Lightweight アクセス ポイントに関する FAQ

内容

概要

このドキュメントでは、Cisco Lightweight アクセス ポイント（LAP）に関するよく寄せられる質問（FAQ）についての情報を示します。

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。

LAP に関する FAQ

Q. Cisco Lightweightアクセスポイント(LAP)とは何ですか。

A. Cisco LAPは、Cisco Unified Wireless Networkアーキテクチャの一部です。LAP は、Wireless LAN（WLAN）Controller（WLC; ワイヤレス LAN コントローラ）に接続するように設計された AP です。 LAP には、IEEE 802.11a、802.11b、および 802.11g をデュアル バンドでサポートし、ダイナミックおよびリアルタイムでの Radio Frequency（RF; 無線周波数）管理のための同時エアー モニタリング機能が備わっています。さらに、Cisco LAP では、レイヤ 2 暗号化などの時間依存型の機能も処理します。これらの機能によって、Cisco WLAN によって、音声、ビデオ、データなどのアプリケーションを安全にサポートできます。

AP が「Lightweight（軽量）」、つまり、ワイヤレス LAN コントローラ（WLC）から独立して動作できないことを意味しています。 WLC では AP の設定とファームウェアを管理します。AP は「ゼロ タッチ」で導入でき、AP の個別の設定は必要ありません。AP は、リアルタイムの MAC 機能しか取り扱えないという意味でも lightweight（軽量）です。AP では、非リアルタイムの MAC 機能はすべて WLC で処理するようになっています。このアーキテクチャは、「スプリット MAC」アーキテクチャと呼ばれます。

Q.ワイヤレスLANコントローラ(WLC)から独立して動作するようにLAPを設定できますか。

A.いいえ。LAPはWLCから独立して機能することはできません。LAP は WLC と一緒に使用されるときだけ機能します。この理由は、登録プロセスで LAP が必要とするファームウェアとすべての設定パラメータが、WLC から供与されるためです。

Q. Lightweight AP Protocol(LWAPP)とは何ですか。

A. LWAPPは、Internet Engineering Task Force（IETF；インターネット技術特別調査委員会）の

ドラフトプロトコルで、設定とパス認証、および実行時の操作の制御メッセージを定義します。また、LWAPP では、データ トラフィックのトンネリング メカニズムも定義しています。

LAP では、LWAPP ディスカバリ メカニズムを使用して、コントローラを検出します。LAP は、コントローラに対して、LWAPP 加入要求を送信します。コントローラが LAP に LWAPP 加入応答を送り、これによってこの AP がコントローラに加入できるようになります。LAP がコントローラに加入したとき、LAP とコントローラとの間でコントローラ ソフトウェアのリビジョンが異なるときには、LAP がソフトウェアをダウンロードします。その後、LAP が完全にコントローラの制御下に入ります。LWAPP は、セキュア鍵配布を使用して、LAP とコントローラの間の制御通信を安全に実行します。安全な鍵配布を行うには、LAP とコントローラの両方に、X.509 デジタル証明書が事前に用意されている必要があります。プレインストール済みの証明書は、「MIC」という用語で呼ばれます。これは Manufacturing Installed Certificate（製造元でインストールされる証明書）の略語です。2005 年 7 月 18 日より前に出荷された Cisco Aironet AP には、MIC はインストールされていません。そのため、Lightweight モードで動作するためにアップグレードされる場合、これらの AP で Self-Signed Certificate（SSC; 自己署名証明書）を作成します。コントローラは、個々の AP の認証に SSC を受け入れるようプログラムされています。

Q. CAPWAPとは何ですか。

A.コントローラソフトウェアリリース5.2以降では、Cisco Lightweightアクセスポイントは、IETF標準のControl and Provisioning of Wireless Access Points protocol(CAPWAP)を使用して、コントローラとネットワーク上の他のLightweightアクセスポイント間で通信します。リリース 5.2 よりも前のコントローラ ソフトウェアは、これらの通信に LWAPP アクセス ポイント プロトコル）を使用します。

LWAPP に基づいた CAPWAP は標準の相互運用可能なプロトコルであり、コントローラがワイヤレス アクセス ポイントの収集を管理できるようにします。CAPWAP は、次のような理由により、コントローラ ソフトウェア リリース 5.2 で実装されています。

- 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 コントローラと LWAPP コントローラは、同じネットワーク上に展開することができます。CAPWAP 対応のソフトウェアを使用すると、アクセス ポイントは CAPWAP または LWAPP のいずれかを実行するコントローラに加入することができます。唯一の例外は Cisco Aironet 1140 シリーズ アクセス ポイントで、CAPWAP のみをサポートするため、CAPWAP を実行するコントローラだけに加入します。たとえば、1130 シリーズ アクセス ポイントは CAPWAP または LWAPP のいずれかを実行するコントローラに加入できるのに対して、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だけに加入できます。

詳細については、構成ガイドの「アクセスポイントの通信プロトコル」を参照してください。

Q.標準（自律）APとLAPを区別するにはどうすればよいのですか。

A.通常のAPとLAPを区別する最も簡単な方法は、APの部品番号を調べることです。

- LAP（Lightweight AP Protocol [LWAPP]）：部品番号は*必ず* **AIR-LAPXXXX** で始まります。
- Autonomous AP（Cisco IOS® ソフトウェア）：部品番号は*必ず* **AIR-APXXXX** で始まります。

Cisco Aironet 1000 シリーズの LAP は、この基準の例外になります。1000 シリーズの LAP の部品番号は、次のとおりです。

- 1010 LAP の場合、AIR-AP1010-A-K9
- 1020 LAP の場合、AIR-AP1020-A-K9
- 1030 LAP の場合、AIR-AP1030-A-K9

注：部品番号は、国や規制区域によって異なる場合があります。ここでリストした部品番号は、一例に過ぎません。

使用している Wireless LAN（WLAN; ワイヤレス LAN）に適した AP を注文するようにしてください。

Q. Lightweight AP Protocol(LWAPP)を実行できるAPモデルはどれですか。

A.次の Cisco Aironet APプラットフォームでは、LWAPPを実行できます。

- Aironet 1500 シリーズ
- Cisco Aironet 1250 シリーズ
- Aironet 1240 AG シリーズ
- Aironet 1230 AG シリーズ
- Aironet 1200 シリーズ
- Aironet 1130 AG シリーズ
- Aironet 1000 シリーズ
- Aironet 1140 シリーズ AP**注：1140**シリーズAPは、5.2リリース以降が稼働するWLCでのみサポートされています。

注：これらの Aironet APとCisco IOSソフトウェアを発注して、自律APとして動作させるか、LWAPPで動作させることができます。部品番号から、AP が Cisco IOS ソフトウェアをベースとする AP か、LWAPP をベースとする AP かを判別できます。次に例を示します。

- AIR-AP1242AG-A-K9 は、Cisco IOS ソフトウェア ベースの AP です。
- AIR-LAP1242AG-P-K9 は、LWAPP ベースの AP です。

注：1000シリーズAPと1500シリーズAPは、この基準の例外です。1000 シリーズの AP と 1500 シリーズの AP では、すべて、LWAPP だけがサポートされています。

Q. LWAPP対応のアクセスポイントをインストールして設定するにはどうすればよいのですか。

A. LWAPP対応のAPはCisco Integrated Wireless Network Solutionの一部であり、マウントする前に手動設定は必要ありません。AP は、LWAPP 対応の Cisco ワイヤレス LAN コントローラ（WLC）で設定します。 LWAPP 対応のアクセス ポイントのインストールと初期設定については、『Cisco Aironet LWAPP 対応アクセス ポイント クイック スタート ガイド』を参照してください。

Q. LAPとワイヤレスLANコントローラ(WLC)を一緒に設定するにはどうすればよいのですか。

A. LAPはLightweight AP Protocol(LWAPP)を使用し、WLCに加入すると、WLCはすべての設定パラメータとファームウェアをLAPに送信します。基本設定については、『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』を参照してください。

Q. Autonomous APをワイヤレスLANコントローラ(WLC)に接続して、APが動作することを期待できますか。

A.いいえ。WLCに接続されているLAPだけが動作します。Autonomous AP では、WLC で使用される Lightweight AP Protocol (LWAPP) または CAPWAP プロトコルを認識できません。Autonomous AP を WLC に接続するには、まずその Autonomous AP を Lightweight モードに変換する必要があります。

Q.自律型のCisco IOSソフトウェアベースのアクセスポイントがあります。これをLightweight モードに変えることはできますか。

A.はいますが、すべての自律型Cisco IOSソフトウェアベースのAPモデルを変換できるわけではありません。Lightweight AP Protocol (LWAPP) モードに変換できるモデルは次のとおりです。

- Cisco Aironet 1130 AG AP の全モデル
- Aironet 1240 AG AP の全モデル
- Cisco IOS ソフトウェア ベースの Aironet 1200 シリーズのモジュラ AP (1200/1220 Cisco IOS ソフトウェア アップグレード、1210、および 1230 AP) プラットフォームの全モデルについては、AP の変換の可否は無線規格によって異なります。無線規格が IEEE 802.11g の場合は、MP21G および MP31G をサポートします。無線規格が IEEE 802.11a の場合は、RM21A および RM22A をサポートします。1200 シリーズの AP は、サポートされている次の無線規格と任意に組み合せてアップグレードできます。G のみA のみG と A の両方

注：自律APは、LWAPPに変換する前に、Cisco IOSソフトウェアリリース12.3(7)JA以降を実行する必要があります。

注：Lightweightモードに変換された自律APをサポートしているのは、Cisco 4400および2006ワイヤレスLANコントローラ(WLC)だけです。Cisco WLCでは、最小ソフトウェアバージョン3.1が稼働している必要があります。Cisco Wireless Control System(WCS)では、最小バージョン3.1が稼働している必要があります。アップグレードユーティリティは、Microsoft Windows 2000およびWindows XPプラットフォームでサポートされています。

変換方法についての詳細は、『Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順』を参照してください。

Q. Lightweightモードに変換した後、Cisco IOSソフトウェアベースのアクセスポイントにはどのような制限が課されますか。

A. Lightweightモードに変換されたAutonomousアクセスポイントを使用する場合は、次のガイドラインに留意してください。

- Lightweight AP Protocol (LWAPP) に変換された AP では、Wireless Domain Service (WDS; 無線ドメイン サービス) がサポートされません。LWAPP に変換された AP は、Cisco ワイヤレス LAN (WLAN) コントローラ (WLC) とだけ通信し、WDS デバイスとは通信できません。しかし、AP を WLC に関連付けた場合、WLC には WDS と同等の機能があります。

- 変換されたアクセス ポイントでは、2006、4400、および WiSM コントローラだけがサポートされます。Autonomous アクセス ポイントを Lightweight モードに変換するときは、アクセス ポイントは Cisco 2006 シリーズ コントローラ、4400 シリーズ コントローラ、または Cisco WiSM 上のコントローラとだけ通信できます。
- リリース 4.2 以降のコントローラ ソフトウェアでは、すべてのシスコの Lightweight アクセス ポイントで、無線規格ごとに合計 16 の BSSID、アクセス ポイントごとに合計 16 のワイヤレス LAN がサポートされます。それ以前のリリースでは、無線規格ごとに合計 8 の BSSID、アクセス ポイントごとに合計 8 のワイヤレス LAN しかサポートされていませんでした。変換されたアクセス ポイントがコントローラに関連付けられると、ID 1 ~ 16 のワイヤレス LAN だけが、アクセス ポイントにプッシュされます。
- LWAPP に変換された AP は、IP アドレスを得て、DHCP、Domain Name System (DNS; ドメイン ネーム システム) または IP サブネット ブロードキャストを使用して WLC を検出する必要があります。
- LWAPP に変換された AP では、レイヤ 2 LWAPP はサポートされません。
- LWAPP に変換された AP には、読み取り専用のコンソール ポートがあります。
- 変換用のアップグレード ツールでは、Cisco WiSM 上のコントローラの 1 つに対してだけ、Self-Signed Certificate (SSC; 自己署名証明書) キーハッシュが追加されます。変換ツールの実行が完了した後で、最初のコントローラの SSC キーハッシュを 2 番目のコントローラにコピーすることによって、Cisco WiSM 上の 2 番目のコントローラにも追加します。SSC キーハッシュをコピーするには、コントローラの GUI の [AP Policies] ページを開き ([Security] > [AAA] > [AP Policies])、[AP Authorization] リストの [SHA1 Key Hash] 列から SSC キーハッシュをコピーします。次に、2 番目のコントローラで同じページを開き、そのキーハッシュを [Add AP to Authorization List] の [SHA1 Key Hash] に貼り付けます。複数の Cisco WiSM を利用している場合は、WCS を使用して、SSC キーハッシュを他のすべてのコントローラにプッシュします。

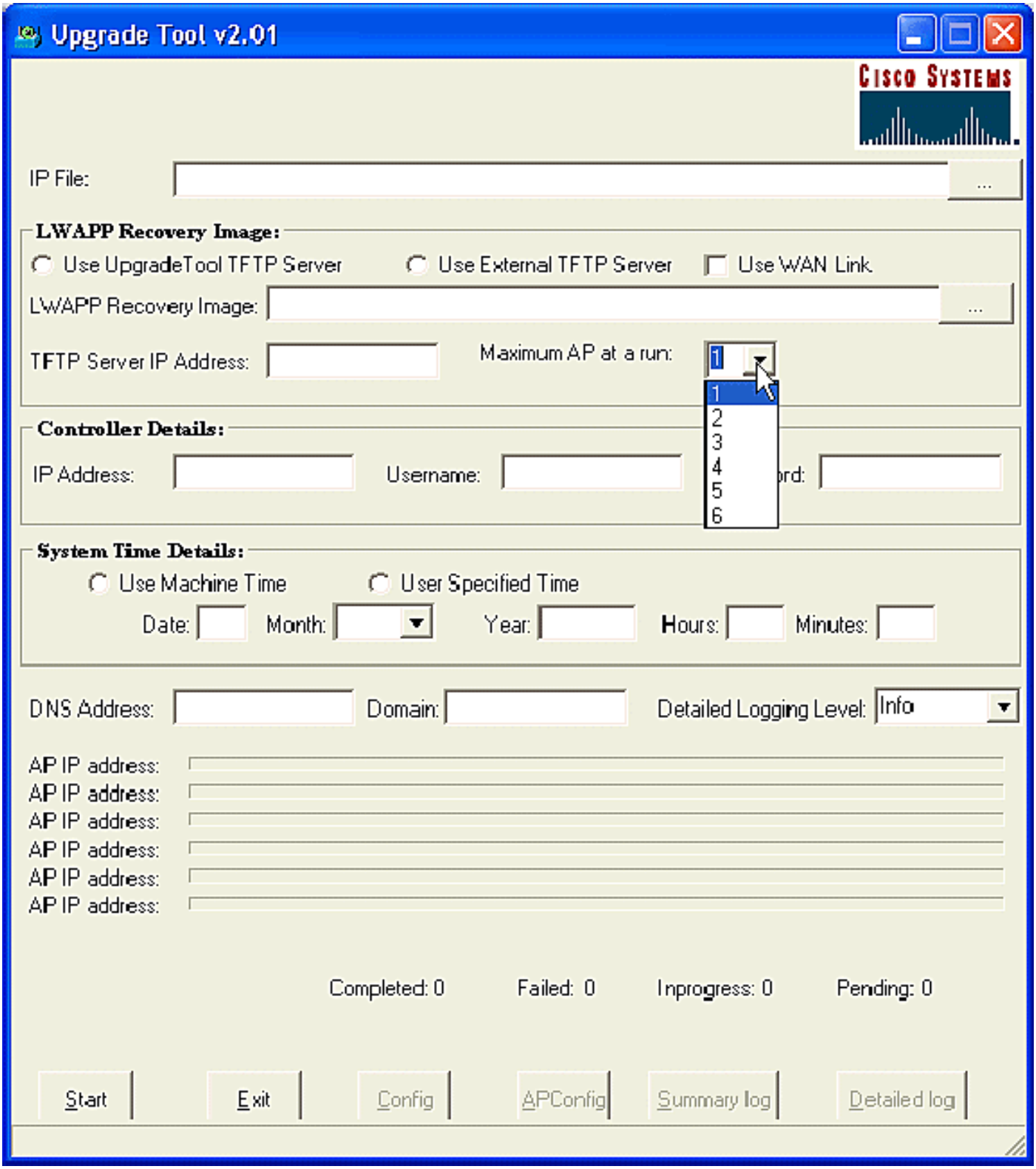
詳細については、『 Cisco IOS リリース 12.3(7)JX 向け Cisco Aironet 1130AG、1200、1230AG、および 1240AG シリーズのアクセス ポイントのリリース ノート』を参照してください。

Q.アクセスポイントをLightweightモードに変換しましたが、Autonomousモードに戻す必要があります。これは可能ですか。

A.はい。Lightweightモードに変換した自律APを自律モードに戻すことができます。『 Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順』の「Lightweight アクセス ポイントから Autonomous モードへの復帰」セクションの手順を実行してください。

Q.アップグレードツールで一度に変換できるアクセスポイントの数はいくつですか。

A.ツールの最新バージョン2.01では、一度に最大6つのAPをアップグレードできます。



Q. APをLightweight AP Protocol(LWAPP)に変換しましたが、APがコントローラに登録されません。メッセージ「LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP」が表示されます。 何が原因でしょうか。

A.このエラーは、X.509デジタル証明書が無効であることを意味します。Cisco Bug ID CSCsd42296（登録ユーザ専用）が発生している可能性があります。 この問題を回避するには、AP を工場出荷時のデフォルト設定にリセットします。

別の可能性として、Self-Signed Certificate（SSC; 自己署名証明書）が WLC に登録されていない

ことが考えられます。この場合は、SSC をコントローラに手作業で追加する必要があります。その手順については、『LWAPP で変換された AP 用のコントローラへの自己署名証明書の手動追加』を参照してください。

Q. Cisco IOSソフトウェアベースのAPをワークグループブリッジとして設定し、Lightweight AP Protocol(LWAPP)ベースのAPと関連付けることはできますか。

A.ワークグループブリッジとして動作するようにアクセスポイントを設定し、イーサネットでワークグループブリッジアクセスポイントに接続されたクライアントに代わって、Lightweightアクセスポイントにワイヤレス接続を提供できます。アクセス ポイントをワークグループ ブリッジとして動作するように設定し、Cisco Unified Network に接続すると、イーサネットでワークグループ ブリッジ アクセス ポイントに接続されている有線クライアントに、ワイヤレス接続を提供できます。たとえば、有線デバイスのグループに対してワイヤレス接続を提供する必要がある場合は、デバイスをハブまたはスイッチに接続して、そのハブまたはスイッチをアクセス ポイントのイーサネット ポートに接続し、そのアクセス ポイントをワークグループ ブリッジとして設定します。

『Cisco Unified Wireless Network でのワークグループ ブリッジの設定例』に設定の例が紹介されていいます。

Q. LWAPP APと自律APの間でワイヤレスクライアントをローミングできますか。

A.いいえ。LAPと自律AP間のローミングはサポートされていません。これは、LWAPP AP に接続した場合、トラフィックは LWAPP トンネルを通過するためです。ワイヤレス LAN コントローラと Autonomous AP の間にはモビリティ トンネルが存在しないため、ローミングは機能しません。

Q. Cisco Aironet 1000シリーズLAPの各種モデルで使用できるアンテナオプションは何ですか。

A. 1000シリーズのLAPエンクロージャには次のものが含まれます。

- IEEE 802.11a、または 802.11b/g の無線アンテナが 1 基
- 高ゲイン内部アンテナ 4 基 (802.11a が 2 基と 802.11b/g が 2 基)

これらのアンテナを別個にイネーブルまたはディセーブルにして、180°の扇型または 360°の全方向型のカバー領域を設定できます。1000 シリーズの LAP の一部には、外部アンテナを使用するものもあります。1000 シリーズの LAP には、次の 3 つのモデルがあります。

- 1010 LAP
- 1020 LAP
- 1030 LAP

使用可能なアンテナ オプションは次のとおりです。

- 1010 LAP の場合高ゲイン内部アンテナ 4 基外部アンテナ用のアダプタなし
- 1020 LAP の場合高ゲイン内部アンテナ 4 基5 GHz 外部アンテナ用アダプタ 1 基2.4 GHz 外部アンテナ用アダプタ 2 基
- 1030 LAP (リモート エッジ LAP) の場合高ゲイン内部アンテナ 4 基5 GHz 外部アンテナ用アダプタ 1 基2.4 GHz 外部アンテナ用アダプタ 2 基

A. External-Antenna Model B. Internal-Antenna Model

注：1000シリーズのLAPでは、FCC要件の違反を回避し、機器を操作するためのユーザ権限の欠落を回避するために、出荷時に用意された内部または外部アンテナを使用する必要があります。

Q. Cisco Aironet 1000シリーズのLAPで使用できる電源オプションは何ですか。

A. Aironet 1000シリーズLAPは、外部の110 ~ 220 VACから48 VDCへの電源、またはPower over Ethernet機器から電力を受け取ることができます。外部電源アダプタ（AIR-PWR-1000）は、安全な 110 ~ 220 VAC のコンセントに接続してください。コンバータによって、1000 シリーズの LAP に必要な 48 VDC の出力が生成されます。コンバータの出力は、48 VDC ジャックを経由して 1000 シリーズの LAP 側に供給されます。

注：AIR-PWR-1000外部電源には、国別の電源コードを付けて発注できます。正しい電源コードを入手するには、発注の際にシスコにお問い合せください。

Q. LWAPPベースのアクセスポイントにTelnet/SSHで接続できますか。

A.ワイヤレスLANコントローラ(WLC)リリース5.0以降では、コントローラはTelnetまたはセキュアシェル(SSH)プロトコルを使用してLightweightアクセスポイントをトラブルシューティングできます。特にアクセス ポイントがコントローラに接続できない場合、これらのプロトコルを使用するとデバッグが容易になります。コントローラ CLI を介してのみ Telnet と SSH のサポートを設定できます。

アクセス ポイントで Telnet または SSH 接続をイネーブルにするには、**config ap {telnet | ssh}コマ**ンドを使用します。Cisco Lightweight アクセス ポイントでは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco ワイヤレス LAN コントローラと関

連付けられます。

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

例

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

Q.アクセスポイントのグローバルクレデンシャルの設定方法リリース 5.0 でのデフォルトのユーザ名とパスワードは何ですか。

A. Cisco IOSアクセスポイントは、デフォルトのイネーブルパスワードとしてCiscoが設定された状態で工場から出荷されます。このパスワードにより、ユーザは非特権モードにログインし、show コマンドおよび debug コマンドを実行できますが、これにはセキュリティ上の脅威の問題があります。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートから設定コマンドを実行できるようにするためには、デフォルトのイネーブル パスワードを変更する必要があります。

リリース 5.0 よりも前のコントローラ ソフトウェアでは、現在コントローラに接続されているアクセス ポイントに対してのみ、アクセス ポイントのイネーブル パスワードを設定できます。コントローラ ソフトウェアリリース 5.0 では、アクセス ポイントがコントローラに加入するのに、すべてのアクセス ポイントが継承するグローバルなユーザ名、パスワード、およびイネーブル パスワードを設定できます。現在コントローラに加入しているすべてのアクセス ポイントと、将来加入するあらゆるアクセス ポイントがこれに含まれます。必要に応じて、グローバル クレデンシャルを上書きして、特定のアクセス ポイントに固有のユーザ名、パスワード、およびイネーブル パスワードを割り当てることができます。

AP のグローバル クレデンシャルを設定する方法については、『アクセス ポイントのグローバル クレデンシャルの設定』を参照してください。

Q.ファームウェアのバージョンが3.2.78.0のワイヤレスLANコントローラ(WLC)2006とアクセスポイント(AP)1242があります。アクセスポイントに問題があり、次のエラーメッセージが表示されます。「lwapp_clinet_error;not receive read response(3). Lwapp_image_broc;unable to open TAR file」が表示されました。

A. AP 1242は、変換されたLightweight Access Point Protocol(LWAPP)APです。AP 1242 を変換して使用しようとすると、AP 1242 はコントローラに加入のためのコントローラを探そうとします。AP がコントローラを見つけられないと、コンソールにこの種類のメッセージが表示されます。ただし、この場合コントローラのファームウェア バージョンは 3.2.78.0 であるため、アップグレードされた AP とともに動作する互換性はありません。アップグレードされた AP とともに動作するには、ファームウェア バージョン 3.2.116.21 が必要です。コントローラのファームウェアがアップグレードされれば、これらの AP はコントローラに加入し、機能するようになります。

Q.クライアントは、アクセスポイントに接続すると00:17:0f:37:65:c4のMACアドレスを表示しますが、アクセスポイントは00:17:0f:37:65:c0のベース無線MACアドレスを持っていることを示します。クライアントがアクセスポイントと異なるMACを表示する理由MAC アドレスが非常に近い 2 台のアクセス ポイントがある場合、デバイスが登録している MAC アドレスを判別する方法はありますか。

A. 詳細モードでアクセスポイントを調べると、ベースの無線MACアドレスとファストイーサネットMACアドレスがあることがわかります。また、WLAN とともに変化するのはベース Radio MAC アドレスです。クライアントでは実際には MAC アドレスの形式で BSSID が認識されます。

Q.リピータとして設定されたアクセスポイントを持つ既存のワイヤレスネットワーク（自律AP）があります。このネットワークを LWAPP 無線ネットワークに移行しようとしています。LWAPP AP をリピータとして使用できますか。

A. LWAPP APはコントローラに加入する必要があり、すべてのAPが最初にコントローラに接続する必要があるため、リピータモードをサポートしていません。シスコ製の Autonomous AP はリピータとして設定できますが、エンド クライアントが使用できる実質的な帯域幅が減少するため、リピータとしての設定は強く推奨できるものではありません。いずれの Cisco Aironet AP モデルまたは LAP モデルも LWAPP モードまたは Autonomous モードで使用できます。この変更を行うには、ソフトウェア イメージの変更が必要です。Autonomous モードから LWAPP モードへの移行は特に複雑です。そのため直接的には、AIR-LAP1232AG-A-K9 では、リピータ モードをネイティブにはサポートしていません。Autonomous ソフトウェアをロードして、リピータ モードをサポートするようにできますが、これにはソフトウェアの変更と、別個の設定が必要です。

Q. WLCは何台のAPをサポートできますか。

A. WLCごとにサポートされるAPの数は、モデル番号によって異なります。

- **2106**：8 基のファスト イーサネット インターフェイスを搭載し、最大 6 台の AP をサポートするスタンドアロン型 WLC。
- **4402**：12、25、または 50 台の AP をサポートするスタンドアロン型 WLC。
- **4404**：100 台の AP をサポートするスタンドアロン型 WLC。
- **5500**：あらゆる設置場所に対応でき、ビジネスクリティカルなワイヤレス サービスに適した、12、25、50、100、または 250 台のアクセス ポイントをサポートするスタンドアロン型の WLC。
- **WLCM**：シスコのサービス統合型ルータ（ISR）シリーズ専用に設計された WLC モジュール。現在利用可能なのは、6、8、または 12 台の AP のバージョン。
- **WS-C3750G**：Catalyst 3750 スイッチに統合された状態で出荷される 25 または 50 台の AP をサポートする WLC。WLC のバックプレーン接続は、2 個のギガビット イーサネット ポートとして装備されており、3750 に接続するために、それぞれを個別の dot1q トランクとして設定できます。または、3750 に EtherChannel で接続するために、1 つの集約リンクとしても設定できます。WLC は直接統合されているため、3750 スタッカブル スイッチで利用できるすべての拡張ルーティングおよびスイッチング機能にアクセスします。この WLC は中規模のオフィスまたは建物に最適です。4 台の 3750 が仮想スイッチとしてスタックされると、「50 台の AP」のバージョンを最大 200 台にまで拡張できます。
- **WiSM**：シスコの Catalyst 6500 スイッチ シリーズ専用に設計された WLC モジュール。モジ

ュールあたり最大 300 台の AP をサポートできます。6500 のプラットフォームによっては、複数の WISM をインストールすることにより、スケーリング キャパシティを大幅に拡大できます。WiSM は、6500 上では 1 つの集約されたリンク インターフェイスとして認識されるため、dot1 トランクとして設定することにより、6500 のバックプレーンに接続できます。このモジュールは、大規模な建物やキャンパスに最適です。

Q.アクセスポイントがサポートできるクライアント関連付けの最大数はいくつですか。

A.アクセスポイントがサポートできるクライアントの関連付けの最大数は、次の要因によって異なります。

- Lightweight アクセス ポイントと Autonomous IOS アクセス ポイントの場合、クライアント アソシエーションの最大数は異なります。
- 無線単位の制限と、AP 単位の全体的な制限が存在する場合があります。
- AP ハードウェア（16 MB の AP では、32 MB 以上の AP よりも制限が厳しくなります）

クライアント アソシエーションの制限に関する詳細については、『Cisco Wireless LAN Controller Configuration Guide, Release 7.0』の「Client Association Limits（クライアント アソシエーションの制限）」のセクションを参照してください。

Q. 1252 APはブリッジングをサポートしていますか。

A.はい、1252シリーズAPではブリッジモードがサポートされています。

Q. Lightweight AP Protocol(LWAPP)インフラストラクチャは、PPP over Ethernet(PPPoE)（PCクライアントからPPPoEサーバ）をサポートしていますか。

A.いいえ。LWAPPインフラストラクチャではPPPoEはサポートされていません。この理由は、PPPoE Ethertype がコントローラで廃棄されるためです。

Q. Cisco Aironet 1000シリーズLAPを手動でリセットするにはどうすればよいのですか。

A.ワイヤレスLAN(WLAN)コントローラ(WLC)を使用して、APを工場出荷時のデフォルトにリセットできます。 リセットするには、LAP が WLC に登録されている必要があります。

次のステップを実行します。

1. WLC の GUI で、**[Wireless]**をクリックします。[Wireless] タブから Cisco WLAN Solution ワイヤレス ネットワーク設定を実行できます。
2. **[Access Points] > [Cisco APs]** の順に選択し、**[Detail]** をクリックして、対象とする AP のウィンドウに移動します。
3. ウィンドウの最下部にある **[Clear Config]** をクリックします。この操作によって、LAP の設定がクリアされ、工場出荷時のデフォルトにリセットされます。

Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して LAP を工場出荷時のデフォルトにリセットするには、WLC の CLI から clear ap-config ap-name コマンドを発行します。

Q. Cisco Aironet 1000シリーズLAPの詳細はどこで入手できますか。

A. 『Cisco 1000シリーズLightweightアクセスポイント – Q&A』を参照してください。このドキュメントには、1000 シリーズ LAP に関する多数の質問への回答が掲載されています。

Q. Lightweight AP Protocol(LWAPP)レイヤ2モードをサポートしているシスコデバイスはどれですか。

A. LWAPPレイヤ2モードは、次のシスコデバイスでのみサポートされています。

- Cisco 4100 シリーズ ワイヤレス LAN コントローラ (WLC)
- Cisco 4400 シリーズ WLC
- Cisco Aironet 1000 シリーズ LAP

Q. Cisco LAPでは、コントローラディスカバリにDHCPオプション43を含むベンダークラス識別子(VCI)文字列が使用されることを理解しています。Cisco LAP の VCI 文字列の値は何ですか。

A. Cisco Aironet 1000シリーズAPはDHCPオプション43に文字列形式を使用しますが、他のAironet APはDHCPオプション43にtype、length、value(TLV)形式を使用します。DHCPサーバをプログラムして、DHCP文字列ををにを返指定しますDHCPオプション60)。 次の表は、各 LAP の VCI ストリングの値の一覧を示しています。

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

Q. DHCPオプション43に関するType Length Value(TLV)ブロック値の意味を教えてください。TLV 値はどのように計算されるのですか。

A. DHCPオプション43は、次のコマンドを使用して、Cisco IOSルータのDHCPサーバで有効にできます。

```
Option 43 hex <string>
```

このコマンドの 16 進数文字列は、オプション 43 のサブオプションの TLV 値を連結することで作成されます。

Type + Length + Value

- **Type** は常にサブオプション コードの 0xf1 です。
- **Length はコントローラの管理 IP アドレスの数の 4 倍の 16 進数表記です。**
- **Value は順番にリストされたコントローラの IP アドレスの 16 進数表記です。**

たとえば、管理インターフェイス IP アドレス 10.126.126.2 と 10.127.127.2 を持つ 2 台のコントローラがあるとします。

- Type は 0xf1 です。
- Length は 2 * 4 = 8 = 0x08 です。
- 各 IP アドレスは 0a7e7e02 (10.126.126.2) と 0a7f7f02 (10.127.127.2) に変換されます。
- 文字列を組み立てると、f1080a7e7e020a7f7f02が生成されます。その後、IOSコマンドがDHCPスコープに追加されます。

```
option 43 hex f1080a7e7e020a7f7f02
```

Q.ワイヤレスLANコントローラ(WLC)はAPロードバランシングをサポートしていますか。

A.はい、WLCでAPロードバランシングを実行できます。詳細は、『ワイヤレス LAN コントローラ (WLC) に関するよくある質問』を参照してください。

Q. LAPのワイヤレスLANコントローラ(WLC)フェールオーバーを設定するにはどうすればよいのですか。

A. WLCフェールオーバーの設定方法の詳細は、『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』を参照してください。

Q. AutonomousモードからLightweightモードへの変換後にAPのリセットボタンをディセーブルにするにはどうすればよいのですか。

A. Lightweightモードに変換したAPのリセットボタンを無効にできます。リセット ボタンは AP の外側にあり、「MODE」というラベルが付けられています。次のコマンドを使用して、コントローラと関連付けられている、1 台またはすべての変換された AP のリセット ボタンを、ディセーブルまたはイネーブルにできます。

```
config ap reset-button {enable | disable} {ap-name | all}
```

変換された AP のリセット ボタンは、デフォルトではイネーブルになっています。

Q.ワイヤレスLANコントローラ(WLC)からWANリンクを介してLightweight AP Protocol(LWAPP)対応のAPを接続できますか。可能な場合、どのようにして動作するのですか。

A.あります。一部のLAPでは、リモートエッジAP(REAP)と呼ばれる機能がサポートされています。 この機能を使用すると、LAP が接続する WLC との間に WAN リンクを経由する LAP を設定できます。REAP モードを使用すると、WAN リンクを経由して LAP を配置し、WLC との通信を維持しながら、通常の LAP 機能を利用できます。この設定の詳細については、『Lightweight AP および Wireless LAN Controller (WLC) でのリモートエッジ AP (REAP) の設定例』を参照してください。

注：REAPモードは、この時点でCisco Aironet 1030 LAPでのみサポートされています。将来的には、より広範囲の LAP で REAP 機能をサポートする予定です。

Q.通常のAPおよびH-REAP APと同じWAN制限がモニタモードAPにありますか。つまり、コントローラとモニタ モード AP との間には 100 ミリ秒またはそれよりも高速な RTD が必要ですか。

A.いいえ、モニタモードAPには100ミリ秒の制限はありません。これは、制限の理由であるクライアント関連付けが存在しないためです。100 ミリ秒のレイテンシ制限は、多様で、多くの場合厳格なクライアント認可の要件により設定されたものです。これが、ローカル モードの AP と H-REAP の AP の両方が同じレイテンシ制限を持つ理由です。当然、モニタ モード AP には同じクライアント制限はありません。

Q. WLCバージョンは3.2です。レイヤ3 Lightweight Access Point Protocol(LWAPP)用に設定されています。 この WLC と Lightweight Access Point (LAP; Lightweight アクセス ポイント) との間のネットワークの MTU は 900 バイトに設定されています。使用している LWAPP AP がこの WLC に加入できません。この理由として何が考えられますか。

A.シナリオで設定されているMTUは900バイトです。しかし、LWAPP 加入要求は 1500 バイトよりも大きいものです。したがって、LWAPP では LWAPP 加入要求をフラグメント化する必要があります。すべての LWAPP AP での ロジックは、最初のフラグメント サイズは 1500 バイト (IP および UDP ヘッダーを含む) であり、2 番目のフラグメント サイズが 54 バイト (IP および UDP ヘッダーを含む) というものです。 この場合のように、LWAPP AP と WLC との間のネットワークの MTU サイズが 1500 より小さいと (VPN、GRE、MPLS など)、WLC で LWAPP 加入要求を処理できなくなります。したがって、その LWAPP はコントローラに加入できません。

この状況に対処するには、コントローラをバージョン 4.0 にアップグレードしてください。このバージョンではレイヤ 3 のフラグメントを処理できます。この問題の詳細については、Cisco Bug ID CSCsd94967(登録ユーザ専用)を参照してください。

Q.シンガポールから入手したWLCがあります。この WLC を使用してリモート オフィスを WLC に接続し (REAP)、無線接続を行うことを考えています。オフィスは他の国にあります。ただし、シンガポールの WLC から、規制区域に関するエラー メッセージが送られてきます。この WLC に、異なる規制区域にある Access Points (AP; アクセス ポイント) を受け入れさせるようにする方法はありますか。表示されたエラー メッセージは、「AP 'AP_NAME' is unable to associate.**The Regulatory Domain configured on it '-R' does not match the Controller 'A.B.C.D' country code 'SG - Singapore**

A. WLCでは、1つの規制ドメインだけがサポートされます。したがって、規制区域 -A を使用する WLC では、規制区域 -A を使用する AP しか使用できません (他の場合も同様)。 この場合は、

WLC がシンガポール向けに -SG に設定されています。そのため、シンガポールの規制領域にある AP しかサポートできません。

AP および WLC を購入するときには、それらが同一の規制ドメインのものかどうかを確認してください。それ以外の場合は、AP は WLC に登録できません。

複数の国コードのサポート：WLC バージョン 4.1.171.0 以降では、WLC に複数の国コードのサポートが導入されています。リリース 4.1.171.0 以降では、コントローラごとに 20 までの国コードを設定できます。複数の国コードをサポートしているため、1 つのコントローラからさまざまな国のアクセス ポイントを管理できます。この機能は、Cisco Aironet メッシュ アクセス ポイントでは使用できません。

Q. Lightweightアクセスポイント(LAP)が動作できるモードにはどのようなものがありますか。

A. LAPは、次のいずれかのモードで動作できます。

- **Local モード**：これはデフォルトの動作モードです。LAP をローカル モードで動作させる場合、AP は、正常に割り当てられたチャネルで送信を実施します。ただし、AP はそれと同時に、帯域内の他チャネルすべてを 180 秒間監視し、非送信時間中に他チャネルそれぞれについて 60 ミリ秒間のスキャンを行います。この間、AP ではノイズ フロア測定を実行し、干渉を測定し、IDS イベントをスキャンします。
- **REAP モード：リモート エッジ アクセス ポイント（REAP）モードを使用すると、WAN リンクを経由して LAP を配置し、WLC との通信を維持しながら、通常の LAP 機能を利用できます。**REAP モードは 1030 LAP のみでサポートされています。
- **H-REAP モード：H-REAP は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。**H-REAP によって、各オフィスにコントローラを導入することなく、ブランチ オフィスやリモート オフィスにあるアクセス ポイント（AP）を本部から WAN リンク経由で設定して制御できます。H-REAP では、コントローラへの接続が失われたときに、クライアント データ トラフィックをローカルでスイッチして、クライアント認証をローカルで実行することができます。コントローラに接続されたときには、H-REAP はトラフィックをコントローラにトンネリングして戻すこともできます。
- **Monitor モード**：Monitor モードは、指定した LWAPP 対応の AP が、クライアントとインフラストラクチャ間のデータ トラフィックの処理から自分自身を除外できるようにするために設計された機能です。代わりに、その AP はロケーション ベース サービス（LBS）、不正なアクセス ポイントの検出、および侵入検知（IDS）用の専用センサーとして動作します。Monitor モードになっていると、AP はクライアントにサービスを提供できませんが、すべての設定済みチャネルを継続的に巡回して、各チャネルを約 60 ミリ秒間リスニングします。**注：コントロー**ラのリリース5.0からは、LWAPPはLocation Optimized Monitor Mode(LOMM)でも設定できます。これにより、RFIDタグの監視とロケーション計算が最適化されます。このモードについての詳細は、『Cisco Unified Wireless Network ソフトウェア リリース 5.0』を参照してください。**注：コントロー**ラ· リリース5.2では、[Location Optimized Monitor Mode (**LOMM)]セクションの名前が[Tracking Optimization]に変更さ**れ、[**LOMM Enabled**]ドロップ· ダウン· ボックスの名前が[Enable Tracking Optimization]に変更されました。**注：トラッキング**最適化の設定方法の詳細については、「アクセスポイントでのRFIDトラッキングの最適化」セクションを参照してください。
- **Rogue detector モード**：Rogue Detector モードで動作する LAP は不正な AP を監視します。このような LAP は不正な AP に送信を行わず、除外します。これは、不正な AP はネットワークの VLAN の任意の場所に接続されている可能性があるため、Rogue Detector はネット

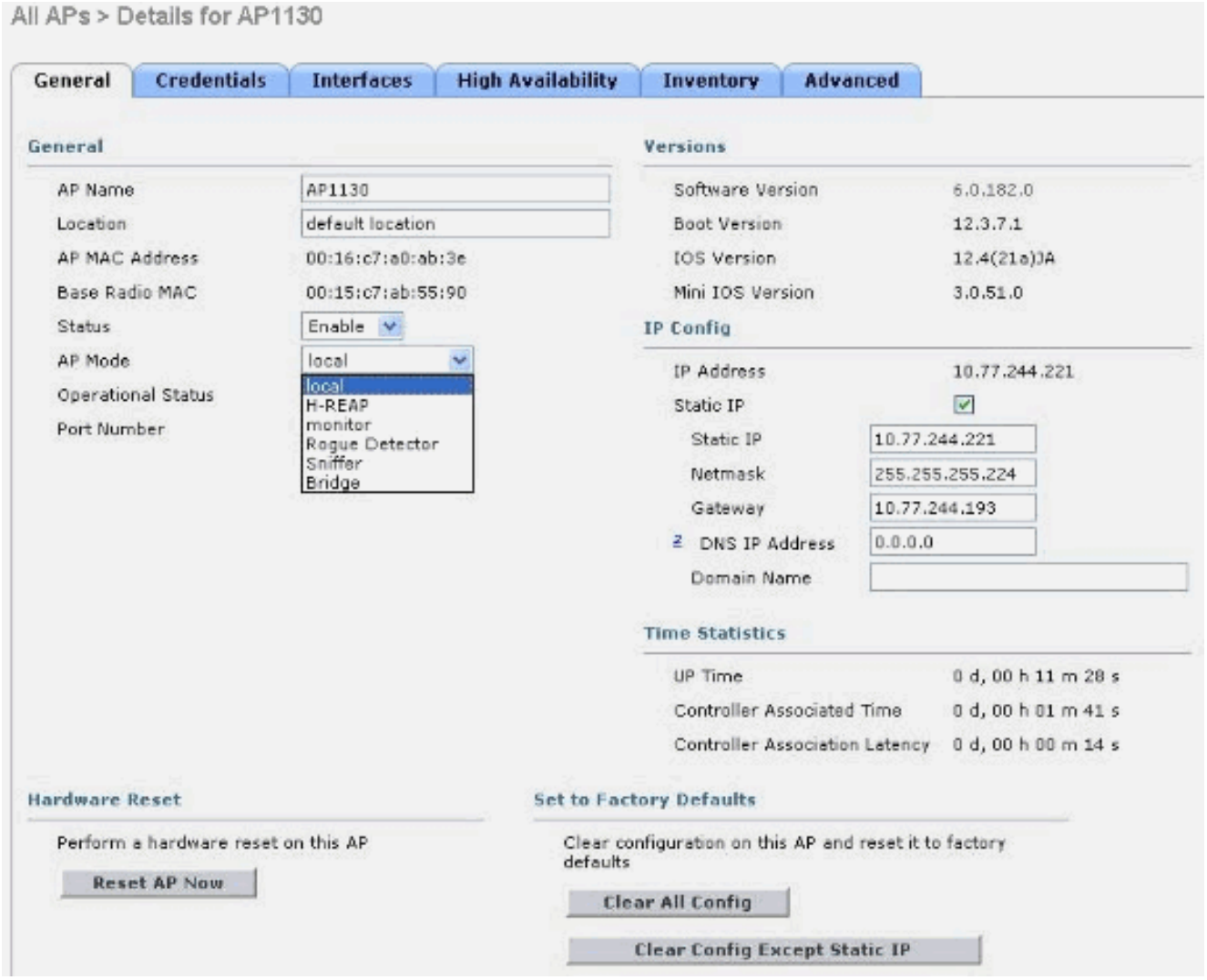
ワークのすべての VLAN を認識できる必要があるという概念に基づいています（そのため Rogue Detector をトランク ポートに接続します）。 スイッチは、すべての不正な AP/クライアントの MAC アドレス リストを Rogue Detector（RD）に送信します。 続いて RD は、WLC AP が無線で検出したクライアントの MAC と比較するために、これらを WLC に転送します。MAC が一致すると、有線ネットワーク上でこれらのクライアントが接続されている不正な AP が WLC で認識されます。

- **Sniffer モード**：Sniffer モードで動作する LWAPP はスニファとして機能し、特定のチャネル上のすべてのパケットをキャプチャして、Airopeek が稼動するリモート マシンに転送します。これらパケットには、タイムスタンプ、信号強度、パケット サイズなどに関する情報が含まれています。スニファ機能は Airopeek が稼働している場合にのみ有効にできます。Airopeek はサードパーティ ネットワーク アナライザ ソフトウェアで、データ パケットのデコードをサポートしています。
- **ブリッジ モード：ブリッジ モードは、アクセス ポイントをメッシュ環境で設定して相互間のブリッジとして使用する場合に使用します。**

Q. Lightweightアクセスポイントのモードを変更するにはどうすればよいのですか。

A. Lightweightアクセスポイントのモードを変更するには、次の手順を実行します。

1. WLC の GUI から、[ワイヤレス（Wireless）] > [アクセスポイント（Access Points）] > [すべてのAP（All APs）] の順に選択し、登録済みの AP のリストから、モード変更の必要がある AP を選択します。
2. [すべてのAP>APの詳細（All APs > Details for AP）] **ページが表示されます。**下の図に示すように、このページの [一般（General）] **タブで、[APモード（AP Mode）] ドロップダウンメニューからモードを選択します。**



Q.特定のコントローラにプライミングされたLAP-1131AGアクセスポイントを新しくインストールしました。コントローラのバージョンは4.0.155.5です。プライミングされているワイヤレスLANコントローラ(WLC)と同じWLCで起動すると、最終的にライトグリーンになります。マニュアルでは、ステータス LED のこの緑の点灯は、アクセス ポイントが WLC に接続されていることを意味すると記載されています。しかし、WLC のアクセス ポイントのリストではこのアクセス ポイントが見つかりません。なぜでしょうか。Lightweight Access Point Protocol (LWAPP) は関連付けられるようになっていますか。

A.アクセスポイントがレイヤ3のWLCにプライミングされているが、起動時にIPアドレスを取得できない場合、WLCのステータスLEDは緑色に点灯し、DHCPからIPアドレスを取得するまで検索とリブートの順序に入りません。

そのため、このようなシナリオでは、ステータス LED が緑色に点灯していても、LWAPP がコントローラに登録されていることを示しているわけではありません。アクセス ポイントでは、DHCP アドレスを取得できるようになると、WLC を探し、見つからない場合は再起動プロセスを実行して期待どおりに進行します。この問題に関連する不具合が存在します。

詳細は、Cisco Bug ID CSCsf10580(登録ユーザー専用)を参照してください。

Q. LAPのLEDは何を示していますか。

A.これは、1130AG Lightweight APのLEDの解釈方法を説明する短いビデオへのリンクです。

『Interpreting LAP LEDs - LAP1130』[英語]

Q.軽量メッシュアクセスポイント(MAP)のモードとして、ルーフトップアクセスポイント(RAP)とポールトップアクセスポイント(PAP)の違いは何ですか。

A.これらは屋外MAPがメッシュネットワークの一部として動作できるモードです。Cisco Unified Wireless Network Solution の一部であるメッシュ ネットワーキング ソリューションにより、複数の Cisco Aironet Lightweight MAP が 1 つ以上のワイヤレス ホップ経由で相互に通信し、複数の LAN に加入したり、802.11b 無線カバレッジを拡張したりできます。

これらのアクセス ポイントはメッシュ ネットワークの一部として使用され、次の 2 つのモードで動作します。

1. RAP
2. PAP

RAP：RAP モードで動作する Cisco MAP は、ブリッジング ネットワークやメッシュ ネットワークの親ノードであり、ブリッジ ネットワークやメッシュ ネットワークを有線ネットワークに接続する役割を果たしています。そのため、ブリッジド ネットワークやメッシュ ネットワークのセグメントに存在できる RAP は 1 つだけになります。メッシュ ネットワークでは、Cisco MAP の設定、監視、操作は、配備されている Cisco ワイヤレス LAN コントローラ（WLC）から、およびこれを経由して行われます。WLC に有線で接続されているすべての MAP が RAP の役割を引き受けます。この RAP はバックホール ワイヤレス インターフェイスを使用して、ネイバーの PAP と通信します。

PAP：PAP モードで動作する Cisco MAP は、Cisco WLC に有線接続されていません。このような MAP は完全なワイヤレス化が可能であるため、他の PAP や RAP と通信するクライアントをサポートすることも、周辺デバイスや有線ネットワークへの接続にも使用できます。デフォルトでは、セキュリティ上の理由によりイーサネット ポートが無効になっていますが、PAP 用には有効にしてください。

MAP がどのように RAP と PAP の役割を引き受けるかについての詳細は、『Cisco メッシュ ネットワーキング ソリューション展開ガイド』の「ゼロ タッチの設定」セクションを参照してください。

Q. 1000シリーズLightweightアクセスポイント(LAP)アンテナの放射パターンはどのように解釈するのですか。

A.方位図は通常、装置/アンテナと通常の動作方向(垂直、上、オムニ用の図の中央に配置されます。水平、中心のマウント、図の「0」向きの順方向）のデバイス/アンテナに関するものです。 ほとんどの場合 A 側が順方向で、アジマス方向の 0 マークと、エレベーション方向の 90 のマークで表されています。B 側は、アジマス方向の 180 マークと、エレベーション方向の 270 で表されています。装置が反転した場合、空き領域ではパターンは変化しません。ただし、隣接している表面が反射/吸収の原因になり、パターンを変化させる可能性があります。送信アンテナの近く（2 波長内程度）に金属物体があると、パターンが大きく歪む可能性もあります。『Cisco Aironet アンテナ リファレンス ガイド』に詳細が記載されています。1000 シリーズのアンテナは、このドキュメントの最後のセクションで説明されています。

Q.コントローラに加入するAPを制限できますか。[SECURITY/AAA/AP Policies] ページが表示されており、AAA または証明書によって AP を許可できます。認証リス

トに AP を追加できますが、それによって、AP の認証リストのみでコントローラへの加入が制限されるようになりますか。

A.いいえ、コントローラはAPを先着順に処理します。プライマリ、セカンダリ、および三次のフィールドを操作すると、優先度に合せて AP 接続の確率を高められる可能性があります。

Q. LWAPPでは、APごとにSSIDを判別できますか。固有の SSID を使用するゾーンで特定の AP を使用しながら、他のすべてでは別の SSID のセットを使用できるようにするには何が必要ですか。

A. WLAN overrideオプションを使用すると、APが提供するSSIDを選択できます。コントローラはそれぞれ最大16のSSIDのみをサポートしているため、サポートされている16の中から選択できます。これはAPごとに行われます。

Q. LAPで一部のLWAPPコマンドを有効にすると、コマンドが無効であるというエラーが表示されます。なぜでしょうか。

```
AccessPoint#clear lwapp ap controller ip address
ERROR!!! Command is disabled.
```

A. APがコントローラに正常に加入すると、LWAPPコマンドは無効になります。LWAPP コマンドを再度有効にするには、config ap username <name> password <pwd> <cisco-ap>/all コマンドを使用して、コントローラ CLI から AP のユーザ名/パスワードを設定する必要があります。この操作を行えば、AP CLI で clear lwapp private-config を実行すると、AP LWAPP 設定コマンドを手動で再発行できます。

注：WLCバージョン5.0以降を実行している場合は、次のコマンドを使用してAPにユーザ名とパスワードを設定します。

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

Q. 2つのAPが同じチャネル上にあり、互いを認識できる場合、3つのチャネルではなく4つのチャネルを使用した場合の影響 (ローミングスループットなど) は何ですか。このような状況では AP はどのように反応し、またクライアントはどのように反応しますか。

A. APが同じチャネル上にあるかどうかは、クライアントのローミングに特に影響しません。問題なのは十分なセルのオーバーラップで、これによって、ある AP のカバレッジ エリアから次の AP へのクライアントのスムーズな移行が可能になります。3 チャネル設計から 4 チャネル設計へ移行する目的は、（「追加の」チャネルにより）設計の柔軟性を高めることです。（別のチャネルがあるので）配備の柔軟性を少し高めている一方で、実際には共用チャネル干渉の量を増やしているため、この方法は近視眼的です。4 チャネル方式を使用して得られる設計の柔軟性は、共用チャネル干渉が高まることで失われます。まとめ4 チャネル設計は使用しないでください。

Q.クライアントがローミングするタイミングを制御できますか。すべてのクライアント アダプタに関して、AP 単位で信号強度だけに基づいてクライアントにローミングさせることはできますか。

A.現在では、ローミングは常にクライアントの機能であり、ローミングするかどうかの選択は異なるクライアントに実装されています。Directed Roaming は CCX の一部ですが、オプション機能であり、現在は使用されていません。

Q.リモートサイトのREAP/HREAP APとメインサイトのWLCの間に実装されるWANリンクに関して、特定の要件や推奨事項はありますか。

A. WANリンクで考慮すべき主な要因は次のとおりです。

- WAN リンクの帯域幅は少なくとも 128kbps にする。
- 特に集中管理型の認証が実装されている場合に、遅延が 300 ミリ秒を超えるとクライアントに対する認証の問題が発生する可能性があるため、WAN リンクの 2 つのサイト間のレイテンシまたはラウンドトリップ遅延は 300 ミリ秒を超えないようにします。

Q. LAPがWLCとの通信を失ったため、数時間ネットワークがシャットダウンされました。これらの AP にスタティック IP アドレスが設定されている場合でも、ネットワークが復帰した後、LAP は DHCP サーバから IP アドレスを取得します。「show ap config general <ap-name>」では「Fallback IP Address」と表示されています。 なぜ、このような現象が発生するのでしょうか。

A. LAPは、LWAPPディスカバリメッセージを使用して、WLCとの関連付けを最大20回試行します。接続できない場合は、DHCP を介して新しい IP アドレスの取得を試みます。LAP が DHCP サーバから 1 つの IP アドレスを取得できると、この IP アドレスがアクティブなアドレスになり、フォールバックには割り当て済みのスタティック IP アドレスが使用されます。この背景には、LAP が別の VLAN（たとえば別の建物）に移動した場合でも、LAP は IP アドレスを取得して、WLC に加入できるという概念があります。この動作については、バグCSCse66714で説明されています。WLCをソフトウェアバージョン4.0.206.0にアップグレードする必要があります。

Q.メッシュネットワークにブリッジグループ名を設定する必要がありますか。

A.ブリッジグループ名(BGN)を使用して、メッシュ内のAPを論理的にグループ化できます。デフォルトでは関連付けを許可するために AP には null 値の BGN が付いていますが、シスコでは BGN を設定することを推奨いたします。この設定変更は、次のコマンドにより CLI か GUI で行うことができます。

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

注： BGN は最大 10 文字まで設定できます。コントローラの GUI のメッシュ アクセス ポイントの設定ページの [BGN] フィールドに 10 文字を超える文字を入力した場合には、エラー メッセージが表示されます。**config ap bridgegroupname set groupname Cisco_MAP** CLI コマンドまたは WCS を介してこのパラメータを設定した場合にも、エラー メッセージが表示されます（CSCsk64812）。

実稼動中のネットワークで BGN を設定する場合、最も遠い MAP から設定し、順に RAP に戻るように作業してください。これが非常に重要であるのは、親と関連付けを確立できない子 MAP を取り残す可能性があり、これで BGN がアップデートされる可能性があるためです。ネットワークの異なる部分を論理的にグループ化するには、異なる BGN を使用します。これは、同じ RF 領域内に複数の RAP があり、メッシュのセグメントの分離を維持する必要がある場合に有用です。

実稼働中のネットワークに新しい AP を追加する場合は、新しい AP 上で BGN を事前に設定する必要があります。新しく開封したばかりの AP を使用して最初からメッシュ ネットワークを構築する場合、AP では BGN が NULL 値にプリセットされています。AP は BGN のこのデフォルト値を使用して新しいネットワークに加入します。AP の BGN は次のコマンドで確認できます。

```
show ap config general Cisco AP
```

Q. BGNが正しく設定されていない場合はどうなりますか。

A. APが意図したブリッジグループ名以外のブリッジグループ名で誤ってプロビジョニングされている場合は、ネットワークの設計によっては、このAPが正しいセクタまたはツリーを見つけることができないか、見つけることができません。互換性のあるセクターに到達できない場合は、取り残される可能性があります。そのような取り残された AP を回復するために、デフォルトのブリッジ グループ名という概念が導入されています。基本的な概念としては、設定されたブリッジ グループ名を使用して他のどの AP にも接続できない AP は、デフォルトのブリッジ グループ名を使用して接続を試みます。

この取り残された状況を検出し回復するために使用されるアルゴリズムは次のとおりです。

1. ブリッジ グループ名に関係なく、すべてのネイバー ノードをパッシブにスキャンして、検索する。
2. AP は、Adaptive Wireless Path Protocol（AWPP）を使用して、独自のブリッジ グループ名で検出されたネイバーに接続を試みる。
3. 手順 2 が失敗した場合、AWPP を使用してデフォルトのブリッジ グループ名で接続を試みる。
4. 手順 3 の失敗した各試行に対して、そのネイバーを exclusion-list に入れ、それに次ぐ最善のネイバーに接続を試みる。
5. 手順 4 で AP がすべてのネイバーとの接続に失敗した場合、AP を再起動する。
6. デフォルトのブリッジ グループ名で 30 分間接続した場合、すべてのチャネルを再スキャンし、正しいブリッジ グループ名を使用して接続を試みる。

注：APがデフォルトのブリッジグループ名で接続できると、親ノードはAPをWLANコントローラのデフォルトの子/ノード/ネイバーエントリとして報告し、ネットワーク管理者が取り残されたAPを認識します。そのような AP は、クライアントや他のメッシュ ノードを子として受け入れることができず、またデータ トラフィックを渡すこともできません。

Q. LAP 1030は他のブリッジモデルにブリッジできますか。また、LAP 1020 はブリッジングをサポートできますか。

A. LAP 1020モデルはブリッジングをサポートしていません。LAP 1030 は別の LAP 1030 へのブリッジング（1 ホップ）をサポートしていますが、現時点では BR1310、BR1400、または LAP 1500 へのブリッジングをサポートしていません。

Q. LAP AP間でワイヤレスブリッジングを設定することはできますか。使用している非有線 LAP の 1 つの無線で、有線ルート ブリッジ LAP（WLC に接続された LAP）に戻るブリッジングを実行する必要があります。 これは可能ですか

A.いいえ。これはLAP APでは実行できません。Cisco Unified Wireless Network では、メッシュ AP が基本的なポイントツーポイント ブリッジングを実行できます。その他に可能な唯一のブリッジングは、WGB（Workgroup Bridge）モードで IOS AP を介する方法です。これらの IOS AP は、LAP AP に対して（背後に有線デバイスがある）クライアントとして機能します。ただし、

ワイヤレス クライアントはこれらの IOS AP に接続できません。

Q. LAP 1131があり、このアクセスポイントはワイヤレスLANコントローラに正常に登録されています。パワー インジェクタのないアクセス ポイントの接続では、無線はアップ (LED ステータスは緑) ですが、パワー インジェクタのある AP の接続では、無線はダウン (LED ステータスはオレンジ) になります。 この問題を解決するには、どうすればよいですか。

A.この問題は、誤って設定されたPower over Ethernet(POE)パラメータが原因である可能性があります。この問題を解決するには、次の手順を実行します。

1. これらのパラメータにアクセスするために、[Wireless] をクリックします。
2. 問題のアクセス ポイントの [Detail] リンクをクリックします。新しいパラメータは [POE settings] の [All APs > Details] ページに表示されます。
3. アクセス ポイントの POE 設定用の [APs > Details] ページで、[Power Injector State] をクリックし、[Installed] を選択します。
4. チェック ボックスにチェックを入れ、アクセス ポイントの [Power Injector State] を有効にします。接続されているスイッチが IPM をサポートしておらず、パワー インジェクタが使用されている場合、このパラメータは必須です。接続されているスイッチが IPM をサポートしている場合、このパラメータは必須ではありません。

Q. Autonomous APでは、このAPに関連付けられたクライアントデバイスがワイヤレスネットワーク上の他のクライアントデバイスと誤ってファイルを共有することを避けるために、Public Secure Packet Forwarding(PSPF)が使用されます。Lightweight AP には同等の機能はありますか。

A.軽量アーキテクチャでPSPFと同様の機能を実行する機能またはモードは、ピアツーピアブロッキングモードと呼ばれます。ピアツーピア ブロッキング モードは、LAP を管理するコントローラで実際に使用できます。

このモードがコントローラ上でディセーブルになっている場合 (デフォルトの設定)、ワイヤレス クライアントはコントローラを介して相互に通信できます。このモードが有効である場合、コントローラを介したクライアント間の通信はブロックされます。

このモードは、同じコントローラに加入している AP の間でのみ機能します。有効である場合、同じモビリティ グループ内でも、このモードはあるコントローラで終端するワイヤレス クライアントが、別のコントローラで終端しているワイヤレス クライアントに到達する機能をブロックしません。

Q. LAP APはIOS APのようなSNMPメッセージを処理できますか。

A. LAP APは、SNMPメッセージを自身で処理できません。SNMP メッセージを処理するためには、LAP の登録先である WLC で SNMP コミュニティを設定する必要があります。すべての AP 情報は WLC により管理されます。

関連情報

- ワイヤレス LAN コントローラ (WLC) のトラブルシューティングに関する FAQ

- Cisco Wireless LAN Controller モジュール
- シスコ ワイヤレス LAN コントローラ (WLC) に関する FAQ
- Cisco ワイヤレス LAN コントローラ設定ガイド 、リリース 3.2
- 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
- テクニカル サポートとドキュメント – Cisco Systems