Cisco Aironet アクセス ポイントに関する FAQ

目次

概要

このドキュメントでは、Cisco Aironet アクセス ポイント（AP）に関するよくある質問（FAQ）に回答しています。

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. Cisco IOS® ソフトウェアベースの AP 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 ソフトウェアベースの AP のデフォルト設定には、ユーザ名とパスワードの組み合わせも含まれています。デフォルトでは、ユーザ名もパスワードも **Cisco**（大文字と小文字が区別される）に設定されています。 工場出荷時のデフォルトにリセットした後、GUI または Command-Line Interface（CLI; コマンドライン インターフェイス）でユーザ名とパスワードの入力を求めるメッセージが表示されたら、両方に Cisco と入力してください。

Q. コンソールの接続には、どのようなケーブルを使用する必要があるのですか。

A. 9 ピン オスと 9 ピン メスのコネクタの付いたストレート型ケーブルを使用して、コンピュータの COM1 または COM2 ポートを AP の RS-232 ポートに接続します。 コンピュータで次のようなターミナル エミュレーション プログラムを使用します。

- Microsoft Windows HyperTerminal
- Symantec ProComm
- Minicom

次のポート設定を使用してください。

速度：	9600 ビット/秒（bps）
データ ビット：	8
ストップ ビット：	1
パリティ：	なし
フロー制御：	Xon/Xoff

注: フロー制御 Xon/Xoff が機能していない場合は、フロー制御なしを使用してください。

Q. Aironet 1231 AP を使用しています。 AP とアンテナを別々のエリアに配置できるような 50 フィートの延長ケーブルを Cisco から入手できますか。

A. はい。50 フィートのケーブルの部品番号は AIR-CAB050LL-R です。 このケーブルを使用して、AP をアンテナに接続できます。

Q. Autonomous AP の無線の種類を確認するにはどうすればよいのですか。

A. 無線の種類に関する情報を入手するには、AP で特権 EXEC モードから **show controllers** コマンドを使用します。

Q. AP の IP アドレスはどのように設定すればよいのですか。

A. デフォルトでは、AP は DHCP による IP アドレスを要求します。

Cisco IOS リリース 12.3(2)JA 以降では、DHCP サーバから IP アドレスを要求する AP のデフォルトの動作を変更できます。

- 1200 または 1230 シリーズの AP をデフォルト設定で LAN に接続すると、これらの AP は DHCP サーバに IP アドレスを要求します。 アドレスを受信できない場合は、要求を無期限に送信し続けます。
- 1100 シリーズ AP をデフォルト設定で LAN に接続すると、この AP は DHCP サーバからの IP アドレスの取得を数回試みます。 アドレスを受信できない場合、アクセス ポイントは 5 分間 IP アドレス 10.0.0.1 を自分自身に割り当てます。 この 5 分間の時間枠内に、デフォルトの IP アドレスを参照し、静的アドレスを設定できます。 5 分経過しても AP が再設定されなかった場合、アクセス ポイントはアドレス 10.0.0.1 を廃棄し、DHCP サーバからのアドレスの取得を再び要求し始めます。 アドレスを受信できない場合には、要求を無期限に送信します。 10.0.0.1 で AP を参照できる 5 分間の時間枠を逃した場合、電源をいったん切り、改めて投入することで AP にこの過程を繰り返させることができます。

ただし、手動でも AP の IP アドレスを設定できます。 イーサネット セグメントに接続されている Microsoft Windows PC では、DOS プロンプトで次のコマンドを発行します。

arp -s *a.b.c.d 00-12-34-56-78-90*

注: AP で設定 されるおよび 00-12-34-56-78-90is を MAC アドレス*表します*条件 *a.b.c.d は* IP アドレス。 このアドレスは AP の下部にあるパネルに表示されます。

アドレスを確認するには、次のコマンドを発行します。

ping *a.b.c.d*

注: 別の方法ですでに IP アドレスが割り当てられている AP の場合、この手順は正しく機能しません。

Q. AP で HTTPS アクセスをイネーブルにするにはどうすればよいのですか。

A. HTTPS をイネーブルにするには、AP に次のコマンドを付加します。

```
AP(config)#ip http secure-server
```
ip http secure-server コマンドを付加する際に、AP で再生成されたセキュア コミュニケーションに必要な RSA 鍵が表示されます。

Q. クライアントは関連付けの対象となる AP をどのように選択するのですか。

A. アクセス ポイント（AP）の選択はクライアントのマシンの無線に基づいて行われます。 この選択には、カードの製造業者、ドライバ、タイプなどに基づいて、さまざまなメトリックを使用できます。 ほとんどのクライアントで最もよく使用される AP 関連付けメカニズムは、AP からクライアントへの受信信号強度に基づいています。 802.11 標準で規定されているのは、無線クライアント カードが、Received Signal Strength Indicator（RSSI）と呼ばれる簡単なメトリックを使用して信号強度を報告することだけです。 信号強度の報告を受けたクライアントは、最も高い信号強度の AP との関連付けを図ります。 このようなアルゴリズムではパフォーマンスの低下が生じる可能性があることが広く知られています。 これは主に、AP にかかる負荷を十分に把握できないことが原因です。

Q. ワイヤレス クライアントは LWAPP AP と Autonomous AP の間でローミングできますか。

A. いいえ、LAP と Autonomous AP の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。 Wireless LAN Controller 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. AP のカバレッジを拡張するにはどうすればよいのですか。

A. AP のカバレッジを拡張するには、いくつかの方法があります。 その中でも特に重要な方法は次のとおりです。

- リピータ モードで AP を使用する。
- チャネルがオーバーラップしない AP モードでセカンダリ AP を使用する。
- 既存 AP のトランスミッタの出力レベルのパラメータを変更して、カバレッジを拡張する。
- AP を最適な場所に配置する。

これらの方法を実装する方法の詳細は、『WLAN の無線カバー領域の拡張方法』を参照してください。

Q. AP がリピータ モードになっているとどのような影響がありますか。

A. リピータ モードでは、イーサネット ポートがディセーブルにされます。 親の AP から 1 ホップ離れるごとに、スループットの実効値が半減します。

リピータをセットアップするには、親（root）の AP とリピータの AP の両方で Aironet 拡張機能をイネーブルにする必要があります。 デフォルトでイネーブルになっている Aironet 拡張機能を使用すると、AP に関連付けられた Cisco Aironet クライアント デバイスの機能を、その AP が認識し易くなります。 Aironet 拡張機能をディセーブルにすると、AP と Cisco 以外のクライアント デバイスとの相互運用性が向上する場合があります。 Cisco 以外のクライアント デバイスでは、リピータの AP やリピータが関連付けられているルート（root）AP とのコミュニケーション上の問題が検出される場合があります。

ネイティブ VLAN にはインフラストラクチャ SSID が割り当てられている必要があります。 AP

やワイヤレス ブリッジに複数の VLAN が作成されている場合、非ネイティブの VLAN にはインフラストラクチャ SSID を割り当てられません。 非ネイティブの VLAN にインフラストラクチャ SSID を設定する際に、次のメッセージが表示されます。

```
SSID [xxx] must be configured as native-vlan before enabling
 infrastructure-ssid
```

AP では各無線インターフェイスに仮想インターフェイスが作成されるため、リピータ AP では、ルート（root）AP に対して二度（実インターフェイスに一度と仮想インターフェイスに一度）関連付けが行われます。

注: リピータ AP には複数の VLAN を設定できません。 リピータ AP でサポートされるのはネイティブ VLAN だけです。

Q. Aironet 拡張機能でサポートされる機能にはどのようなものがあるのですか。

A. Aironet 拡張機能は Cisco により実装される独自の機能です。 Aironet 拡張機能には、下記の機能をサポートする情報要素が備わっています。

- **ロード バランシング：** AP では、ユーザ数、ビット エラー レート、負荷、および信号強度などの要素に基づいたネットワークへの最適な接続を提供する AP にクライアント デバイスを誘導するために、Aironet 拡張機能が使用されます。ロードバランシングは、Aironet 拡張機能が認識されるデバイス間で特有の機能です。 ロード バランシングは、下記の情報を提供する AP のビーコンやプローブ応答での拡張機能により実装されています。ベースステーションの信号強度ベースステーションの負荷（% transmitter busy）バックボーンまでのホップ数クライアントの関連付け数クライアントでは下記の項目を評価して、「最適な」AP に関連付けを行います。 Cisco 以外のクライアントでは、これらの拡張機能は認識されません。
- **MIC：** Cisco 固有の Message Integrity Check（MIC）：MIC は付加的な WEP セキュリティ機能で、ビットフリップ攻撃と呼ばれる暗号化パケットでの攻撃を阻止するものです。 MIC は AP とすべての関連付けられたクライアント デバイスの両方で実装されています。
- **Cisco 固有の Temporal Key Integrity Protocol（CKIP）：**これは WEP 鍵ハッシュとも呼ばれますが、侵入者が WEP 鍵を算出するために暗号化パケットで初期ベクトル（IV）と呼ばれる非暗号化セグメントを使用するような WEP での攻撃を防御する付加的な WEP セキュリティ機能です。
- これらに加えて、Aironet 拡張機能では下記の情報も提供されます。現在 AP で処理されている負荷有線ネットワークからのホップ数Cisco の管理システムで製品の識別に有効なデバイス タイプデバイス名関連付けられたクライアント数無線タイプ、つまり、データレート、無線タイプ（1310、1200、352 あるいは 342）、セキュリティ タイプ（WEP/802.1x）などの無線に関する特定の特性を判別するために使用するフィーチャ

CCX 互換のデバイスでは、一部の Aironet 拡張機能を利用することもできます。 Cisco 互換拡張機能のさまざまなバージョンで使用できる機能のリストが次の URL で公開されています。

Cisco Compatible Extensions：バージョンと機能

Q. AP なしで無線インターフェイス カードを使用して 2 台のコンピュータを接続できますか。

A. はい。 Aironet Client Utility（ACU）を使用すると、アドホック モードで動作するようにクライアントを設定できます。 ただし、ピアツーピア接続の場合に限ります。 一方の PC が親になって、接続を制御します。 アドホック モードの他方の PC は子ステーションになります。

Q. 暗号化をサポートするには特別なハードウェアが必要ですか。

A. 個々のハードウェアのモデルによって、ユニットでの暗号化レベルが決まります。

- モデル 341 と 351 では、40 ビットの暗号化だけがサポートされています。
- モデル 342 と 352 では、40 ビットと 128 ビット両方の暗号化がサポートされます。
- 1100、1200、1300 シリーズのすべてのモデルで、40 ビットと 128 ビットの両方の暗号化がサポートされます。

Q. 単一の AP から、特定のネットワークまたはインフラストラクチャに所属する AP とその関連付けられたクライアントをすべて表示できますか。

A. VxWorks AP から表示可能です。 単一の VxWorks AP から、ネットワーク内のすべてのクライアントとその AP を表示できます。 このためには、[Association] > [Entire Network] > [Apply] の順にクリックします。 IOS ベースの AP では、AP のイメージが LWAPP イメージである場合、ネットワーク内の関連付けられたクライアントをすべて表示するには、1 つの AP が WDS またはコントローラとして機能する WLSE などの管理デバイスを利用する必要があります。

Q. ネットワークで CCKM を使用しているのに、クライアント デバイスがローミングするたびに認証プロセス全体が実行されます。 つまり、高速セキュアローミングが意図したとおりに機能しません。 これは、なぜですか。

A. これは、不具合 CSCsg10128 が原因である可能性があります。 この不具合は、バージョン 3.1.03 で修正されています。

Q. Cisco アクセス ポイントでは、レイヤ 1 またはレイヤ 2 ケーブルに障害がある場合にスイッチへのイーサネット接続をシャットダウンするために、UniDirectional Link Detection (UDLD; 単方向リンク検出) 機能がサポートされていますか。

A. いいえ。Cisco アクセス ポイントでは UDLD 機能はサポートされていません。

Q. Aironet AP に電力を供給するにはどうすればよいのですか。

A. AP の電源オプションは、使用している AP モデルによって異なります。 詳細は、『Cisco Aironet および WLAN コントローラ製品の電源オプション』を参照してください。

Q. AP1010、AP1030、および AIR-LAP-1232AG を保有しています。 これらは、Power over Ethernet (PoE) の WS-PWR-PANEL を使用できますか。

A. WS-PWR-PANEL では、1 種類の無線の AP のみがサポートされています。 詳細は、『Cisco Aironet Power Over Ethernet アプリケーション ノート』の「*Cisco PoE および Cisco Intelligent Power Management*」セクションに記載されている互換性マトリクスを参照してください。

Q. AP の設定を保存するにはどうすればよいのですか。

A. 設定に対する変更はただちに保存されます。 [Setup] メニューから、現在の設定をテキスト形式でダンプできます。 次に、**[Cisco Services] > [Manage System Configuration]** の順に選択し、システム設定をダウンロードします。

Q. AP またはブリッジが使用する特定の周波数またはチャネルを決定するには、どうすればよいのですか。

A. AP またはブリッジが使用している周波数およびチャネルを表示するには、**show controllers dot11Radio0** コマンドを使用します。 次の出力例は、情報の記載場所を示しています。

```
ap#show controllers dot11Radio0 ! interface Dot11Radio0 Radio AIR-AP1242GA, Base Address
0014.1b58.08f Version 5.80.12 Serial number: GAM09200992 Number of supported simultaneous BSSID
on Dot1 Carrier Set: Americas (US ) DFS Required: No Current Frequency: 2412 MHzChannel 1
```

Q. AP を他の IEEE 802.11b デバイスとともに使用するにはどうすればよいのですか。

A. AP が別の 802.11b デバイスと通信できるようにするには、Aironet 拡張機能を無効にします。 [Express Setup] ウィンドウで [Non-Aironet 802.11] チェックボックスをオンにします。 または、[Advanced AP Radio] ウィンドウの [Use Aironet Extension] オプション ボタンをクリックすることもできます。

Q. AP と関連付けることができるデバイスはどれですか。

- AP からクライアント
- AP から AP (リピータ モード)
- AP (リピータ モード) からベース ステーション (AP モード)
- AP からワークグループ ブリッジ

Q. AP はどの周波数で通信できますか。

A. 米国では、IEEE 802.11b の AP は、2.4 GHz の周波数帯の 11 チャネルのいずれかを使用して送受信を行います。 IEEE 802.11a AP は、5 GHz の周波数帯の 8 チャネルのいずれかを使用して送受信を行います。 IEEE 802.11g AP は、2.4 GHz の周波数帯の 11 チャネルのいずれかを使用して送受信を行います。 これらは公衆周波数帯であり、FCC からのライセンスは不要です。

Q. AP の無線リンクでデータのセキュリティを確保するには、どうすればよいのですか。

A. AP の無線リンクでデータのセキュリティを確保するには、いくつかの方法があります。 さまざまなセキュリティ方式の詳細は、『Cisco Aironet の無線セキュリティに関する FAQ』を参照してください。

Q. AP に関連付けることができるクライアントの数はいくつですか。

A. AP には 2048 の MAC アドレスを処理する物理的なキャパシティが備わっていますが、AP は共有メディアであり、無線ハブとして機能するため、個々の AP 上のユーザ数が増加するにつれて、各ユーザのパフォーマンスは低下します。 AP にクライアントを関連付けるたびに AP のスループットが低下するため、AP に関連付けるクライアントは 24 以下に抑えるのが理想的です。

Q. AP に設定できる MAC アドレス フィルタの数に制限はありますか。

A. CLI を使用すると、2,048 までの MAC アドレスをフィルタリングに設定できますが、Web ブラウザ インターフェイスを使用すると、43 までの MAC アドレスしかフィルタリングに設定でき

ません。

Q. AP の標準的なカバレッジはどのくらいですか。

A. この質問に対する答えは、次に挙げるような数多くの要因に左右されます。

- 希望するデータ レート（帯域幅）
- アンテナの種類
- アンテナのケーブルの長さ
- 伝送を受信するデバイス

最適な環境に設置された場合、最大 90 m の範囲をカバーできます。

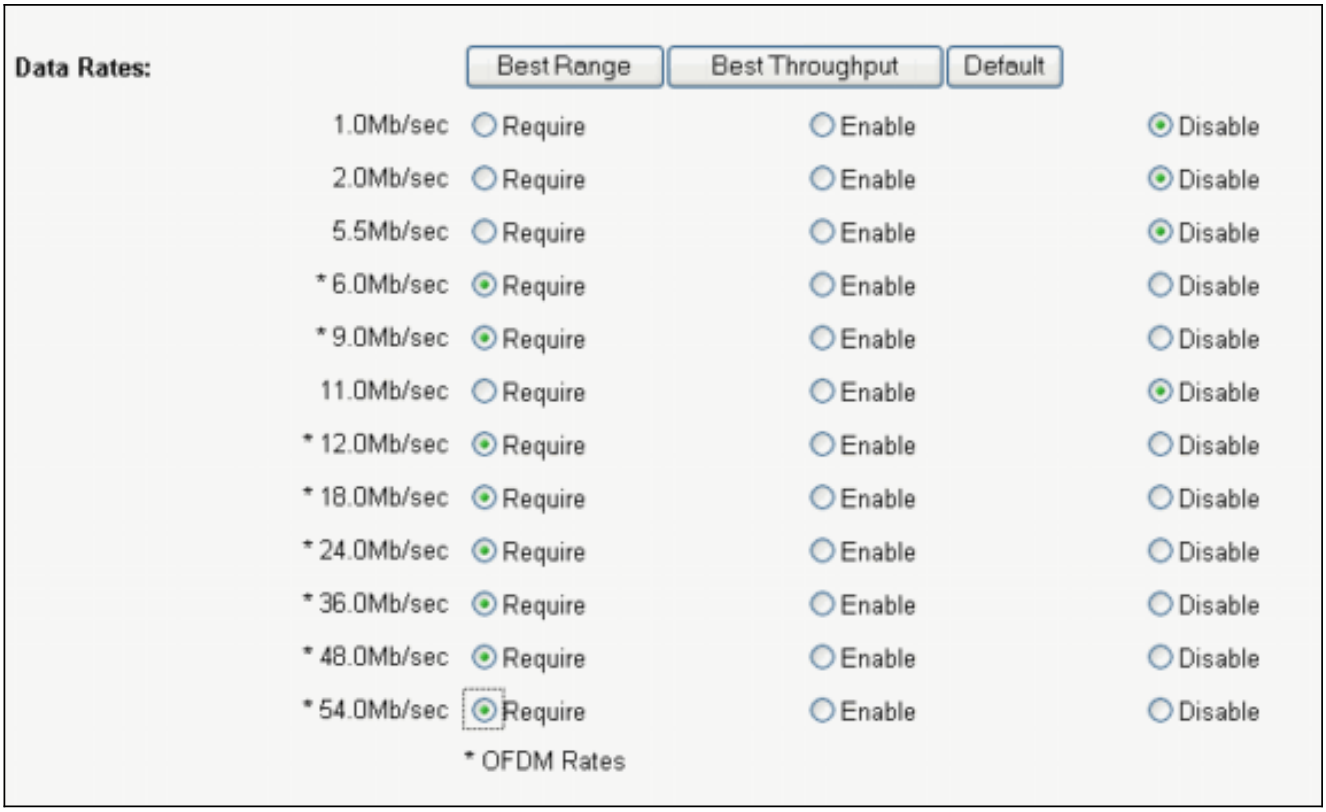
Q. 1200 AP に設定できる伝送出力レベルはどのくらいですか。

A. 伝送出力レベルはさまざまで、使用する無線によって異なります。 出力設定レベルについての詳しいリストは、『Cisco Aironet 1200 シリーズ アクセス ポイント データ シート』を参照してください。 出力設定はチャネルによって異なるため、サイト調査を行ってください。 サイト調査は、使用する出力設定に関して正確な情報を収集するためには重要な作業です。 サイト調査の詳細は、『ワイヤレス サイト調査に関するよくある質問』を参照してください。

Q. IEEE 802.11g のクライアントのみが接続できるように AP を設定するには、どうすればよいのですか。 IEEE 802.11b のクライアントが接続して無線ネットワークの速度が低下することは望ましくありません。 セキュリティ保護されていないクライアント用にもう 1 つパラレルの 802.11b ネットワークがあります。

A. AP が 802.11g のクライアントのみを受信するようにするには、GUI で次の手順を実行します。

1. [Network Interfaces] セクションに移動し、[Radio 0-802.11G] をクリックします。
2. [Radio 0-802.11G] ウィンドウの上部にある **[Settings]** タブをクリックします。
3. 次の各データ レートに対して [Disable] を選択します。 1.02.05.511.0
4. それ以外のデータ レートに対して **[Require]** を選択します。 これには、次のデータ レートがあります。 6.0 ~ 9.012.018.024.036.048.054.0
5. ウィンドウの一番下にある [Apply] をクリックします。 次のウィンドウは一例です。



Q. 無線ネットワークで IEEE 802.11g クライアントのみを許可した場合、使用する変調方式が異なるため、このクライアントがパラレル IEEE 802.11b ネットワークと干渉しないというのは本当ですか。

A. いいえ。本当ではありません。 複数の 802.11g クライアントが同じ周波数を使用する場合には、互いに干渉することがあります。 使用するチャネルを異なるものにしてください。 オーバーラップしないチャネルは 1、6、11 の 3 つです。

Q. AP のイーサネット ポートの速度はどのくらいですか。

A. AP のイーサネット ポートでは、半二重または全二重で、10 Mbps か 100 Mbps のいずれかの速度が RJ-45 コネクタを介してサポートされます。 速度および半二重か全二重かの指定を、使用中のスイッチまたはハブに合わせてハード設定してください。

Q. AP 向けのフェールオーバーや冗長性のメカニズムはありますか。

A. プライマリ AP の障害に備えて冗長性を確保するには、ホットスタンバイを設定します。 詳細については、『Cisco Aironet 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. WEP 鍵とは何ですか。

A. WEP は、Wired Equivalent Privacy の略です。 WEP を使用すると、wireless LAN (WLAN; 無線 LAN) デバイス間で送信されるデータ信号を暗号化および復号化できます。 WEP は IEEE 802.11 のオプション機能で、転送中のパケットの暴露や改ざんを防止し、ネットワーク使用のアクセス コントロールを行います。 WEP によって、WLAN リンクは有線リンクと同程度の安全性になります。 この規格で規定されているように、WEP では 40 ビットまたは 10 ビットのキーによる RC4 アルゴリズムが使用されます。 RC4 ではデータの暗号化と復号化に同一のキーを使用するため、RC4 は対称アルゴリズムです。 WEP をイネーブルにすると、各無線ステーションには鍵が設定されます。 このキーは、電波を介してデータを送信する前に、データをスクランブル

するために使用されます。 あるステーションが適切なキーでスクランブルされていないパケットを受信すると、そのステーションはそのパケットを廃棄します。このようなパケットはホストに配信されません。 WEP を設定する方法については、『Aironet アクセス ポイントおよびブリッジの Wired Equivalent Privacy (WEP) に関する設定例』を参照してください。

Q. Light Extensible Authentication Protocol (LEAP) を使用する場合、Cisco Secure Access Control Server (ACS) と通信するには、何番のポート番号を指定すればよいのですか。

A. デフォルトでは、ACS はポート 1645 で認証要求をリッスンし、ポート 1646 でアカウンティングをリッスンしますが、認証にポート 1812 を、アカウンティングにポート 1813 を設定することもできます。 AP の Authentication Server Setup ページでこれらのポートが正しく設定されていることを確認してください。

Q. Cisco IOS ソフトウェアベースの AP では、認証のために同じ AP で静的な Wired Equivalent Privacy (WEP) 鍵と Extensible Authentication Protocol (EAP) を実行できますか。 VxWorks ベースの AP では正常に機能していました。

A. いいえ。暗号化用の静的な WEP 鍵と認証用の EAP を同じ SSID で実行することはできません。 VxWorks でこの設定が可能になっているのは、ソフトウェアの脆弱性のためであり、機能としてそのようになっているのではありません。 有効な対処方法は、SSID を 2 つ作成し、それぞれの SSID ごとに 1 つずつ計 2 つの VLAN を作成することです。 次に、1 つの SSID に WEP によるオープン認証を設定し、もう 1 つの SSID に EAP 認証を設定します。

Q. サイト調査は必ず行う必要がありますか。

A. はい。 Radio Frequency (RF; 無線周波数) による伝送は元来、環境要因に敏感であるため、現在気づいていないものも含めて、他にどのような RF トラフィックが使用環境に存在する可能性があるのかを理解しておく必要があります。 サイト調査を行うと、無線デバイスの良好なパフォーマンスに対する目に見えない脅威となる問題を一層よく理解できるようになります。 また、必要な RF カバレッジをインストール担当者が確認するうえでも有効です。 『ワイヤレスサイト調査に関するよくある質問』を参照してください。

Q. AP を修正しようとした場合に、ユーザ名とパスワードの入力を求めるメッセージが表示されたときは、何を入力すればよいのですか。

A. ユーザ名とパスワードの入力を求めるメッセージが表示されるのは、User Manager がイネーブルにされているためです。 使用するユーザ名とパスワードについては、AP の管理者に問い合せてください。 自身が AP 管理者で、どのユーザ アカウントを使用すればよいかかわからない場合は、パスワード回復を実行する必要があります。 『Cisco Aironet 機器のパスワード回復手順』を参照してください。

Q. 2 基の外部アンテナを使用して 2 つの無線セルを (たとえば、アンテナ 1 でセル 1 をアンテナ 2 でセル 2 を) カバーできますか。

A. 1 台の AP に 2 基のアンテナがあっても、2 つの無線セルを カバーすることはできません。 これらのアンテナで 2 つの無線セルをカバーしようとすると、接続上の問題が発生する場合があります。 アンテナが 2 基あるのは、マルチパスによる歪みと信号の空白によって発生する問題を解

決して 1 つのセルのカバレッジを向上させるためです。 ダイバーシティおよびマルチパスによる歪みについての詳細は、『マルチパスとダイバーシティ』を参照してください。

Q. AP で mobility network-id コマンドを使用する目的は何ですか。

A. **mobility network-id** コマンドは、無線ネットワークでレイヤ 3 モビリティを設定するのに使用します。 **mobility network-id ssid** コマンドは、サービス セット識別子（SSID）をレイヤ 3 モビリティのネットワーク ID に関連付けるのに使用します。 レイヤ 3 モビリティでは、クライアントは異なるサブネットにあるさまざまな AP にローミングできます。 ローミングを実行するクライアントではネットワークに接続された状態が維持され、IP アドレスが変更されることもありません。

レイヤ 3 モビリティを正しく設定するには、Wireless LAN Wervice Module（WLSM; ワイヤレス LAN サービス モジュール）を Wireless Domain Service（WDS; ワイヤレス ドメイン サービス）デバイスとして使用する必要があります。 AP を WDS デバイスとして使用するときには、レイヤ 3 モビリティはサポートされません。 レイヤ 3 モビリティの詳細は、『WDS、高速セキュアローミング、および無線管理の設定』の「*レイヤ 3 モビリティについて*」セクションを参照してください。

このコマンドは、レイヤ 3 モビリティがある（WDS デバイスとして機能する）WLSM モジュールを搭載した WDS インフラストラクチャに AP が参加している場合に使用することになっています。 このコマンドの使い方を誤ると、WLAN ネットワークで次のような接続に関する問題が発生します。

- クライアントが DHCP から IP アドレスを取得しない。
- クライアントを AP と関連付けることができない場合がある。
- ワイヤレス クライアントを AP と関連付けることができない。
- Extensible Authentication Protocol（EAP）認証が実行されない。 **mobility network-id** コマンドが設定されている場合、AP は EAP パケットを転送するために generic routing encapsulation（GRE; 総称ルーティング カプセル化）トンネルを構築しようとします。 トンネルが確立されない場合、EAP パケットはどこにも転送できません。
- WDS デバイスとして設定されている AP は想定どおりに機能せず、WDS 設定も機能しない。

Q. VLAN ごとにいくつの SSID を設定できますか。

A. VLAN ごとに 1 つの SSID のみを設定できます。 Aironet AP では、単一の VLAN で複数の SSID を使用することはできません。

Q. 複数の ESSID が AP に割り当てられたときの BSSID 値は何になりますか。

A. AP が Lightweight モードで稼働している場合、AP 上の各 ESSID は異なる BSSID 経由で処理されます（ここで、それぞれの BSSID は無線ベース MAC に基づいており、下位二ブル内だけが異なっています）。

AP が IOS を稼働している場合、AP 上のすべての ESSID は同じ BSSID 経由で処理されます（MBSSID が設定された場合は異なる BSSID 経由で処理されます）。

Q. ブリッジ用に a 無線を、AP 機能用に g 無線をそれぞれ設定できますか。 設定できる場合は、どうすればよいのですか。

A. はい。AP の各無線をそれぞれ異なる機能に設定できます。 質問のシナリオを実現するには、g 無線および a 無線に異なる SSID を設定します。 次に、g 無線を AP に、a 無線をルート ブリッジに設定するロールを無線ネットワーク パラメータに設定します。

Q. 同じサブネットに接続されている 2 つの異なる AP に 2 台のクライアントを関連付けている場合、通信は有線ネットワークで行われますか、無線で行われますか。

A. このシナリオの場合、2 つの AP がルート（root）モードに設定されていると、この 2 つの AP 間の通信は有線ネットワークで行われます。 一方の AP がリピータ モードに設定され、他方の AP がルート モードに設定されている場合、AP 間の通信は無線で行われます。

Q. Cisco AP でルーティングまたはネットワーク アドレス変換（NAT）をイネーブルにできますか。

A. いいえ。AP ではルーティングも NAT 機能もサポートされていません。

Q. Cisco IOS ソフトウェアベースの AP が使用可能な時間をスケジュールする方法はありますか。 AP に接続するクライアントに時間ベースでアクセスしようと考えています。

A. 時間範囲を使用して、時間ベース Access Control List（ACL; アクセス コントロール リスト）を設定できます。 時間ベース ACL を使用すると、たとえば、午前 9 時 00 分から午後 5 時 00 分まで（0900 ~ 1700）の特定の期間内にユーザが無線ネットワークにアクセスできます。 時間ベース ACL を使用しても、AP または無線はシャットダウンされません。 ユーザがネットワークにアクセスできないように、AP にトラフィックが渡されなくなります。 この機能を設定する方法については、『IP アクセス リストの設定』の「*時間範囲を使用する時間ベース ACL*」セクションを参照してください。

Q. AP にサブネットが異なる複数の DHCP プールを設定できますか。

A. AP を DHCP サーバとして設定した場合、IP アドレスはその DHCP サーバと同じサブネットにあるデバイスに割り当てられます。 デバイスは同じサブネット上の他のデバイスとは通信しますが、サブネットを越えて通信することはありません。 サブネットを越えてデータを渡す必要がある場合は、デフォルト ルータを割り当てる必要があります。 デフォルト ルータの IP アドレスは、DHCP サーバとして設定した AP と同じサブネットにある必要があります。

Q. dBm 測定とは何ですか。 Aironet AP のリストにある信号強度（mW 単位）に相当する dBm 値を特定するには、どうすればよいのですか。

A. dB という単位は、他の標準値との相対的な比率で信号出力を示すものです。 この省略形の dB は、他の省略形と組み合せて、比較対象の値を表すことがよくあります。 したがって、dBm は dB を標準参照値 1 mW と比較して得られた値となります。

mW 単位で所定の信号強度からこの dBm 値を計算するための数式は次のとおりです。

```
Power (in dB) = 10 * log10 (Signal/Reference)
```

数式の用語の定義を次のリストに示します。 log10 は 10 を底とする対数です。

- Signal は信号の電力を指します（たとえば 50 mW）。
- Reference は基準電力です（たとえば 1 mw）。

例：

信号強度 50 mW の出力を dB で計算する場合は、次の数式を適用します。

```
Power (in dB) = 10 * log10 (50/1) = 10 *log10 (50) = 10 * 1.7 = 17 dBm
```

この数式から、次の共通規則が得られます。

- 3 dB（ここでは dBm）増やすごとに、現在の伝送パワー（mW）が倍増します。 3 dB 減らすごとに、伝送パワーの現在値が半減します。
- 10 dB（ここでは dBm）増やすごとに、現在の伝送パワー（mW）が 10 倍に増えます。 10 dB 減らすごとに、伝送パワーの現在値が 1/10 に減ります。
- 30 dB（ここでは dBm）増やすごとに、現在の伝送パワー（mW）が 1000 倍に増えます。 30 dB 減らすごとに、伝送パワーの現在値が 1/1000 に減ります。

dBm と mW の概算値を次の表に示します。

dBm	mW
0	1
1	1.25
2	1.56
3	2
4	2.5
5	3.12
6	4
7	5
8	6.25
9	8
10	10
11	12.5
12	16
13	20
14	25
15	32
16	40
17	50
18	64
19	80
20	100
21	128
22	160
23	200
24	256
25	320
26	400
27	512
28	640
29	800
30	1000 or 1 W

詳細は、『RF 電力値』を参照してください。

Q. Cisco 1231 AP で日付と時刻の設定を変更するには、どうすればよいのですか。

A. Web インターフェイス (GUI) に移動し、[Services] > [SNTP] の順に選択し、[Time Settings] を選択してから時刻を変更します。

Q. CCKM がクライアントでは設定されないものの、AP では設定される場合、クライアントを AP に関連付けることができますか。 クライアントは正常にローミング

できますか。

A. この動作は AP の設定によって異なります。 クライアントで CCKM が設定およびサポートされていない場合、クライアントは CCKM が「mandatory」に設定されている AP に関連付けられません。 インフラストラクチャ（AP）で CCKM が「optional」に設定されている場合、クライアントは関連付けられ、非 CCKM ハンドシェイクが行われます。

配置するクライアントによって異なりますが、一般に、どのデバイスにもアソシエーションを許可しながら、高機能デバイスまたは CCKM 関連デバイスに対してのみ高速ローミングをサポートするインフラストラクチャでは CCKM を「optional」に設定することを推奨いたします。

Q. AP 1240 と 1230 では、メモリ容量にどのような違いがありますか。

A. AP 1240 と 1230 のメモリ容量は次のとおりです。

- AP 1240 は 32 MB プラットフォーム AP です。
- AP 1230 は 16 MB プラットフォーム AP です。

Q. リンク ロールの柔軟性をサポートする AP 1240 を 2 つ保有しています。 これらの AP 間を 802.11a でブリッジして、802.11b/g 帯域にクライアントを加入させたいと考えています。 その際に考慮する必要のある制限はありますか。

A. AP のリンク ロールの柔軟性は、二重帯域機能を備えた AP（1200、1230、および 1240AG シリーズ）を対象にブリッジ モード機能をサポートするものです。 今回実現する設定では、802.11a 無線はブリッジ モードで動作するのに対して、802.11g 無線はアクセス ポイント モードで動作します。

この場合に必要なことは、リンク ロールの柔軟性を備える AP を設定する際、AP の無線のいずれかをルート AP として設定し、ブリッジするもう 1 つの AP をルート AP へのリピータ モードまたは WGB モードにすることです。

Q. AP ごとに無線 IP テレフォニーの受話器を何台用意するのが推奨されますか。

A. ミッション クリティカルな音声トラフィックを伝送できるように適切な帯域幅とリソースを確保するには、IP テレフォニー ネットワークの規模を決定することが不可欠です。 通常の IP テレフォニーで PSTN ゲートウェイ ポート、トランスコーダ、WAN 帯域幅などのコンポーネントの規模を決定するための設計ガイドラインに加え、無線 IP テレフォニー ネットワークの規模を決定する際には、下記の 802.11b に関する問題を考慮します。

- AP あたりの 802.11b デバイスの数： この数は 15 ~ 25 程度にすることを推奨いたします。
- AP あたりの 802.11b 電話機の数。

ネットワーク プランを巡って議論が起きる前に、ネットワーク キャパシティ全体の基本について理解していると役立ちます。 無線 IP テレフォニー ネットワークの規模を決定する際には、ネットワーク キャパシティに関する次のガイドラインに従ってください。

- AP あたりの同時 G.711 コールを 7 以下にする。
- AP あたりの同時 G.729 コールを 8 以下にする。

注: これらの推奨設計では、音声アクティビティ検出（VAD）が Cisco 7920 Wireless IP Phone で無効にされているものとしています。

Cisco 7920 Phone で VAD を使用すると帯域幅を節約できますが、音声品質全体を高めるためには、すべての Cisco CallManager サーバで VAD をディセーブルにすることを推奨いたします。 802.11b VoIP コールで必要になる帯域幅の量を決定することに加えて、RF チャネルごとに無線全体のコンテンションも検討する必要があります。 一般規則は、AP ごとに 20 ~ 25 以上の 802.11b エンドポイントを配置しないというものです。 AP に追加するエンドポイントを増やすと、その分だけ帯域幅全体の量が減り、伝搬遅延が発生する可能性が高くなります。 AP あたりの電話機の最大数は、個々のユーザのコール パターンによって異なります (アーラン比率に基づきます)。 G.711 を使用する同時コールを 7 以下にするか、または G.729 を使用する同時コールを 8 以下にすることを推奨いたします。 このコール数を超え、バックグラウンド データがあまりにも多いと、すべてのコールの音声品質が許容できない品質になります。 ここで示す推奨事項のパケット レートは、VAD がディセーブルで、サンプル レートが 20 ミリ秒であるものとしています。 このレートにすると、各方向で毎秒 50 パケット (pps) が生成されます。 サンプル サイズを大きくすると (40 ミリ秒など)、同時コールの数が増えるだけでなく、VoIP コールのエンドツーエンド遅延も増えることがあります。

レイヤ 2 サブネットまたは VLAN ごとに配置できる 802.11b 電話機の数は、次の要因に左右されます。

- AP ごとに 7 以下の G.711 アクティブ コールまたは 8 以下の G.729 アクティブ コールを使用する。
- コール比率に基づいて、アクティブ コールおよび非アクティブ コールの数が決まる。 この比率は、アーラン カルキュレータで決定されることがよくあります。 これらの要因および通常のビジネス向けのアーラン比率 (3 : 1 ~ 5 : 1) に基づいて、レイヤ 2 サブネットまたは VLAN ごとに 450 ~ 600 台程度の Cisco 7920 Phone を配置することを推奨いたします。

詳細については、『無線ネットワーク インフラストラクチャ』の「*ネットワーク規模の決定*」セクション、および『WLAN の音声対応』 を参照してください。

Q. あらかじめ設定しておいた試行回数の後、AP 1200 で認証要求の処理を停止するには、どうすればよいのですか。

A. クライアントがネットワークへのアクセスを試行できる回数を制限するには、AAA サーバで最大リトライ オプションを使用します。 最大リトライの値は、AAA サーバで手動で設定できます。また、使用する AAA サーバに応じて設定されるデフォルトのリトライ回数を使用することもできます。

Q. AP および LAP の各種プラットフォームの相違点に関する情報はどこで入手できますか。

A. 『シスコ ワイヤレスハードウェアに関する FAQ』を参照してください。 このドキュメントには、AP と LAP の各種モデルを比較した有用な情報が記載されています。

Q. Cisco Aironet アクセス ポイントでは、Point-to-Point-Protocol over Ethernet (PPPoE) がサポートされていますか。

A. いいえ。Cisco Aironet アクセス ポイントでは、PPPoE はサポートされません。

Q. Cisco Aironet アクセス ポイントでは、VLAN Trunking Protocol (VTP) がサポートされていますか。

A. いいえ。Cisco Aironet アクセス ポイントでは、VTP はサポートされません。

Q. Cisco Aironet AP では、802.11f 標準の Inter-Access Point Protocol（IAPP）がサポートされますか。

A. いいえ。Cisco Aironet AP では、802.11f ベースの IAPP はサポートされません。 Cisco のアクセス ポイントには、堅牢かつ機能豊富で、実績のある独自の Inter-Access Point Protocol が搭載されています。

Q. AP で bridge-group 1 block-unknown-source コマンドおよび bridge-group 1 source-learning コマンドを使用する目的は何ですか。

A. **bridge-group block-unknown-source** コンフィギュレーション インターフェイス コマンドは、特定のインターフェイスで未知の MAC アドレスから送出されたトラフィックをブロックするのに使用します。 このコマンドの **no 形式**は、特定のインターフェイスで未知の発信元のブロックを無効にするのに使用します。

STP を正しく機能させるには、STP に参加するインターフェイスに対して **block-unknown-source** を無効にする必要があります。

```
bridge-group group block-unknown-source
```

インターフェイスで STP を有効にすると、**block-unknown-source** はデフォルトで無効にされます。

bridge-group 1 source-learning コマンドは、AP にクライアントの送信元アドレスを学習させるのに使用します。 このコマンドの **no 形式**は、AP にクライアントの送信元アドレスを学習させる機能をディセーブルにするのに使用します。

Q. AP に設定した特定の SSID から送出されたトラフィックが同じ AP の他の SSID よりも大きい帯域幅を使用するように、AP を通過するトラフィックに優先順位を付ける方法がありますか。

A. これは、AP に QoS（Quality Of Service）を実装すると実現できます。

- QoS ポリシーを作成し、AP に設定されている VLAN にそのポリシーを適用します。 次のドキュメントでは、QoS および AP で QoS ポリシーを設定する方法について説明しています。[無線 QoSAironet アクセス ポイントでの QoS の設定]
- 次に、前述の個々の VLAN に AP で設定されている SSID をマップします。 このように、VLAN に基づいてトラフィックに優先順位を付けた場合、続いて SSID に基づいてトラフィックに優先順位を付けることができます。

Q. 単一の Autonomous アクセス ポイントに接続できるクライアント デバイスの最大数を制限する方法がありますか。

A. Cisco クライアント デバイスのデフォルトの動作は、最適な信号強度を持つ AP に接続するというものです。 しかし、MAC 認証を使用すると、特定の AP に接続できるクライアントを制限できます。 そのためには、AP にクライアントの MAC アドレスを提供して、AP がそのクライアントのみを許可し、許可された MAC アドレスのリストにないどのクライアントもその AP に接続できないようにする必要があります。

Q. 最新のソフトウェアはどこでダウンロードできるのですか。

A. Cisco Aironet の機器を最良の状態で動作させるには、すべてのコンポーネントに最新バージョンのソフトウェアをロードすることを推奨いたします。 最新のソフトウェアおよびドライバをダウンロードするには、Cisco ワイヤレス ソフトウェア センター（登録ユーザ専用）を参照してください。

Q. AP をアップグレードするときはラップトップなどの無線デバイスをすべて停止する必要がありますか。

A. いいえ。デバイスを停止する必要はありません。 AP アップグレードは安全なプロセスであるため、停止する必要のあるものはありません。 TFTP サーバに接続した状態であることを確認してください。

Q. Cisco Aironet AP で Cisco IOS® をアップグレードする方法に関する説明はどこで入手できるのですか。

A. AP で Cisco IOS をアップグレードする方法については、『ソフトウェア イメージの操作』を参照してください。

注: archive download-sw コマンドでは、force-reload オプションを使用してください。

注: CLI で archive download-sw コマンドを入力して、AP またはブリッジ システム ソフトウェアをアップグレードするときは、force-reload オプションを使用する必要があります。 アップグレード後に AP またはブリッジによってフラッシュ メモリがリロードされない場合、ブラウザ インターフェイスのページにアップグレードが反映されていない可能性があります。 次の例では、archive download-sw コマンドを使用してシステム ソフトウェアをアップグレードする方法を示しています。

```
AP#archive download-sw /force-reload / overwrite tftp://10.0.0.1/image-name
```

Q. 1100 AP を保有しています。 IEEE 802.11b から IEEE 802.11g に AP 無線をアップグレードしたいと考えています。 AP の無線をアップグレードする場合、既存の PC カードを使用できますか。 また、PC カードもアップグレードする必要がありますか。 カードは現在 802.11b カードです。

A. 802.11b クライアントのみを使用している場合、802.11b 無線を 802.11g にアップグレードしても、パフォーマンスは向上しません。 無線を 802.11g にアップグレードする利点は、AP に 802.11b クライアントおよび 802.11g クライアントを接続できることです。 このアップグレードを行うと、802.11b クライアントは 11 Mbps で接続し、802.11g クライアントは 54 Mbps で接続します。

Q. AP を工場出荷時のデフォルト設定に戻すには、どうすればよいのですか。

A. 『Cisco Aironet 機器のパスワード回復手順』を参照してください。

トラブルシューティングに関する FAQ

Q. AP の一部の設定を変更しました。 変更内容を保存しようとすると、AP で次の

メッセージが表示されます。 ""Error writing new config file "flash: //config.txt.new" nv_done: unable to open "flash: //config.txt.new" nv_done: unable to open "flash: //private-multiple-fs.new"[OK]".

A. このエラー メッセージは、フラッシュに新しいコンフィギュレーションを保存するための領域がないことを意味しています。 古いクラッシュ ファイルをすべて削除します。 また、Cisco IOS ソフトウェア バージョンが複数ある場合は、使用しないバージョンを削除します。 これにより、フラッシュに空き領域を確保できます。 削除できる古い例外クラッシュ情報ファイルまたは使用していない古いイメージがあるかどうかを特定するには、**dir flash** コマンドを発行します。 メモリに設定を書き込むことができるように空き領域を確保するには、**write memory コマンド**を発行します。

Q. Aironet Client Utility (ACU) 6.3 と、Cisco IOS ソフトウェア リリース 12.3(8)JA が稼働する Cisco 1200 アクセス ポイント (AP) を使用しています。 無線クライアントを AP に関連付けても、AP 名が ACU に表示されません。 これは、なぜですか。

A. [AP Name] は、AP のホスト名です。 Aironet 拡張機能を AP でイネーブルにすると、AP 名は ACU に表示されます。

AP 名を参照する必要がない場合は、IEEE 802.11b 標準への Cisco Aironet 拡張機能をディセーブルにできます (無線インターフェイスでは **no dot11 extensions aironet**)。 AP では、Cisco Aironet 拡張機能はデフォルトでイネーブルになっています。

ディセーブルにしてある場合は、次のコマンドで Cisco Aironet 拡張機能をイネーブルにできます。

```
AP(config-if)#dot11 extension aironet
```

AP は、AP 名が含まれる Cisco 独自の情報要素をビーコンに含めます。 AP で Aironet 拡張機能をディセーブルにすると、AP は名前を含むビーコンを送信しません。 Aironet 拡張機能の詳細は、『Aironet 拡張機能のイネーブルとディセーブル』を参照してください。

Q. AP で一度に 1 つのクライアントしか受け入れと接続ができません。 どのような理由が考えられますか。

A. 考えられる理由の 1 つは、service-set identifier (SSID; サービス セット ID) 設定で **max-associations** パラメータが **1** に設定されていることです。 (指定した SSID の) 無線インターフェイスでサポートされるアソシエーションの最大数を設定するには、**max-associations** という SSID 設定モード コマンドを使用します。 このパラメータをデフォルト値にリセットするには、このコマンドの **no 形式**を使用します。 このデフォルトの最大値は 255 です。

Q. パスワードを忘れたら、どのようにして回復できるのですか。

A. 『Cisco Aironet 機器のパスワード回復手順』を参照してください。

Q. 手持ちの BR350 や AP350 では、コマンドではシリアル番号が表示されません。 いずれも VxWorks であり、IOS に変換されていません。 これらのデバイスからシリアル番号を取得するには、どうすればよいのですか。

A. VxWorks が稼働する 350 シリーズの AP およびブリッジのシリアル番号は、ソフトウェアで

は表示されません。 これらのデバイスのシリアル番号を確認するには、デバイス自体に貼られた物理的なラベルを調べる以外に方法はありません。

Q. AP の無線周波数（RF）リンクの干渉源となる可能性のあるものには何がありますか。

A. 干渉には次のような数多くの発生源があります。

- 2.4 GHz のコードレス電話
- 遮蔽が不適切な電子レンジ
- 他社製の無線機器

電気モーターおよび機械の中の可動金属部品も干渉を起こす場合があります。 詳細は、次のドキュメントを参照してください。

- 無線周波通信に影響を及ぼす問題に関するトラブルシューティング
- ワイヤレス ブリッジで接続が断続する問題

Q. 次のエラー メッセージが表示されます。 %C4K_EBM-4-HOSTFLAPPING:Host [mac-addr] in vlan [num] is flapping between port [num] and port [num] connected to the Access Points. これを解決するには、どうすればよいのですか。

A. このエラー メッセージが発生するのは、スイッチで複数のポートから同じ MAC アドレスが学習された場合です。 これは次のいずれかの理由による可能性があります。

1. ある AP から別の AP にクライアントがローミングすると、その MAC アドレスのクライアントの情報が、新しい AP からスイッチに渡されます。 両方の AP が同じスイッチに接続されていると、それぞれの AP に接続された両方のスイッチ ポートに、そのクライアントの MAC アドレスが関連付けられます。 これにより、そのクライアントに対する重複エントリが作成されて、スイッチで CAM テーブルの同期が行われるまで、このエラー メッセージが表示されます。 無線環境では、このエラー メッセージはまったく正常ですが、ローミングが多く発生しすぎると、スイッチの CPU が過負荷状態になる可能性があります。 クライアントのドライバとファームウェアをチェックしてください。 さらに、カバレッジが良好であることを確認して、クライアントのローミングが頻発しないようにします。
2. ループが発生している場合は、スイッチでは他のスイッチに接続された複数のポートから同じ MAC アドレスが学習される場合があります。 スイッチで TP がイネーブルになっていることを確認してください。

Q. クライアント カードが最も近い AP に関連付けられないのはなぜですか。

A. 無線トポロジ内に複数の AP がある場合、クライアントでは最初に関連付けられた AP との関連付けが、その AP からのキープアライブ ビーコンが失われるまで維持されます。 接続が失われ、元の AP との接続を回復しようとして失敗すると、クライアントは別の AP を探します。 クライアントに新しい AP に対する十分な権限と許可が付与されている場合、クライアントはその AP との関連付けを試みます。

Q. Cisco AP および Cisco Secure Access Control Server（ACS）3.2 を保有しています。 ネットワークに Extensible Authentication Protocol（EAP）を実装しています。 ユーザが RADIUS サーバで認証されません。 AP で debug コマンドを発行す

ると、次の出力が返されます。 "Jun 2 15:58:13.553: %%RADIUS-4-RADIUS_DEAD: RADIUS server 10.10.1.172:1645,1646 is not responding. Jun 2 15:58:13.553: %%RADIUS-4-RADIUS_ALIVE: RADIUS server 10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664: %%DOT11-7-AUTH_FAILED: Station 0040.96a0.3758 Authentication failed. AP でこのエラー メッセージが表示されるのはなぜですか。

A. このようなエラー メッセージが表示される理由の 1 つは、AP と ACS で共有秘密鍵が同じ値になっていないことです。 この誤りは、EAP を設定するときによく見られます。 AP と ACS 3.2 との間で共有秘密鍵に不一致が見られる場合、EAP は機能しません。 RADIUS サーバは、AP が転送するパケットを受け入れません。 AP の共有秘密鍵が ACS サーバで設定されているものと一致していることを確認してください。 デバッグする方法については、『認証のデバッグ』を参照してください。

Q. AP でログを表示したときに、次のエラーを見つけました。「 "Mar 9 11:05:26.225 Information Group rad_acct: Radius server 10.10.1.172:1645,1646 is responding again (previously dead). Mar 9 11:03:09.361 Error Group rad_acct: No active radius servers found. このエラーの原因は何ですか。この問題を解決するには、どうすればよいのですか。

A. AP に設定値 radius-server deadtime が設定されている場合、このログが記録されるのは通常の動作です。 これは情報ログであり、大きな問題ではありません。 radius-server deadtime コマンドは、応答しないサーバを AP が使用しないようにする間隔を設定するのに使用します。これにより、タイムアウトまで要求を待機することなく、次の設定済みサーバを試すことができます。 以後の要求では、デッドとマーク付けされたサーバが指定の分数（最大 1440（24 時間））だけスキップされます。

Q. Cisco IOS ソフトウェア リリース 12.3(4)JA を実行する AP 1230 を保有しています。 アクセス コントロール リスト（ACL）を更新すると、次のメッセージが返されます。 "%% Warning: Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]: "」

A. これはエラーではなく、警告メッセージです。 [no] を選択すると、アクセス ポイント（AP）に保存されません。 設定は、non-volatile RAM（NVRAM; 不揮発性 RAM）には保存されず、フラッシュに保存されます。

警告ではありますが、この AP でメモリの問題が発生していることを示しています。 .rcore ファイルが数多くあり、メモリ上の領域が大量に消費されています。 次に出力の例を示します。

```
3 -rwx 262144 Mar 3 2002 22:40:04 +00:00 r13_5705_9760_1EA7A81E.rcore

4 -rwx 262144 Mar 1 2002 17:21:44 +00:00 r13_5705_9760_709D16F4.rcore

5 -rwx 262144 Mar 7 2002 20:19:12 +00:00 r13_5705_9760_9D2DE9CD.rcore

6 -rwx 262144 Mar 26 2002 23:42:22 +00:00 r13_5705_9760_AAE78172.rcore

151-rwx 262144 Mar 1 2002 17:22:00 +00:00 r13_5705_9760_7187935C.rcore
```

このメモリを解放するには、フラッシュから .rcore ファイルをすべて消去します。

イネーブル モードで入力する必要があるコマンドの例を次に示します。

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

注: この delete flash: コマンドは、 フラッシュの各 .rcore ファイルに対して発行します。

Q. Cisco IOS ソフトウェア リリース 12.4(4)T1 がインストールされたワイヤレス LAN サービス モジュール (WLSM) を保有しています。 クライアントへの接続が廃棄されています。 ログを調べると、「Previous authentication no longer valid」や「Disassociated because sending station is leaving (or has left) BSS」など数多くのメッセージが記録されています。 問題は何ですか。

A. どちらのメッセージも、RF 問題を指摘するものです。 この問題を修正するには、AP に割り当てるチャネルを変更してください。

Q. WLAN ネットワークの Cisco Aironet AP が SSID をブロードキャストしません。 どのような理由が考えられますか。 AP で特定の機能をイネーブルにする必要がありますか。

A. SSID Manager で Guest モードをイネーブルにしない限り、AP はビーコンで SSID をブロードキャストしません。 問題の SSID がリストにないことを確認するには、クライアントで SSID をスキャンします。

SSID で Guest モードをイネーブルにするには、グローバル コンフィギュレーション モードの AP で次のコマンドを入力します。

```
Ap<config>#dot11 ssid ssid-string Ap<config-ssid>#guest-mode
```

Q. AIR-AP1231G-A-K9 AP を保有しています。 この AP には a 無線を有効にするためのオプションはなく、g 無線を有効にするためのオプションのみがあるのはなぜですか。 この AP に 802.11b クライアントを関連付けることはできないのですか。

A. AIR-AP1231G-A-K9 AP には g 無線があります。 AP1231G という部品番号は、g 無線のみがあることを示しています。 G 無線には B 無線との下位互換性があります。どちらも同じ周波数で機能するためです。 このユニットには a 無線がないため、これを有効にすることはできません。 a 無線モジュールを追加することが必要になる場合があります。 a 無線は、g 無線および b 無線（2.4 GHz）とは異なる周波数（5 GHz）で動作します。

Q. Cisco Wireless IP Phone 7920 を Cisco AP に接続しています。 7920 は AP に関連付けられているものの、IP アドレスが割り当てられません。 Extensible Authentication Protocol（EAP）を使用しています。 「Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated」というメッセージが表示され、続いて「Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated」および「Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4」が表示されます。 さらに、「Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid'」が続きます。 問題は何でしょうか。

A. これらのメッセージが返される理由は、AP の共有秘密鍵が RADIUS サーバの共有秘密鍵と異なっていることです。 両方で EAP の共有秘密鍵が同じになるようにします。 AP および RADIUS サーバで共有秘密鍵を再入力する必要があります。

Q. AP で問題が発生しています。 あまりにも多くの RTS メッセージを一気に送信し続けるため、クライアントの関連付けが予期せず解除されます。 いずれのクラ

イアントも、-91 ~ -95 dBm の信号レベルでこの AP に関連付けていました。 関連付けが予期せず解除される理由は何ですか。 これは AP の正常な動作ですか。

A. はい。これは、正常な動作です。 クライアントは 1 Mbps セルの端にあります。 -91 ~ -95 dBm にあるため、このように動作が不規則になると考えられます。

この問題に対処するには、設置する AP の数を増やしてください。 カバレッジを全方向とするのではなく、絞られた領域にする場合は、指向性アンテナを使用してください。

RTS は、リトライ メカニズムの起動によってもたらされます。 クライアントは CTS で RTS に応答しますが、クライアントのスニファに RTS フレームが 8 つほど集まったものが表示され、しかも対応する CTS がない場合、クライアントは AP をリッスンしないか、または AP 側でリッスンできないほど遠く離れた位置にあります。 AP がクライアントをリッスンするだけではなく、両デバイスが相互にリッスンする必要があります。 そのため、クライアント側のアンテナに設計上の問題がある場合（十分に考えられます）、トランスミッタが 100 mW で送信しない場合（かなりの確率で考えられます）、またはレシーバが -90 ~ -95 dBm の感度の近くにない場合（クライアントが Cisco のクライアントでない場合は、ほぼ間違いなくこの状態にあります）、質問のような動作になります。

Q. Cisco の LWAPP 無線 AP を使用しています。 クライアントでは TCP が何度も再送信され、ACK が重複しているのに、有線の環境ではこのようなことが起きません。 この動作は無線では正常なのでしょうか。

A. パケットの破損および再送信はどちらも、802.11 WLAN の基本的なメトリックです。 802.11 で実施されるパケットの破損および再送信の分析は、次の 3 つの理由から、有線 LAN での分析とは異なります。

- 第一に、802.11 WLAN は一般に有線 LAN よりも破損するパケットの数が多くなるため、802.11 WLAN ではフレームの破損に対する重要性が高まります。
- 第二に、802.11 では信頼できるデータリンク レイヤが定義されます。つまり、破損したパケットはどれも再送信する必要があります。 有線 LAN では一般に信頼できるデータリンク レイヤが定義されないため、再送信が発生するのは信頼性が高い上位層プロトコルを使用している場合に限られます。
- 最後に、上位層の信頼性は一般にエンドツーエンドです。つまり、送信元から宛先までのどこでパケットが破損しても再送信が発生します。 802.11 の再送信は、レイヤ 2 で発生するため、無線インターフェイス間に実装されます。したがって、802.11 の再送信が発生するのは、ローカルな「セグメント」でパケットが破損した場合に限られます。 つまり、従来の有線 LAN よりも 802.11 WLAN の方が、破損の発生場所をはるかに容易に特定できます。 両者の違いにどのような意味があるのか検討してみます。

無線環境の課題の 1 つに、アナライザが参照するものと、クライアントが参照するものが同じであるかどうかを見極めるのが難しいというものがあります。 アナライザとクライアントとの間に差異（無線、アンテナ、または物理的位置）があると、アナライザの参照するものが、クライアントとは異なるものになることがあります。 たとえば、アナライザは AP から遠く離れた位置にあるものの、無線クライアントは AP に近い位置にある場合、アナライザは破損したフレームを参照しているのに対して、クライアントは破損していないフレームを参照していることがあります。 破損したフレームは必ず再送信されることがわかっているため、再送信と破損したフレームの相対数に基づいて、ネットワーク上のクライアントが参照するものをアナライザがどの程度参照しているかを評価できます。

Q. ネットワークで次の syslog メッセージのブロードキャストが発生しています。

これが起こる理由とそれを阻止する方法を教えてください。 AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN <id>

A. これらのメッセージは、警告メッセージであり、WLAN オーバーライドが有効で、特定の WLAN ID がスロット/無線機で選択またはアドバタイズされていない場合に表示されます。

Q. TFTP サーバを使用して AP をアップグレードするときに問題が発生します。 アップグレードしようとするたびに、アップグレード イメージ ファイル c1200-k9w7-tar.default に拡張子 .tar が追加されるのですが、このファイルは AP で認識されません。 追加された拡張子 .tar を削除する方法がわかりません（solarwind と tftpd32 のどちらもダウンロードして試してみました）。 この問題を解消するには、どうすればよいのですか。

A. 問題は、オペレーティング システムが登録されている拡張子を表示していないことであると考えられます。 [My Computer]に移動します。 [Tools] > [Folder Options] > [View] の順にクリックし、パラメータ [Hide extensions for known file types] が表示されるまで下にスクロールして、このボックスのチェックマークを外します。 これで問題は解消されます。

Q. AP で「high CPU utilization」というアラーム メッセージがよく発生します。 このような場合、ハードウェアをリブートすると、AP は稼働状態に戻ります。 この問題を解決するには、どうすればよいのですか。

A. AP が「high CPU utilization」に達する理由がいくつかあります。

- Cisco AP がスイッチ経由でネットワークに接続されている場合、AP で「high CPU utilization」が観測されることがあります。 これは、デフォルトではどの VLAN も AP の接続先のスイッチから AP まで許可されているためです。 大規模なネットワークでこのようなデフォルトを適用している場合などには、問題になることがあります。 どの VLAN も AP まで許可した場合、AP が high CPU utilization に達することがあり、接続性に影響が出ることがあります。 その AP に関連付けられたクライアントではスループットの問題が発生し、CPU 使用率が高いために無線ネットワークがダウンすることもあります。この問題を回避するには、AP が対象とする VLAN トラフィックのみが AP を通過するように、スイッチで VLAN をプルーニングします。
- AP でループバック インターフェイスが設定されている場合、AP で「high CPU utilization」が観測されることがあります。 Cisco AP にループバック インターフェイスを設定できるものの、このような設定を禁止しているため、ループバック インターフェイスはサポート対象ではありません。 AP にループバック インターフェイスが設定されている場合は、そのループバック インターフェイスを削除することを推奨いたします。**注:** AP およびブリッジでは、interface loopback コマンドはサポートされません。

この問題をトラブルシューティングするための最初の手順として、AP で show process cpu コマンドを発行します。 これで、どのようなプロセスが CPU を使用するかがわかります。

また、AP で 12.3(2)JA2 よりも前のバージョンが動作している場合、そのバージョンを 12.3(2)JA2 にアップグレードします。旧バージョンでは、サービス リクエストが CPU を停止した場合に既知の問題が発生するためです。

Q. 871W Wi-Fi ルータでは wi-fi で確立したセッションが切断されるため、常にユーザの VPN セッションを再確立する必要があります。 この理由は何ですか。

A. この問題を引き起こす可能性のある理由はいくつか考えられます。 両方のアンテナを 871W ルータに接続してください。 チャネルを 1、6、または 11 に変更し、どのチャネルで最大のパフォーマンスが得られるかを確認します。 また、ネイバーフッドに干渉の発生源となる他の AP が存在する可能性もあります。 これは、考えられる理由の 1 つにすぎません。

関連情報

- Cisco ダウンロード：ワイヤレス製品 (登録ユーザ専用)
- Cisco Aironet 1240 AG シリーズに関する Q&A
- Cisco Aironet 1230 AG シリーズに関する Q&A
- VxWorks のための Cisco Aironet アクセス ポイント ソフトウェア設定ガイド
- Cisco Aironet アクセス ポイント用 Cisco IOS ソフトウェア設定ガイド、12.2(13)JA
- Cisco Aironet 350 シリーズ トラブルシューティング テクニカル ノート
- ワイヤレス製品に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems