config network ap-priority {**enable** | **disable**}

ステップ 2 次のコマンドを入力して、アクセス ポイントのプライオリティを指定します。

config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

ここで、1 は最も低いプライオリティ レベルであり、4 は最も高いプライオリティ レベルです。デフォルト値は 1 です。

ステップ 3 **save config** コマンドを入力して、変更を保存します。

フェールオーバー プライオリティの設定の表示（CLI）

- 次のコマンドを入力して、ネットワーク上でアクセス ポイントのフェールオーバー プライオリティが有効かどうかを確認します。

  show network summary

  以下に類似した情報が表示されます。

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority........................... Enabled

...
```

- 次のコマンドを入力して、各アクセス ポイントのフェールオーバー プライオリティを表示します。

  show ap summary

  以下に類似した情報が表示されます。

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured
```

```
AP Name  Slots  AP Model          Ethernet MAC      Location   Port Country Priority
-------  -----  ----------------- ----------------  ---------  ---- ------- --------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

特定のアクセス ポイントの概要を表示するには、アクセス ポイント名を指定します。また、アクセス ポイントのフィルタリングを行うときは、ワイルドカード検索を使用できます。

AP の再送信間隔および再試行回数

AP 再送信間隔および再試行回数の設定について

コントローラおよび AP は、信頼性のある CAPWAP 転送プロトコルを使用してパケットを交換します。各要求に対して、応答が定義されています。この応答を使用して、要求メッセージの受信を確認します。応答メッセージは明示的に確認されません。したがって、応答メッセージが受信されない場合は、再送信間隔後に元の要求メッセージが再送信されます。最大再送信回数が過ぎても要求が確認されないと、セッションが終了し、AP は別のコントローラに再アソシエートされます。

アクセス ポイントの再送信間隔と再試行回数の制約事項

- 再送信間隔と再試行回数の両方とも、グローバルと特定のアクセス ポイント レベルで設定できます。グローバル設定では、これらの設定パラメータがすべてのアクセス ポイントに適用されます。つまり、再送信間隔と再試行回数は、すべてのアクセス ポイントに均一になります。また、特定のアクセス ポイント レベルで再送信間隔と再試行回数を設定すると、値はその特定のアクセス ポイントに適用されます。アクセス ポイント固有の設定は、グローバル設定よりも優先されます。
- 再送信間隔および再試行回数は、メッシュ アクセス ポイントには適用されません。

AP の再送信間隔と再試行回数の設定（GUI）

再送信間隔と再試行回数は、すべての AP にグローバルに設定することも、特定の AP に設定することもできます。

手順

ステップ 1 コントローラ GUI を使用して、再送信間隔、および再試行回数をグローバルに設定するようにコントローラを設定するには、次の手順を実行します。

a) [Wireless] > [Access Points] > [Global Configuration] の順に選択します。

b) [AP Transmit Config Parameters] セクションから、次のいずれかのオプションを選択します。

- [AP Retransmit Count]：アクセス ポイントからコントローラに要求を再送信する回数を入力します。このパラメータには、3 ～ 8 の値を指定できます。

- [AP Retransmit Interval]：要求の再送信から次の再送信までの時間を入力します。このパラメータには、2 ～ 5 の値を指定できます。

c) [Apply] をクリックします。

ステップ 2 特定のアクセス ポイントに対して、再送信間隔、および再試行回数を設定するようにコントローラを設定するには、次の手順を実行します。

a) [Wireless] > [Access Points] > [All APs] の順に選択します。
b) 値を設定するアクセス ポイントに対応する [AP Name] リンクをクリックします。

[All APs > Details] ページが表示されます。

c) [Advanced] タブをクリックして、[Advanced Parameters] ページを開きます。
d) [AP Transmit Config Parameters] セクションから、次のいずれかのパラメータを選択します。

- [AP Retransmit Count]：アクセス ポイントからコントローラに要求を再送信する回数を入力します。このパラメータには、3 ～ 8 の値を指定できます。
- [AP Retransmit Interval]：要求の再送信から次の再送信までの時間を入力します。このパラメータには、2 ～ 5 の値を指定できます。

e) [Apply] をクリックします。

アクセス ポイントの再送信間隔と再試行回数の設定（CLI）

再送信間隔と再試行回数は、すべてのアクセスポイントにグローバルに設定することも、特定のアクセス ポイントに設定することもできます。

- 次のコマンドを入力して、すべてのアクセスポイントにグローバルに再送信間隔と再試行回数を設定します。

  config ap retransmit {**interval** | **count**} *seconds* **all**

  interval パラメータの有効な範囲は 3 ～ 8 です。**count** パラメータの有効な範囲は 2 ～ 5 です。

- 次のコマンドを入力して、特定のアクセスポイントに再送信間隔と再試行回数を設定します。

  config ap retransmit {**interval** | **count**} *seconds Cisco_AP*

  interval パラメータの有効な範囲は 3 ～ 8 です。**count** パラメータの有効な範囲は 2 ～ 5 です。

- 次のコマンドを入力して、すべて、または特定の AP に設定した retransmit パラメータのステータスを表示します。

  show ap retransmit all

（注） retransmit 値と retry 値は、メッシュ モードのアクセス ポイントに設定できないので、これらの値は N/A（適用外）として表示されます。

- 次のコマンドを入力して、特定のアクセス ポイントに設定した retransmit パラメータのステータスを表示します。

  show ap retransmit *Cisco_AP*

アクセス ポイントの認可

SSC を使用したアクセス ポイントの認可

無線アクセス ポイントのコントロールおよびプロビジョニング（CAPWAP）プロトコルは、アクセスポイントおよびコントローラの両方でX.509証明書を必要とするセキュアなキーを配布することにより、アクセスポイントとコントローラの間の制御通信を保護します。CAPWAPは、X.509 証明書のプロビジョニングに依存します。2005 年 7 月 18 日よりも前に出荷されたCisco Aironet アクセス ポイントには MIC がありません。このため、これらのアクセス ポイントではLightweightモードで動作するようにアップグレードされた場合、SSCが作成されます。コントローラは特定のアクセス ポイントの認証についてローカル SSC を許可するようにプログラムされており、これらの認証要求をRADIUSサーバに転送しません。これは、許容できるセキュアな動作です。

SSC を使用する仮想コントローラのアクセス ポイントの許可

物理コントローラによって使用される、製造元がインストールした証明書（MIC）の代わりにSSC 証明書を使用する仮想コントローラ。コントローラを AP が仮想コントローラの SSC を検証するように設定できます。AP が SSC を検証する場合、AP は仮想コントローラ ハッシュ キーがフラッシュに保存されるハッシュ キーと一致するかどうかを確認します。一致が見つかった場合、APはコントローラに関連付けます。一致がない場合、検証は失敗し、APはコントローラから切断され、ディスカバリ プロセスを再起動します。デフォルトでは、ハッシュ検証は有効です。AP は仮想コントローラに関連付ける前に、フラッシュの仮想コントローラのハッシュ キーが必要です。SSC のハッシュ検証を無効にすると、AP はハッシュ検証をバイパスし、Run状態に直接移動します。APSは物理コントローラに関連付けることが可能で、ハッシュ キーをダウンロードし、次に仮想コントローラに関連付けます。AP が物理コントローラに関連付けられ、ハッシュ検証が無効にされている場合、AP はハッシュ検証なしで任意の仮想コントローラに関連付けます。仮想コントローラのハッシュ キーをモビリティ グループ メンバに設定することができます。このハッシュキーは、AP がコントローラのハッシュ キーを検証できるように、AP にプッシュされます。

SSC の設定（GUI）

手順

ステップ 1 **[Security]** > **[Certificate]** > **[SSC]** の順に選択して、[Self Significant Certificates（SSC）] ページを開きます。

SSC のデバイス認証の詳細が表示されます。

ステップ 2 ハッシュ キー検証を有効にするには、[Enable SSC Hash Validation] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックして、変更を確定します。

SSC の設定（CLI）

手順

ステップ 1 SSC のハッシュ検証を設定するには、次のコマンドを入力します。

config certificate ssc hash validation {**enable** | **disable**}

ステップ 2 ハッシュ キーの詳細を表示するには、次のコマンドを入力します。

show certificate ssc

MIC を使用したアクセス ポイントの認可

RADIUS サーバによって、MIC を使用してアクセス ポイントを認可するようにコントローラを設定できます。コントローラでは、情報を RADIUS サーバに送信する際、アクセス ポイントの MAC アドレスがユーザ名とパスワードの両方に使用されます。たとえば、アクセス ポイントの MAC アドレスが 000b85229a70 の場合、コントローラでアクセス ポイントを認可する際に使用されるユーザ名もパスワードも 000b85229a70 になります。

（注） アクセス ポイントの MAC アドレスでは、パスワードが強力ではないことは問題にはなりません。コントローラでは RADIUS サーバを介したアクセス ポイントの許可の前に、MIC を使用してアクセス ポイントが認証されるためです。MIC の使用により、強力に認証されます。

（注） MACアドレスをRADIUS AAAサーバのアクセスポイントの認証に対するユーザ名とパスワードに使用する場合には、同じ AAA サーバをクライアント認証に使用しないでください。

LSC を使用したアクセス ポイントの認可

独自の公開鍵インフラストラクチャ（PKI）でセキュリティを向上させ、認証局（CA）を管理し、生成された証明書上の方針、制限、および使用方法を定義する場合、LSC を使用できます。

LSC CA 証明書は、アクセス ポイントおよびコントローラにインストールされています。アクセス ポイント上のデバイス証明書はプロビジョニングが必要です。アクセス ポイントは、コントローラに certRequest を送信して署名された X.509 証明書を取得します。コントローラは CA プロキシとして動作し、このアクセス ポイントのために CA が署名した certRequest を受信します。

注意事項および制約事項

- リリース 8.3.112.0 以降、LSC を有効にするにはデバイス証明書が必要です。この要件があるため、以下のガイドラインに従うことお勧めします。
  - AP を LSC 対応コントローラと関連付けるために、AP が LSC でプロビジョニングされていることを確認します。
  - 一部の AP が MIC を使用し、一部の AP が LSC を使用する混在環境でないことを確認します。
  - [Number of attempts to LSC] および [AP Ethernet MAC addresses] を指定する必要はありません。

    この詳細については、CSCve63755 を参照してください。

- CA サーバが手動モードにあり、保留中の登録である LSC SCEP テーブルに AP エントリがある場合、コントローラは保留中の応答を返すように、CA サーバを待ちます。CA サーバからの応答がない場合、コントローラは応答の取得を3回まで試みます。その後、フォールバック モードに入り、AP プロビジョニングはタイムアウトとなり、AP はリブートして、MIC を提示します。
- コントローラの LSC ではパスワードの確認は行われません。このため、LSC を機能させるには、CA サーバでパスワードの確認を無効にする必要があります。

ローカルで有効な証明書の設定（GUI）

手順

ステップ 1 **[Security]** > **[Certificate]** > **[LSC]** を選択して、[Local Significant Certificates (LSC) - General] ページを開きます。

ステップ 2 [CA Server URL] テキスト ボックスで、CA サーバへの URL を入力します。ドメイン名を入力することも IP アドレスを入力することもできます。

ステップ 3 [Params] テキスト ボックスに、デバイス証明書のパラメータを入力します。（オプション）keysize の値は 2048 ～ 4096（ビット）で、デフォルト値は 2048 です。

ステップ 4 [Apply] をクリックして、変更を確定します。

ステップ 5 コントローラの証明書データベースに CA 証明書を追加するには、証明書タイプの青いドロップダウン矢印にマウス オーバーして、[Add] を選択します。

ステップ 6 コントローラの証明書データベースにデバイス証明書を追加するには、証明書タイプの青いドロップダウン矢印にマウス オーバーして、[Add] を選択します。

ステップ 7 [Enable LSC on Controller] チェックボックスをオンにして、システムの LSC を有効にします。

ステップ 8 [Apply] をクリックして、変更を確定します。

ステップ 9 [AP Provisioning] タブを選択して、[Local Significant Certificates (LSC) - AP Provisioning] ページを開きます。

ステップ 10 [Enable] チェックボックスをオンにして [Update] をクリックし、アクセス ポイントに LSC をプロビジョニングします。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 アクセス ポイントがリブートされることを示すメッセージが表示されたら、[OK] をクリックします。

ステップ 13 [Number of Attempts to LSC] フィールドに、アクセス ポイントが、証明書をデフォルト（MIC または SSC）に戻す前に、LSC を使用してコントローラに join を試みる回数を入力します。範囲は 0 ～ 255（両端の値を含む）で、デフォルト値は 3 です。

（注） リリース 8.3.112.0 以降を使用している場合は、CSCve63755の要件により、このタスクを実行する必要はありません。AP を LSC 対応コントローラと関連付ける前に、その AP が LSC でプロビジョニングされていることを確認する必要があります。

（注） 再試行回数を 0 以外の値に設定した場合に、アクセス ポイントが設定された再試行回数後に LSC を使用してコントローラに join できなかった場合、アクセス ポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセス ポイントが LSC 使用によるコントローラへの join に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの join を試みません。

（注） 初めて LSC を設定する場合は、ゼロ以外の値を設定することが推奨されます。

ステップ 14 [AP Ethernet MAC Addresses] フィールドにアクセス ポイントの MAC アドレスを入力し、[Add] をクリックして、アクセス ポイントをプロビジョン リストに追加します。

（注） リリース 8.3.112.0 以降を使用している場合は、CSCve63755 の要件により、このタスクを実行する必要はありません。AP を LSC 対応コントローラと関連付ける前に、その AP が LSC でプロビジョニングされていることを確認する必要があります。

（注） アクセス ポイントをプロビジョン リストから削除するには、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

（注） アクセス ポイント プロビジョン リストを設定すると、AP プロビジョニングを有効にした場合に、プロビジョン リスト内のアクセス ポイントのみがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに join する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

ステップ 15 [Apply] をクリックして、変更を確定します。

ステップ 16 [Save Configuration] をクリックして、変更を保存します。

ローカルで有効な証明書の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、URL を CA サーバに設定します。

config certificate lsc ca-server *http://url:port/path*

ここで、*url* にはドメイン名を入力することも IP アドレスを入力することもできます。

（注） 1 つの CA サーバだけを設定できます。別の CA サーバを設定するには、**config certificate lsc ca-server delete** コマンドを使用して設定済みの CA サーバを削除してから、別の CA サーバを設定します。

ステップ 2 次のコマンドを入力して、デバイス証明書のパラメータを設定します。

config certificate lsc subject-params *country state city orgn dept e-mail*

（注） Common Name（CN）は、現在の MIC/SSC 形式である C*xxxx*-*MacAddr* を使用して、アクセス ポイント上で自動的に生成されます。ここで、*xxxx* は製品番号です。

ステップ 3 （オプション）次のコマンドを入力して、keysize を設定します。

config certificate lsc other-params *keysize*

keysize の値は 2048 ～ 4096（ビット）で、デフォルト値は 2048 です。

ステップ 4 次のコマンドを入力して、LSC CA 証明書をコントローラの証明書データベースに追加します。

config certificate lsc ca-cert {**add** | **delete**}

ステップ 5 次のコマンドを入力して、LSCデバイス証明書をコントローラの証明書データベースに追加します。

config certificate lsc device-cert {**add** | **delete**}

ステップ 6 次のコマンドを入力して、システム上で LSC を有効にします。

config certificate lsc {**enable** | **disable**}

ステップ 7 次のコマンドを入力して、アクセス ポイントの LSC をプロビジョニングします。

config certificate lsc ap-provision {**enable** | **disable** }

ステップ 8 次のコマンドを入力して、アクセス ポイントがデフォルトの証明書（MIC または SSC）に復帰する前に、LSC を使用してコントローラに join を試みる回数を設定します。

config certificate lsc ap-provision revert-cert *retries*

ここで、*retries* の値は 0 ～ 255、デフォルト値は 3 です。

（注） リリース 8.3.112.0 以降を使用している場合は、CSCve63755 の要件により、このタスクを実行する必要はありません。AP を LSC 対応コントローラと関連付ける前に、その AP が LSC でプロビジョニングされていることを確認する必要があります。

（注） 再試行回数を 0 以外の値に設定した場合に、アクセスポイントが設定された再試行回数後に LSC を使用してコントローラに join できなかった場合、アクセス ポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセスポイントが LSC 使用によるコントローラへの join に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの join を試みません。

（注） 初めて LSC を設定する場合は、0 以外の値を設定することをお勧めします。

ステップ 9 次のコマンドを入力して、アクセス ポイントをプロビジョン リストに追加します。

config certificate lsc ap-provision auth-list add *AP_mac_addr*

（注） リリース 8.3.112.0 以降を使用している場合は、CSCve63755 の要件により、このタスクを実行する必要はありません。AP を LSC 対応コントローラと関連付ける前に、その AP が LSC でプロビジョニングされていることを確認する必要があります。

（注） プロビジョニング リストからアクセス ポイントを削除するには、**config certificate lsc ap-provision auth-list delete** *AP_mac_addr* コマンドを入力します。

（注） アクセス ポイント プロビジョニング リストを設定する場合は、AP プロビジョニングを有効にしたときに（手順 *8*）プロビジョニング リストのアクセス ポイントだけがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに join する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

ステップ 10 次のコマンドを入力して、LSC の概要を表示します。

show certificate lsc summary

以下に類似した情報が表示されます。

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
 Provision-List................................. Not Configured
 LSC Revert Count in AP reboots................. 3

LSC Params:
 Country........................................ US
 State.......................................... ca
 City........................................... ss
 Orgn........................................... org
 Dept........................................... dep
 Email.......................................... dep@co.com
 KeySize........................................ 2048

LSC Certs:
 CA Cert........................................ Not Configured
 RA Cert..................................... Not Configured
```

ステップ 11 次のコマンドを入力して、LSC を使用してプロビジョニングされたアクセス ポイントについての詳細を表示します。

show certificate lsc ap-provision

以下に類似した情報が表示されます。

```
LSC AP-Provisioning..................... Yes
Provision-List.......................... Present

Idx  Mac Address
---  ------------
1  00:18:74:c7:c0:90
```

アクセス ポイントの認可（GUI）

手順

ステップ 1 [Security] > [AAA] > [AP Policies] の順に選択して、[AP Policies] ページを開きます。

ステップ 2 アクセス ポイントに自己署名証明書（SSC）、製造元でインストールされる証明書（MIC）、またはローカルで有効な証明書（LSC）を受け入れさせる場合は、該当するチェックボックスをオンにします。

ステップ 3 アクセス ポイントを認可する際に AAA RADIUS サーバを使用する場合は、[Authorize MIC APs against auth-list or AAA] チェックボックスをオンにします。

ステップ 4 アクセス ポイントを認可する際に LSC を使用する場合は、[Authorize LSC APs against auth-list] チェックボックスをオンにします。

ブリッジ モード（無線 MAC アドレスを入力する必要がある）の場合を除いて、すべての AP に対してイーサネット MAC アドレスを入力します。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 アクセス ポイントをコントローラの許可リストに追加する手順は、次のとおりです。

a) [Add] をクリックして、[Add AP to Authorization List] 領域にアクセスします。
b) [MAC Address] テキスト ボックスに、アクセス ポイントの MAC アドレスを入力します。
c) [Certificate Type] ドロップダウン リストから、[MIC]、[SSC]、または [LSC] を選択します。
d) [Add] をクリックします。アクセス ポイントが認可リストに表示されます。

（注） アクセス ポイントを認可リストから削除するには、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

（注） 特定のアクセス ポイントを認可リストで検索するには、[Search by MAC] テキスト ボックスにアクセス ポイントの MAC アドレスを入力して [Search] をクリックします。

アクセス ポイントの認可（CLI）

手順

- 次のコマンドを入力して、アクセス ポイントの認可ポリシーを設定します。

  config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

- 次のコマンドを入力して、アクセス ポイントが製造元でインストールされる証明書（MIC）、自己署名証明書（SSC）、またはローカルで有効な証明書（LSC）を受け入れるよう設定します。

  config auth-list ap-policy{**mic** | **ssc** |**lsc** {**enable** |**disable**}}

- ユーザ名がアクセス ポイント認証要求で使用されるように設定します。

  config auth-list ap-policy{**authorize-ap username** {**ap_name** |**ap_mac** |**both**}}

- 次のコマンドを入力して、許可リストにアクセス ポイントを追加します。

  config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  ap_key は 20 バイト、つまり 40 桁のオプション キーハッシュ値です。

（注） アクセス ポイントを認可リストから削除するには、**config auth-list delete ap_mac** コマンドを入力します。

- 次のコマンドを入力して、アクセス ポイントの認可リストを表示します。

  show auth-list

プラグ アンド プレイ（PnP）

プラグ アンド プレイ（PnP）について

PnP ソリューションは AP が WLC に参加する前にステージング パラメータを提供します。このステージング設定を使用して、APはWLCに参加するときにランタイム設定を取得します。PNP は、AP が新規出荷時の状態、または工場出荷時の初期状態にリセットされた場合にのみ AP でアクティブになります。PnP は AP が WLC に初めて接続した後では初期化されません。

PnP IPv4 機能は、Cisco Aironet 1600、2600、3600、700、1700、2700、および 3700 シリーズ アクセス ポイントでサポートされています。

リリース 8.5 以降は、PnP IPv4 と IPv6 の両方の機能が、Cisco Aironet 2800、3800、1850、1830、および 1815 シリーズ アクセス ポイントでサポートされています。

AP PnP のシナリオ

- オンプレミス リダイレクション：顧客は内部ネットワークで PnP サーバをホストしています。AP は、DHCP オプションまたは DNS 解決を使用して PnP サーバを検出します。
- クラウド リダイレクション：AP は、顧客が DHCP や DNS に対する制御を保有していない、または PNP サーバをホストしていないサードパーティのネットワークに接続しています。このシナリオでは、AP は Cisco Cloud リダイレクト サービスに接続して、WLC または PnP のアドレスを取得します。WLC アドレスは、PnP サーバを保有していない顧客のためにリダイレクト サービスで設定されます。

PnP の詳細については、
http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_wireless_plug_and_play_deployment_guide.html
で ワイヤレス プラグ アンド プレイ導入ガイド [英語] のマニュアルを参照してください。

AP 802.1x サプリカント

アクセス ポイントに対する認証の設定について

IEEE 802.1x ポートベースの認証は、不正なデバイス（サプリカント）によるネットワーク アクセスを防止するためにデバイスに設定されます。デバイスでは、固定構成やインストールされているモジュールに基づいて、アクセス ポイントの機能を組み合わせることができます。

Lightweight アクセス ポイントとシスコのスイッチの間で 802.1X 認証を設定できます。スイッチは、サプリカント AP デバイスの認証に EAP-FAST と匿名 PAC プロビジョニングを使用する RADIUS サーバ（Cisco ISE）を使用します。

コントローラに現在関連付けられている、または今後関連付けられるすべてのアクセスポイントにグローバル認証を設定できます。グローバル認証設定を上書きし、特定のアクセスポイントに一意の認証設定を割り当てることもできます。

802.1 x 認証が設定されたスイッチでは、802.1 x 認証デバイスのトラフィックだけが許可されます。

認証モデルには次の 2 つのモードがあります。

- グローバル認証：すべての AP の認証設定
- AP レベルの認証：特定の AP の認証設定

デフォルトでは、スイッチはポートごとに 1 つのデバイスを認証します。この制限は、Cisco Catalyst スイッチにはありません。スイッチに設定されているホストモードタイプによって、1 つのポートで許可されるエンドポイントの数とタイプが決まります。ホストモードオプションは次のとおりです。

- 単一ホスト モード：1 つのポートで単一の IP または MAC アドレスが認証されます。これがデフォルトの設定です。
- マルチホスト モード：最初の MAC アドレスを認証後、その他の MAC アドレスが無制限に許可されます。接続された AP がローカル スイッチング モードに設定されている場合は、スイッチ ポートでホスト モードを有効にします。これにより、クライアントのトラフィックがスイッチ ポートを通過できます。セキュアなトラフィック パスにする場合は、WLAN で dot1x を有効にしてクライアント データを保護します。

  この機能は、ローカル モード、FlexConnect モード、スニファ モード、およびモニタ モードで AP をサポートします。また、中央スイッチング モードとローカル スイッチング モードで WLAN をサポートします。

（注） FlexConnect モードでは、正しいネイティブ VLAN が設定されている AP で VLAN サポートが有効になっていることを確認します。

表 *2:* 展開オプション

AP の 802.1x	スイッチ	結果
OFF	ENABLED	AP はコントローラに参加しません。
ENABLED	DISABLED	AP はコントローラに参加します。EAP 応答の受信に失敗すると、非 dot1x CAPWAP ディスカバリに自動的にフォールバックします。

AP の 802.1x	スイッチ	結果
ENABLED	ENABLED	APがコントローラに参加し、ポート認証をポストします。

AP のクレデンシャルを訂正する必要がある場合は、スイッチ ポートの dot1x 認証を無効にして、クレデンシャルの更新後にポート認証を再度有効にします。

アクセス ポイントの認証を設定するための前提条件

手順

ステップ 1 アクセス ポイントが新しい場合は、次を実行します。

a) アクセス ポイントを、インストールされたリカバリ イメージでブートします。

b) この提案フローに従う代わりに、アクセス ポイントがコントローラにjoinする前にアクセス ポイントに接続されたスイッチ ポートで 802.1X 認証を有効化するには、次のコマンドを入力します。

lwapp ap dot1x username *username* **password** *password*

（注） この提案フローに従って、アクセス ポイントがコントローラにjoin されて設定済みの 802.1X 資格情報を受信してからスイッチ ポートで 802.1X 認証を有効化する場合は、このコマンドを入力する必要はありません。

（注） このコマンドは、適用可能な回復イメージを実行しているアクセス ポイントでのみ使用できます。

アクセス ポイントをスイッチ ポートに接続します。

ステップ 2 必要なソフトウェア イメージをコントローラにインストールして、コントローラをリブートします。

ステップ 3 すべてのアクセス ポイントによるコントローラへの join を許可します。

ステップ 4 コントローラ上で認証を設定します。

ステップ 5 スイッチを設定して認証を許可します。

アクセス ポイントの認証に関する制約事項

- AP に接続されたスイッチ ポートでは、ブリッジ プロトコル データ ユニット（BPDU）ガードを常に無効にする必要があります。BPDUガードの有効化は、スイッチによりポートが PortFast モードになった場合にのみ許可されます。

アクセス ポイントの認証の設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[Global Configuration]** の順に選択して、[Global Configuration] ページを開きます。

ステップ 2 [802.1x Supplicant Credentials] で、[802.1x Authentication] チェックボックスをオンにします。

ステップ 3 [Username] テキスト ボックスに、そのコントローラに join するすべてのアクセス ポイントが継承するユーザ名を入力します。

ステップ 4 [Password] ボックスと [Confirm Password] ボックスに、コントローラに join するすべてのアクセス ポイントによって継承されるパスワードを入力します。

（注） これらのテキストボックスには、強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

ステップ 5 [Apply] をクリックして、グローバル認証ユーザ名およびパスワードを、コントローラに現在 join しているアクセス ポイント、および今後 join するすべてのアクセス ポイントに送信します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

ステップ 7 必要に応じて、次の手順に従って、グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセス ポイントに割り当てることができます。

a) **[Access Points]** > **[All APs]** の順に選択して、[All APs] ページを開きます。
b) 認証設定を無効にするアクセス ポイントの名前をクリックします。
c) [Credentials] タブをクリックして [All APs > Details for]（Credentials）ページを開きます。
d) [802.1x Supplicant Credentials] で [Over-ride Global Credentials] チェックボックスをオンにして、このアクセスポイントがグローバル認証のユーザ名およびパスワードをコントローラから継承しないようにします。デフォルト値はオフです。
e) [Username]、[Password]、および [Confirm Password] テキスト ボックスに、このアクセス ポイントに割り当てる一意のユーザ名およびパスワードを入力します。

（注） 入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

f) [Apply] をクリックして、変更を確定します。
g) [Save Configuration] をクリックして、変更を保存します。

（注） このアクセスポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

アクセス ポイントの認証の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、コントローラに現在 join しているアクセス ポイント、および今後 joinするすべてのアクセスポイントについて、グローバル認証のユーザ名とパスワードを設定します。

config ap 802.1Xuser add username *ap-username* **password** *ap-password* **all**

（注） *ap-password* パラメータには強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

ステップ 2 （任意）グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセスポイントに割り当てることができます。そのためには、次のコマンドを入力します。

config ap 802.1Xuser add username *ap-username* **password** *ap-password Cisco_AP*

（注） *ap-password* パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、ステップ 1 の注記を参照してください。

このコマンドに入力した認証設定は、コントローラやアクセスポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

（注） このアクセスポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、**config ap 802.1Xuser delete** *Cisco_AP* コマンドを入力します。このコマンドの実行後、「`AP reverted to global username configuration`」というメッセージが表示されます。

ステップ 3 **save config** コマンドを入力して、変更を保存します。

ステップ 4 （オプション）次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセスポイントに対して 802.1X 認証を無効にします。

config ap 802.1Xuser disable {**all** | *Cisco_AP*}

（注） 特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

ステップ 5 次のコマンドを入力して、コントローラに join するすべてのアクセス ポイントの認証設定を表示します。

show ap summary

以下に類似した情報が表示されます。

```
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

ステップ 6 次のコマンドを入力して、特定のアクセス ポイントの認証設定を表示します。

show ap config general *Cisco_AP*

（注） アクセス ポイントの名前では、大文字と小文字が区別されます。

（注） このアクセス ポイントがグローバル認証用に設定されている場合は、[AP Dot1x User Mode] テキスト ボックスに [Automatic] と表示されます。このアクセス ポイントのグローバル認証設定が上書きされている場合は、[AP Dot1x User Mode] テキスト ボックスに「Customized」と表示されます。

ステップ 7 次のコマンドを入力して、AP の認証ステータスを確認します。

show authentication interface wired-port status

スイッチの認証の設定

スイッチ ポートで 802.1X 認証を有効にするには、スイッチ CLI で次のコマンドを入力します。

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**

- Switch(config-if)# **end**

インフラストラクチャ MFP

管理フレーム保護について

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。

- インフラストラクチャ MFP：DoS 攻撃を引き起こしたり、ネットワーク上で過剰なアソシエーションやプローブを生じさせたり、不正なアクセス ポイントとして介入したり、QoS と無線測定フレームへの攻撃によりネットワーク パフォーマンスを低下させたりする敵対者を検出することにより、管理フレームを保護します。インフラストラクチャ MFP は、フィッシング インシデントを検出および報告するための迅速かつ効果的な手段を提供するグローバル設定です。

  インフラストラクチャ MFP は特に、アクセス ポイントによって送信され（クライアントによって送信されたのではなく）、次にネットワーク内の他のアクセス ポイントによって検証される管理フレームに、Message Integrity Check Information Element（MIC IE; メッセージ整合性情報要素）を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- クライアント MFP：認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多くの一般化した攻撃が効力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを悪化させます。

  具体的には、クライアント MFP は、アクセス ポイントと CCXv5 クライアント間で送受信される管理フレームを暗号化します。その結果、スプーフィングされたクラス 3 管理フレーム（つまり、アクセス ポイントと、認証およびアソシエートされたクライアントとの間でやり取りされる管理フレーム）をドロップすることにより、アクセス ポイントとクライアントの両方で予防措置をとることができます。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP は、最も一般的な種類のサービス拒否攻撃から、クライアントとアクセス ポイント間のセッションを保護します。また、セッションのデータ フレームに使用されているのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしており、TKIP または AES-CCMP のいずれかを使用して WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用されます。CCKM およびコントローラのモビリティ管理は、レイヤ 2 およびレイヤ 3 の高速ローミングのために、アクセス ポイント間でセッション キーを配布するのに使用されます。

（注） ブロードキャスト フレームを使用した攻撃を防ぐため、CCXv5 をサポートするアクセス ポイントでは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントおよびアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄する必要があります。

インフラストラクチャ MFP は、クライアント MFP 対応でないクライアントに送信された無効なユニキャスト フレームと、無効なクラス 1 およびクラス 2 管理フレームを引き続き検出および報告するため、クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足するものであると言えます。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- 管理フレーム保護：アクセス ポイントは、送信される各管理フレームに MIC IE を追加することによってフレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。MFP は、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。
- 管理フレーム検証：インフラストラクチャ MFP では、アクセス ポイントによって、ネットワーク内の他のアクセス ポイントから受信する各管理フレームが検証されます。MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能するように、すべてのコントローラでネットワーク タイム プロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントで異常が検出されるとコントローラに通知されます。コントローラでは、受信した異常イベントが集計され、その結果が SNMP トラップを使用してネットワーク管理システムに報告されます。

（注） クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで無効になっており、システム全体で有効にできます。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント認可が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はシステム全体で無効になります。インフラストラクチャ MFP がグローバルに有効化されると、選択した WLAN に対してシグニチャの生成（MIC を送信フレームに追加する）を無効にでき、選択したアクセス ポイントに対して検証を無効にできます。

クライアント MFP は、WPA2 に対して設定された WLAN 上でデフォルトで有効にされています。選択した WLAN 上で無効にすることも、必須にする（その場合、MFP をネゴシエートするクライアントのみがアソシエーションを許可されます）こともできます。

管理フレーム保護の制約事項

- Lightweight アクセス ポイントでは、インフラストラクチャ MFP はローカル モードおよび監視モードでサポートされます。アクセス ポイントがコントローラに接続しているときは、FlexConnect モードでサポートされます。クライアント MFP は、ローカル モード、FlexConnect モード、およびブリッジ モードでサポートされます。
- OEAP 600 シリーズのアクセス ポイントでは、MFP はサポートされません。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでの使用のみがサポートされています。
- クライアント MFP が無効にされているか、オプションである場合は、非 CCXv5 クライアントは WLAN にアソシエートできます。
- スタンドアロン モードの FlexConnect アクセス ポイントで生成されるエラー レポートは、コントローラに転送することはできず、ドロップされます。

管理フレーム保護の設定（GUI）

手順

ステップ 1 [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[AP Authentication Policy] ページを開きます。

ステップ 2 [Protection Type] ドロップダウン リストから [Management Frame Protection] を選択して、コントローラに対してインフラストラクチャ MFP をグローバルに有効にします。

ステップ 3 [Apply] をクリックして、変更を確定します。

（注） 複数のコントローラがモビリティ グループに含まれている場合は、インフラストラクチャ MFP に対して設定されているモビリティ グループ内のすべてのコントローラ上で、NTP/SNTP サーバを設定する必要があります。

ステップ 4 コントローラに対してインフラストラクチャ MFP をグローバルに有効にしたあと、次の手順を実行して、特定の WLAN にクライアント MFP を設定します。

a) [WLANs] を選択します。

b) 目的の **WLAN** のプロファイル名をクリックします。[WLANs > Edit] ページが表示されます。

c) [Advanced] を選択します。[WLANs > Edit]（[Advanced]）ページが表示されます。

d) [MFP Client Protection] ドロップダウン リストから、[Disabled]、[Optional]、または [Required] を選択します。デフォルト値は [Optional] です。[Required] を選択した場合、MFP がネゴシエートされている場合（つまり、WPA2 がコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 に対して設定されている場合）のみ、クライアントはアソシエーションを許可されます。

（注） Cisco OEAP 600 では MFP はサポートされません。[Disabled] または [Optional] を選択してください。

e) [Apply] をクリックして、変更を確定します。

ステップ 5 [Save Configuration] をクリックして設定を保存します。

管理フレーム保護の設定の表示（GUI）

コントローラの現在のグローバル MFP の設定を表示するには、[Security] > [Wireless Protection Policies] > [Management Frame Protection] の順に選択します。[Management Frame Protection Settings] ページが表示されます。

このページでは、次の MFP 設定が表示されます。

- [Management Frame Protection] フィールドは、インフラストラクチャ MFP がコントローラでグローバルに有効化されているかどうかを示します。
- [Controller Time Source Valid] フィールドは、コントローラの時刻が（時刻を手動で入力することにより）ローカルで設定されているか、外部ソース（NTP/SNTP サーバなど）を通じて設定されているかを示します。時刻が外部ソースによって設定される場合は、このフィールドの値が "True" になります。時刻がローカルに設定される場合は、この値が "False" になります。時刻源は、モビリティ グループ内の複数のコントローラのアクセスポイント間の管理フレーム上のタイムスタンプを検証するために使用されます。
- [Client Protection] フィールドは、クライアント MFP が個別の WLAN に対して有効化されているかどうかと、オプションまたは必須のいずれであるかを示します。

管理フレーム保護の設定（CLI）

手順

- 次のコマンドを入力して、コントローラに対してインフラストラクチャ MFP をグローバルに有効または無効にします。

  config wps mfp infrastructure {enable | disable}

- 次のコマンドを入力して、特定の WLAN でクライアント MFP シグニチャを有効または無効にします。

  config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

  クライアント MFP を有効にしてオプションの **required** パラメータを使用すると、MFP がネゴシエートされている場合のみ、クライアントはアソシエーションを許可されます。

管理フレーム保護の設定の表示（CLI）

手順

- 次のコマンドを入力して、コントローラの現在の MFP の設定を表示します。

  show wps mfp summary

- 次のコマンドを入力して、特定の WLAN の現在の MFP の設定を表示します。

  show wlan wlan_id

- 次のコマンドを入力して、特定のクライアントに対してクライアント MFP が有効になっているかどうかを表示します。

  show client detail *client_mac*

- 次のコマンドを入力して、コントローラの MFP 統計情報を表示します。

  show wps mfp *statistics*

（注） 実際に攻撃が進行中でない限り、このレポートにデータは含まれません。この表は5分ごとにクリアされ、データはネットワーク管理ステーションに転送されます。

管理フレーム保護の問題のデバッグ（CLI）

手順

- MFP に関する問題が発生した場合は、次のコマンドを使用します。

  debug wps mfp ? {**enable** | **disable**}

ここで、? は、次のいずれかを示します。

client：クライアント MFP メッセージのデバッグを設定します。

capwap：コントローラとアクセス ポイント間の MFP メッセージのデバッグを設定します。

detail：MFP メッセージの詳細デバッグを設定します。

report：MFP レポートのデバッグを設定します。

mm：MFP モビリティ（コントローラ間）メッセージのデバッグを設定します。

アクセスポイント接続プロセスのトラブルシューティング

アクセス ポイントがコントローラへの join を失敗する理由として、RADIUS の許可が保留の場合、コントローラで自己署名証明書が有効になっていない場合、アクセス ポイントとコントローラ間の規制ドメインが一致しない場合など、多くの原因が考えられます。

コントローラ ソフトウェア リリース 5.2 以降のリリースでは、すべての CAPWAP 関連エラーを syslog サーバに送信するようアクセス ポイントを設定できます。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。

アクセス ポイントの状態は、アクセス ポイントからの CAPWAP join request を受信するまでコントローラで維持されません。そのため、特定のアクセス ポイントからの CAPWAP discovery request が拒否された理由を判断することは難しい場合があります。そのような join の問題をコントローラで CAPWAP デバッグ コマンドを有効にせずトラブルシューティングするために、コントローラは discovery メッセージを送信してきたすべてのアクセス ポイントの情報を収集し、このコントローラに正常に join したアクセス ポイントの情報を保持します。

コントローラは、CAPWAP discovery request を送信してきた各アクセス ポイントについて、join 関連のすべての情報を収集します。収集は、アクセス ポイントから最初に受信した discovery メッセージから始まり、コントローラからアクセスポイントに送信された最後の設定ペイロードで終わります。

join 関連の情報を表示できるアクセス ポイントの数は、次のとおりです。

コントローラが最大数のアクセス ポイントの join 関連情報を維持している場合、それ以上のアクセス ポイントの情報は収集されません。

以上のいずれかの条件と一致しているのにアクセス ポイントがコントローラに join しない場合には、DHCP サーバを設定し、サーバ上のオプション 7 を使用して syslog サーバの IP アドレスをアクセス ポイントに戻すこともできます。それにより、アクセス ポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

（注） アクセス ポイントは、WLC に設定されている内部 DHCP プールの DHCP アドレスを使用してコントローラに join します。WLC で DHCP リース アドレスが削除されると、アクセス ポイントは、次のメッセージをリロードします。

AP が再起動中：リセットの理由： Admin のリロード。これは、Cisco IOS および Wave 2 AP では一般的な動作です。

capwap ap log-server *syslog_server_IP_address* コマンドを入力することにより、アクセス ポイントが現在コントローラに接続していない場合、アクセス ポイントの *CLI* を介して *syslog* サーバの *IP* アドレスを設定することもできます。

アクセス ポイントが最初にコントローラに join する際に、コントローラはグローバルな syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセス ポイントにコピーします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセス ポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントは同じコントローラに接続されたままで、コントローラ上のグローバル syslog サーバの IP アドレスの設定が、**config ap syslog host global** *syslog_server_IP_address* コマンドを使用して変更されている場合。この場合、コントローラは新しいグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントは同じコントローラに接続されたままで、特定の syslog サーバの IP アドレスが **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* コマンドを使用してコントローラ上のアクセス ポイントに対して設定されている場合。この場合、コントローラは新しい特定の syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントはコントローラから接続を切断されており、syslog サーバの IP アドレスが **lwapp ap log-server** *syslog_server_IP_address* コマンドを使用して、アクセス ポイントの CLI から設定されている場合。このコマンドは、アクセス ポイントが他のコントローラに接続されていない場合に限り機能します。
- アクセス ポイントがコントローラから join を切断され、別のコントローラに join している。この場合、新しいコントローラはそのグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存される。アクセス ポイントはその syslog サーバの IP アドレスに到達できれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

コントローラ GUI を使用してアクセス ポイントの syslog サーバを設定したり、コントローラ GUI または CLI を使用してアクセス ポイントの接続情報を表示したりできます。

アクセス ポイントの名前が **config ap name** *new_name old_name* コマンドを使用して変更された場合、新しい AP 名が更新されます。更新された新しい AP 名は、**show ap join stats summary all** コマンドと **show ap summary** コマンドの両方で確認できます。

（注） リリース 8.0 イメージの AP が Cisco WLC リリース 8.3（フラッシュでリリース 8.2 がプライマリ イメージおよびリリース 8.2.1 がセカンダリ イメージ）に参加しようとすると、AP は無期限ループになります。（リリース番号はあくまで3種類のイメージのシナリオを説明するための例として使用されており、記載のリリースには適用されません。）このループはバージョン不一致が原因で発生します。ダウンロード後、AP がそのイメージを Cisco WLC のイメージと比較すると、バージョン不一致が発生します。AP はプロセス全体を再度開始し、結果としてループになります。

アクセス ポイントの Syslog サーバの設定（CLI）

手順

ステップ 1 次のいずれかの操作を行います。

- このコントローラに join するすべてのアクセス ポイントに対して、グローバルな syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host global *syslog_server_IP_address*

  （注） デフォルトでは、すべてのアクセス ポイントのグローバル syslog サーバ IPv4/IPv6 アドレスは 255.255.255.255 です。コントローラ上の syslog サーバを設定する前に、アクセス ポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセス ポイントは syslog メッセージを送信できません。

  （注） 1 台の syslog サーバだけが、IPv4 と IPv6 の両方に使用されます。

- 特定のアクセス ポイントの syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  （注） デフォルトでは、各アクセス ポイントの syslog サーバ IPv4/IPv6 アドレスは 0.0.0.0 で、これはまだアクセス ポイントが設定されていないことを示しています。このデフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスがアクセス ポイントにプッシュされます。

ステップ 2 **save config** コマンドを入力して、変更を保存します。

ステップ 3 次のコマンドを入力して、コントローラに join するすべてのアクセス ポイントに対して、グローバルな syslog サーバの設定を表示します。

show ap config global

以下に類似した情報が表示されます。

```
AP global system logging host..................... 255.255.255.255
```

ステップ 4 次のコマンドを入力して、特定のアクセス ポイントの syslog サーバの設定を表示します。

show ap config general *Cisco_AP*

アクセス ポイントの join 情報の表示

CAPWAP discovery request をコントローラに少なくとも 1 回送信するアクセス ポイントの join に関する統計情報は、アクセスポイントがリブートまたは切断されても、コントローラ上に維持されます。これらの統計情報は、コントローラがリブートされた場合、または統計情報のクリアを選択した場合のみ削除されます。

アクセス ポイントの join 情報の表示（GUI）

手順

ステップ 1 [Monitor] > [Statistics] > [AP Join] の順に選択して、[AP Join Stats] ページを開きます。

このページには、コントローラに join している、または join を試みたことのあるすべてのアクセス ポイントが表示されます。無線 MAC アドレス、アクセス ポイント名、現在の join ステータス、イーサネット MAC アドレス、IP アドレス、および各アクセス ポイントの最後の join 時刻を示します。

ページの右上部には、アクセス ポイントの合計数が表示されます。アクセス ポイントのリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページを表示できます。各ページには最大 25 台のアクセス ポイントの join 統計情報を表示できます。

（注） アクセス ポイントをリストから削除する必要がある場合は、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] をクリックします。

（注） すべてのアクセス ポイントの統計情報をクリアして統計を再開したい場合は、[Clear Stats on All APs] をクリックします。

ステップ 2 [AP Join Stats] ページのアクセス ポイント リストで特定のアクセス ポイントを検索する場合は、次の手順に従って、特定の基準（MAC アドレスやアクセス ポイント名など）を満たすアクセス ポイントのみを表示するフィルタを作成します。

（注） この機能は、アクセスポイントのリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

a) [Change Filter] をクリックして、[Search AP] ダイアログ ボックスを開きます。
b) 次のチェックボックスのいずれかをオンにして、アクセスポイントを表示する際に使用する基準を指定します。

- [MAC Address]：アクセス ポイントのベース無線 MAC アドレスを入力します。
- [AP Name]：アクセス ポイントの名前を入力します。

（注） これらのフィルタのいずれかを有効にすると、もう 1 つのフィルタは自動的に無効になります。

c) [Find] をクリックして、変更を適用します。検索基準と一致するアクセス ポイントのみが [AP Join Stats] ページに表示され、ページ上部の [Current Filter] はリストを生成するのに使用したフィルタ（MAC Address:00:1e:f7:75:0a:a0、または AP Name:pmsk-ap など）を示します。

（注） フィルタを削除してアクセス ポイント リスト全体を表示するには、[Clear Filter] をクリックします。

ステップ 3 特定のアクセス ポイントの詳細な join 統計情報を表示するには、アクセス ポイントの無線 MAC アドレスをクリックします。[AP Join Stats Detail] ページが表示されます。

このページには、コントローラ側からの join プロセスの各段階に関する情報と発生したエラーが表示されます。

アクセス ポイントの join 情報の表示（CLI）

次の CLI コマンドを使用して、アクセス ポイントの join 情報を表示します。

- 次のコマンドを入力して、コントローラに join している、または join を試行した、すべてのアクセス ポイントの MAC アドレスを表示します。

  show ap join stats summary all

- 次のコマンドを入力して、特定のアクセス ポイントの最新 join エラーの詳細を表示します。

  show ap join stats summary *ap_mac*

  ap_mac は、802.11 無線インターフェイスの MAC アドレスです。

（注） 802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントで **show interfaces Dot11Radio 0** コマンドを入力します。

以下に類似した情報が表示されます。

```
Is the AP currently connected to controller.............
Yes
Time at which the AP joined this controller last time......
Aug 21 12:50:36.061
Type of error that occurred last.......................
AP got or has been disconnected
Reason for error that occurred last....................
The AP has been reset by the controller
Time at which the last join error occurred.............. Aug
 21 12:50:34.374
```

- 次のコマンドを入力して、特定アクセス ポイントで収集されたすべての join 関連の統計情報を表示します。

  show ap join stats detailed *ap_mac*

  以下に類似した情報が表示されます。

```
Discovery phase statistics
- Discovery requests received.............................. 2
- Successful discovery responses sent...................... 2
- Unsuccessful discovery request processing................ 0
- Reason for last unsuccessful discovery attempt........... Not applicable
- Time at last successful discovery attempt................ Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt.............. Not applicable

Join phase statistics
- Join requests received................................... 1
- Successful join responses sent........................... 1
- Unsuccessful join request processing..................... 1
- Reason for last unsuccessful join attempt................ RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..................... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt................... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.......................... 1
- Successful configuration responses sent.................. 1
- Unsuccessful configuration request processing............ 0
- Reason for last unsuccessful configuration attempt....... Not applicable
- Time at last successful configuration attempt............ Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.......... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure............... Not applicable

Last AP disconnect details
- Reason for last AP connection failure.................... The AP has been reset
by the controller

Last join error summary
```

```
- Type of error that occurred last..... AP got or has been
disconnected
- Reason for error that occurred last..... The AP has been reset
by the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

- 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントの join 統計情報をクリアします。

  clear ap join stats {**all** | *ap_mac*}