Wireless LAN Controller（WLC）の設計と機能に関する FAQ

Document ID: 118833

Updated: 2015 年 3 月 02 日

関連製品

- **Cisco 4400 シリーズ ワイヤレス LAN コントローラ**
- Cisco 5500 シリーズ ワイヤレス コントローラ
- Cisco Wireless Services Module 2（WiSM2）
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco 2100 シリーズ ワイヤレス LAN コントローラ
- Cisco Catalyst 3750 シリーズ統合型ワイヤレス LAN コントローラ
- Cisco Catalyst 6500 シリーズ/7600 シリーズ ワイヤレス サービス モジュール（WiSM）
- **Cisco 2000 シリーズ ワイヤレス LAN コントローラ**
- Cisco ワイヤレス LAN コントローラ モジュール
- **Cisco 4100 シリーズ ワイヤレス LAN コントローラ**
- + 詳細情報

目次

概要

このドキュメントでは、ワイヤレス LAN コントローラ（WLC）で使用できる設計と機能に関して最もよくある質問（FAQ）について説明しています。

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

設計に関する FAQ

Q. WLC と接続するには、スイッチをどのように設定するのですか。

A. WLC が接続されているスイッチ ポートを IEEE 802.1Q トランク ポートとして設定します。 必要な VLAN だけがスイッチで許可されていることを確認してください。 一般的に、WLC の管理インターフェイスと AP マネージャ インターフェイスにはタグが付いていません。 つまり、接続されているスイッチのネイティブ VLAN が想定されます。 これは必要ありません。 これらのインターフェイスには別個の VLAN を割り当てることができます。 詳細は、『*ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本設定例*』の「WLC 用のスイッチの設定」を参照してください。

Q. アクセス ポイント (AP) がコントローラに登録されると、WLAN クライアント間のすべてのネットワーク トラフィックが、ワイヤレス LAN コントローラ (WLC) を経由してトンネリングされるのでしょうか。

A. AP が WLC に結合すると、Control And Provisioning of Wireless Access Points (CAPWAP) プロトコル トンネルが 2 つのデバイス間で形成されます。 すべてのトラフィック (すべてのクライアント トラフィックを含む) が、CAPWAP トンネルを経由して送信されます。

唯一の例外としては、AP が Hybrid REAP モードになっている場合があります。 Hybrid REAP アクセス ポイントは、コントローラへの接続が失われた場合、クライアント データ トラフィックをローカルにスイッチして、ローカルにクライアント認証を行うことができます。 コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

Q. Lightweight アクセス ポイント (LAP) をリモート オフィスに、ワイヤレス LAN コントローラ (WLC) を本社に設置することはできるのですか。 LWAPP/CAPWAP は WAN で動作しますか。

A. はい、AP から WAN を経由する場所に WLC を配置できます。 LWAPP/CAPWAP は、LAP が Remote Edge AP (REAP) モードまたは Hybrid Remote Edge AP (H-REAP) モードに設定されている場合に WAN 上で機能します。 これらのどちらのモードを使用しても、WAN リンク経由で接続されているリモート コントローラからの AP の管理が可能です。 トラフィックはローカルに LAN リンクでブリッジされるため、不要なローカル トラフィックが WAN リンクで送信されることはありません。 これは、ワイヤレス ネットワークで WLC を使用する大きな利点の一つです。

注: すべての Lightweight AP でこれらのモードがサポートされているわけではありません。 たとえば、H-REAP モードは 1131、1140、1242、1250、および AP801 LAP でのみサポートされています。 REAP モードは 1030 AP だけではサポートされていますが、1010 AP と 1020 AP では REAP はサポートされていません。 これらのモードの実装を計画する前に、LAP でこれらのモードがサポートされているかどうかを確認してください。 LWAPP に変換された Cisco IOS® ソフトウェアの AP (Autonomous AP) では、REAP はサポートされていません。

Q. REAP モードおよび H-REAP モードはどのように動作するのですか。

A. **REAP** モードでは、認証トラフィックを含むすべての制御トラフィックと管理トラフィックはトンネルを経由して WLC に戻されます。 しかし、すべてのデータ トラフィックはリモート オフィス LAN 内でローカルにスイッチングされます。 WLC への接続が失われると、最初の WLAN (WLAN1) 以外のすべての WLAN が終了されます。 この最初の WLAN に現在関連付けられているすべてのクライアントは保持されます。 ダウンタイム時にこの WLAN 上で新規のクライアントが認証とサービスの享受に成功するためには、この WLAN の認証方法を WEP または WPA-PSK に設定して、認証が REAP でローカルに実行されるようにします。 REAP 導入についての詳細は、『ブランチオフィスでの REAP 導入ガイド』を参照してください。

H-REAP モードでは、アクセス ポイントによって、認証トラフィックを含むすべての制御トラフィックと管理トラフィックはトンネルを経由して WLC に戻されます。 WLAN が H-REAP ローカル スイッチングに設定されている場合、WLAN からのデータ トラフィックはリモート オフィスでローカルにブリッジされますが、そうではない場合は、データ トラフィックは WLC に戻されます。 WLC への接続が失われると、H-REAP ローカル スイッチングを使用して設定された最初の 8 つの WLAN 以外のすべての WLAN が終了されます。 この最初の 8 つの WLAN に現在関連付けられているすべてのクライアントは保持されます。 ダウンタイム時にこれらの WLAN 上で新規のクライアントが認証とサービスの享受に成功するためには、この WLAN の認証方法を WEP、WPA PSK、または WPA2 PSK に設定して、認証が H-REAP でローカルに実行されるようにします。

H-REAP の詳細は、『H-REAP の設計および導入ガイド』を参照してください。

Q. Remote-Edge AP (REAP) と Hybrid-REAP (H-REAP) の違いは何ですか。

A. REAP では IEEE 802.1Q VLAN タギングがサポートされていません。 したがって、複数の VLAN はサポートされていません。 すべての Service Set Identifier (SSID) からのトラフィックは同じサブネットで終端されますが、H-REAP では IEEE 802.1Q VLAN タギングがサポートされています。 各 SSID からのトラフィックは、一意の VLAN にセグメント化することが可能です。

WLC への接続が失われると (つまり、スタンドアロン モード)、REAP では 1 つの WLAN (つまり、最初の WLAN) だけにサービスが提供されます。 他のすべての WLAN は非アクティブ化されます。 H-REAP では、ダウンタイム時に最大 8 つの WLAN がサポートされます。

もう 1 つの大きな違いは、REAP モードでは、データ トラフィックがローカルでのみブリッジングされることです。 これをセントラル オフィスに戻すことはできませんが、H-REAP モードでは、トラフィックをセントラル オフィスに戻すオプションが提供されます。 H-REAP ローカル スイッチングに設定された WLAN からのトラフィックはローカルにスイッチングされます。 他の WLAN からのデータ トラフィックはセントラル オフィスに戻されます。

REAP の詳細は、『Lightweight AP とワイヤレス LAN コントローラ (WLC) での Remote-Edge AP (REAP) の設定例』を参照してください。

H-REAP の詳細は、『Hybrid REAP の設定』を参照してください。

Q. WLC では WLAN がいくつサポートされますか。

A. ソフトウェア バージョン 5.2.157.0 以来、WLC は Lightweight アクセス ポイント用に 512 までの WLAN を制御できるようになりました。 各 WLAN には個別の WLAN ID (1 ~ 512)、個別のプロファイル名、および WLAN SSID があり、一意のセキュリティ ポリシーを割り当てることができます。 コントローラは接続されたアクセス ポイントごとに最大 16 の WLAN を公開しますが、ユーザはコントローラで最大 512 の WLAN を作成し、アクセス ポイントのグループを使用して、これらの WLAN を別々のアクセス ポイントを選択して公開し、ワイヤレス ネットワークをより効率的に管理します。

注: Cisco 2106、2112、および 2125 コントローラは最大 16 の WLAN にしか対応していません。

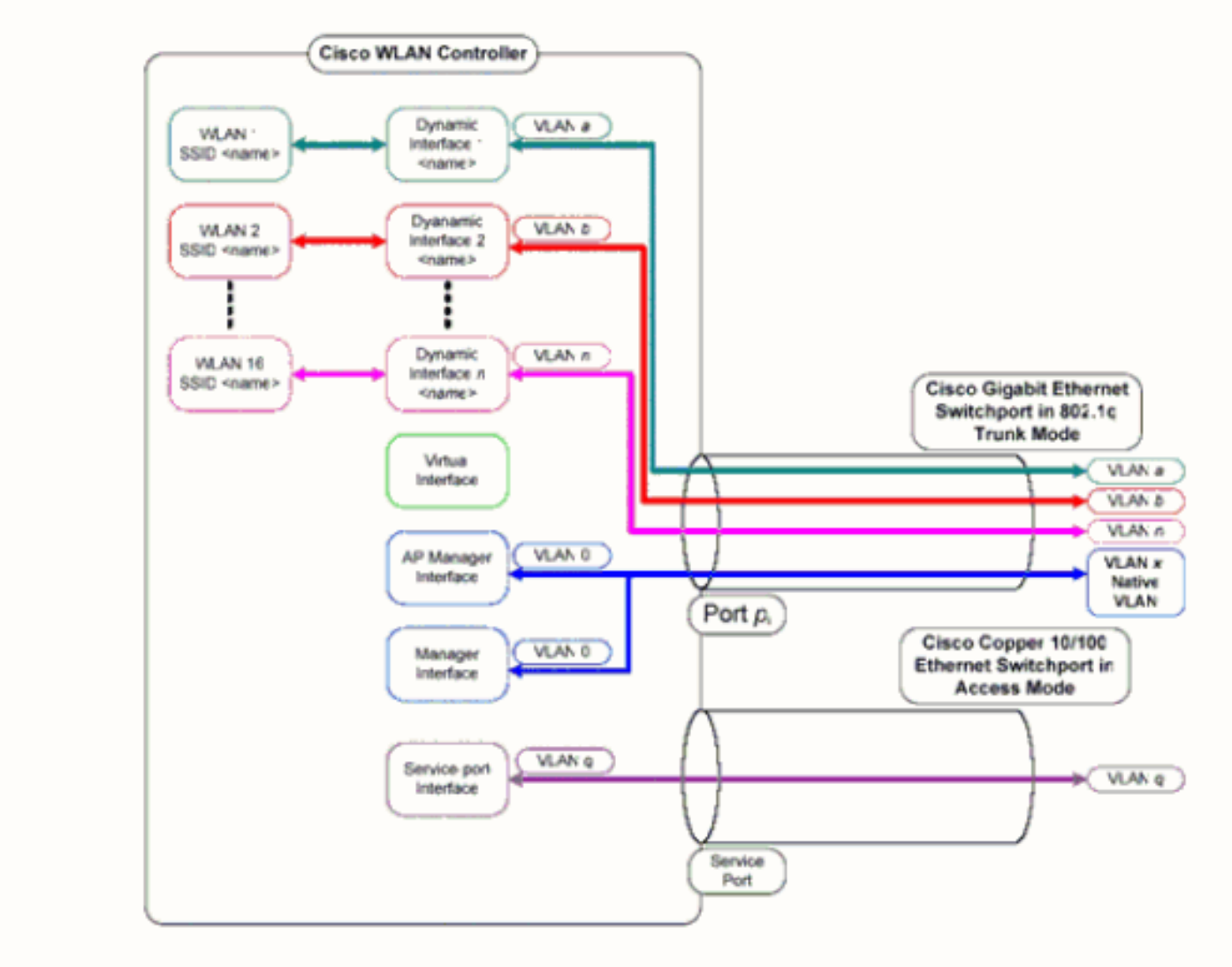
注: WLC で WLAN を設定する場合のガイドラインについて詳しくは、『Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0.116.0』の「WLAN の作成」を参照してください。

Q. WLC で VLAN を設定するには、どのようにすればよいのですか。

A. WLC では、VLAN は一意の IP サブネットに設定されたインターフェイスに関連付けられています。 このインターフェイスは WLAN へマッピングされます。 次に、この WLAN に関連付けられるクライアントが、そのインターフェイスの VLAN へ属し、そのインターフェイスが属するサブネットから IP アドレスが割り当てられます。 WLC で VLAN を設定するには、『ワイヤレス LAN コントローラでの VLAN の設定例』の手順を実行してください。

Q. 2 つの WLAN を、それぞれ異なる 2 つのダイナミック インターフェイスでプロビジョニングしました。 各インターフェイスには、管理インターフェイス VLAN 以外の VLAN が個別に設定されています。 WLAN で使用する VLAN に必要なトランク ポートは、まだプロビジョニングしていないのですが、正しく機能しているように見えます。 アクセス ポイント (AP) が、パケットに管理インターフェイス VLAN のタグを付けているのでしょうか。

A. AP では、パケットに管理インターフェイス VLAN のタグ付けはしていません。 AP は、クライアントから受け取ったパケットを Lightweight AP Protocol (LWAPP) /CAPWAP でカプセル化し、このパケットを WLC に渡します。 続いて WLC は LWAPP/CAPWAP ヘッダーを取り除き、このパケットに適切な VLAN タグを付けてゲートウェイに転送します。 この VLAN タグは、クライアントが属している WLAN によって決まります。 パケットをそれぞれの宛先にルーティングする処理については、WLC はゲートウェイに依存します。 トラフィックが複数の VLAN に送信されるようにするには、アップリンク スイッチをトランク ポートとして設定する必要があります。 次のダイアグラムは、コントローラにより VLAN がどのように機能するかを示しています。



Q. AAA サーバでの認証には、WLC のどの IP アドレスが使用されるのですか。

A. AAA サーバが関連するどの認証メカニズム（レイヤ 2 またはレイヤ 3）でも、WLC では管理インターフェイスの IP アドレスが使用されます。 WLC でのポートとインターフェイスについての詳細は、『*Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0*』の「ポートとインターフェイスの設定」セクションを参照してください。

Q. 1 つの VLAN で、10 台の Cisco 1000 シリーズ Lightweight アクセス ポイント（LAP）と 2 台の WLC を使用しています。 6 台の LAP を WLC1 に、残りの 4 台の LAP を WLC2 に関連付けるには、どのようにすればよいのですか。

A. LWAPP/CAPWAP では動的な冗長性とロード バランシングが可能です。 たとえば、オプション 43 に複数の IP アドレスを指定すると、AP が受信する各 IP アドレスに対して、LAP から LWAPP/CAPWAP ディスカバリ要求が送信されます。 WLC の LWAPP/CAPWAP ディスカバリ応答には、WLC によって次の情報が組み込まれます。

- 現在の LAP の負荷に関する情報（そのとき WLC に加入している LAP の数）
- LAP の容量
- WLC に接続されているワイヤレス クライアントの数

続いて、LAP は、負荷が最小の WLC（使用可能な LAP の容量が最大の WLC）への加入を試みます。 さらに、LAP は、WLC に加入すると、モビリティ グループ内の他の WLC の IP アドレスを加入した WLC から取得します。

いったん LAP が WLC に加入すると、次のリブート時に特定の WLC にその LAP を加入させることができます。 これを実行するには、プライマリ、セカンダリ、および三次の WLC を LAP に割り当てます。 LAP のリブート時にプライマリの WLC が検索され、その WLC 上での負荷状態に関係なく、その WLC への加入が行われます。 プライマリ WLC が応答しない場合はセカンダリが検索されますが、セカンダリも応答しない場合は三次が検索されます。 LAP へのプライマリ WLC の設定方法についての詳細は、『Lightweight アクセス ポイントのための WLAN コントローラのフェールオーバーの設定例』の「*Lightweight AP のためのプライマリ、セカンダリ、ターシャリ コントローラの割り当て*」のセクションを参照してください。

Q. 2100 シリーズ ワイヤレス LAN コントローラ (WLC) でサポートされていない機能は何ですか。

A. 次のハードウェア機能は、2100 シリーズ コントローラではサポートされていません。

- サービス ポート (個別アウトオブバンド管理による 10/100 Mbps イーサネット インターフェイス)

次のソフトウェア機能は、2100 シリーズ コントローラではサポートされていません。

- VPN 終端 (IPSec および L2TP など)
- ゲスト コントローラ トンネルの終端 (ゲスト コントローラ トンネルの開始はサポートされます)
- 外部 Web 認証 Web サーバ リスト
- レイヤ 2 LWAPP
- スパニング ツリー
- ポート ミラーリング
- Cranite
- Fortress
- AppleTalk
- QoS ユーザ別の帯域幅コントラクト
- IPv6 パススルー
- リンク集約 (LAG)
- マルチキャスト ユニキャスト モード
- 有線ゲスト アクセス

Q. 5500 シリーズ コントローラでサポートされていない機能はどれですか。

A. 次のソフトウェア機能は、5500 シリーズ コントローラではサポートされていません。

- スタティック AP マネージャ インターフェイス**注:** 5500 シリーズ コントローラでは、AP マネージャ インターフェイスを設定する必要はありません。 管理インターフェイスがデフォルトで AP マネージャ インターフェイスの役割を果たし、アクセス ポイントはこのインターフェイスに参加できます。
- アシンメトリック モビリティ トンネリング
- スパニング ツリー プロトコル (STP)
- ポート ミラーリング
- レイヤ 2 アクセス コントロール リスト (ACL) のサポート
- VPN 終端 (IPSec および L2TP など)
- VPN パススルー オプション

- 802.3 ブリッジ、AppleTalk、および Point-to-Point Protocol over Ethernet（PPPoE）の設定

Q. メッシュ ネットワークでサポートされていない機能はどれですか。

A. 次の機能は、メッシュ ネットワークでサポートされていません。

- 複数の国のサポート
- ロード ベースの CAC（メッシュ ネットワークは帯域幅ベース、またはスタティックの CAC のみサポートしています）
- ハイ アベイラビリティ（高速ハートビートおよびプライマリ検出 join タイマー）
- EAP-FASTv1 および 802.1X 認証
- アクセス ポイント参加優先度（メッシュ アクセス ポイントには固定優先度があります）
- ローカルで重要な証明書
- ロケーション ベース サービス

Q. ワイヤレス LAN コントローラの製造業者インストール済み認証（MIC）と lightweight AP 認証の有効期間とは何か。

A. WLC の MIC の有効期間は 10 年です。 10 年の同じ有効期間は作成から lightweight AP に（それが MIC または自己署名証明書（SSC）であるかどうか）認証を加えます。

Q. 2 つのワイヤレス LAN コントローラ（WLC）を WLC1 と WLC2 という名前で、フェールオーバー用に同じモビリティ グループ内に設定しています。 Lightweight アクセス ポイント（LAP）は、現在、WLC1 に登録されています。 WLC1 に障害が発生した場合、WLC1 に登録されている AP は、稼働している WLC（WLC2）に移行するときにリブートするのでしょうか。 また、このフェールオーバー中は、WLAN クライアントでは LAP との WLAN 接続が失われるのでしょうか。

A. はい、WLC1 で障害が発生した場合、LAP は WLC1 での登録が解除されてリブートされ、WLC2 に再登録されます。 LAP がリブートされるため、関連付けられている WLAN クライアントでは、リブート中の LAP への接続が失われます。 関連情報は、『Unified Wireless Network での AP ロード バランシングおよび AP フォールバック』を参照してください。

Q. ローミングは、WLC で使用するように設定されている Lightweight Access Point Protocol（LWAPP）モードに依存しますか。 レイヤ 2 LWAPP モードで動作している WLC は、レイヤ 3 ローミングを実行できるのですか。

A. コントローラでモビリティ グループが正しく設定されていれば、クライアントのローミングは正常に実行されます。 ローミングが、LWAPP モード（レイヤ 2 とレイヤ 3 のいずれの場合も）の影響を受けることはありません。 しかし、できればレイヤ 3 LWAPP の使用が推奨されます。

注: レイヤ 2 モードは、WLC の Cisco 410x と 440x シリーズおよび Cisco 1000 シリーズ アクセス ポイントのみでサポートされます。 レイヤ 2 LWAPP は、その他のワイヤレス LAN コントローラおよび Lightweight アクセス ポイント プラットフォームでサポートされません。

Q. クライアントが新しい AP またはコントローラへローミングすることを決定した

際には、どのようなローミング処理が行われるのですか。

A. クライアントが新しい AP にローミングするときには、次に示す一連のイベントが発生します。

1. クライアントから LAP 経由で WLC に再関連付け要求が送信されます。
2. 元々、どの WLC にクライアントが関連付けられていたのかを確認するために、WLC からモビリティ グループ内の他の WLC にモビリティ メッセージが送信されます。
3. 元の WLC からは、クライアントに関する MAC アドレス、IP アドレス、QoS、セキュリティ コンテキストなどの情報がモビリティ メッセージで応答されます。
4. WLC は提供されたクライアントの詳細でデータベースを更新します。 続いてクライアントは、必要に応じて再認証プロセスに進みます。 クライアントが現在関連付けられている新規の LAP も、WLC のデータベース内の他の詳細情報に従ってアップデートされます。 この方法によって、WLC 間でローミングを行ってもクライアント IP アドレスが維持され、中断のないローミングの提供に役立ちます。

統合環境でのローミングについての詳細は、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』の「*モビリティ グループの設定*」セクションを参照してください。

注: ワイヤレス クライアントは、再関連付けの間に（802.11）認証要求を送信しません。 ワイヤレス クライアントは、再関連付けをすぐに送信するのみです。 その後で、802.1x 認証を実行します。

Q. ネットワークにファイアウォールが存在する場合、LWAPP/CAPWAP の通信のために、どのポートを許可する必要があるのですか。

A. 次のポートを有効にする必要があります。

- LWAPP トラフィックのために次の UDP ポートを有効にします。データ トラフィック：12222制御トラフィック：12223
- 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 トラフィック：5247制御トラフィック：5246
- 次の UDP ポート（モビリティ トラフィック）をイネーブルにします。16666：セキュア モード16667：非セキュア モード

通常、モビリティ メッセージとデータ メッセージは EtherIP パケット通じて交換されます。EtherIP パケットを許可するためには、**IP protocol 97** がファイアウォール上で許可されている必要があります。 モビリティ パケットをカプセル化するために **ESP** を使用する場合、**UDP port 500** を開く際に **ISAKMP** によるファイアウォールの通過を許可する必要があります。 また、暗号化データのファイアウォールの通過を許可するには、**IP protocol 50** を開く必要もあります。

次のポートはオプションです（必要に応じて有効にしてください）。

- 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）。
- 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 またはセキュア シェル（SSH）。CLI アクセスで使用）

Q. ワイヤレス LAN コントローラは SSHv1 と SSHv2 の両方をサポートしています

か。

A. ワイヤレス LAN コントローラは SSHv2 のみサポートしています。

Q. 逆アドレス解決プロトコル（RARP）は、WLC 経由ではサポートされるのですか。

A. 逆アドレス解決プロトコル（RARP）は、イーサネット アドレスなどの特定のリンク レイヤ アドレスの IP アドレスを取得するのに使用されるリンク レイヤ プロトコルです。 RARP は、ファームウェアのバージョンが 4.0.217.0 以降の WLC でサポートされています。 これよりも前のバージョンでは、RARP はサポートされていません。

Q. WLC の内部 DHCP サーバを使用して、Lightweight アクセス ポイント（LAP）に IP アドレスを割り当てることはできるのですか。

A. コントローラには内部 DHCP サーバが含まれます。 このサーバは、通常、DHCP サーバをまだ持っていないブランチ オフィスで使用されます。 DHCP サービスにアクセスするには、WLC の GUI から [Controller] メニューをクリックします。 次に、ページの左側の [Internal DHCP Server] オプションをクリックします。 WLC で DHCP スコープを設定する方法の詳細は、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』の「*DHCP の設定*」セクションを参照してください。

この内部サーバからは、ワイヤレス クライアント、LAP、管理インターフェイスのアプライアンス モード AP、および LAP から中継される DHCP 要求に対し、DHCP アドレスが提供されます。 WLC では、有線ネットワーク内のアップストリームのデバイスに対してのアドレスの提供は行われません。 DHCP オプション 43 は内部サーバではサポートされていないため、AP では、ローカル サブネット ブロードキャスト、DNS、プライミング、地上波（Over-the-Air）ディスカバリなどの代替手段を使用して、コントローラの管理インターフェイスの IP アドレスを特定する必要があります。

注: バージョン 4.0 よりも前の WLC ファームウェアでは、LAP が WLC に直接接続されている場合を除き、LAP に対する DHCP サービスはサポートされていません。 内部 DHCP サーバの機能は、ワイヤレス LAN ネットワークに接続するクライアントに IP アドレスを提供するためにのみ使用されていました。

Q. WLAN における DHCP Required フィールドは何を示しているのですか。

A. DHCP Required は、WLAN にイネーブルにできるオプションです。 このオプションによって、特定の WLAN に関連付けられるすべてのクライアントは DHCP を通じて IP アドレスを取得することが必要になります。 固定 IP アドレスが割り当てられているクライアントは、WLAN への関連付けが許可されません。 このオプションは、WLAN の [Advanced] タブにあります。 WLC では、クライアントとの送受信トラフィックは、その IP アドレスが WLC の MSCB テーブルに存在する場合にのみ許可されます。 WLC では、DHCP 要求または DHCP 更新の間にクライアントの IP アドレスが記録されます。 ローミング プロセスやセッション タイムアウトの一環で、クライアントで関連付けが解除されるたびに、そのエントリが MSCB テーブルから消去されるため、WLC へ再度関連付けられるたびにクライアントによる IP アドレスの更新が必要になります。 クライアントでは WLC に対する再認証と再度の関連付けが必要であり、これによってクライアント エントリがテーブル内に再度作成されます。

Q. Cisco Centralized Key Management（CCKM）は LWAPP/CAPWAP 環境でどの

ように動作しますか。

A. ワイヤレス クライアントが 802.1x 認証に成功した後は、初期クライアント関連付けの間に、AP または WLC が Pair-wise Master Key (PMK) をネゴシエートします。 WLC または WDS AP は、クライアントごとに PMK をキャッシュします。 ワイヤレス クライアントが再関連付けまたはローミングを行うときは、802.1x 認証を省略して、PMK をただちに検証します。

CCKM での WLC の唯一の特別な実装は、WLC が UDP 16666 などのモビリティ パケットを介して、クライアントの PMK を交換することです。

Q. WLC と LAP でデュプレックスを設定するには、どのようにすればよいのですか。

A. シスコのワイヤレス製品は速度とデュプレックスの両方を自動ネゴシエートするときに最善に動作しますが、WLC および LAP でデュプレックスを設定することもできます。 AP の速度とデュプレックスを設定するには、コントローラで LAP のデュプレックスを設定した後、それを LAP にプッシュできます。

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> は、CLI を介してデュプレックスを設定するコマンドです。このコマンドは、バージョン 4.1 以降でのみサポートされています。

WLC の物理インターフェイスにデュプレックスを設定するには、config port physicalmode {all | port} {100h | 100f | 10h | 10f} コマンドを使用します。

このコマンドは、指定されたフロントパネル 10/100BASE-T イーサネット ポートまたは全部のフロントパネル 10/100BASE-T イーサネット ポートを、10 Mbps または 100 Mbps、半二重または全二重の動作専用に設定します。 ポートの物理モードを手動で設定するには、先に、config port autoneg disable コマンドで自動ネゴシエートをディセーブルにする必要があることに注意してください。 また、config port autoneg コマンドは、config port physicalmode コマンドで行われた設定より優先されることにも注意してください。 デフォルトでは、すべてのポートが自動ネゴシエートに設定されています。

注: ファイバ ポートの速度設定を変更する手段はありません。

Q. LAP がコントローラに登録されていない場合に、その名前を追跡する手段はあるのですか。

A. AP が完全にダウンしていて、コントローラに登録されていない場合、コントローラを通して LAP を追跡できる手段はありません。 残されている唯一の手段は、AP が接続されているスイッチにアクセスできる場合は、次のコマンドを使用して AP が接続されているスイッチポートを検索することです。

show mac-address-table address *<mac address>*
これにより、その AP が接続されているスイッチのポート番号がわかります。 続いて、次のコマンドを発行します。

show cdp nei *<type/num>* **detail**
このコマンドの出力からは、LAP の名前もわかります。 ただし、この方法は、AP の電源が入っていて、スイッチに接続されている場合にしか使用できません。

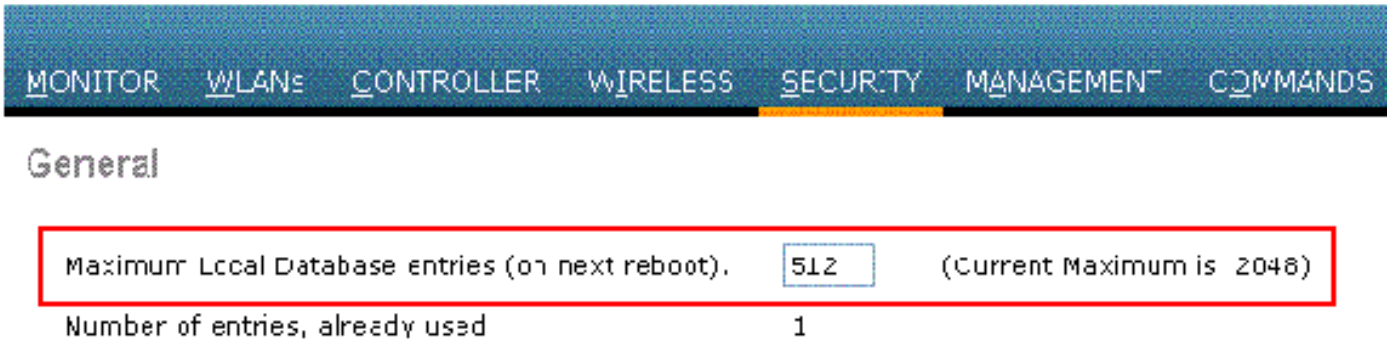
Q. コントローラに 512 人のユーザを設定してあります。 WLC のユーザ数を増やす方法はあるのですか。

A. ローカル ユーザ データベースは、[Security] > [General] ページで最大 2048 エントリに制限されています。 このデータベースは、ローカル管理ユーザ（Lobby Ambassador を含む）、ネット ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、アクセス ポイント認可リスト エントリ、除外リスト エントリで共有されます。 これらのすべてのタイプのユーザの合計が、設定されているデータベース サイズを超えることはできません。

ローカル データベースを増やす場合は、CLI から次のコマンドを使用します。

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

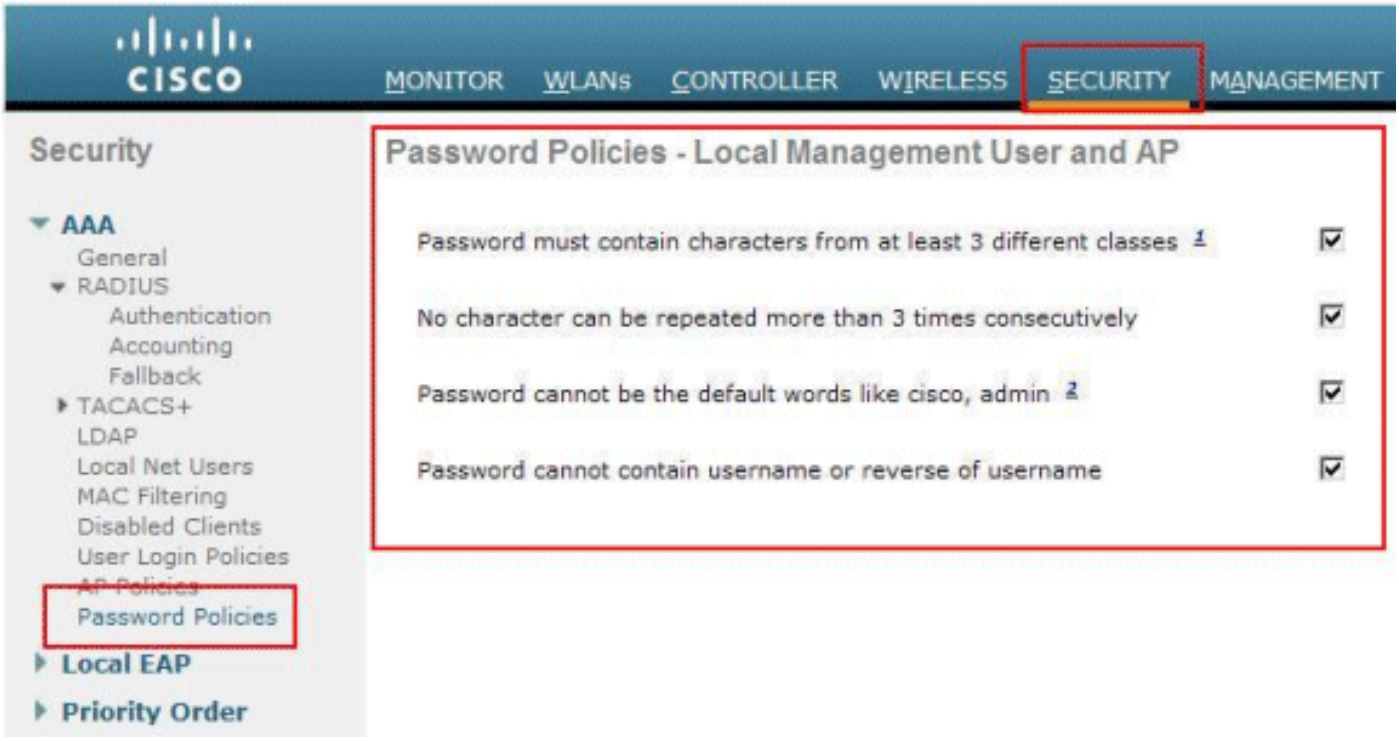
注: 変更を有効にするには、設定を保存してシステムをリセットする（**reset system** コマンドを使用）必要があります。



Q. WLC ではどのようにして強力なパスワード ポリシーを実施しますか。

A. WLC では強力なパスワード ポリシーを定義できます。 これは、CLI か GUI のいずれかを使用して実行できます。

GUI では、[Security] > [AAA] > [Password Policies] に移動します。 このページには一連のオプションがあり、これを選択して強力なパスワードを実施できます。 次に例を示します。



これを WLC CLI から実行するには、**config switchconfig strong-pwd {case-check** | *consecutive-check* | *default-check* | *username-check* | *all-check}* {*enable* | **disable}** コマンドを使用します。

- **case-check** - 同じ文字が 3 回 連続して発生することを確認します。
- **consecutive-check** - デフォルト値または そのバリアントが使用されているかどうかを確認します。
- **default-check** - ユーザ名または その反転が使用されているかどうかを確認します。
- **all-checks** - すべての強力なパスワードが イネーブルまたはディセーブルになっているかどうかを確認します。

Q. パッシブ クライアント機能はワイヤレス LAN コントローラでどのように使用されますか。

A. パッシブ クライアントは、スタティック IP アドレスを使用して設定される スケールやプリンタなどのワイヤレス デバイスです。 これらのクライアントは、アクセス ポイントに 関連付けられたときに、IP アドレス、サブネット マスク、ゲートウェイ情報 などの IP 情報を送信しません。 その結果、パッシブ クライアントが使用されている場合、 クライアントが DHCP を使用していない限り、コントローラは IP アドレスを認識しません。

現在、WLC は ARP 要求のプロキシとして動作します。 コントローラは、 ARP 要求を受信したときに、この要求を直接クライアントに渡すのではなく、 ARP 応答を使用して応答します。 このシナリオには、次の 2 つの利点があります。

- クライアントに ARP 要求を送信するアップストリーム デバイスは、 クライアントが配置されている場所を認識しません。
- 携帯電話やプリンタなどの電池式デバイスの電源は、 すべての ARP 要求に応答する必要がないため 保持されます。

ワイヤレス コントローラには、パッシブ クライアントの IP 関連情報がないため、 すべての ARP 要求に応答できません。 現在の 動作では、パッシブ クライアントへの ARP 要求の転送は許可されません。 [Any] アプリケーションによるパッシブ クライアントへのアクセス試行も失敗します。

パッシブ クライアント機能により、有線クライアントとワイヤレス クライアント間 で交換される ARP 要求と応答がイネーブルになります。 この機能がイネーブルの場合、 コントローラは、目的のワイヤレス クライアントが RUN 状態になるまで、 有線クライアントからワイヤレス クライアントに ARP 要求を渡すことができます。

パッシブ クライアント機能を設定する方法の 詳細については、 「GUI を使用した パッシブ クライアントの設定」セクション（『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』にあります）を参照してください。

Q. 3 分ごとまたは指定した時間間隔で、RADIUS サーバを使用して再認証を行うには、 どのようにクライアントを設定すればよいですか。

A. これを実現するには、WLC のセッション タイムアウト パラメータを 使用できます。 デフォルトでは、再認証が実行されるまでのセッション タイムアウト パラメータ は 1800 秒に設定されています。

この値を 180 秒に変更すると、クライアントが 3 分後に 再認証されるようになります。

セッション タイムアウト パラメータにアクセスするには、GUI で [WLAN] メニューをクリックします。 WLC で設定された WLAN の 一覧が表示されます。 クライアントが属する WLAN をクリックします。 次に [Advanced] タブに移動すると、[Enable Session Timeout] パラメータが表示されます。 デフォルト値を 180 に変更して、 [Apply] をクリックして変更を有効にします。

RADIUS-Request の Termination-Action 値とともに Access-Accept で送信される場合、 Session-Timeout 属性は、再認証までに提供される サービスの最大秒数を指定します。 この場合、Session-Timeout 属性は、802.1X の Reauthentication Timer 状態マシン 内で ReAuthPeriod 定数をロードするために使用されます。

Q. ゲスト トンネリングと Ethernet over IP（EoIP）トンネルが、 アンカー WLC として機能する 4400 ワイヤレス LAN コントローラ（WLC）と 複数のリモート WLC 間に設定されています。 このアンカー WLC では、リモート コントローラに関連付けられたワイヤレス クライアントに、有線ネットワークから EoIP トンネルを経由して サブネット ブロードキャストを転送できるのですか。

A. いいいえ、WLC 4400 では、EoIP トンネルを介して有線側から ワイヤレス クライアントに IP サブネット ブロードキャストを転送することはありません。 この機能はサポートされて いません。 シスコでは、サブネット ブロードキャストのトンネリングやゲスト アクセス トポロジでのマルチキャストは サポートされません。 ゲスト WLAN では、クライアントのアクセス ポイントが ネットワーク（主にファイアウォールの外側）の特定の位置に強制的に置かれるため、 サブネット ブロードキャストのトンネリングは、セキュリティ上の問題となる可能性があります。

Q. ワイヤレス LAN コントローラ（WLC）と Lightweight Access Point Protocol（LWAPP） の設定では、音声トラフィックに、どのような DiffServ コード ポイント（DSCP）値が 渡されるのですか。 WLC で、QoS はどのように実装されるのですか。

A. Cisco Unified Wireless Network（UWN）Solution WLAN では、次の 4 レベルの QoS が サポートされています。

- Platinum/音声

- Gold/ビデオ
- Silver/ベスト エフォート（デフォルト）
- Bronze//バックグラウンド

音声トラフィックの WLAN では Platinum QoS を使用するように設定し、 低帯域幅の WLAN には Bronze QoS を使用するように割り当て、 それ以外のすべてのトラフィックには他の QoS レベルを割り当てることができます。 PortFast を有効にする方法の詳細については、 「WLAN への QoS プロファイルの割り当て」を参照してください。

Q. Linksys イーサネット ブリッジは、Cisco Wireless Unified Solution ではサポートされて いるのですか。

A. いいえ。WLC でサポートされているのは Cisco WGB 製品だけです。 Linksys WGB は サポートされていません。 Cisco Wireless Unified Solution は Linksys WET54G および WET11B イーサネット ブリッジをサポートしていませんが、次のガイドラインを 使用すれば、Wireless Unified Solution 構成でこれらのデバイスを使用できます。

- WET54G または WET11B には 1 つのデバイスのみを接続します。
- WET54G または WET11B の MAC クローニング機能をイネーブルにして、接続されているデバイスのクローンを作成します。
- WET54G または WET11B に接続されているデバイスに、最新のドライバまたは ファームウェアをインストールします。 このガイドラインは、JetDirect プリンタに対して特に重要です。 古いファームウェア バージョンでは、DHCP に関する問題が発生します。

注: 他のサードパーティ製ブリッジはサポートされていません。 説明した手順は、 他のサードパーティ製ブリッジにも試すことができます。

Q. ワイヤレス LAN コントローラ（WLC）でコンフィギュレーション ファイルを保存するには、 どのように動作するのですか。

A. WLC には次の 2 種類のメモリが含まれています。

- 揮発性 RAM：現在のアクティブ コントローラの 保持します
- 不揮発性 RAM（NVRAM）：リブートの設定を 保持します

WLC でオペレーティング システムを設定する場合は、 揮発性 RAM を修正します。 WLC を確実に現在の設定でリブートするには、 揮発性 RAM から NVRAM に設定を保存する必要があります。

以下のタスクを実行する際に、どのメモリが変更されるかを理解すること が重要です。

- 設定ウィザードの使用
- コントローラ設定のクリア
- 設定の保存
- コントローラのリセット
- CLI からのログアウト

各機能に関する FAQ

Q. WLC で Extensible Authentication Protocol（EAP）タイプを設定するには、 の用途は何ですか。 Access Control Server（ACS）アプライアンス に対して認証を

実行すると、 ログに「unsupported EAP」タイプと表示されてしまいます。

A. WLC では、個別の EAP タイプの設定はありません。 Light EAP (LEAP)、 EAP Flexible Authentication via Secure Tunneling (EAP-FAST)、または Microsoft Protected EAP (MS-PEAP) の場合は、 単に、IEEE 802.1x または Wi-Fi Protected Access (WPA) (802.1x と WPA を一緒に使用する場合) を設定してください。 クライアントおよび RADIUS のバックエンドで サポートされている すべての EAP タイプは、802.1x のタグでサポートされています。 EAP の設定は、 クライアントと RADIUS サーバで一致している必要があります。

WLC の GUI から EAP をイネーブルにするには、 次の手順を実行します。

1. WLC の GUI で、 [WLAN] をクリックします。
2. WLC 上で設定されている WLAN のリストが表示されます。 該当する WLAN をクリックします。
3. [WLAN] > [Edit] で、 [Security] タブをクリックします。
4. [Layer 2] をクリックし、[Layer 2 Security] に [802.1x] または [WPA+WPA2] を選択します。 また、このウィンドウでは、802.1x の使用可能なパラメータを 設定することもできます。 これで、WLC は、ワイヤレス クライアントと認証サーバ間の EAP 認証 パケットを転送するようになります。
5. AAA サーバをクリックして、 この WLAN のドロップダウン メニューから認証サーバを選択します。 認証サーバは すでにグローバルに設定されているものと仮定します。 Fast SSID Changing を で WLC の EAP オプションをイネーブルにする 方法についての詳細は、「*RADIUS を設定するための CLI の使用方法*」 」セクション (『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』にあります) を参照してください。

Q. Fast SSID Changing とは何ですか。

A. Fast SSID Changing を使用して、クライアントは SSID 間を移動できます。 設定が完了したら、 クライアントが異なる SSID の新しいアソシエーションを送信すると、 クライアントが新しい SSID に追加される前に、コントローラ接続テーブルの SSID] に設定します。 Fast SSID Changing をディセーブルにすると、 クライアントが新しい SSID に移動できるようになる前に、コントローラが遅延を強制します。 Fast SSID Changing を イネーブルにする方法についての詳細は、 「*ポートと の設定*」 」セクション (『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』にあります) を参照してください。

Q. ワイヤレス LAN に接続できるクライアント数の制限を 設定できますか。

A. WLAN に接続できるクライアントの数に制限を設定できます。 これは、コントローラに接続できるクライアント数が限られている 場合に便利です。 WLAN ごとに設定できるクライアント数は、 使用しているプラットフォームによって異なります。

各種プラットフォームの WLAN ごとのクライアント数の詳細は、 「TACACS+ クライアントの最大数の設定」セクション (『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』 にあります) を参照してください。

Q. PKC とは何ですか。ワイヤレス LAN コントローラ (WLC) で どのように動作するのですか。

A. PKC は Proactive Key Caching の略です。 これは IEEE 802.11i 標準の 拡張機能として設計されたものです。

PKC は、Cisco 2006/410x/440x シリーズ コントローラで使用できる機能で、 ワイヤレス クライアントに正しく実装すると、AAA サーバで完全な再認証を実行しなくても、 ローミングが実行できるようになります。 PPKC を理解するには、 まず Key Caching を理解する必要があります。

Key Caching は、WPA2 に追加された機能です。 この機能を使用すると、 モバイル ステーションは、アクセス ポイント（AP）への認証が成功したときに取得したマスター鍵（Pairwise Master Key（PMK））をキャッシュしておき、 **後で同じ AP への関連付けを実行するときに、この鍵を再利用できます**。 つまり、特定のモバイル デバイスで、 個々の AP に対する認証が必要なのは 1 回だけで、 後からの使用に備えて鍵がキャッシュされます。 Key Caching は、PMK 識別名（PMKID）と呼ばれるメカニズムを使用して 処理されます。PMKID は、PMK のハッシュとなる文字列で、ステーション と AP の MAC アドレスで構成されます。 PMKID により、PMK は一意に識別されます。

Key Caching を使用しても、ワイヤレス ステーションは、 サービスを受ける各 AP に対して、認証を実行する必要があります。 これが原因で、深刻な遅延やオーバーヘッドが発生し、 引き渡しの処理が遅延して、リアルタイム アプリケーションをサポートするための処理能力に 悪影響を与えてしまうことになります。 この問題を解決するため、 PKC が WPA2 に導入されました。

PKC を使用すると、ステーションは、以前に認証処理が成功したときに 取得した PMK を再利用できるようになります。 これにより、ローミング時に新しい AP に対して 認証を実行する必要がなくなります。

したがって、コントローラ内のローミング、つまりモバイル デバイスがある AP から 同じコントローラの別の AP に移動するとき、クライアントは、 以前に使用した PMK を使用して PMKID を再計算し、関連付けの処理時にはこの PMKID を提示します。 WLC では、その PMK キャッシュを検索して、該当するエントリがあるかどうかを確認します。 エントリがあれば、 802.1x 認証処理はバイパスされ、すぐに WPA2 の 鍵交換が開始されます。 保有していない場合は、標準の 802.1X 認証 処理が実行されます。

PKC は、WPA2 ではデフォルトでイネーブルになっています。 そのため、WLC の WLAN 設定で レイヤ 2 セキュリティとして WPA2 をイネーブルにすると、 の WLC に加入します。 また、AAA サーバとワイヤレス クライアントを適切な EAP 認証に合わせて 設定してください。

また、PKC を使用するには、クライアント側で使用するサプリカントが WPA2 を サポートしている必要があります。 PKC は、コントローラ間のローミング環境でも 実装が可能です。

注: PKC は、Aironet Desktop Utility（ADU）では、クライアント サプリカントとして 機能しません。

Q. コントローラのタイムアウト設定について教えてください。 アドレス解決プロトコル（ARP）タイムアウト、ユーザ アイドル タイムアウト、セッション タイムアウト とは何ですか。

A. **ARP タイムアウト**、WLC で、ネットワークから学習された デバイスの ARP エントリを削除するために使用されます。

ユーザ アイドル タイムアウト： ユーザ アイドル タイムアウトとして 設定された時間内に LAP との通信が行われず、ユーザがアイドル状態の場合、 WLC によってクライアントに対する認証が解除されます。 クライアントは、WLC への再認証と 再関連付けが必要になります。 これは、

LAP に通知することなく、関連付けられた LAP から クライアントがドロップされる可能性がある状況で使用されます。 これが発生する可能性があるのは、 クライアントでバッテリが完全になくなった場合やクライアントの関連付けが削除された場合です。

注: WLC の GUI で ARP とユーザ アイドル タイムアウトにアクセスするには、 [Controller] メニューを開きます。 左側で [General] を選択して、 [ARP] フィールドと [User Idle Timeout] フィールドを表示します。

セッション タイムアウトは、WLC を使用したクライアント セッション の最大時間です。 この時間を超えると、WLC によってクライアントの認証が解除され、 クライアントにはすべての認証（再認証）プロセスが再度発生します。 これは、暗号鍵のローテーションのためのセキュリティ予防策の一部です。 EMM をディセーブルにすると、 で Extensible Authentication Protocol（EAP）方式を使用する場合、 新しい暗号鍵を得るために鍵の再生成が一定の間隔ごとに 発生します。 鍵管理をしない場合、このタイムアウト値はワイヤレス クライアントが 完全な再認証を行うのに必要とする時間です。 セッション タイムアウトは、 WLAN 固有です。 このパラメータは、[WLAN] > [Edit] メニューからアクセスできます。

Q. RFID システムとは何ですか。 シスコでは、どの RFID タグが現在サポートされているのですか。

A. Radio Frequency Identification（RFID）は、 非常に短距離の通信用に無線周波数通信が使用されるテクノロジーです。 基本的な RFID システムは、 RFID タグ、RFID リーダ、および処理ソフトウェアから構成されます。

現在、シスコでは AeroScout 社と Pango 社の RFID タグがサポートされています。 多くのため設定方法についての詳細は、 「AeroScout RFID タグ のための WLC 設定」を参照してください。

Q. WLC でローカルに EAP 認証を実行できますか。 この ローカル EAP 機能が説明されたドキュメントはあるのですか。

A. はい。EAP 認証を WLC でローカルに実行することができます。 ローカル EAP は 認証方法であり、これを使用して、ユーザとワイヤレス クライアント を WLC でローカルに認証できます。 この機能は、バックエンド システムが 中断したり外部認証サーバが停止したりした場合でもワイヤレス クライアント との接続を維持する必要があるリモート オフィスでの使用を想定して作られています。 ローカル EAP をイネーブルにすると、 WLC は認証サーバとして機能します。 多くのため の EAP-Fast 認証用に WLC を設定する方法 方法についての詳細は、 「ワイヤ レス LAN コントローラでの EAP-FAST および LDAP サーバを使用したローカル EAP 認証 の設定例」を参照してください。

Q. WLAN オーバーライド機能とは何ですか。 この機能を設定するにはどうすればよいのでしょうか。 LAP では、 バックアップ WLC へフェールオーバーする際に、WLAN オーバーライド値が 設定できるのですか。

A. WLAN オーバーライド機能を使用すると、個々の LAP 上でアクティブに 使用できる WLC 上に設定された WLAN からの WLAN の選択が可能になります。 WLAN オーバーライド機能を設定するには、次の手順を実行します。

1. WLC の GUI で、[Wireless] メニュー クリックします。
2. 左側にあるオプション [Radios] をクリックして、 [802.11 a/n] または [802.11 b/g/n] を選択

します。
3. WLAN オーバーライド機能を設定する AP の名前に対応する、右側に表示されるドロップダウン メニューから [Configure] リンク をクリック します。
4. [WLAN Override] ドロップダウン メニューから [Enable] を クリックします。 [WLAN Override] メニューは、ウィンドウの 左側の最後の項目です。
5. WLC で設定されているすべての WLAN のリスト が表示されます。
6. リストから、LAP に表示する **WLAN** にチェック マークを付け、 [Apply] をクリックして変更を 有効にします。
7. これらの変更を行ったら、 設定を保存します。

オーバーライドする WLAN プロファイルと SSID が すべての WLC に設定されている場合は、AP が他の WLC に登録されると、AP によって WLAN オーバーライド値 が維持されます。

注: コントローラ ソフトウェア リリース 5.2.157.0 では、WLAN オーバーライド機能が コントローラ GUI と CLI の両方から削除されています。 コントローラが WLAN オーバーライド用に設定され、 コントローラ ソフトウェア リリース 5.2.157.0 へアップグレードする場合、 コントローラによって WLAN 設定が削除され、 すべての WLAN がブロードキャストされます。 アクセス ポイント グループを設定すると、 特定の WLAN だけが送信されるように指定することができます。 各アクセス ポイントでは、そのアクセス ポイント グループに属する WLAN で イネーブルになっているものだけがアドバタイズされます。

注: アクセス ポイント グループは、AP の無線インターフェイスごとに 送信される WLAN をイネーブルにしません。

Q. IPv6 は Cisco ワイヤレス LAN コントローラ（WLC）と Lightweight Access Point（LAP）でサポートされているのですか。

A. 現在、4400 および 4100 シリーズ コントローラでサポートされているのは、 IPv6 のクライアント パススルーだけです。 ネイティブの IPv6 サポートは、サポートされていません。

WLC で IPv6 をイネーブルにするには、[WLAN] > [Edit] ページで WLAN SSID 設定の [IPv6 Enable] チェックボックス にチェックマークを入れます。

さらに、IPv6 をサポートするためには Ethernet Multicast Mode（EMM）が必要です。 EMM をディセーブルにすると、 IPv6 を使用するクライアント デバイスは接続できません。 EMM をイネーブルにするには、 [Controller] > [General] ページの順に移動し、[Ethernet Multicast Mode] ドロップ ダウン メニューから、 [Unicast] または [Multicast] を選択してください。 これにより、ユニキャスト モードまたは マルチキャスト モードのどちらかでマルチキャストがイネーブルにされます。 マルチキャストがマルチキャスト ユニキャストとしてイネーブルにされる場合、 パケットは各 AP のために複製されます。 これはプロセッサに負荷がかかる可能性があるため、 注意して使用してください。 マルチキャスト マルチキャストとしてイネーブルにされたマルチキャストでは、 AP に対してより従来型のマルチキャストを行うために、ユーザによって割り当てられるマルチキャスト アドレスが使用されます。

注: IPv6 は 2006 コントローラではサポートされません。

また、Cisco Bug ID CSCsg78176 があり、AAA Overrride 機能が 使用されている場合に IPv6 パススルーが使用できなくなります。

Q. Cisco 2000 シリーズの WLC では、 ゲスト ユーザの Web 認証がサポートされているのですか。

A. Web 認証は、すべての Cisco WLC でサポートされています。 Web 認証 簡単な認証クレデンシャルでユーザを認証するために 使用されるレイヤ 3 認証方式です。 暗号化は含まれていません。 この機能をイネーブルにするには、 次の手順を実行します。

1. GUI で、[WLAN] メニューを クリックします。
2. 該当する **WLAN** をクリックします。
3. [Security] タブに移動し、[Layer] を選択します。 **3.**
4. [Web Policy] ボックスにチェックマークを入れ、 [Authentication] を選択します。
5. [Apply] をクリックして変更を保存します。
6. ユーザを認証するために照会するデータベースを WLC に作成するには、 GUI で [Security] メニューに移動し、 [Local Net User] を選択して、次の手順を実行します。 ゲストがログインするときに使用するゲスト ユーザ名とパスワードを 定義します。 これらの値では大文字と小文字が区別されます。使用する WLAN ID を選択します。**注:** 設定についての詳細は、「 LAN コントローラの Web 認証の設定例」を参照してください。

Q. WLC をワイヤレス モードで管理できますか。

A. ワイヤレス モードをイネーブルにすれば、WLC をワイヤレス モードで管理できます。 多くのため ワイヤレス モードをイネーブルにする方法については、「*GUI および CLI への ワイヤレス接続をイネーブルにする*」 」セクション（『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』にあります）を参照してください。

Q. リンク集約（LAG）とは何ですか。 WLC で LAG をイネーブルにするには、 どのようにすればよいのですか。

A. LAG では、WLC 上のすべてのポートが 1 つの EtherChannel インターフェイスに バンドルされます。 システムによってトラフィックのロード バランシングと LAG のポート の冗長性が動的に管理されます。

一般的に WLC のインターフェイスには、IP アドレス、デフォルト ゲートウェイ（IP サブネット用）、 プライマリの物理ポート、セカンダリの物理ポート、VLAN タグ、および DHCP サーバなど、 それに関連付けられた複数のパラメータがあります。 LAG が使用されない場合は、 通常、各インターフェイスが物理ポートへマッピングされますが、複数のインターフェイスが 単一の WLC ポートへマッピングされる可能性もあります。 LAG が使用されると、 システムによってインターフェイスが集約ポート チャネルへ動的にマッピングされます。 これは、 ポートの冗長性とロード バランシングに有効です。 ポートに障害が発生すると インターフェイスは次の利用可能な物理ポートへ動的にマッピングされ、 ポート全体で LAP のバランシングが行われます。

LAG が WLC でイネーブルになると、データ フレームが受信された 同じポート上にデータ フレームが WLC によって転送されます。 WWLC では、EtherChannel 全体での トラフィックのロード バランシングを隣接スイッチに依存しています。 WLC では、 独自に EtherChannel のロード バランシングを実行することはありません。

Q. WLC のどのモデルでリンク集約（LAG）が サポートされているのですか。

A. Cisco 4400 シリーズ コントローラでは、 ソフトウェア リリース 3.2 以降で LAG がサポートされており、 Cisco WiSM および Catalyst 3750G Integrated Wireless LAN Controller Switch 内のコントローラでは、LAG が自動的にイネーブルになります。 LAG を使用しない場合、 コントローラの各ディストリビューション システム ポートでは、 最大 48 のアクセス ポイントがサポートされます。 LAG がイネーブルになっている場合、 4402 コントローラの論理ポートでは最大

50 のアクセス ポイントが、 4404 コントローラの論理ポートでは最大 100 のアクセス ポイントが、 各 Cisco WiSM コントローラの論理ポートでは 最大 150 のアクセス ポイントがサポートされます。

Cisco 2106 および 2006 WLC では、LAG はサポートされていません。 Cisco 4000 シリーズ WLC などの 古いモジュールでも、LAG はサポートされていません。

Q. Unified Wireless Network の自動アンカー モビリティ機能とは、 どのようなものですか。

A. 自動アンカー モビリティ (またはゲスト WLAN モビリティ) を使用すると、 ワイヤレス LAN (WLAN) 上のクライアントがローミングするときのロード バランシングとセキュリティが向上します。 通常のローミング状態では、 クライアント デバイスは WLAN に加入すると、 最初に通信したコントローラにアンカーされます。 クライアントが別のサブネットにローミングする場合は、 クライアントのローミング先のコントローラによって、 クライアントとアンカー コントローラの外部セッションがセットアップされます。 自動アンカー モビリティ機能を使用すると、 WLAN のクライアントのアンカー ポイントとして、 1 つまたは複数のコントローラを指定できます。

注: レイヤ 3 モビリティには、モビリティ アンカーを設定しないでください。 これらのモジュールでの が使用されるのは、ゲスト トンネリングのためだけです。

Q. Cisco 2006 WLC は、WLAN のアンカーとして 設定できるのですか。

A. Cisco 2000 シリーズ WLC は、WLAN のアンカーとして指定できません。 ただし、Cisco 2000 シリーズ WLC で作成された WLAN では、 アンカーとして Cisco 4100 シリーズ WLC および Cisco 4400 シリーズ WLC を置くことができます。

Q. ワイヤレス LAN コントローラでは、どのタイプのモビリティ トンネリングが使用されるのですか。

A. コントローラ ソフトウェア リリース 4.1 ~ 5.1 では、アシンメトリク モビリティ トンネリング とシンメトリック モビリティ トンネリングの両方がサポートされています。 コントローラ ソフトウェア リリース 5.2 以降では シンメトリック モビリティ トンネリングだけがサポートされ、 これは常にデフォルトでイネーブルになっています。

アシンメトリック トンネリングでは、有線ネットワークへのクライアント トラフィックが 外部コントローラを介して直接ルーティングされます。 上流のルータで Reverse Path Filtering (RPF) が イネーブルになっている場合、アシンメトリック トンネリングに破綻が発生します。 この場合、 RPF チェックによって、送信元アドレスへ戻るパスがパケットの送信元のパスと一致することが確認されるため、 ルータでクライアント トラフィックがドロップされます。

シンメトリック モビリティ トンネリングがイネーブルになっている場合、 すべてのクライアント トラフィックがアンカー コントローラへ送信されるため、RPF チェックを問題なく通過します。 シンメトリック モビリティ トンネリングは、次の状況でも役に立ちます。

- 送信元 IP アドレスがパケットが受信されたサブネットに一致しないために、 クライアント パケット パス内のファイアウォール インストールによってパケットが ドロップされる場合、これが役に立ちます。
- アンカー コントローラ上のアクセス ポイント グループの VLAN が 外部コントローラ上の

WLAN インターフェイス VLAN と異なる場合。 この場合、 モビリティ イベントの間にクライアント トラフィックが誤った VLAN へ送信される 可能性があります。

Q. ネットワークが停止したときに WLC にアクセスする方法を 教えてください。

A. ネットワークが停止した場合は、サービス ポートによって、WLC にアクセスできます。 このポートには、WLC の他のポートとまったく異なるサブネットの IP アドレスが割り当てられているため、 アウトオブバンド管理と呼ばれています。 詳細 ついては、 「ポートと インターフェイスの設定 」セクション （『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0』にあります ）を参照してください。

Q. Cisco WLC ではフェールオーバー （ 冗長性 ）機能が サポートされているのですか。

A. はい、WLAN ネットワークで 2 つ以上の WLC を使用する場合は、 冗長構成を設定できます。 一般的に、LAP は設定されたプライマリ の WLC に加入します。 プライマリの WLC に障害が発生すると、LAP はリブートされ、 モビリティ グループ内の別の WLC に加入します。 フェールオーバー機能は、LAP によってプライマリの WLC がポーリングされ、 プライマリの WLC が機能するようになるとそれに加入する機能です。 詳細については、 「Lightweight アクセス ポイントの WLAN コントローラ フェールオーバーの設定例」 参照してください。

Q. ワイヤレス LAN コントローラ （ WLC ）で事前認証アクセス コントロール リスト （ ACL ）を使用するのは、 どのような場合ですか。

A. 事前認証 ACL を使用すると、その名前からわかるように、 クライアントの認証前であっても特定の IP アドレスから送受信されるクライアント トラフィックを許可することができます。 Web 認証に外部 Web サーバを使用すると、WLC プラットフォームの一部は 外部 Web サーバ （ Cisco 5500 シリーズ コントローラ、Cisco 2100 シリーズ コントローラ、Cisco 2000 シリーズ 、および コントローラ ネットワーク モジュール ）のために事前認証 ACL が必要になります。 その他の WLC プラットフォームでは、 事前認証 ACL は必須ではありません。 ただし、 外部 Web 認証を使用する場合は、外部 Web サーバのために事前認証 ACL を 設定することをお勧めします。

Q. ネットワークに MAC フィルタ処理された WLAN と完全にオープンな WLAN があります。 クライアントは、デフォルトではオープンな WLAN を選択するのですか。 それとも、 クライアントは MAC フィルタで設定されている WLAN ID に自動的に関連付けられるのでしょうか。 また、 MAC フィルタに interface オプションが用意されているのはなぜですか。

A. クライアントは、クライアントの接続先として設定されているどの WLAN にも 関連付けが可能です。 MAC フィルタの interface オプションを使用すると、フィルタを WLAN と インターフェイスのいずれかに適用することができます。 複数の WLAN が 1 つのインターフェイスに 関連付けられている場合に、それぞれの WLAN ごとにフィルタを作成しなくても、 インターフェイスに MAC フィルタを適用することができます。

Q. WLC で管理ユーザの TACACS 認証を設定するには、 の用途は何ですか。

A. TACACS がサポートされるのは、WLC バージョン 4.1 からです。 詳細に 『 「TACACS+ の設定」 を参照してください。

Q. ワイヤレス LAN コントローラ（WLC）での認証失敗回数超過設定 の用途は何ですか。

A. この設定は、クライアントの除外ポリシーの 1 つです。 クライアントの除外は、 コントローラでのセキュリティ機能です。 このポリシーは、 ネットワークへの不正アクセスまたはワイヤレス ネットワークへの攻撃を防ぐために、 クライアントをブラックリストに載せるのに使用されます。

この Web 認証失敗回数超過ポリシーをイネーブルにすると、 クライアントの Web 認証の試行失敗回数が 5 回を超過したときに、 コントローラはクライアントによる Web 認証の最大試行数が超過したとして、 そのクライアントをブラックリストに載せます。

この設定をイネーブルまたはディセーブルにするには、 次の手順を実行してください。

1. WWLC の GUI から、[Security] > [Wireless Protection Policies] > Client Exclusion Policies] に移動します。
2. [Excessive Web Authentication Failures] にチェックマークを付けるか、またはチェックマークを外します。

Q. Autonomous アクセス ポイント（AP）を Lightweight モードに変更しました。クライアントの アカウンティング用に AAA RADIUS サーバを使用する Lightweight AP Protocol（LWAPP）モードでは、 通常、クライアントは WLC の IP アドレスを 基に RADIUS アカウンティングで追跡されます。 WLC の IP アドレスではなく、WLC に関連付けられた AP の MAC アドレスを 基にするように RADIUS アカウンティングを 設定できるのですか。

A. はい、WLC 側の設定により可能です。 次の手順を 実行します。

1. コントローラの GUI で、[Security] > [Radius Accounting] に進むと、[Call Station ID Type] ドロップダウン ボックスがあります。 選択して下さい [AP MAC Address] を選択します。
2. LWAPP AP のログでこれを確認します。 このログには、called-station ID フィールドに、特定のクライアントが関連付けられている AP の MAC アドレスが表示されます。

Q. CLI で WLC の Wi-Fi Protected Access（WPA）ハンドシェーク タイムアウト値を 変更するには、どのようにすればよいのですか。 Cisco IOS® の AP で dot11 wpa handshake timeout value コマンドを使用して行う方法は知っていますが、WLC で行う方法がわかりません。

A. WLC を介して WPA ハンドシェークのタイムアウトを設定する機能は、 ソフトウェア リリース 4.2 以降で統合されています。 以前の WLC ソフトウェア バージョンでは このオプションは必要ありません。

WPA ハンドシェークのタイムアウトを変更するには、次のコマンドを使用します。

config advanced eap eapol-key-timeout <value> **config advanced eap eapol-key-retries** <value>
デフォルト値には継続して WLC の現在の動作が 反映されます。

```
- the default value for eapol-key-timeout is 1 second.
- the default value for eapol-key-retries is 2 retries
```

注: IOS AP では、**dot11 wpa handshake** コマンドを使用してこれを設定することができます。

またオプションで他の EAP パラメータを設定できます **config advanced eap** コマンドのオプションを使用して、他の EAP パラメータを設定することも可能です。

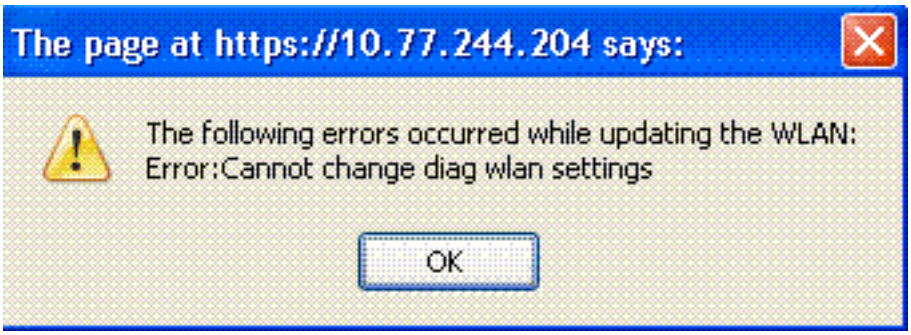
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

Q. [WLAN] > > [Edit] > [Advanced] ページの診断チャネル機能の目的は何ですか。

A. 診断チャネル機能を使用すると、WLAN とのクライアント通信 に関する問題のトラブルシューティングが可能になります。 クライアントとアクセス ポイントには 定義された一連のテストを適用することができ、 これにより、クライアントに発生している通信の問題の原因を識別し、ネットワーク上でクライアントを稼働可能にするための修正方法を適用することができます。 診断チャネルをイネーブルにするために コントローラの GUI か CLI を使用でき、 診断テストを実行するためにコントローラ CLI または WCS を使用できます。

診断チャネルは、テストだけに使用できます。 診断チャネルが イネーブルになっている場合に WLAN に認証または暗号化を設定しようとすると、 次のエラーが表示されます。



Q. WLC で設定できる AP グループの最大数はいくつですか。

A. 次のリストは、WLC で設定できる AP グループの最大数 を示します。

- Cisco 2100 シリーズ コントローラおよびコントローラ ネットワーク モジュールの場合は 最大 50 のアクセス ポイント グループ
- Cisco 4400 シリーズ コントローラ、Cisco WiSM、および Cisco 3750G ワイヤレス LAN コントローラ スイッチの場合は 最大 300 の スイッチ

- Cisco 5500 シリーズ コントローラの場合は、最大 500 の アクセス ポイント グループ

関連情報

- ワイヤレス LAN コントローラ (WLC) に関する FAQ
- ワイヤレス LAN コントローラ (WLC) のエラー メッセージとシステム メッセージに関する FAQ
- Lightweight アクセス ポイントに関する FAQ
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 7.0.116.0
- ワイヤレス LAN コントローラでの IPv6 サポート (英語)
- ワイヤレス 製品のサポート
- テクニカルサポートと マニュアル：シスコ

Cisco サポート コミュニティ - 特集対話

Ciscoサポート コミュニティは質問を、共有推奨事項し、答える、あなたのためのフォーラムです 同位と協力して下さい。

Updated: 2015 年 3 月 02 日
Document ID: 118833