ワイヤレスLANコントローラ(WLC)のエラーメッセージとシステムメッセージに関するFAQを確認する

内容

[はじめに](#)

- [表記法](#)

[エラー メッセージに関する FAQ](#)

[関連情報](#)

はじめに

このドキュメントでは、CiscoワイヤレスLAN(WLAN)コントローラ(WLC)のエラーメッセージとシステムメッセージに関するFAQについて説明します。

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。

エラー メッセージに関する FAQ

Q.Cisco IOS®ソフトウェアからCisco 4404 WLCを使用したLightweight AP Protocol(LWAPP)への200を超えるアクセスポイント(AP)の変換が開始されました。48個のAPの変換が完了し、WLCで受信したメッセージに「**[ERROR] spam_lrad.c 4212: AP cannot join because the maximum number of APs on interface 1 is reached**」と書かれていました。 なぜこのようなエラーが発生するのでしょうか。

A. 48を超えるAPをサポートするには、追加のAPマネージャインターフェイスを作成する必要があります。これを行わないと、次のようなエラーが発生します。

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

複数の AP マネージャ インターフェイスを設定し、他の AP マネージャ インターフェイスでは使用されないプライマリ ポートまたはバックアップ ポートを設定してください。追加のAPを起動するには、2番目のAPマネージャインターフェイスを作成する必要があります。ただし、各マネージャのプライマリポートとバックアップポートの設定が重複していないことを確認してください。つまり、AP マネージャ 1 ではプライマリにポート 1、バックアップにポート 2 が使用されている場合、AP マネージャ 2 ではプライマリにポート 3、バックアップにポート 4 を使用する

必要があります。

Q.ワイヤレス LAN コントローラ（WLC）4402 があり、1240 Lightweight Access Point（LAP; Lightweight アクセス ポイント）を使用しています。WLCで128ビット暗号化を有効にしました。WLCで128ビットのWEP暗号化を選択すると、「128ビットは1240でサポートされていない」というエラーが表示されます。**[ERROR] spam_lrad.c 12839: Not creating SSID mde on CISCO AP xx:xx:xx:xx:xx:xx because WEP128 bit is not supported**」なぜこのエラーが表示されるのですか。

A. WLCに表示されるキーの長さは、実際には共有秘密鍵内のビットの長さであり、初期ベクトル(IV)の24ビットは含まれていません。Aironet 製品を含む多くの製品では、これを 128 ビット WEP キーと呼んでいます。これは、実際には 24 ビットの IV が付加された 104 ビットのキーです。128 ビット WEP 暗号化のためには、WLC で 104 ビットのキー サイズをイネーブルにする必要があります。

WLC で 128 ビットのキー サイズを選択すると、実際には 152 ビット（128 + 24 IV）の WEP キー暗号化となります。WLC の 128 ビット WEP キー設定の使用をサポートするのは、Cisco 1000 シリーズ LAP（AP1010、AP1020、AP1030）だけです。

Q.なぜWLCで「**WEP key size of 128 bits is not supported on 11xx, 12xx and 13xx model APs.WLC**でWEPを設定しようとすると、エラーメッセージが表示されるのはなぜですか。

A.ワイヤレスLANコントローラでは、レイヤ2セキュリティ方式としてStatic WEPを選択する際、次のオプションまたはWEPキーサイズを使用できます。

- 設定しない
- 40 ビット
- 104 ビット
- 128 ビット

これらのキー サイズ値には、WEP キーに連結される 24 ビットの Initialization Vector（IV; 初期ベクトル）は含まれません。そのため、64ビットのWEPに対しては、WEPキーサイズとして40ビットを選択する必要があります。コントローラは 64 ビットの WEP キーを作成するために、これに 24 ビットの IV を追加します。同様に、128ビットのWEPキーに対しては104ビットを選択します。

また、コントローラは 152 ビットの WEP キー（128 ビット + 24 ビット IV）をサポートします。この設定は、11xx、12xx、13xx モデルの AP ではサポートされません。そのため、144 ビットで WEP を設定しようとすると、コントローラから、この WEP 設定は 11xx、12xx、および 13xx モデルの AP にはプッシュされないというメッセージが表示されます。

Q. WPA2用に設定されたWLANに対してクライアントが認証できず、コントローラで「**apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Could not process the RSN and WARP IE. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>**」という エラーメッセージが表示されます。なぜこのエラーが表示されるのですか。

A.この問題は主に、クライアント側の非互換性が原因で発生します。この問題を解決するには、

次の手順を実行します。

- クライアントが WPA2 用に Wi-Fi 認定されているかどうかと、WPA2 用のクライアントの設定を確認します。
- クライアント ユーティリティが WPA2 をサポートしているかどうかについて、データ シートを確認します。ベンダーから WPA2 をサポートするパッチ リリースが提供されていれば、インストールします。Windowsユーティリティを使用する場合は、WPA2をサポートするMicrosoftからのWPA2パッチをインストール済みであることを確認します。詳細は、Microsoftサポートを参照してください。
- クライアントのドライバとファームウェアをアップグレードします。
- WLAN 上の Aironet 拡張機能をオフにします。

Q.WLCをリブートすると、「**Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event(s) found as violated by the radio 0 0:XX:XX:XX:XX**」と表示され、**300**秒で**AP 00:XX:XX:XX**のスロット**0**の**dot11**インターフェイスによってプローブ応答のビーコンフレームのエラーメッセージが観測されたときに検出されました。なぜこのエラーが発生するのでしょうか。また、どうすれば エラーがなくなるのでしょうか。

A.このエラーメッセージは、誤ったMIC値が設定されたフレームがMFP対応LAPで検出された場合に表示されます。MFPの詳細は、『WLCとLAPでのインフラストラクチャ管理フレーム保護(MFP)設定例』を参照してください。次の 4 つの手順のうちの 1 つを実行します。

1. ネットワーク内の不正または無効な AP またはクライアントを確認して削除します。これは、無効なフレームを生成するものです。
2. LAP は MFP をイネーブルにしていないグループ内の他の WLC の LAP からの管理フレームを受信できるため、モビリティ グループの他のメンバ上で MFP がイネーブルにされていない場合、インフラストラクチャ MFP をディセーブルにします。モビリティグループの詳細は、『ワイヤレスLANコントローラ(WLC)モビリティグループに関するFAQ』を参照してください。
3. このエラー メッセージの修正は、WLC リリース 4.2.112.0 および 5.0.148.2 で利用できます。WLC をこれらのリリースのどちらかにアップグレードします。
4. 最後の選択肢として、このエラー メッセージを生成する LAP をリロードします。

Q.クライアントAIR-PI21AG-E-K9は、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling(EAP-FAST)を使用して、アクセスポイント(AP)と正常に関連付けられています。ところが、関連付けられた AP をスイッチ オフすると、クライアントは別の AP にローミングしません。次のメッセージが、コントローラメッセージログに継続的に表示されます。「**Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - probably the user is already logged onto the system?**」6月2日（金） **14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4**」を参照してください。これは、なぜですか。

A.クライアントカードは、ローミングが必要になると認証要求を送信しますが、キーを正しく処理しません（APやコントローラに通知せず、再認証に応答しません）。

この問題は、Cisco Bug IDCSCsd02837に記載されています。このバグは Cisco Aironet 802.11a/b/g クライアント アダプタ Install Wizard 3.5 で修正されています。

一般に、次のいずれかの理由により、「Unable to delete username for mobilemessage」というエラーメッセージも表示されます。

- 特定のユーザ名が複数のクライアント デバイスで使用されている。
- WLAN に使用されている認証方法に、外部の匿名 ID がある。たとえば、PEAP-GTC や EAP-FAST では、一般的なユーザ名を外部（表示）ID として定義し、実際のユーザ名はクライアントと RADIUS サーバ間の TLS トンネル内に隠されている可能性があります。そのため、コントローラでは実際のユーザ名の参照と使用ができません。このような場合、このメッセージが表示される場合があります。この問題は、一部のサードパーティのクライアントや一部の旧版ファームウェアのクライアントで一般的に見られます。

注:Cisco Bugsの内部情報およびツールにアクセスできるのは、登録ユーザのみです。

Q.6509スイッチに新しいWireless Services Module(WiSM)ブレードをインストールし、Microsoft IASサーバでProtected Extensible Authentication Protocol(PEAP)を実装すると、次のエラーが表示されます。 ***Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.700: %SYS-RELOAD: Requested by by LWAPP CLIENT.Reload理由：FAILED CRYPTO INIT. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPPの状態がDOWNに変わりました*Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPPの状態がDISCOVERYに変わりました*Mar 1 00:00:23.57: LWAPP_ERROR crypto_init_ssc_keys_and_certs SSCプライベートファイルに証明書なし*Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00 :23.557: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.** 」というエラーメッセージが表示されます。これは、なぜですか。

A.RADIUSおよびdot1xのデバッグでは、WLCがアクセス要求を送信するのに対し、IASサーバから応答がないことがわかります。この問題のトラブルシューティングを行うには、次の手順を実行します。

1. IAS サーバの設定をチェックし、確認する。
2. ログ ファイルをチェックする。
3. 認証についての詳細情報を表示する Ethereal などのソフトウェアをインストールする。
4. IAS サービスを停止してから、再スタートさせる。

Q.コントローラで Lightweight Acess Points（LAP; Lightweight アクセス ポイント）が登録されません。どのような原因が考えられますか。コントローラに次のエラーメッセージが表示されます。**Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0.2028年2月3日（木）03:20:47: Unable to free public key for AP 00:0B:85:68:F4:F0.**

A.アクセスポイント(AP)は、WLCにLightweightアクセスポイントプロトコル(LWAPP)加入要求を送信する際に、LWAPPメッセージにX.509証明書を埋め込みます。また、ランダムなセッションID を生成し、LWAPP 加入要求に付加します。WLCはLWAPP加入要求を受信すると、AP公開キーを使用してX.509証明書の署名を検証し、その証明書が信頼できる認証局から発行されたもの

であることを確認します。また、AP証明書の有効期間の開始日時を調べ、その日時を自身の日時と比較します。

この問題は、WLC のクロック設定が誤っているために発生します。WLCのクロックを設定するには、 show time コマンドと config time コマンドを発行します。

Q.Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）APがコントローラに加入できません。ワイヤレスLANコントローラ(WLC)ログに、「`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01`」のようなメッセージが表示されます。これは、なぜですか。

A.このエラーメッセージは、APとWLCの間のLWAPPトンネルが1500バイト未満のMTUでネットワークパスを通過する場合に発生します。これにより、LWAPP パケットのフラグメンテーションが発生します。これはコントローラの既知の不具合です。Cisco Bug IDCSCsd39911を参照してください。

ソリューションは、コントローラのファームウェアを 4.0（155）にアップグレードすることです。

注:Cisco Bugsの内部情報およびツールにアクセスできるのは、登録ユーザのみです。

Q.内部コントローラと非武装地帯(DMZ)上の仮想アンカーコントローラの間にゲストトンネリングを確立する必要があります。ところが、ユーザがゲスト SSID との関連付けをしようとすると、DMZ から期待通りに IP アドレスを受信できません。そのため、そのユーザ トラフィックは DMZ にあるコントローラにトンネリングされません。debug mobile handoffコマンドの出力には、`Security Policy Mismatch for WLAN <Wlan ID>`のようなメッセージが表示されます。スイッチIPからのアンカーエクスポート要求：<コントローラのIPアドレス>無視。この問題の原因は何ですか?

A.ゲストトンネリングにより、企業のワイヤレスネットワークへのゲストユーザアクセスに対するセキュリティが強化されます。これにより、ゲスト ユーザはまず企業のファイアウォールを通過しなければ社内ネットワークにアクセスできなくなります。ゲスト WLAN として指定されている WLAN にユーザが関連付けを行うと、そのユーザ トラフィックは企業ファイアウォールの外部にある DMZ 内の WLAN コントローラにトンネリングされます。

ここで、このシナリオを検討してみると、このゲスト トンネリングが期待通りに機能しないのには、いくつかの理由が考えられます。debugコマンドの出力が示すように、社内およびDMZ内の特定のWLANに対して設定されているいずれかのセキュリティポリシーの不一致が問題として考えられます。セキュリティ ポリシーおよびセッションのタイムアウト設定などその他の設定が一致しているか確認してください。

この問題のもう1つの一般的な原因は、その特定のWLANに対してDMZコントローラがそれ自体にアンカーされていないことです。ゲスト トンネリングが適切に機能し、ユーザ（ゲスト WLAN に属するユーザ）の IP アドレスを DMZ が管理できるようにするためには、特定の WLAN に対するアンカーが適切であることが重要です。

Q.「CPU Receive Multicast Queue is full on Controller」というメッセージが 2006 ワイヤレス LAN コントローラ（WLC）で多数発生しますが、4400 WLC では発生しません。これは、なぜですか。コントローラではマルチキャストをディセーブルにして

います。**2006 WLC** プラットフォームと **4400 WLC** プラットフォームでの、マルチキャスト キュー制限の違いは何ですか。

A.コントローラではマルチキャストが無効になっているため、このアラームの原因となったメッセージはAddress Resolution Protocol（ARP；アドレス解決プロトコル）メッセージである可能性があります。2006 WLC と 4400 WLC では、キュー項目数（512 パケット）に違いはありません。4400 では NPU で ARP パケットのフィルタリングが行われるのに対し、2006 ではすべての処理がソフトウェアで行われる点が異なっています。2006 WLC ではメッセージが表示され、4400 WLC では表示されないのはこのためです。44xx WLC では、マルチキャスト パケットが（CPU を介して）ハードウェアで処理されます。2006 WLC では、マルチキャスト パケットがソフトウェアで処理されます。CPU による処理は、ソフトウェアによる処理よりも効率的です。そのため、4400 のキューはより短時間でクリアされますが、2006 WLC ではこれらのメッセージが多数発生すると、処理に多少時間がかかります。

Q.コントローラのいずれかで「**[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port.**」というエラーメッセージが表示されます。このエラーは何を意味しますか。また、このエラーを解決するには、どのような手順を実行する必要がありますか。

A.このメッセージは、コントローラが、ステートマシンのないMACアドレスに対するDHCP要求を受信したときに表示されます。これは一般に、VMware などの仮想マシンが稼働するブリッジやシステムで表示されます。コントローラは DHCP スヌーピングを実行するため、DHCP 要求をリッスンします。そのため、そのアクセス ポイント（AP）に接続されているクライアントに関連付けられているアドレスを認識できます。ワイヤレス クライアントへのすべてのトラフィックは、コントローラを経由します。パケットの宛先がワイヤレス クライアントである場合、このパケットはコントローラに送られてから、Lightweight Access Point Protocol（LWAPP）トンネルを通過して AP へ、そしてクライアントへ送信されます。このメッセージの対応策として考えられるのは、スイッチで**switchport vlan** allowcommandを使用することにより、コントローラに向かうトランクにおいて、コントローラで使用されるVLANを許可することだけです。

Q.コンソールに「**Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc**」というエラーメッセージが表示されるのはなぜですか。

A.これはCPUの高負荷が原因である可能性があります。コントローラ CPU は、ファイルのコピーなどの作業を行って過負荷になると、設定メッセージへの応答として NPU が送信する ACK をすべて処理する時間がありません。この状態になると、CPU でエラー メッセージが発生します。ただし、このエラー メッセージによるサービスや機能への悪影響はありません。

詳細は、『CiscoワイヤレスLANコントローラ』を参照してください。

Q.Wireless Control System(WCS)でWired Equivalent Privacy(WEP)キーエラーメッセージ「**The WEP Key configured at the station can be wrong.Station MAC Address is 'xx:xx:xx:xx:xx:xx', AP base radio MAC is 'xx:xx:xx:xx:xx:xx' and Slot ID is '1'**」しかし、ネットワークではセキュリティ パラメータに **WEP** を使用していません。使用しているのは **Wi-Fi Protected Access（WPA）**だけです。なぜ、このような **WEP** エラー メッセージが表示されるのですか。

A.セキュリティ関連の設定にすべて問題がなければ、現在表示されているメッセージは不具合によるものです。コントローラには既知の不具合がいくつかあります。Cisco Bug IDCSCse17260およびCisco but ID CSCse11202を参照してください。これらのバグには、「The WEP Key configured at the station can be wrong with **WPA and TKIP clients respectively**」と記載されています。実際には、Cisco Bug ID **CSCse17260**は Cisco Bug ID **CSCse11202**と重複しています。CiscoでID **CSCse11202**の修正は、WLCリリース3.2.171.5ですでに提供されています。

注：最新のWLCリリースでは、これらのバグが修正されています。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.外部RADIUSサーバを使用して、コントローラ経由でワイヤレスクライアントを認証しています。コントローラは「no radius servers are responding」エラーメッセージを定期的に送信します。これらのエラーメッセージが表示されるのはなぜですか。

A.要求がWLCからRADIUSサーバに送信されると、各パケットにはシーケンス番号が割り当てられ、WLCはこれに対して応答を待ちます。応答がない場合は、radius-server not respondingというメッセージが表示されます。

WLC が RADIUS サーバからの応答を待つデフォルトの待機時間は 2 秒です。これは、WLCのGUIの**Security** > **authentication-server**で設定されます。最大時間は 30 秒です。したがって、この問題を解決するには、このタイムアウト値を最大値に設定すると便利です。

RADIUSサーバでは、WLCからの要求パケットに対して「サイレント破棄」が行われることがあります。RADIUS サーバでは、証明書の不一致やその他いくつかの理由に基づき、これらのパケットが拒否される場合があります。これは、サーバによる有効なアクションです。また、このような場合、コントローラはRADIUSサーバが応答していないとマーキングする可能性があります

サイレント破棄の問題を解決するためには、WLCでアグレッシブフェールオーバー機能をディセーブルにします。

アグレッシブ フェールオーバー機能をWLCでイネーブルにすると、WLCは非常にアグレッシブになるため、AAAサーバがnot respondingであるとマーキングされてしまいます。ただし、AAAサーバはその特定のクライアントにのみ応答できないため（サイレント廃棄を行います）、これは実行しないでください。他の有効な（有効な証明書を持つ）クライアントに対しては応答している可能性があります。ただし、WLCはAAAサーバを「not responding」および「not functional」としてマーキングすることはできます。

これを解決するには、アグレッシブフェールオーバー機能を無効にします。これを実行するには、コントローラのCLIから**config radius aggressive-failover** disablecommandを発行します。この機能をディセーブルにすると、コントローラでは RADIUS サーバからの応答を 3 つのクライアントが連続して受信できなかった場合にのみ、次の AAA サーバへのフェールオーバーを行います。

Q.一部のクライアントはLWAPPに関連付けすることができず、コントローラは「**IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt returned error**」エラーメッセージをログに記録します。なぜ、このような現象が発生するのでしょうか。

A.これは主に、CCX v4をサポートしているが、10.5.1.0より前のクライアントバンドルバージョンを実行しているIntelアダプタの

問題が原因で発生します。このソフトウェアを 10.5.1.0 以降にアップグレードすると、この問題は修正されます。このエラーメッセージの詳細については、Cisco Bug IDCSCsi91347を参照してください。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.ワイヤレスLANコントローラ(WLC)に「Reached Max EAP-Identity Request retries (21) for STA 00:05:4e:42:ad:c5」というエラーメッセージが表示されます。これは、なぜですか。

A.このエラーメッセージが発生するのは、EAPで保護されたWLANネットワークにユーザが接続しようとして、事前設定された回数のEAP試行が失敗した場合です。ユーザが認証に失敗すると、コントローラはクライアントを除外し、除外タイマーが時間切れになるか、管理者が手動で上書きするまで、クライアントはネットワークに接続できません。

除外では、単一のデバイスによる認証の試行が検出されます。デバイスが失敗回数の上限を上回ると、その MAC アドレスはそれ以降、関連付けが許可されなくなります。

除外が発生するのは次の場合です。

- 共有認証については、連続して 5 回認証に失敗した場合（6 回目の試行が除外されます）。
- MAC 認証については、連続して 5 回関連付けに失敗した場合（6 回目の試行が除外されます）
- EAP/802.1X 認証については、連続して 3 回失敗した場合（4 回目の試行が除外されます）
- すべての外部ポリシー サーバの失敗（NAC）
-

すべての IP アドレス重複インスタンス

- Web 認証については、連続して 3 回失敗した場合（4 回目の試行が除外されます）

クライアントをどれくらい長く除外するかを決めるタイマーは設定可能であり、除外はコントローラまたは WLAN レベルでイネーブルまたはディセーブルにできます。

Q.ワイヤレスLANコントローラ(WLC)に次のエラーメッセージが表示されます。「An Alert of Category Switch is generated with severity 1 by Switch WLCSCH01/10.0.16.5 The message of the alert is Controller '10.0.16.5'.RADIUS server(s) are not responding to authentication requests.」どこに問題があるか？

A.これは、Cisco Bug ID CSCsc05495が原因で発生する可能性があります。この不具合が原因で、コントローラで間歇的に誤った AV ペア（アトリビュート 24、「ステート」）が認証要求メッセージに注入され、これが RADIUS RFP に違反するため、一部の認証サーバで問題が発生します。この不具合は、3.2.179.6 で修正されています。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.[Monitor] > [802.11b/g Radios] ページで、**ノイズ プロファイル失敗**メッセージを受け取ります。この **FAILED** メッセージが表示されるのはなぜですか。

A.ノイズプロファイルのFAILED/PASSEDステータスは、WLCによるテスト結果に基づき、現在設定されているしきい値と比較して設定されます。デフォルトでは、ノイズ値は -70 に設定されています。FAILED ステータスは、その特定のパラメータまたは Access Point（AP; アクセス ポイント）のしきい値を超過していることを示しています。プロファイルのパラメータは調整できますが、ネットワーク設計と、それがネットワークのパフォーマンスに与える影響を明確に理解した上で、設定を変更することをお勧めします。

Radio Resource Management(RRM)のPASSED/FAILEDしきい値は、**802.11a Global Parameters** > **Auto** RFand **802.11b/g Global Parameters** > **Auto** RFpagesですべてのAPに対してグローバルに設定されます。**802.11 AP Interfaces** > **Performance** Profilepageでは、このAPに対してRRM PASSED/FAILEDしきい値が個別に設定されています。

Q.ポート 2 を AP マネージャのインターフェイスのバックアップ ポートとして設定できません。「Could not set port configuration」というエラー メッセージが返されています。ポート 2 を、管理インターフェイスに対するバックアップ ポートとしては設定できます。両インターフェイスの現在のアクティブ ポートはポート 1 です。これは、なぜですか。

A. APマネージャにはバックアップポートがありません。これは、以前のバージョンではサポートされていました。バージョン 4.0 以降、AP マネージャ インターフェイスのバックアップ ポートはサポートされなくなっています。原則として、各ポートに単一のAPマネージャを設定する必要があります (バックアップなし) 。リンク集約 (LAG) を使用する場合、AP マネージャは 1 つだけです。

スタティック (または固定) AP マネージャ インターフェイスは、ディストリビューション システム ポート 1 に割り当て、一意の IP アドレスを持つようにする必要があります。バックアップ ポートにはマッピングできません。通常、管理インターフェイスと同じ VLAN または IP サブネット上で設定されていますが、これは要件ではありません。

Q.エラーメッセージ「**The AP '00:0b:85:67:6b:b0' received a WPA MIC error on protocol '1' from Station '00:13:02:8d:f6:41'.Counter measures have been activated and traffic has been suspended for 60 seconds.**」これは、なぜですか。

A. Wi-Fi Protected Access(WPA)に組み込まれているMessage Integrity Check(MIC)には、中間者攻撃(man-in-the-middle attack)を防ぐフレームカウンタが備わっています。このエラーは、ネットワーク内の誰かが元のクライアントから送信されたメッセージを再生しようとしているか、クライアントに障害があることを意味している可能性があります。

クライアントが MIC チェックで繰り返し失敗する場合、コントローラはエラーが検出された AP インターフェイスの WLAN を 60 秒間ディセーブルにします。最初の MIC 障害が記録されると、対応策の強制をイネーブルにするためにタイマーが設定されます。前回の最新の障害から60秒以内にさらにMIC障害が発生した場合、サプリカントとして動作していたIEEE 802.1Xエンティティ のSTAは、そのIEEE 802.1Xエンティティがオーセンティケータとして動作していた場合、それ自体を無効にするか、セキュリティアソシエーションのあるすべてのSTAを無効にします。*

さらに、デバイスは、2回目の障害を検出してから少なくとも60秒間、TKIPで暗号化されたデータフレームを送受信せず、IEEE 802.1Xメッセージ以外の暗号化されていないデータフレームをピアとの間で送受信しません。デバイスがAPの場合、この60秒間はTKIPとの新しいアソシエーションを拒否します。60秒間の終了時には、APは通常の動作を再開し、STAの (再) アソシエーションを許可します。

これにより、暗号化スキームへの潜在的な攻撃が防止されます。これらの MIC エラーは、4.1 よりも前のバージョンの WLC ではオフにはできません。ワイヤレス LAN コントローラ バージョン 4.1 以降では、MIC エラーのスキャン時間を変更するコマンドが存在します。コマンド**isconfig wlan security tkip hold-down <0-60 seconds> <wlan id>**。対抗策として、MIC 障害の検出をディセーブルにするために値 0 を使用します。

*Invalidate：認証を終了します。

Q.コントローラのログに次のエラーメッセージが表示されます。**[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed**。これは、なぜですか。

A.これらのエラーメッセージはほとんどの場合、コントローラのサービスポートでDHCPがイネーブルになっているにもかかわらず、DHCPサーバからIPアドレスが割り当てられていない場合に表示されます。

デフォルトでは、物理サービス ポート インターフェイスには DHCP クライアントがインストールされており、DHCP を介してアドレスが探索されます。WLC はサービス ポートの DHCP アドレスを要求しようとします。使用可能な DHCP サーバがない場合、サービス ポートのための DHCP 要求は失敗します。このため、エラー メッセージが生成されます。

回避策としては、（サービス ポートが接続解除されている場合も含め）サービス ポートにスタティック IP アドレスを設定するか、サービス ポートに IP アドレスを割り当てられる DHCP サーバを置くようにします。次に、必要に応じてコントローラをリロードします。

実際には、サービス ポートはコントローラとシステムの復旧についてのアウトオブバンド管理、およびネットワーク障害発生時のメンテナンスのために予約されています。また、コントローラがブート モードである場合にアクティブなただ 1 つのポートでもあります。サービス ポートでは 802.1Q タグを搬送することはできません。そのため、隣接スイッチのアクセス ポートに接続する必要があります。サービス ポートの使用はオプションです。

サービス ポート インターフェイスは、通過する通信を制御し、システムによってサービス ポートに静的にマッピングされます。サービス ポート インターフェイスは、管理インターフェイス、AP マネージャ インターフェイス、およびすべての動的インターフェイスからの異なるサブネットでの IP アドレスを持っている必要があります。また、バックアップ ポートにはマッピングできません。サービス ポートは、DHCP を使用して IP アドレスを取得するか、スタティック IP アドレスを割り当てることができますが、サービス ポート インターフェイスにデフォルトのゲートウェイを割り当てることはできません。スタティック ルートは、サービス ポートへのリモート ネットワーク アクセス用のコントローラを通じて定義できます。

Q.ワイヤレス クライアントをワイヤレス LAN（WLAN）ネットワークに接続できません。アクセスポイント(AP)が接続されているWiSMが、「Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00」というメッセージを報告しています。これはどういう意味ですか。

A.メディアにアクセスする条件として、MACレイヤはNetwork Allocation Vector(NAV)の値をチェックします。NAV は各ステーションに常駐するカウンタで、前のフレームがそのフレームを送信するのに必要とする時間を表しています。ステーションがフレームの送信を試行できるようになるには、NAV はゼロである必要があります。ステーションは、フレームを送信する前に、フレーム長とデータレートに基づいて、フレームを送信するために必要な時間を計算します。ステーションでは、この時間を表す値をフレームのヘッダーのデュレーション フィールドに挿入します。ステーションではフレームを受信すると、このデュレーション フィールドの値を検査し、対応する NAV を設定する基準としてこの値を使用します。このプロセスで、送信側ステーションのメディアが予約されます。

NAV が高いということは、NAV 値高騰を示しています（802.11 の仮想キャリア センス メカニズム）。報告されたMACアドレスが00:00:00:00:00:00の場合、おそらくスプーフィングされています（実際の攻撃の可能性あり）。これをパケットキャプチャで確認する必要があります。

Q.コントローラを設定してリブートすると、セキュアWeb(https)モードでコントローラにアクセスできません。コントローラのセキュアWebモードにアクセスしようとすると、次のエラーメッセージが表示されます。Secure Web: Web Authentication Certificate not found (error)。この問題の原因は何ですか。

A.この問題にはいくつかの原因が考えられます。共通する原因の 1 つは、コントローラの仮想インターフェイス設定に関連している可能性があります。この問題を解決するには、仮想インターフェイスを削除してから、次のコマンドで仮想インターフェイスを再生成します。

<#root>

WLC>

config interface address virtual 1.1.1.1

次に、コントローラをリブートします。コントローラをリブートした後で、次のコマンドにより、コントローラでローカルにwebauth 証明書を再生成します。

<#root>

WLC>

config certificate generate webauth

このコマンドの出力では、Web Authentication certificate has been generatedというメッセージが表示されます。

リブート時にコントローラのセキュアWebモードにアクセスできるようになりました。

Q.コントローラでは、攻撃者のMACアドレスが、そのコントローラに加入しているアクセスポイント(AP)のMACアドレスである有効なクライアントに対して、このIDS解除フラッドシグニチャ攻撃のアラートメッセージが報告されることがあります。**Alert: IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'。The Signature description is 'Disassociation flood', with precedence 'x'.攻撃者のMACアドレスは'hh:hh:hh:hh:hh:hh'、チャネル番号は'x'、検出数は'x'です。なぜこのような現象が発生するのでしょうか。**

A.これは、Cisco Bug IDCSCsg81953（登録ユーザ専用）によるものです。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

攻撃者のMACアドレスがそのコントローラに加入しているAPのMACアドレスである場合、有効なクライアントに対するIDS解除フラッディング攻撃が報告されることがあります。

クライアントがAPに関連付けられていても、カードの取り外しのために通信を停止したり、APへのローミングが範囲外になったりすると、APはアイドルタイムアウトまで待機します。アイドル タイムアウトになると、AP からそのクライアントに関連付け解除フレームが送信されます。クライアントから関連付け解除フレームに対する確認応答がない場合、AP は複数回フレームを再送信します (60 フレーム前後) 。コントローラの IDS サブシステムがこれらの再送信を受信すると、このメッセージで警告を発します。

この不具合は、バージョン 4.0.217.0 で解決されています。有効なクライアントと AP に対してこの警告メッセージが発生する問題を解決するには、コントローラのバージョンをこのバージョンにアップグレードしてください。

Q.コントローラのsyslogに次のエラーメッセージが表示されます。[WARNING] apf_80211.c 2408: Received a message with an invalid supported rate from station <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Missing Supported Rate。これは、なぜですか。

A.実際には、「Missing Supported Rate」メッセージは、WLCがワイヤレス設定で特定の必須データレートに設定されているにもかかわらず、必要なレートがNICカードでは欠落していることを示しています。

コントローラで 1 および 2M などのデータ レートを必要に応じて設定しているのに、NIC カードがこれらのデータ レートで通信しない場合には、このようなメッセージを受信する可能性があります。これは NIC カードの誤作動です。一方、コントローラで 802.11g がイネーブルになっており、クライアントが 802.11b (専用) カードである場合、これは妥当なメッセージです。これらのメッセージで問題が発生せず、カードで引き続き接続が可能である場合には、これらのメッセージを無視して構いません。このメッセージが特定のカードに固有である場合、このカードのドライバが最新であることを確認してください。

Q.エラーメッセージ「AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN ID <id>」がネットワークでブロードキャストされます。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。

A.このメッセージはLAPによってブロードキャストされます。これは、WLAN に対して WLAN オーバーライド機能を設定しており、その WLAN がアドバタイズされていないときに発生します。

Configureconfig ap syslog host global 0.0.0.0を発行して停止するか、syslogサーバがある場合は特定のIPアドレスを割り当てて、メッセージがサーバだけにブロードキャストされるようにすることもできます。

Q.ワイヤレスLANコントローラ(WLC)で次のエラーメッセージが表示されます。[ERROR]ファイル：apf_mm.c ：回線：581：Announce collision for mobile 00:90:7a:05:56:8a, deleting。これは、なぜですか。

A.通常、このエラーメッセージは、コントローラがワイヤレスクライアントに対してコリジョンをアナウンスした（つまり、別々のAPがクライアントの存在をアナウンスした）ことを示しており、あるAPから次のAPへのハンドオフがコントローラで受信されなかったことを示しています。維持すべきネットワーク ステートはありません。ワイヤレス クライアントを削除し、クライアントに再試行させてください。この問題が頻繁に発生する場合は、モビリティの設定に問題がある可能性があります。そうでない場合は、特定のクライアントまたは状態に関連する異常である可能性があります。

Q.コントローラで「Coverage threshold of '12' violated」というアラームメッセージが表示されます。このエラーは何ですか。どのように解決できますか。

A.このアラームメッセージは、クライアントのSignal-to-Noise Ratio（SNR；信号対雑音比）が特定の無線のSNRしきい値を下回ったときに発生します。カバレッジ ホール検出用のデフォルトの SNR しきい値は 12 です。

カバレッジホールの検出と補正アルゴリズムは、クライアントのSNRレベルが所定のSNRしきい値未満のときにカバレッジホールが存在するかどうかを判断します。このSNRしきい値は、AP送信電力とコントローラカバレッジプロファイル値の2つの値に基づいて変化します。

詳しく述べると、クライアントの SNR しきい値は、各 AP の伝送パワー（dBm 単位で表示）から定数値 17dBm を引き、ユーザが設定可能なカバレッジ プロファイル値（この値のデフォルトは 12 dB）を引いた値です。

- **クライアントの SNR 遮断値（|dB|） = [AP 伝送パワー（dBm） – 定数（17 dBm） – カバレッジ プロファイル（dB）]**

このユーザ設定可能なカバレッジ プロファイル値は、次のようにしてアクセスできます。

1. WLC の GUI で、メイン ヘッディング [Wireless] に移動し、[Network] オプションを左側にある WLAN 標準の選択肢から選択します（802.11a または 802.11b/g）。次に、ウィンドウの右上部で [Auto RF] を選択します。

2. [Auto RF Global parameters] ページで、[Profile Thresholds] セクションを探します。このセクションに、カバレッジの値があります（3 ~ 50 dbm）。この値は、ユーザが設定可能なカバレッジ プロファイル値です。

3.

この値を編集して、クライアント SNR しきい値に影響を与えることができます。SNR しきい値に影響を与えるその他の方法としては、伝送パワーを増加して、カバレッジ ホール検出を補正します。

Q.ACS v 4.1と 4402 Wireless LAN Controller(WLC)を使用しています。WLCがワイヤレスクライアントをACS 4.1に対してMAC認証しようとすると、ACSがACSでの応答に失敗し、「*Internal error has occurred*」というエラーメッセージが報告されます。設定はすべて適切です。なぜこの内部エラーが発生するのでしょうか。

A.ACS 4.1には認証関連のCisco Bug IDCSCsh62641があり、ACSで「`Internal error has` occurederror」メッセージが表示されます。

この不具合が問題である可能性があります。この不具合に対しては、ACS 4.1ダウンロードサイトで、問題を修正できるパッチが提供されています。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.Cisco 4400シリーズワイヤレスLANコントローラ(WLC)がブートできません。`** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg: 10 ** Cannot read from device 0`というエラーメッセージがコントローラで表示されます。これは、なぜですか。

A.このエラーは、ハードウェアの問題が原因である可能性があります。TAC のサービス リクエストをオープンして、この問題のトラブルシューティングを続けてください。TAC ケースを開くには、シスコとの契約が必要です。Cisco TAC に連絡するには、テクニカル サポートを参照してください。

Q.ワイヤレス LAN コントローラ (WLC) でメモリ バッファの問題が発生します。メモリ バッファがフルになるとコントローラはクラッシュするため、オンラインに戻すためにはリブートが必要です。次のエラーメッセージがメッセージログに表示されます。`Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Cannot allocate new Mbuf.Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbufs.`これは、なぜですか。

A.これはCisco Bug IDCSCsh93980が原因です。このバグは WLC バージョン 4.1.185.0 で解決されています。このメッセージの問題を解決するには、コントローラをこのソフトウェア バージョン以降にアップグレードします。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.ワイヤレスLANコントローラ(WLC)4400を4.1コードにアップグレードしたところ、syslogに次のメッセージが大量に表示されました。 May03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op) received with with invalid with spa) 192.168.1.233/TPA 192.168.1.233**です。これらのメッセージは何を示しているのですか。**

A.これは、WLANがDHCP required（DHCPが必要）とマーキングされている場合に発生する可能性があります。そのような場合、DHCP 経由で IP アドレスを受信するステーションだけが関連付けを許可されます。スタティック クライアントはこの WLAN への関連付けを許可されません。WLC は DHCP リレー エージェントとして動作し、すべてのステーションの IP アドレスを記録します。このエラー メッセージは、WLC がステーションから DHCP パケットを受信してその IP アドレスを記録する前に、ステーションから ARP 要求を受信すると生成されます。

Q.Power over Ethernet（PoE）を Cisco 2106 ワイヤレス LAN コントローラで使用すると、AP 無線がイネーブルになりません。「AP is unable to verify sufficient in-line power.`Radio slot disabled.`」というエラーメッセージが表示されます。これはどのように解決すればいいですか。

A.このエラーメッセージが発生するのは、アクセスポイントに電源を投入するスイッチがプレスタンダードスイッチであるにもかかわらず、APが入力パワーのプレスタンダードモードをサポートしていない場合です。

Cisco プレスタンダード スイッチは、インテリジェント電力管理（IPM）をサポートしませんが、標準アクセス ポイントには十分なパワーがあります。

このエラーメッセージが発生したAPで、電源の事前標準モードを有効にする必要があります。これは、コントローラのCLIで **config ap power pre-standard {enable | disable} {all | Cisco_AP}** コマンドを使用して実行できます。

以前のリリースからソフトウェアリリース4.1にアップグレードする場合は、必要に応じてこのコマンドがすでに設定されている必要があります。ただし、新規インストールの場合や、AP を工場出荷時のデフォルト設定にリセットした場合は、このコマンドを入力する必要がある可能性があります。

次のような Cisco プレスタンダード 15 ワット スイッチが販売されています。

- AIR-WLC2106-K9
- WS-C3550、WS-C3560、WS-C3750

- C1880
- 2600、2610、2611、2621、2650、2651
- 2610XM、2611XM、2621XM、2650XM、2651XM、2691
- 2811、2821、2851
- 3631-telco、3620、3640、3660
- 3725、3745
- 3825、3845

Q.コントローラが`dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: Unable to add an ARP entry for xx:xx.-xxx.x to the network processor. entry does not exist.`というsyslogメッセージを生成します。このsyslogメッセージは何を意味していますか。

A. ARP応答を送信するワイヤレスクライアントがある一方で、ネットワークプロセッサユニット(NPU)はその応答を知っている必要があります。そのため、ARP応答はNPUに転送されますが、WLCソフトウェアはこのエントリをネットワークプロセッサに追加しようとしないでください。追加しようとすると、これらのメッセージが生成されます。この問題によるWLCの機能への影響はありませんが、WLCはこのsyslogメッセージを生成します。

Q.新しい Cisco 2106 WLC をインストールし、設定しました。WLC は、温度センサーに障害があることを示しています。Web インターフェイスにログインすると、[controller summary] の下にある内部温度の横に「sensor failed」と表示されます。その他すべての情報は、正常に機能していることを示しています。

A.内部温度センサーの障害は表面的なものであり、WLCバージョン4.2.61.0にアップグレードすると解決できます。

2007年1月7日以降に製造された WLC 2106とWLC 526では、他のベンダーの温度センサーチップが使用されている可能性があります。この新しいセンサーは正常に動作しますが、4.2リリース以降のソフトウェアとは互換性がありません。したがって、古いソフトウェアでは温度を読み取ることができず、このエラーが表示されます。コントローラのその他すべての機能は、この障害の影響を受けません。

この問題に関連する既知のCiscoバグIDCSCsk97299があります。この不具合は、WLC バージョン 4.2 のリリース ノートに記載されています。

注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

Q.すべてのSSIDについて`radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Could not find appropriate RADIUS server for WLAN <WLAN ID> - unable to find a default server`"メッセージを受信します。このメッセージは、AAA サーバを使用していない SSID に対しても表示されます。

A.このエラーメッセージは、コントローラがデフォルトのRADIUSサーバに接続できなかったか、デフォルトのRADIUSサーバが定義されていないことを意味しています。

この動作の原因の1つとして考えられるのは、バージョン4.2で解決されたCiscoバグIDCSCsk08181です。コントローラをバージョン 4.2 にアップグレードしてください。

Q.`Message: Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.`というエラーメッセージがワイヤレスLANコントローラ(WLC)で表示されます。これは何を示しているのですか。

A.これは、CPUから送信されたパケットの送信中にコントローラにエラーが発生したことを意味します。

Q.ワイヤレス LAN コントローラ (WLC) に次のエラー メッセージが表示されます。

-

7月10日14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'cliWebInitParms.cfg'

- 7月10日14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL：コンフィギュレーションファイル「rfidInitParms.cfg」を読み取れませんでした
- 7月10日14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'dhcpParms.cfg'
- 7月10日14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL：コンフィギュレーションファイル「bcastInitParms.cfg」を読み取れませんでした
- 3月18日16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED：ファイルを削除できませんでした：sshpmInitParms.cfgファイルの削除に失敗しました。 - プロセス：名前：fp_main_task、Id:11ca7618
- Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file : bcastInitParms.cfg. file removal failed. - プロセス：名前：fp_main_task、Id:11ca7618

Q. これらのエラー メッセージは何を示しているのですか。

A.これらのメッセージは情報提供のメッセージであり、通常のブート手順の一部です。これらのメッセージはいくつかの異なる設定ファイルの読み取りまたは削除に失敗したために表示されます。特定の設定ファイルが見つからなかったときや設定ファイルを読み取ることができない場合、各プロセスの設定シーケンスが、DHCP サーバ設定がない、タグ（RF ID）設定がないなどのメッセージを送信します。これらは、問題なく無視することのできる重大度の低いメッセージです。これらのメッセージがコントローラの動作を中断することはありません。

Q.HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAINED: Unable to keep rogue 00:14:XX:02:XX:XX in contained state - no available AP to contain.というエラーメッセージが表示されます。これは何を示しているのですか。

A.これは、不正抑止機能を実行したAPが使用できなくなり、コントローラが不正抑止を実行するのに適したAPを見つけられなくなったことを意味します。

Q.DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206というシステムメッセージがワイヤレス**LAN**コントローラに表示されます。このメッセージは何を示しているのですか。

A.システムがARPスプーフィングまたはARPポイズニングを検出した可能性があります。しかし、このメッセージは、悪意のあるARPスプーフィングが発生したことを必ずしも意味するものではありません。メッセージは、次の条件が成立する場合にだけ表示されます。

- WLANはDHCP Requiredで設定され、クライアントデバイスはそのWLANに関連付けられた後、最初にDHCPを完了せずにARPメッセージを送信します。これは正常な動作である可能性があります。たとえば、クライアントにスタティックにアドレスが指定された場合や、クライアントが以前のアソシエーションから有効なDHCPリースを保持している場合に発生する可能性があります。表示されるエラー メッセージは次のようになります。

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.16
```

この条件が成立した場合、結果として、クライアントは WLC 経由で DHCP を実行するまでデータ トラフィックを送受信できなくなります。

詳細については、『Cisco Wireless LAN Controllerシステムメッセージガイド』の「DTLメッセージ」を参照してください。

Q. LAPの電源投入には、Power over Ethernet(POE)は使用されません。ワイヤレス **LAN** コントローラのログは次のようになっています。

<#root>

AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power

Q. どこに問題があるか？

A.これは、Power over Ethernet(PoE)設定が正しく設定されていない場合に発生する可能性があります。アクセス ポイントが Lightweight モードに変換されている場合、たとえば、AP1131 または AP1242、または 1250 シリーズのアクセス ポイントが Cisco pre-Intelligent Power Management（pre-IPM）スイッチに接続されているパワー インジェクタから電力が供給される場合、インライン パワーとも呼ばれる Power over Ethernet（PoE）を設定する必要があります。

詳細は、『Power over Ethernet、イーサネットサポートの設定』を参照してください。

Q.ワイヤレス LAN コントローラ（WLC）に次のメッセージが表示されます。

<#root>

***Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6**

Q.これは何を示しているのですか。

A.Lightweightアクセスポイントは、コントローラを見つけるために特定のアルゴリズムをトレースします。ディスカバリと加入のプロセスの詳細については、『ワイヤレスLANコントローラ(WLC)へのLightweight AP(LAP)の登録』を参照してください。

このエラー メッセージは、WLC が AP の最大容量に到達した後でディスカバリ要求を受け取ったときに WLC 上で表示されます

。

LAP のプライマリ コントローラは、設定されていないか、それが出荷直後の状態の LAP である場合、到達可能なすべてのコントローラに対して LWAPP ディスカバリ要求を送信します。ディスカバリ要求が、APの最大容量で稼働しているコントローラに到達すると、WLCは要求を受け取り、それが最大AP容量であることを認識して、要求に応答せず、このエラーを返します。

Q.LWAPP システム メッセージについての詳細な情報はどこで入手できますか。

A.LWAPPシステムメッセージの詳細は、『CiscoワイヤレスLANコントローラシステムメッセージガイド4.2（廃止）』を参照してください。

Q.「Error extracting webauth files」エラーメッセージがワイヤレスLANコントローラ(WLC)に表示されます。これは何を示しているのですか。

A.バンドルされているファイルの中に、ファイル拡張子を含む30文字を超えるファイルが含まれている場合、WLCはカスタムWeb認証/パススルーバンドルのロードに失敗します。カスタマイズWeb認証バンドルにファイル名の30文字の制限があります。バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

Q.多数のAPグループがある5.2または6.0コードを実行するWireless LAN Controller（WLC；ワイヤレスLANコントローラ）では、設定されているAPグループがすべてWeb GUIに表示されるわけではありません。どこに問題があるか？

A.欠落したAPグループは、CLIのshow wlan ap-groupsコマンドを使用すると表示できます。

リストに 1 個の AP グループを追加してください。たとえば、51台のAPグループを導入したが、51台目が見つからなかった（ページ3）。52番目のグループを追加すると、Page 3がWeb GUIに表示されます。

この問題を解決するには、WLCバージョン7.0.220.0にアップグレードします。

関連情報

- **WiSM トラブルシューティングに関する FAQ**
- ワイヤレスに関するサポート ページ

- 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。