ワイヤレス LAN コントローラ（WLC）の設計と機能に関する FAQ の確認

内容

WLC機能に関するFAQ

はじめに

SSHv1

このドキュメントでは、ワイヤレス LAN コントローラの設計と機能に関する最新情報について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

コンポーネントの使用

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

WLC設計に関するFAQ

Q. WLCに接続するようにスイッチを設定するにはどうすればよいのですか。

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。詳細については、『WLC用のスイッチの設定』を参照してください。

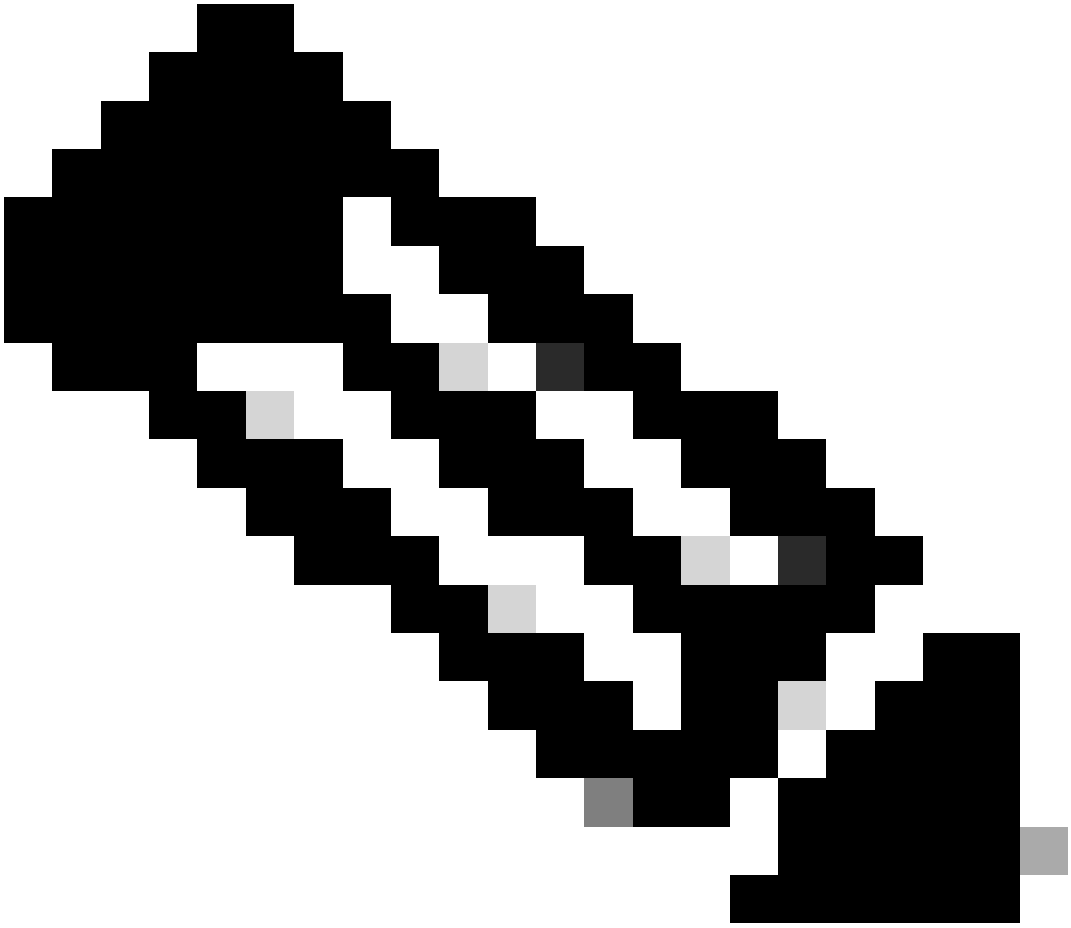
Q.アクセス ポイント（AP）がコントローラに登録されると、WLAN クライアント間のすべてのネットワーク トラフィックが、ワイヤレス LAN コントローラ（WLC）を経由してトンネリングされるのでしょうか。

A. APがWLCに加入すると、Control and Provisioning of Wireless Access Points protocol(CAPWAP)トンネルが2台のデバイス間に形成されます。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を経由してWLCを設定できます。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、WLCにトンネル経由で戻されます。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の詳細については、『FlexConnectワイヤレスブランチコントローラ導入ガイド』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タギングは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。

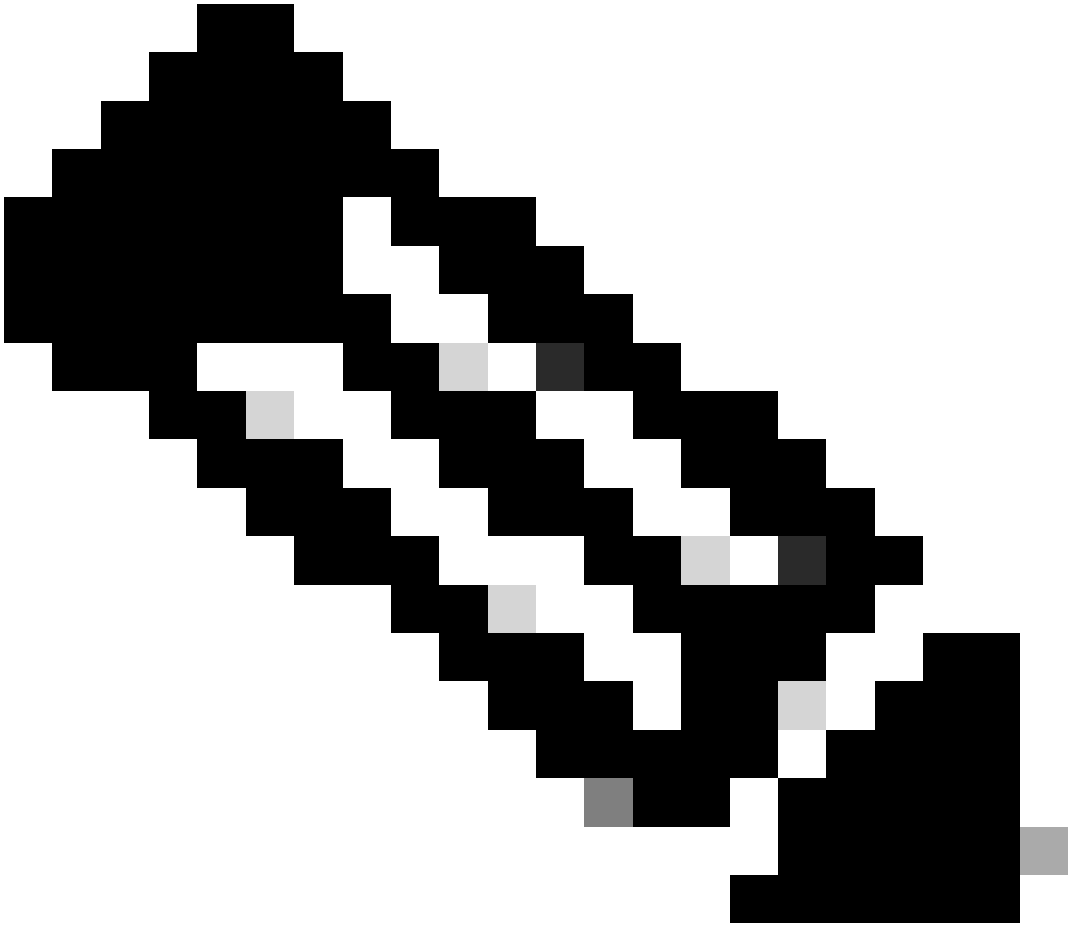
もう 1 つの大きな違いは、REAP モードでは、データ トラフィックがローカルでのみブリッジングされることです。これをセントラル オフィスに戻すことはできませんが、H-REAP モードでは、トラフィックをセントラル オフィスに戻すオプションが提供されます。H-REAP ローカル スイッチングに設定された WLAN からのトラフィックはローカルにスイッチングされます。他の WLAN からのデータ トラフィックはセントラル オフィスに戻されます。

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。

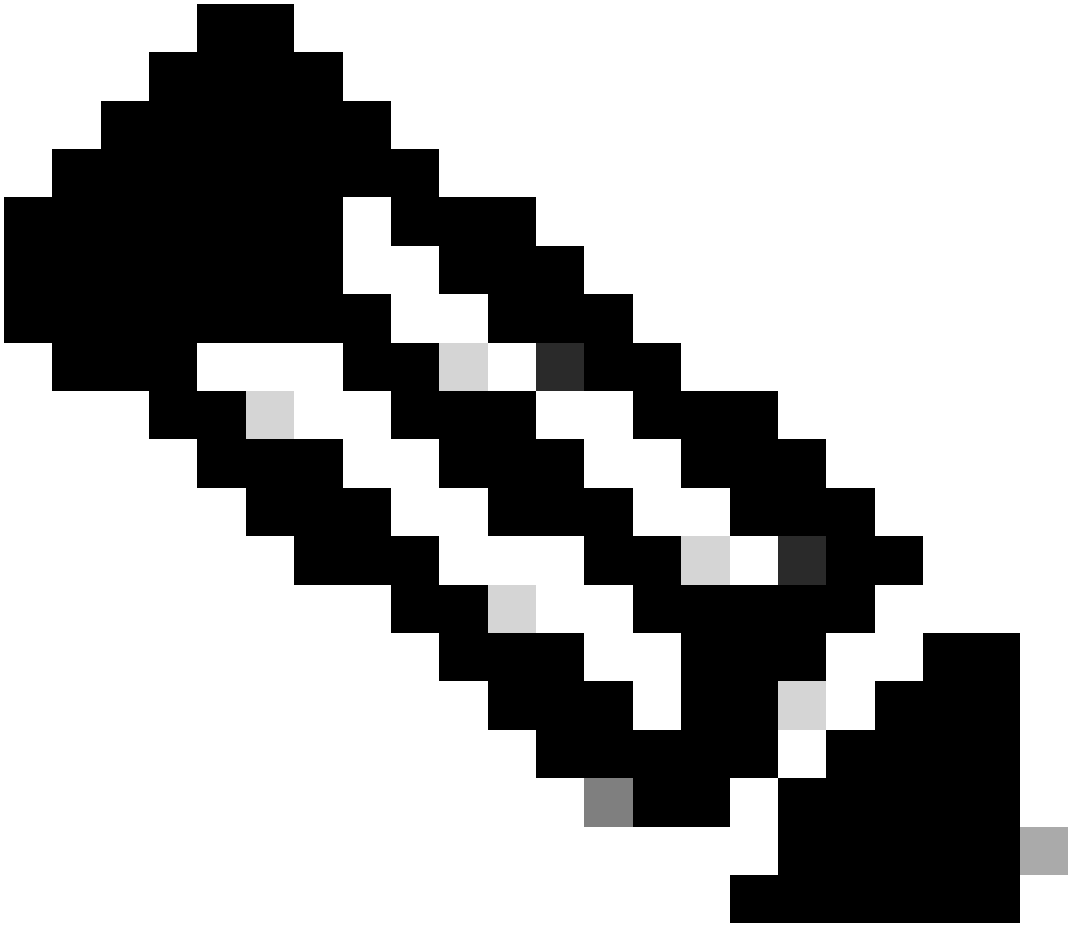
H-REAPの詳細は、『Hybrid REAPの設定』を参照してください。

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以降では、WLCはLightweightアクセスポイントに対して最大512のWLANを制御できます。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コントローラがサポートするWLANは最大16個です。



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「WLANの作成」セクションを参照してください。

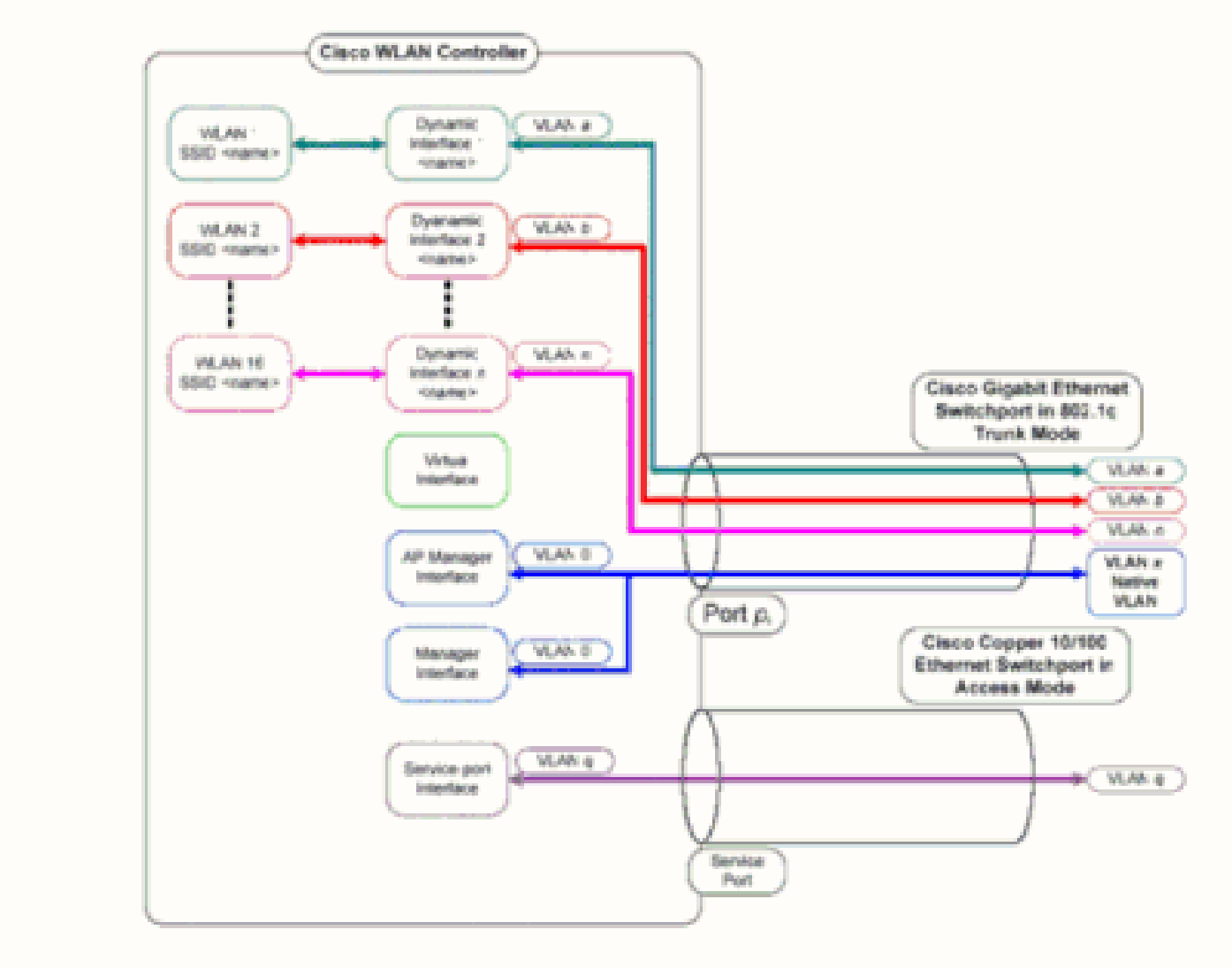
Q.WLC で VLAN を設定するには、どのようにすればよいのですか。

A. WLCでは、VLANは一意のIPサブネットで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、『無線 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.WLCでは、AAAサーバが関与する認証メカニズム (レイヤ2またはレイヤ3) では、管理インターフェイスのIPアドレスを使用します。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のプライマリWLCの設定方法についての詳細は、

」セクション（

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の設定は必要ありません。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. 次のコントローラ機能は、メッシュネットワークではサポートされていません。

- 複数国サポート
- 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）
- Locally Significant Certificate; ローカルで有効な証明書
- ロケーション ベース サービス

Q.ワイヤレスLANコントローラ上のManufacturer Installed Certificate(MIC)とLightweight AP証明書の有効期間はどのくらいですか。

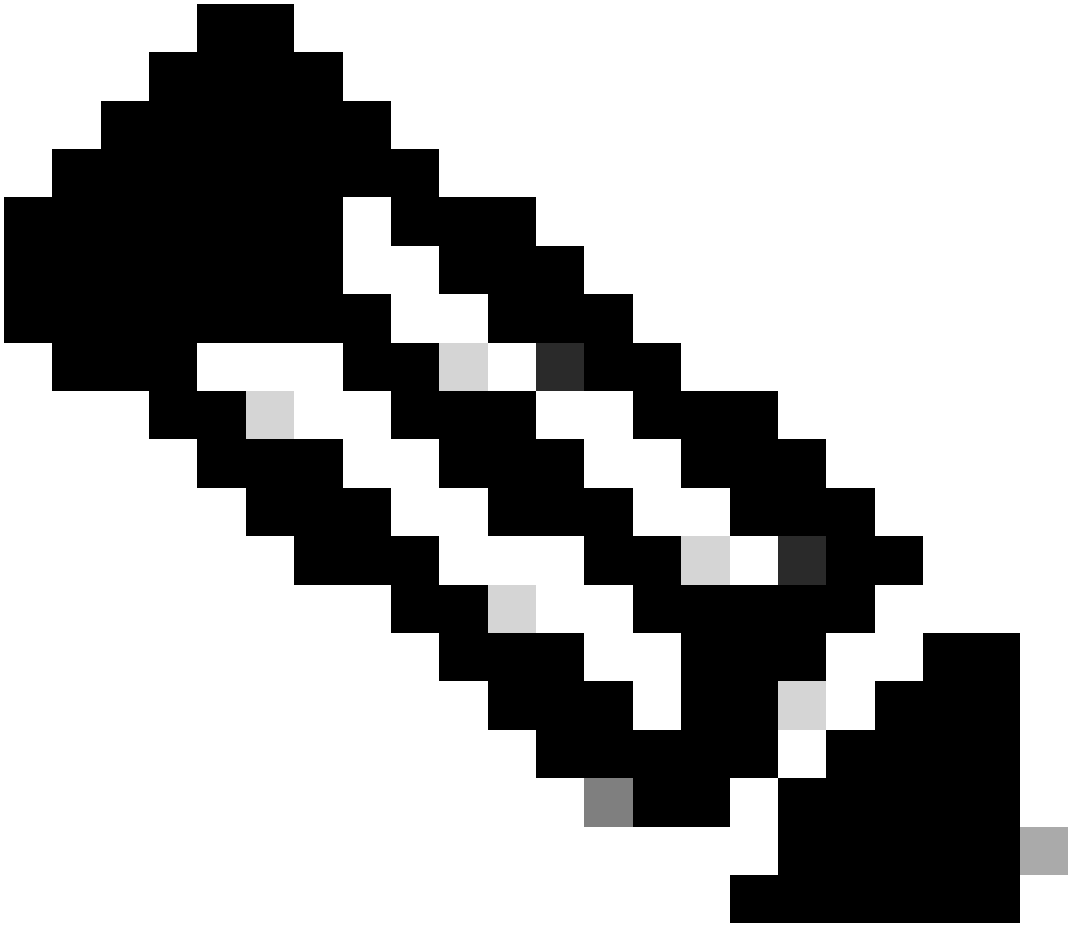
A. WLCでのMICの有効期間は10年です。作成されたLightweight AP証明書(MICまたは自己署名証明書(SSC)のどちらか)には、同じ10年の有効期間が適用されます。

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る限り、クライアントのローミングは正常に動作します。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。



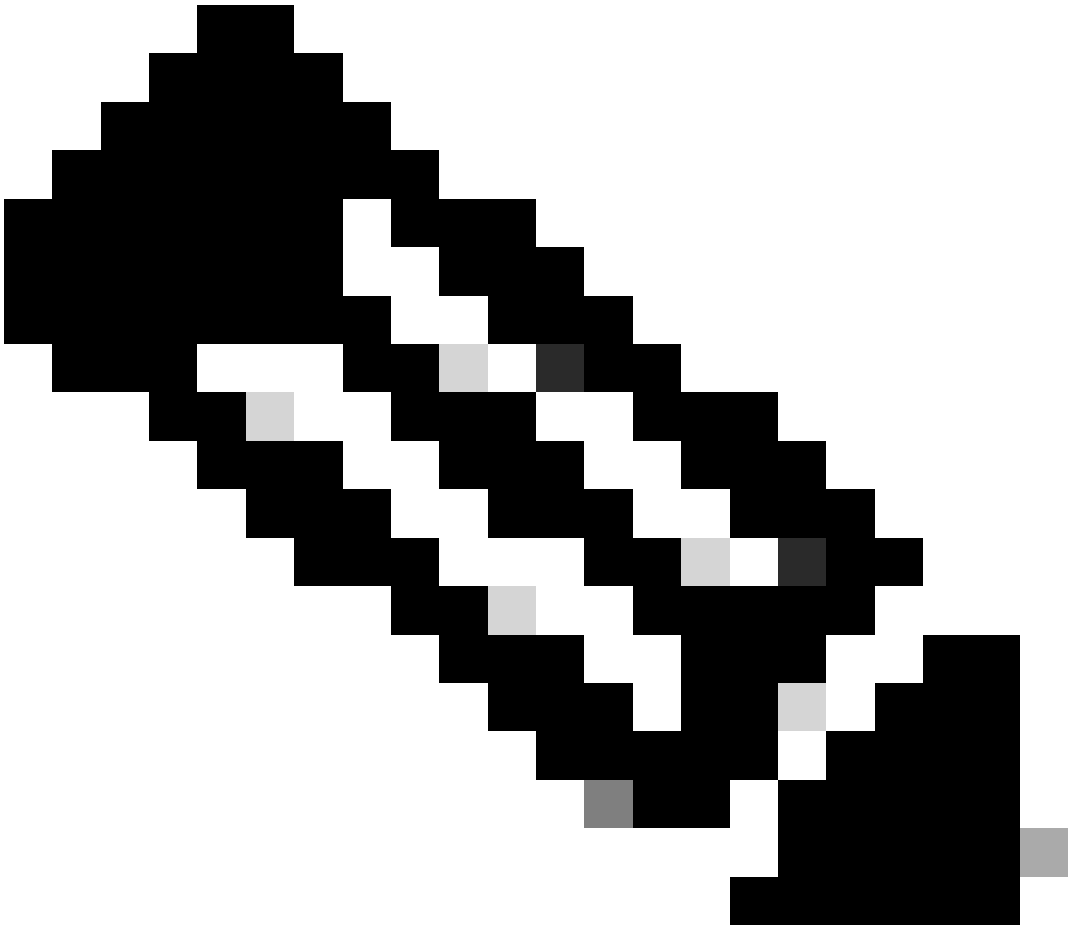
注：レイヤ2モードは、Cisco 410xおよび440xシリーズのWLCとCisco 1000シリーズアクセスポイントでのみサポートされています。レイヤ 2 LWAPP は、その他のワイヤレス LAN コントローラおよび Lightweight アクセス ポイント プラットフォームでサポートされません。

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は、モビリティメッセージを介して、クライアントに関する情報（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）で応答します。

4. WLC では、提供されたクライアントの詳細情報を使用してデータベースが更新され、必要に応じてクライアントへの再認証プロセスが発生します。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。



注：ワイヤレスクライアントは、再関連付け中に(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、802.1x認証を通過できます。

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：5247
  - 制御：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のみをサポートしています。

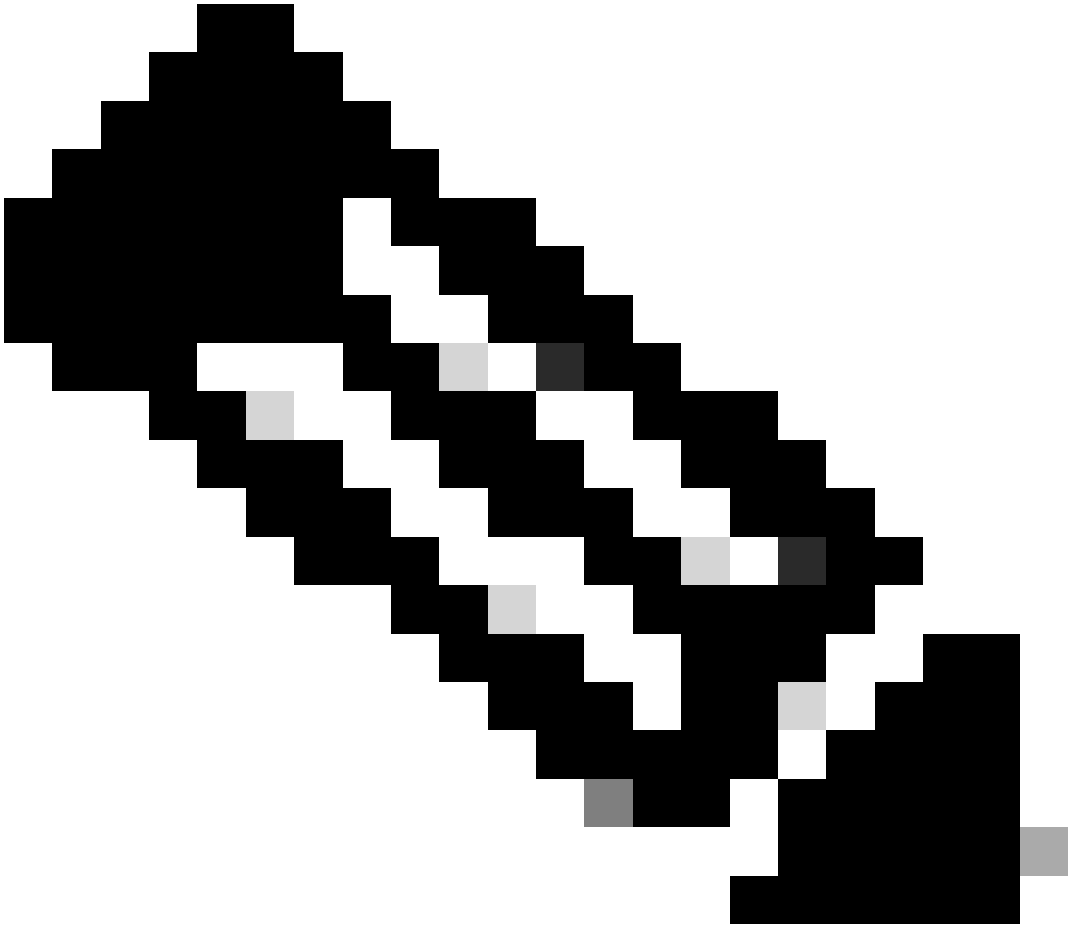
Q.逆アドレス解決プロトコル（RARP）は、WLC 経由ではサポートされるのですか。

A. Reverse Address Resolution Protocol（RARP；逆アドレス解決プロトコル）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ために使用されるリンク層プロトコルです。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サーバが含まれています。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。この DHCP サービスにアクセスするには、WLC GUI から Controller メニューをクリックし、ページの左側にある 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「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に対して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、最初のクライアント関連付けの間に、APまたはWLCがPair-wise Primary 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と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。

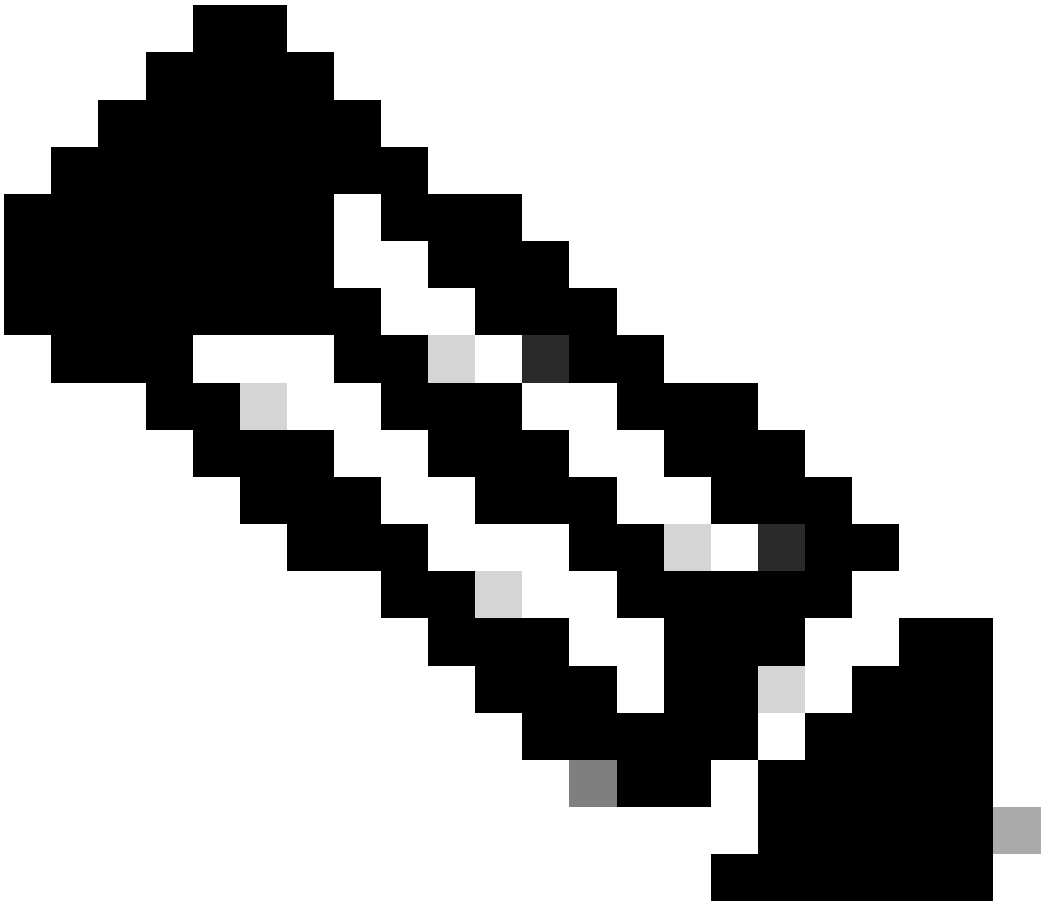
configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name>

は、CLIを使用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方法はありません。

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、コントローラを介してLAPを追跡できる方法はありません。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。

<#root>

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。

<#root>

show cdp nei <type/num> detail

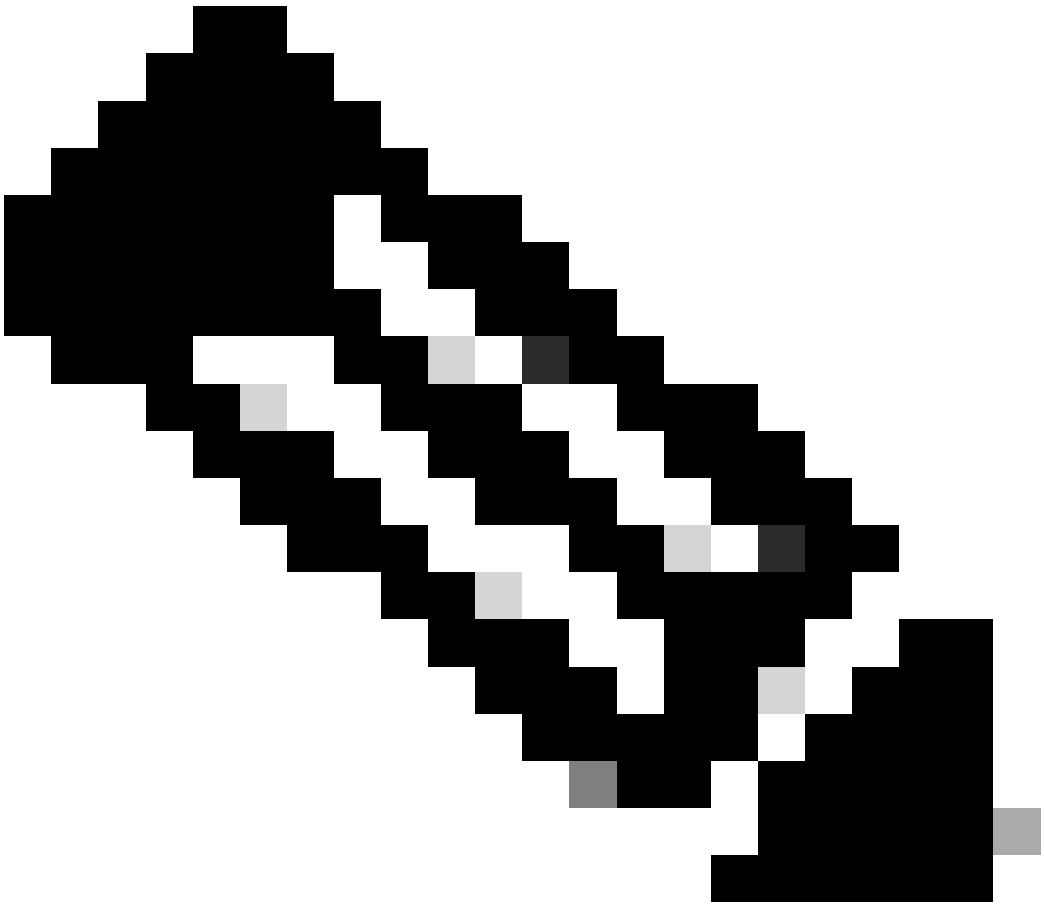
このコマンドの出力からは、LAP の名前もわかります。ただし、この方法は、AP の電源が入っていて、スイッチに接続されている場合にしか使用できません。

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。

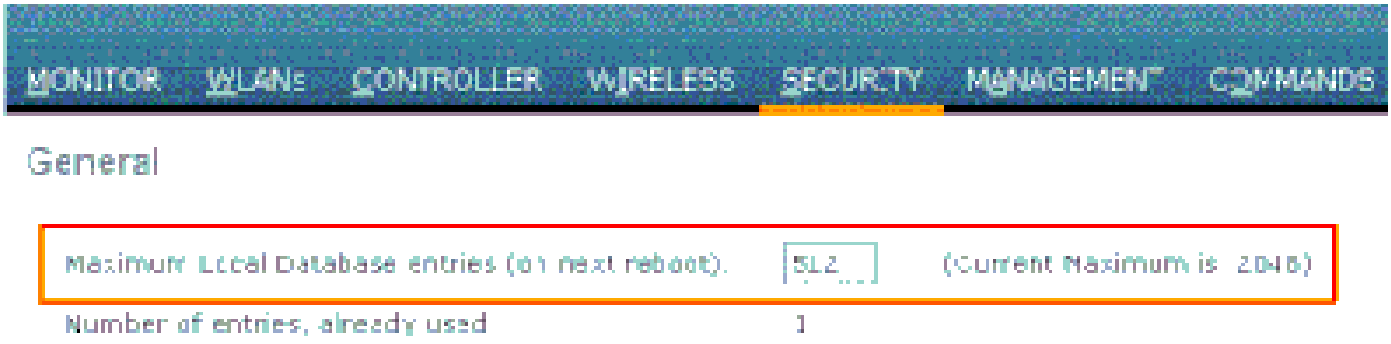
A. ローカルユーザデータベースのセキュリティ>一般ページでの制限は、最大2048エントリです。このデータベースは、ローカル管理ユーザ (Lobby Ambassador を含む) 、ネット ユーザ (ゲスト ユーザを含む) 、MAC フィルタ エントリ、アクセス ポイント認可リスト エントリ、除外リスト エントリで共有されます。これらのすべてのタイプのユーザの合計が、設定されているデータベース サイズを超えることはできません。

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)
```



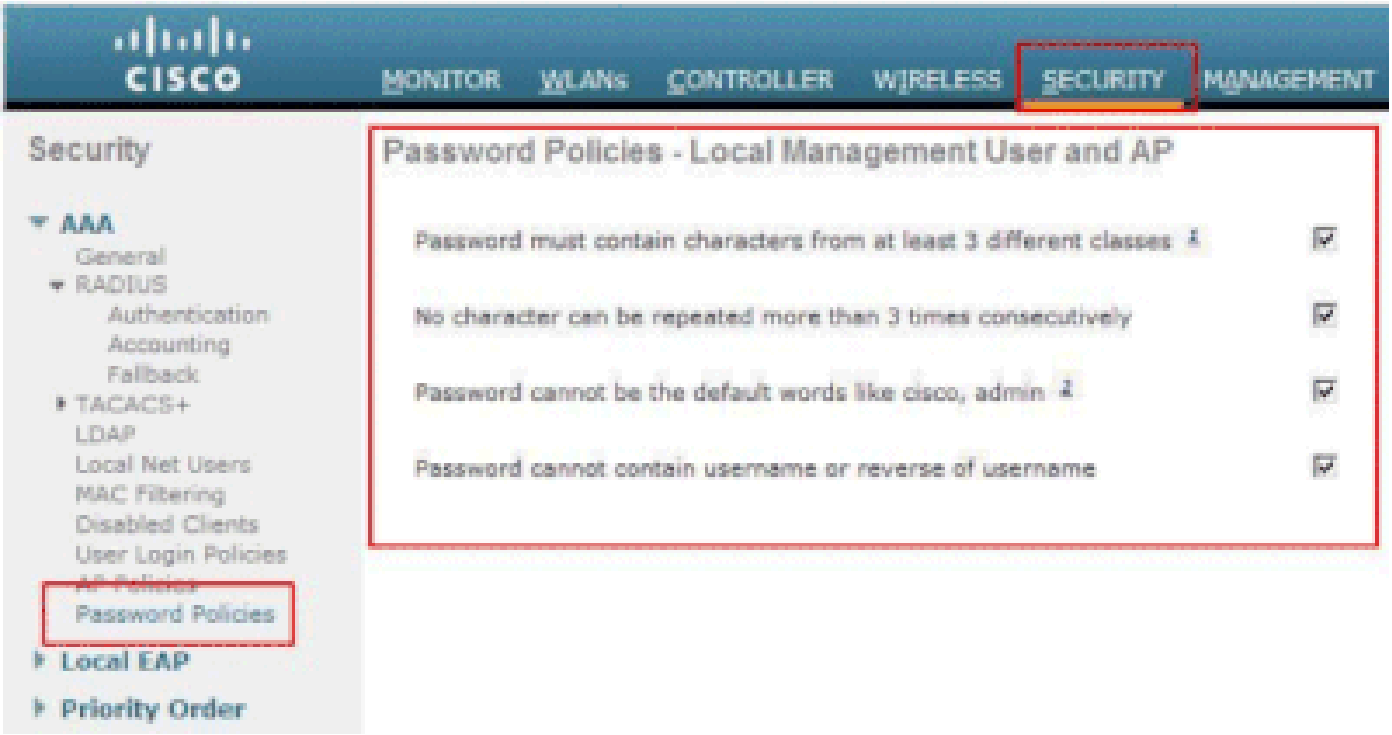
注：変更を有効にするには、設定を保存し、reset systemコマンドを使用してシステムをリセットする必要があります。



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。ランダム データの例は次のとおりです。



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とは、固定IPアドレスを使用して設定された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 ポイントにアソシエートするとき、IP アドレス、サブネット マスク、および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た場合、それらのクライアントが DHCP を使用しない限り、コントローラではその IP アドレスは認識されません。

現在、WLC は ARP 要求のプロキシとして動作します。ARP 要求を受信すると、コントローラは、クライアントに直接要求を渡

す代わりに、ARP 応答で応答します。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、クライアントの場所を認識できません。
- 携帯電話やプリンタなどのバッテリ駆動デバイスでは、すべての ARP 要求に応答する必要がないため、電力が保持されます。

ワイヤレス コントローラには、パッシブ クライアントに関する IP 関連の情報がないため、ARP 要求に応答できません。現在の動作では、ARP 要求のパッシブ クライアントへの転送は許可されていません。パッシブクライアントへのアクセスを試みるアプリケーションはすべて失敗する可能性があります。

パッシブ クライアント機能は、有線クライアントとワイヤレス クライアント間の ARP 要求および応答の交換を可能にします。この機能が有効である場合、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 クライアントへ 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の設定方法については、『Cisco Wireless LAN Controllerコンフィギュレーションガイド、リリース 7.0.116.0』の「GUIを使用したパッシブクライアントの設定」を参照してください。

Q.クライアントが、3 分ごと、または指定による時間間隔で RADIUS サーバによる再認証を実行するように設定するには、どのようにすればよいのですか。

A.これを行うには、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 [WLANs] メニューをクリックします。WLC で設定された WLAN のリストが表示されます。クライアントが属する WLAN をクリックします。**Advanced**< **span**> タブに移動すると、*Enable Session* Timeoutparameterが表示されます。デフォルト値を 180 に変更して、[Apply] をクリックすると、変更が有効になります。

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）値が渡されますか。WLC で、QoS はどのように実装されるのですか。

A.Cisco Unified Wireless Network(UWN)ソリューションのWLANでは、次の4つのレベルのQoSがサポートされています。

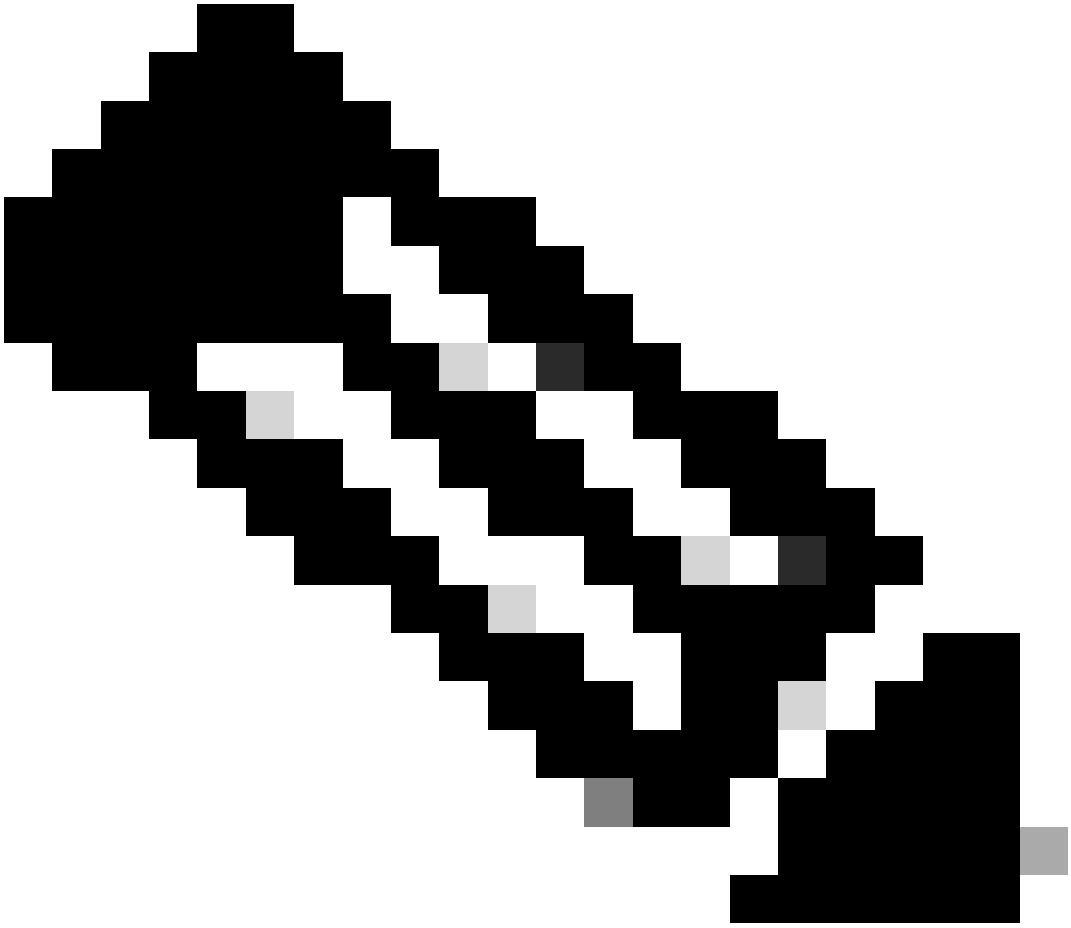
- Platinum/音声
- Gold/ビデオ
- Silver/ベスト エフォート（デフォルト）
- Bronze/バックグラウンド

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いずれかの QoS レベルを割り当てることができます。詳細は、『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ソリューションでサポートされていますか。

A.いいえ、WLCはCisco WGB製品のみをサポートしています。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）では設定ファイルをどのように保存しますか。

A. WLCには、次の2種類のメモリが搭載されています。

- 揮発性 RAM：現在のアクティブなコントローラ設定を保持します。
- 不揮発性 RAM（NVRAM）：リブート設定を保持します。

オペレーティング システムを WLC で設定するときは、揮発性 RAM を変更しています。現在の設定で WLC リブートを行うには、揮発性 RAM から NVRAM に設定を保存する必要があります。

次のタスクを実行するときは、どちらのメモリを変更しているかを知ることが重要です。

- 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

WLC機能に関するFAQ

Q. Wireless LAN Controller(WLC)でExtensible Authentication Protocol(EAP)タイプを設定するにはどうすればよいのですか。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、[WLANs] 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. [WLANs] > [Edit] で [Security] タブをクリックします。
4. **Layer 2**をクリックし、802.1xまたはWPA+WPA2としてLayer 2 Security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。

Q.Fast SSID Changing とは何ですか。

A.Fast SSID Changingを使用すると、クライアントはSSID間を移動できます。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クライアント エントリが消去されます。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「Fast SSID Changingの設定」セクション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の数に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の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の数は、使用しているプラットフォームによって決まります。

ワイヤレスLANコントローラのさまざまなプラットフォームにおける、WLANごとのクライアント制限についての詳細は、『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ごとのクライアントの最大数の設定」セクション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有効な機能であり、テクニカルライターに対して適切にwireleTalkを装備することを許可します。ssクライアントは、AAAサーバとの完全な再認証なしでローミングできます。PKC 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。これにより、モバイルステーションは、アクセスポイント(AP)への認証が成功することによって取得したプライマリキー(Pairwise Primary Key [PMK])をキャッシュし、今後の同じ**AP**への関連付けでそれを再利用できます。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。

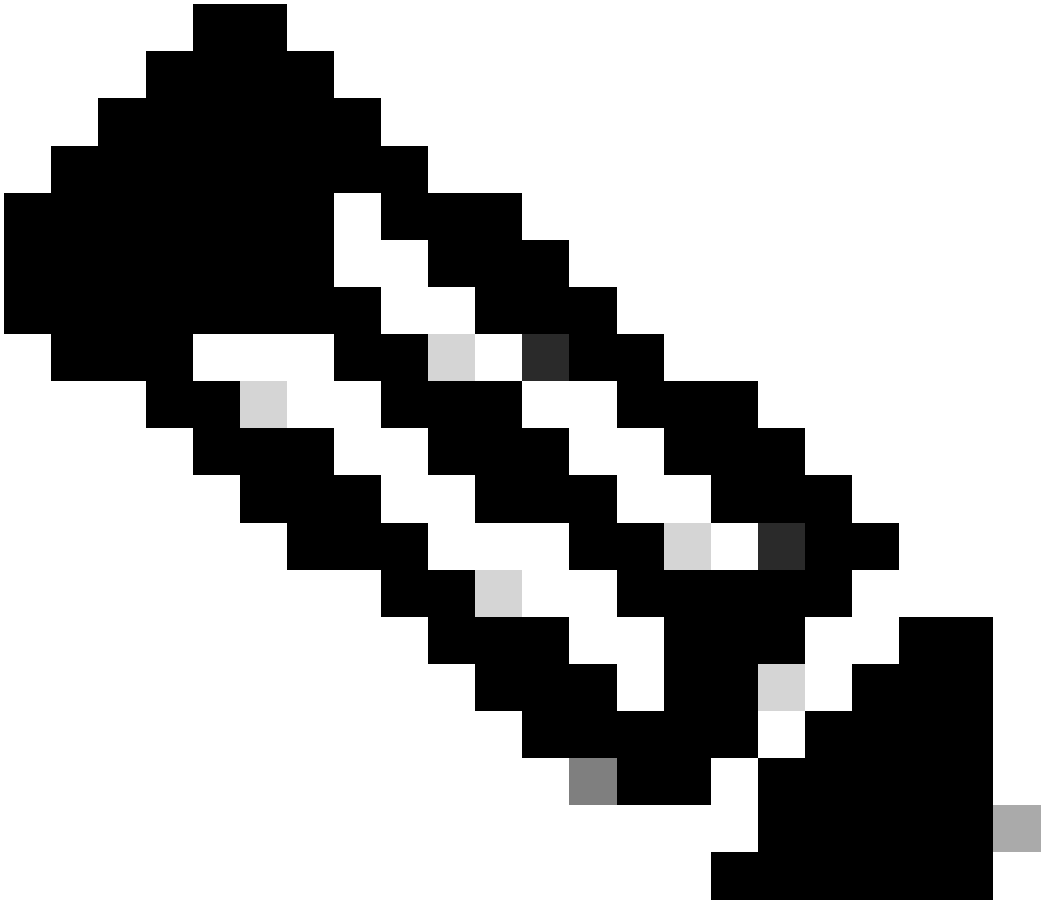
PKC を使用すると、ステーションは、以前に認証処理が成功したときに取得した PMK を再利用できるようになります。これにより、ローミング時に新しい AP に対して認証を実行する必要がなくなります。

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 を使って 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、WLC で PKC がイネーブルになります。また、AAA サーバとワイヤレス クライアントを適切な EAP 認証に合せて設定してください。

クライアント側で使用されるサプリカントも、PKCを機能させるためにWPA2をサポートする必要があります。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。

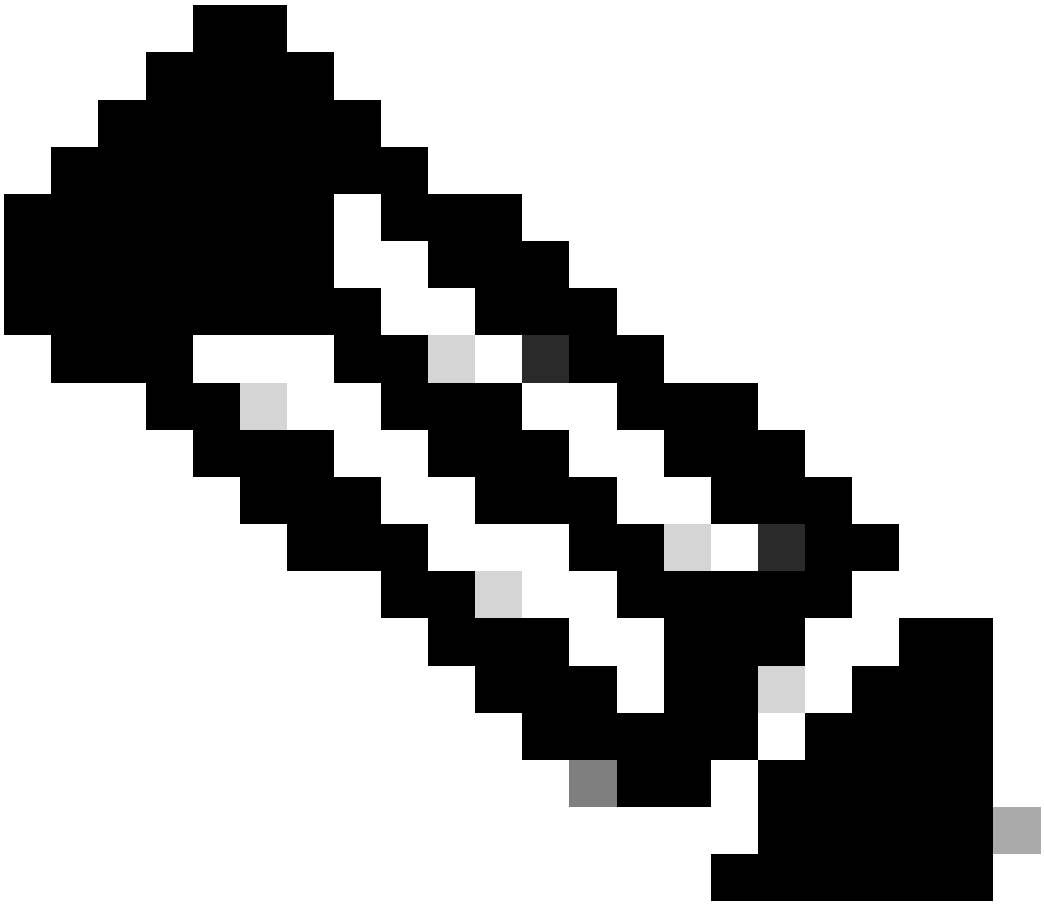


注:PKCは、クライアントサプリカントとしてAironet Desktop Utility(ADU)では動作しません。

Q.コントローラのタイムアウト設定（Address Resolution Protocol（ARP）タイムアウト、ユーザ アイドル タイムアウトおよびセッション タイムアウト）を説明してください。

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、LAPとの通信なしでユーザがアイドル状態になると、クライアントはWLCによって認証解除されます。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 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、コントローラメニューに移動します。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。

Session Time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。鍵管理で 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、**WLANs**>Editmenu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.RFID(Radio Frequency Identification)とは、無線周波数通信を使用して、比較的短距離の通信を行う技術です。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。AeroScoutタグの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認証はWLCでローカルに実行できます。ローカル EAP の認証方法を使用すると、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。ローカルの EAP-Fast 認証用に WLC を設定する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すか。LAPは、バックアップWLCにフェールオーバーする際にWLANオーバーライド値を維持できますか。

A. WLANオーバーライド機能を使用すると、WLCに設定されているWLANの中から、個々のLAPでアクティブに使用できるWLANを選択できます。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] メニューをクリックします。

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。

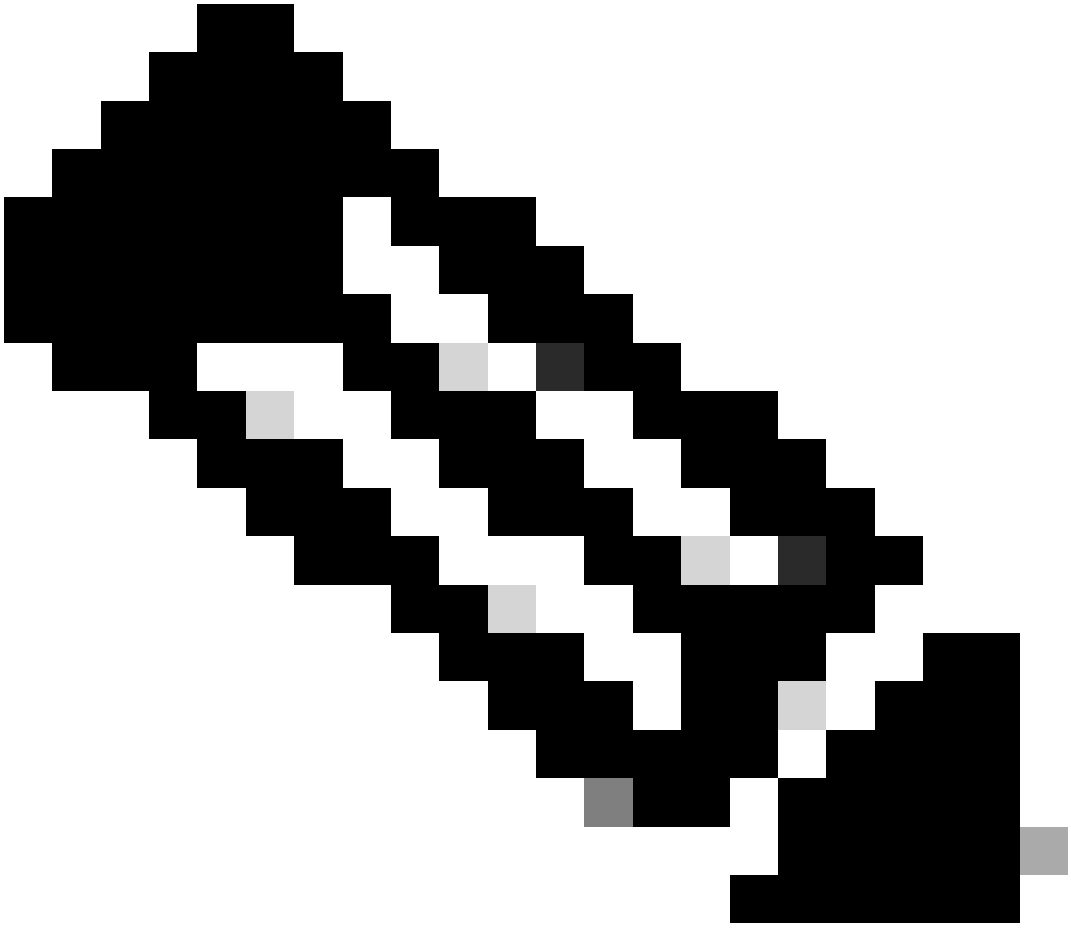
4. [WLAN Override] ドロップダウン メニューから [Enable] を選択します。[WLAN Override] メニューは、ウィンドウの左側の最後の項目です。

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。

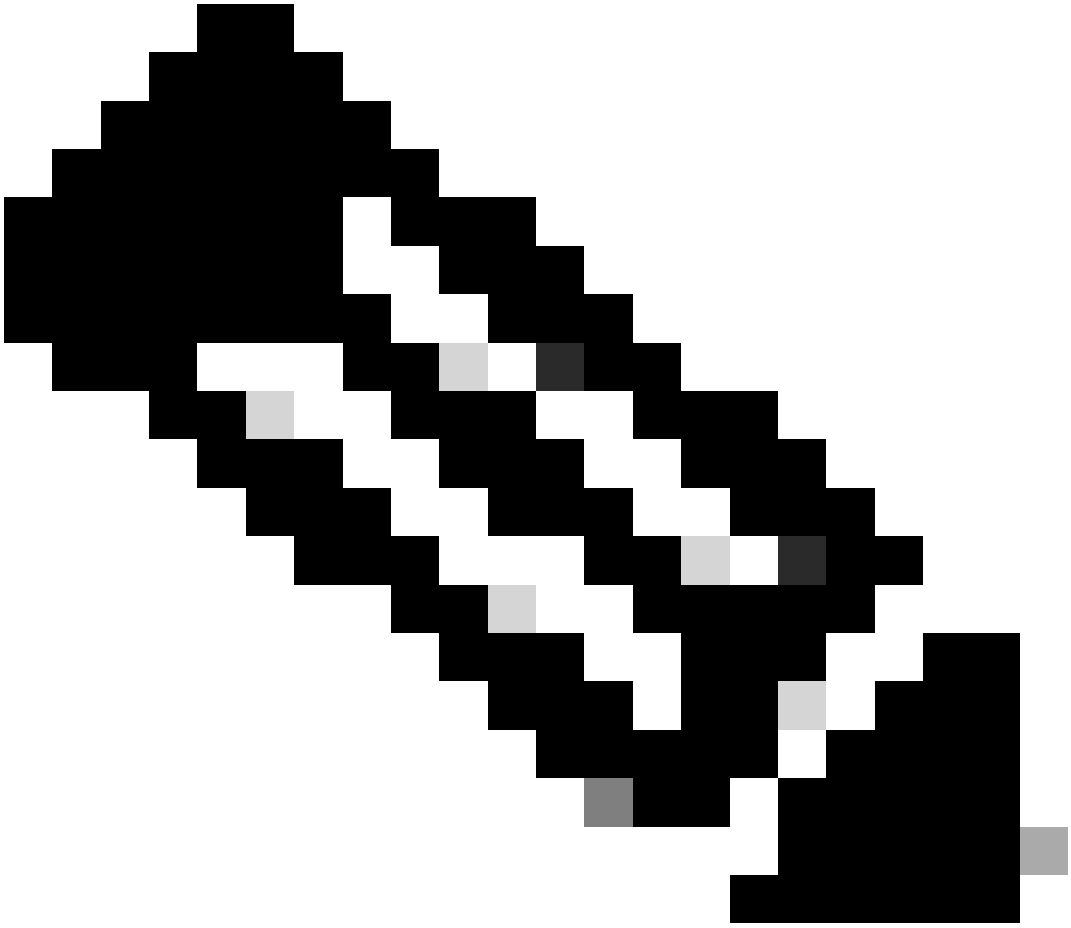
6. リストから、LAP に表示する WLAN にチェック マークを付け、[Apply] をクリックして変更を有効にします。

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はコントローラの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。



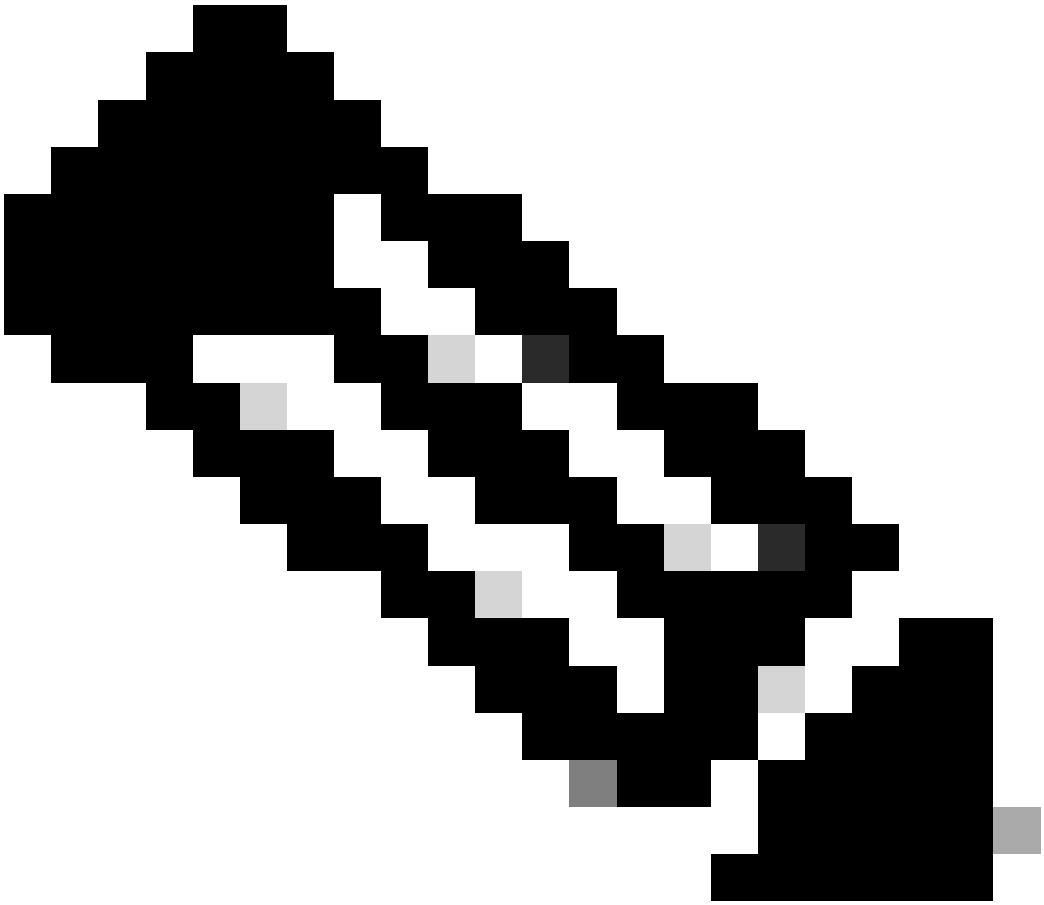
注：アクセスポイントグループは、APの無線インターフェイスごとにWLANを送信できるようにするものではありません。

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。

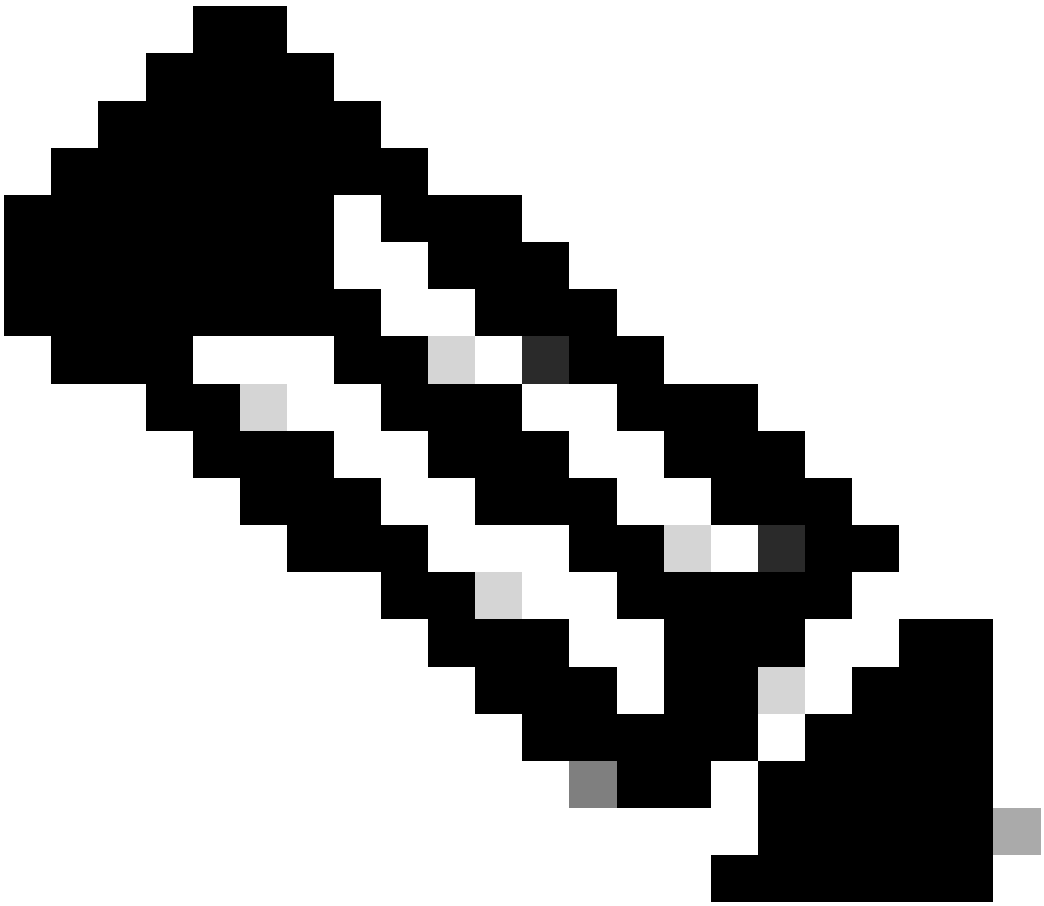
WLC で IPv6 をイネーブルにするには、[WLAN] > [Edit] ページで WLAN SSID 設定の [IPv6 Enable] チェック ボックスにチェック マークを入れます。

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ていません。

また、Cisco Bug ID CSCsg78176 があり、AAA Override 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。



注：シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

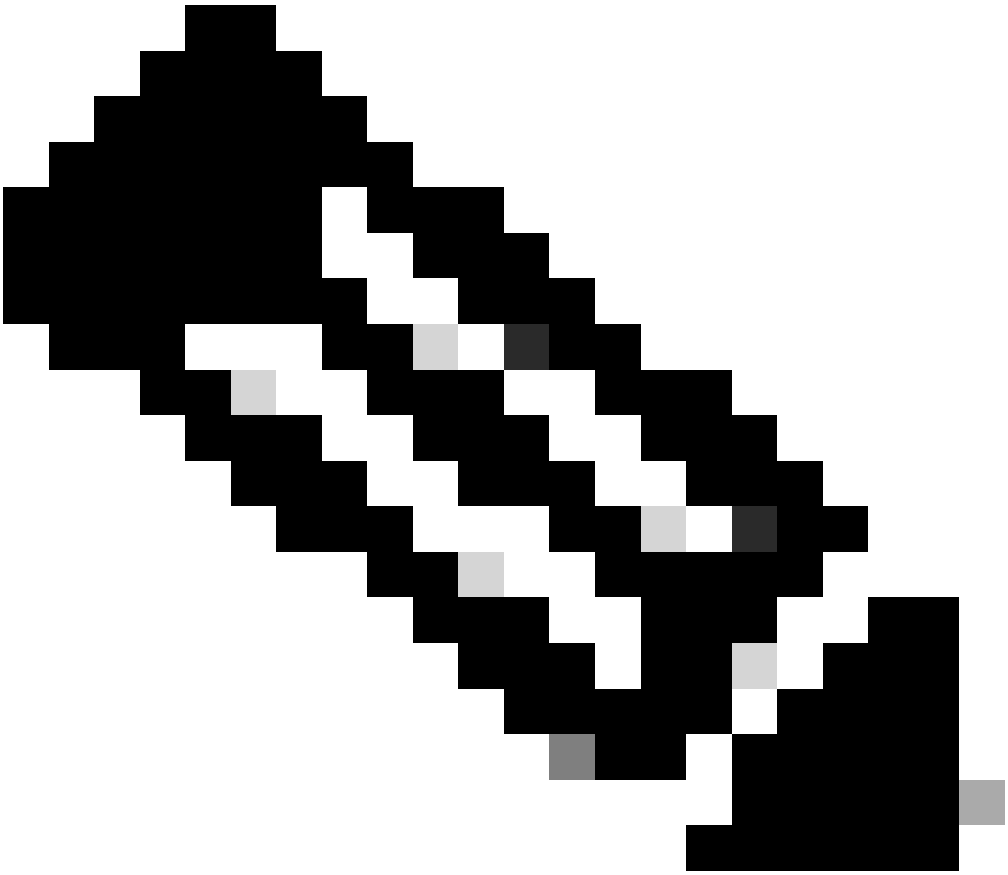
Q.Cisco 2000 シリーズの WLC では、ゲスト ユーザの Web 認証がサポートされているのですか。

A. Web認証は、すべてのCisco WLCでサポートされています。Web 認証は、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 3] を選択します。
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. ユーザを認証するデータベースをWLC上に作成するには、GUIの**Security**メニューに移動し、**Local Net User**< **/strong**>を選択して、次のアクションを実行します。

    a. 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。

    b. 使用する WLAN ID を選択します。



注：設定についての詳細は、『ワイヤレス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. WLCは、イネーブルにすると、ワイヤレスモードで管理できます。ワイヤレスモードを有効にする方法の詳細については、『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「GUIおよびCLIへのワイヤレス接続の有効化」セクション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ています。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。WLC 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。

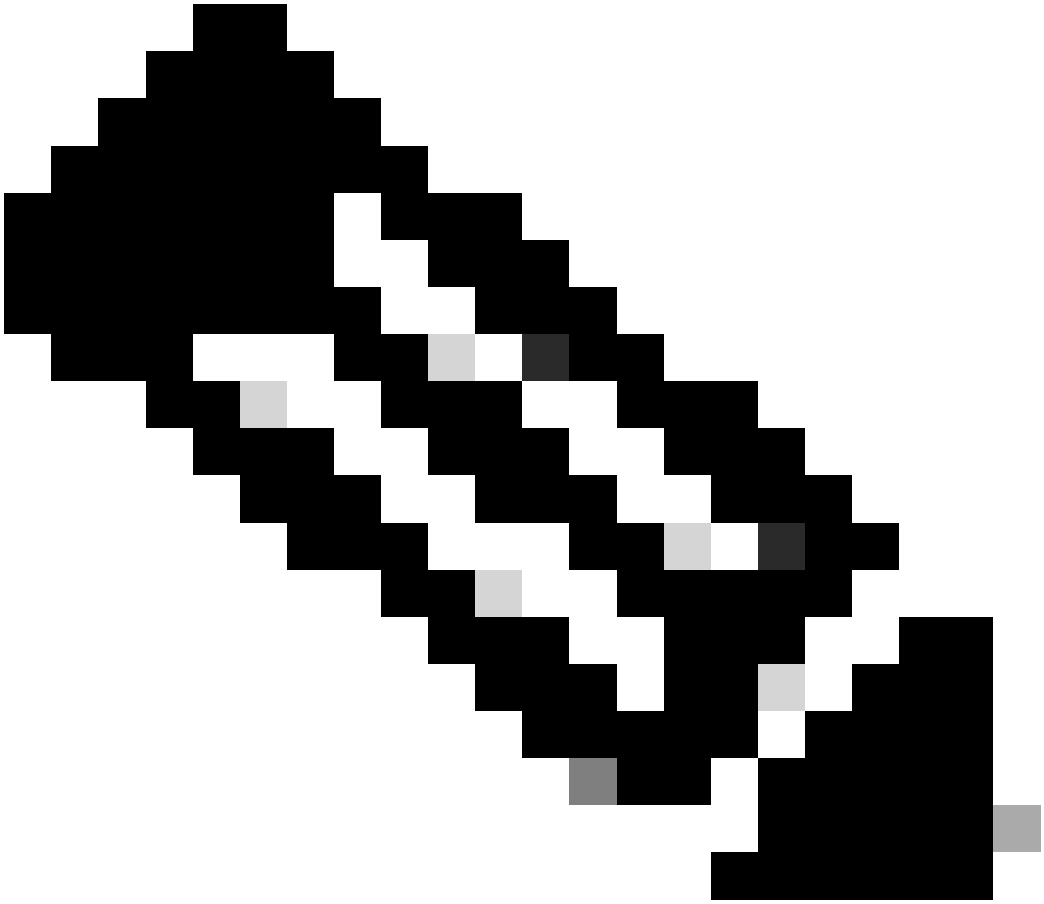
Q.WLC のどのモデルでリンク集約（LAG）がサポートされているのですか。

A.Cisco 5500シリーズコントローラではソフトウェアリリース6.0以降で、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はCisco WiSMおよびCatalyst 3750G Integrated Wireless LAN Controller Switch内のコントローラで自動的にイネーブルになります。LAG を使用していない場合、Cisco 4400 シリーズ コントローラ上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 個のアクセス 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、Cisco 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、Cisco 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、Catalyst 3750G統合ワイヤレスLANコントローラスイッチと各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：モビリティアンカーはレイヤ3モビリティ用に設定しないでください。モビリティ アンカーが使用されるのは、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 以降は、シンメトリック モビリティ トンネリングのみをサポートしており、デフォルトでは常に有効です。

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 トラフィックが廃棄されます。

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廃棄される場合、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インターフェイスのVLANと異なる場合、モビリティイベント中にクライアントトラフィックが誤ったVLANに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.ネットワークがダウンすると、サービスポートから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。詳細については、『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.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ネットワークに2つ以上のWLCがある場合は、冗長性を設定できます。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』を参照してください。

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、その名前が示すように、クライアントの認証前であっても特定のIPアドレスとの間でクライアントトラフィックを行うことが可能です。外部 Web サーバを Web 認証に使用しているときは、WLC プラットフォーム（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、コントローラ ネットワーク モジュール）の一部で外部 Web サーバの事前認証 ACL が必要です。その他の WLC プラットフォームの場合、事前認証 ACL は必須ではありません。ただし、外部 Web 認証を使用しているときは、外部 Web サーバの事前認証 ACL を設定することを推奨します。

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、どのようにすればよいのですか。

A. WLCバージョン4.1以降では、TACACSがWLCでサポートされています。WLCの管理ユーザを認証するためのTACACS+の設定方法については、『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。ポリシーは、ネットワークへの不正アクセスやワイヤレスネットワークへの攻撃を防ぐために、クライアントを除外するために使用されます。

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、クライアントによるWeb認証の試行失敗回数が5回を超えると、コン

トローラで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みなして、そのクライアントを除外します。

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. WLC の GUI で、[Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に移動します。
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側の設定によって可能です。次のステップを実行します。

1. コントローラの GUI で、[Security] > [Radius Accounting] の下に、[Call Station ID Type] のドロップダウン ボックスがあります。[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(R)のAPで**dot11 wpa handshake timeoutvalue**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を使用してWPAハンドシェーク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。

```
<#root>
```

config advanced eap eapol-key-timeout

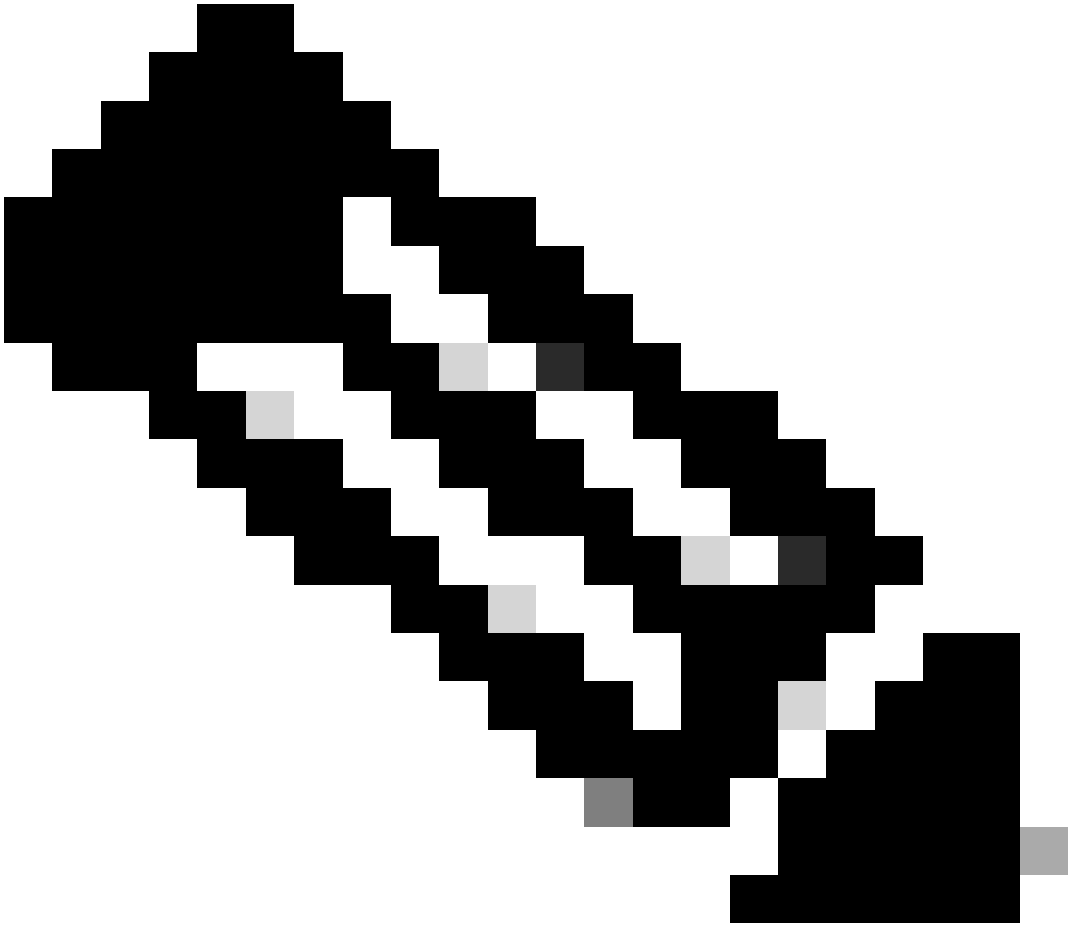
```
<value>
```

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:Cisco 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。

---

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。

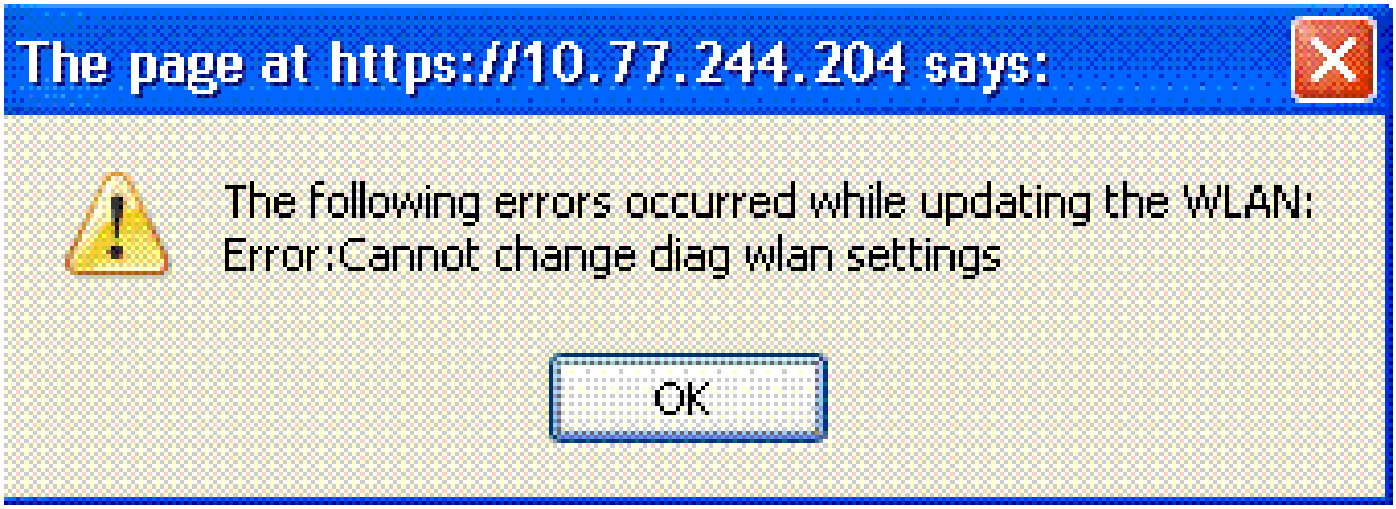
```
(Cisco Controller) >config advanced eap ?

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をトラブルシューティングできます。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ています。

- 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、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 のアクセス ポイント グループ
- 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

- **Wireless LAN Controller（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**
- **ワイヤレス LAN コントローラでの IPv6 サポート**
- **ワイヤレス製品に関するサポート**
- **シスコのテクニカル サポートとダウンロード**

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