Unified Wireless Network： クライアントの問題のトラブルシューティング

目次

はじめに

無線周波（RF）環境は複雑で動的です。 優れたワイヤレス環境を作成するには、さまざまな要素を考慮する必要があります。 このドキュメントでは、Cisco Unified Wireless 環境でワイヤレスクライアントを接続する際に発生する可能性があるさまざまな問題、およびこれらの問題をトラブルシューティングし解決するために実行する手順について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Wireless ソリューション
- Cisco ワイヤレス LAN コントローラ（WLC）GUI の基本設定

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されない、シスコの統合環境に参加しているすべてのデバイスに適用されます。

表記法

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。

背景説明

Cisco Unified 環境では、WLC は中心的な役割を担います。 これはワイヤレス ネットワーク全体を管理します。 ワイヤレス クライアントにサービスを提供する Lightweight アクセス ポイント（LAP）は、WLC に自身を登録し、すべての設定を WLC からダウンロードします。 最初に、LAP が WLC に登録されているかどうかを確認します。 WLC の GUI から [Wireless] メニューをクリックし、LAP がページにリストされているかどうかを確認します。

設定の問題

正常なワイヤレス接続のためには、WLC の設定が正しく行われていることが重要です。 このセクションでは、最も一般的な設定の問題の一部について説明します。

SSID のミスマッチ

クライアントは SSID を使用してワイヤレス ネットワークを識別して関連付けるため、SSID が WLC とクライアントで同じように設定されていることを確認します。 WLC で設定されている SSID を確認するには、[WLANs] ページをクリックします。 適切な [WLAN] をクリックして、[General] タブで設定されている SSID を確認します。

注: SSID では大文字と小文字が区別されます。 これは、WLAN を削除して再作成する場合に、ワイヤレス クライアントが WLAN に関連付けるのに役立つことがあります。

セキュリティの不一致

セキュリティ設定は、WLC とクライアント間で一致する必要があります。 認証タイプが Static WEP の場合、WLC 上の適切な暗号キーとキー インデックスがクライアントのものと一致するかどうかを確認します。 認証タイプが 802.1x または WPA の場合、クライアントと WLC の間で認証タイプと暗号キーのサイズが一致することを確実にします。 さまざまなセキュリティ ソリューションのために WLC とクライアントを設定する方法の詳細については、『ワイヤレス LAN コントローラでの認証の設定例』を参照してください。

注: WPA または 802.1x などのレイヤ 2 セキュリティ ソリューションは、Web 認証またはパススルーなどのレイヤ 3 のセキュリティ ソリューションで設定された WLAN には使用できません。 互換性のあるセキュリティ ソリューションの詳細については、『ワイヤレス LAN コントローラ

レイヤ 2 およびレイヤ 3 セキュリティの互換性マトリクス』を参照してください。

無効な WLAN

正常なワイヤレス接続のためには、対応する WLAN が WLC でアクティブである必要があります。 デフォルトでは、WLAN のステータスは WLC で有効になっていません。 WLAN をアクティブにするには、WLC で [WLAN] メニューをクリックします。 WLC 上で設定されている WLAN のリストが表示されます。 クライアントを関連付ける、SSID を使用して設定された [WLAN] をクリックします。 [WLANs] > [Edit] **ページの [General] タブで、[Status] チェックボックスにチェックマークを入れます**をオンにします。

サポートされていない Data-Rates

802.11b/g または 802.11a のいずれかの特定の標準では、WLC で特定のデータ レートを必須、他のデータ レートをサポート対象または無効に設定できます。 関連付けが正しく動作するには、ワイヤレス クライアントが WLC で必須として設定されたデータ レートをサポートしている必要があります。 WLC で設定されたデータ レートを確認するには、WLC の GUI で[Wireless] メニューをクリックし、ページの左側に表示される [802.11b/g/n] > [Network] または [802.11a/n] > [Network] オプションで設定されたデータ レートを確認します。 これを調べるには、クライアントのベンダーのサポート ページを確認します。 クライアントのドライバをアップグレードすると、必要なデータ レートをクライアントがサポートするのに役立つ場合があります。

注: より良い接続のために、WLC で最も低いデータ レートを [mandatory]、その他のデータ レートを [supported] に設定します。

無効なクライアント

WLC には、手動でクライアントを無効にするオプションがあります。 この機能は、不正クライアントのネットワークへのアクセス試行を防ぐのに役立ちます。 無効なクライアントのリストに関連付けられなかったクライアントの MAC アドレスが存在するかどうかを確認し、存在する場合はそのアドレスを削除します。 無効なクライアントのリストは、GUI の [Security] メニューの下の[Disabled Clients] オプションをクリックすると表示されます。

注: クライアントが WLC で設定されたデフォルトのクライアント除外ポリシーに準拠しない場合は、ネットワークへの関連付けを拒否できます。 クライアント除外ポリシーの詳細については、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.2』の「クライアント除外ポリシーの設定」セクションを参照してください。

無線プリアンブル

無線プリアンブル（ヘッダーと呼ばれることもある）は、パケットの先頭にあるデータの部分であり、ワイヤレス デバイスがパケットの送受信を行うときに必要な情報を含んでいます。

一部のクライアントでは、short preamble がサポートされていないため、short preamble が有効になってる WLAN に接続できません。 ショート プリアンブルの方がスループット パフォーマンスが向上するため、WLAN のデフォルトではこちらが有効になっています。 short preamble を無効にするには、WLC の GUI で [Wireless] メニューをクリックします。 次に、左側にある [802.11b/g] > [network] メニューをクリックします。 [short preamble] ボックスのチェックマークを外します。

シスコ独自の機能：サードパーティ製のクライアントとの問題

ネットワークに接続できないクライアント デバイスが Cisco 以外のデバイスである場合、シスコ独自の機能の一部を無効にすることによって正しく接続できることがあります。 クライアントでサポートされる機能のリストについては、サードパーティ製のクライアント デバイスのベンダーにお問い合わせください。

重要な独自の機能の一部を次に示します。

- **Aironet IE**：Aironet IE には、WLAN のビーコンとプローブ応答でアクセス ポイントから送信されたアクセス ポイント名、負荷、関連付けられたクライアントの数などの情報が格納されています。 CCX クライアントはこの情報を使用して、関連付ける最適なアクセス ポイントを選択します。
- **MFP**： 管理フレーム保護（Management Frame Protection）とは、認証解除、関連付け解除、ビーコン、プローブなどの管理フレームの整合性を保証するために導入された機能であり、アクセス ポイントは各フレームに Message Integrity Check Information Element（MIC IE）を追加するときに送信される管理フレームを保護します。 侵入者がフレームをコピー、変更、再送しようとすると MIC が無効になり、MFP フレームを検出するように設定されている受信側のアクセス ポイントが不一致を報告します。WLC 上に作成されるすべての WLAN では、デフォルトでこれらの機能がイネーブルになります。 これらの機能を無効にするには、WLC で [WLANs] メニューをクリックします。 WLC 上で設定されている WLAN のリストが表示されます。 クライアントを関連付ける WLAN をクリックします。 WLAN の [Advanced] タブで [Edit] ページへ進み、[Aironet IE] と [MFP] に対応するボックスのチェックマークを外します。
- **無線プリアンブル**：無線プリアンブル（ヘッダーと呼ばれることもある）は、パケットの先頭にあるデータの部分であり、ワイヤレス デバイスとクライアント デバイスがパケットの送受信を行うときに必要な情報を含んでいます。 ワイヤレス クライアントでどちらの設定がサポートされているかによって、無線プリアンブルを長いプリアンブルまたは短いプリアンブルに設定できます。
- **イーサネット カプセル化の変換**：ワイヤレス デバイスで 802.3 パケットではないデータ パケットを受信する場合、ワイヤレス デバイスはパケットを 802.3 にフォーマットするためにカプセル化の変換方式を使用する必要があります。 この変換方式には次の 2 種類があります。802.1H： Cisco Aironet 無線製品に最適なパフォーマンスを提供します。 802.1H がデフォルトの設定です。RFC1042： Cisco Aironet 以外の無線機器との相互運用性を確保するには、この設定を使用します。 RFC1042 では、802.1H ほどの相互運用性は保証されませんが、他のメーカーの無線機器で使用されています。
- **WPA ハンドシェイク タイムアウト**：一部のベンダーは、より長い WPA ハンドシェイク タイムアウトを必要とします。 **dot11 wpa handshake timeout** コマンドを使用して、WPA ハンドシェイク タイムアウトを変更できます。
- **SSID**：一部のベンダーでは、SSID をブロードキャストする必要があります。 SSID をブロードキャストするには、SSID の設定で *guest-mode* を有効にします。

IP アドレスの問題

ワイヤレス クライアントは、他のネットワークと通信するために有効な IP アドレスを必要とします。

コントローラは IP ヘルパー アドレスが設定されたルータのように動作します。 つまり、ゲートウェイ IP アドレスを入力し、クライアントがインストールされているダイナミック インターフェイス経由で DHCP サーバにユニキャストします。 デフォルトでは、スイッチの DHCP スヌー

ピングによって信頼できないポートにある、これらの DHCP パケットがブロックされることに注意してください。

DHCP オファーがコントローラに戻ると、DHCP サーバ IP アドレスが仮想 IP アドレスに変換されます。 これは、Windows が AP 間でローミングするときに、最初に DHCP サーバへの接続とアドレスの更新が試行されるために行われます。

DHCP サーバ アドレスが 1.1.1.1 (コントローラの一般的な仮想 IP アドレス) の場合、コントローラはそのパケットを代行受信し、Windows を装うことができます。 これは、仮想 IP アドレスがすべてのコントローラで同一である理由の 1 つです。 Windows ラップトップは、別のコントローラの AP にローミングするときにはコントローラの仮想インターフェイスへの接続を試行します。 モビリティ イベントとコンテキスト転送により、Windows クライアントのローミング先の新しいコントローラには Windows を再び装うための情報がすでにすべて準備されています。

内部 DHCP サーバを使用する場合に必要な操作は、サブネットに作成するダイナミック インターフェイスで DHCP サーバとして管理 IP アドレスを指定するだけです。 これによりそのインターフェイスが WLAN に割り当てられます。 コントローラに各サブネット内の IP アドレスが必要な理由として、このようにすることで、DHCP 要求に DHCP ゲートウェイ アドレスを指定できることがあります。

DHCP と IP アドレスに関する問題は、多数発生します。 これらの問題の原因と解決手順を次に示します。

1. 設定されている認証タイプが 802.1x または WPA などのレイヤ 2 セキュリティ ソリューションのいずれかである場合、有効な IP アドレスを取得するにはクライアントが正常に認証される必要があります。 最初に、クライアントが正常に認証されていることを確認します。**注:** 例外として、クライアントに Web 認証や Web パススルーなどのレイヤ 3 セキュリティ ソリューションが設定されている場合は、認証前にクライアントに IP アドレスが割り当てられます。
2. WLC で定義された各 WLAN は、一意のサブネットに属する VLAN で設定されている WLC のダイナミック インターフェイスにマッピングされています。 この WLAN に関連付けるクライアントには、VLAN のインターフェイス サブネットからの IP アドレスが割り当てられます。 この WLAN の IP サブネットとゲートウェイが、このサブネットの IP アドレスを取得するようにクライアントの DHCP サーバで定義されているかどうかを確認します。 DHCP サーバを設定するには、適切なベンダーのマニュアルを参照してください。**注:** 前提条件として、DHCP サーバが WLC から到達可能であるかどうか、および DHCP サービスがオンになっているかどうかを確認します。
3. DHCP サーバの IP アドレスが WLAN にマッピングされている WLC のインターフェイスで正しく定義されていることを確認します。 これを確認するには、GUI で [Controller] メニューをクリックします。 左側にある [Interfaces] メニューをクリックし、[DHCP server] フィールドを確認します。 同じページで、インターフェイスがアップ状態でアクティブな *物理ポート*にマッピングされていることを確認します。 DHCP に関する問題をトラブルシューティングするには、WLC で **debug dhcp packet enable** と **debug dhcp message enable** コマンドを使用します。**注:** また、WLC を DHCP サーバとして設定することもできます。 WLC での DHCP サーバの設定方法については、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.0』ドキュメントの「GUI を使用した DHCP の設定」セクションを参照してください。
4. WLC では、DHCP プロキシはデフォルトで有効になっています。 WLC は WLAN のインターフェイスに設定された DHCP サーバまたは WLAN 自体へパケットをユニキャストします。 DHCP サーバで Cisco DHCP プロキシの動作がサポートされていない場合は、WLC で

DHCP プロキシを無効にします。 WLC で DHCP プロキシを無効にする方法の詳細については、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.2』の「DHCP プロキシの設定」セクションを参照してください。

5. WLC は通常、スイッチを介して有線ネットワークに接続しています。 WLC と DHCP サーバに接続されているスイッチ ポートがトランクとして設定されているかどうか、これらのポートで適切な VLAN が許可されていることを確認します。 Cisco スイッチを設定する方法の詳細については、『WLC を使用したゲスト WLAN と内部 WLAN の設定例』ドキュメントの「WLC にトランク ポートとして接続するレイヤ 2 スイッチ ポートの設定」セクションを参照してください。
6. WLAN に対して [DHCP Addr. Assignment] フィールドが有効になっている場合、スタティック クライアントは WLAN への関連付けを許可されません。 このオプションによって、この WLAN に関連付けられるすべてのクライアントは DHCP を通じて IP アドレスを取得することが必要になります。 このオプションが有効になっているかどうかを確認するには、WLC の GUI で [WLANs] メニューをクリックします。 WLC 上で設定されている WLAN のリストが表示されます。 該当する WLAN をクリックします。 [Advanced] タブに移動し、[DHCP Address Assignment] フィールドを見つけます。
7. Cisco PIX ファイアウォールなどの一部の DHCP サーバは、DHCP リレー サービスをサポートしていません。 これらのサーバは DHCP リレー エージェントからのユニキャスト パケットではなく、ブロードキャスト DHCP パケットのみを受け入れるため、DHCP クライアントがサーバがイネーブルになっているインターフェイスに直接接続されていることを確認します。**注:** DHCP リレーのサポートについては、適切なベンダーのドキュメントを確認してください。

クライアントの問題

クライアント側が適切に配置されていることも同様に重要です。 クライアント側で次を確認します。

1. 場合によっては、クライアント カードがコンピュータによって認識されません。 この場合は、別のスロットでカードを試してください。 動作しない場合は、別のコンピュータで試します。 インストレーション内の問題の詳細については、『Cisco Aironet 340、350、および CB20A ワイヤレス LAN クライアント アダプタ インストレーション コンフィギュレーション ガイド Windows 版』の「トラブルシューティング」セクションを参照してください。**注:** ワイヤレス カードがマシンにインストールされているオペレーティング システムと互換性があることを確認します。 これは、クライアント カードのデータ シートから確認できます。
2. クライアントがマシンに正しくインストールされているかどうかを確認します。 クライアント カードの状態は [Windows Device Manager] 画面から確認できます。 「*This device is working properly*」と表示されるメッセージを探します。 それ以外のメッセージは、ドライバが正しくインストールされていないことを示します。 ドライバをアンインストールして、マシンにドライバを再インストールします。 ドライバをアンインストールするには、[Device Manager] 画面でワイヤレス アダプタを右クリックし、[Uninstall] をクリックします。 クライアント アダプタを再インストール方法の詳細については、『Cisco Aironet 340、350、および CB20A ワイヤレス LAN クライアント アダプタ インストレーション コンフィギュレーション ガイド Windows 版』ドキュメントの「クライアント アダプタのインストール」セクションを参照してください。**注:** クライアント カードを設定するために ACU を使用する場合は、ACU で無線が無効になっていないことを確認します。 また、Windows のコ

ントロール パネルの [Network Connection] の下でカードの状態が有効になっているかどうかを確認します。**注:** ワイヤレス カードには 1 つのサプリカント ソフトウェアのみを使用します。 必ずベンダーが提供するサプリカントをカードに使用することが推奨されます。 第二のオプションとして、PC ベンダーの提供するサプリカントや Windows の提供する WZC のいずれかを使用することもできます。**注:** WZC をデバッグするには、次の手順を実行します。**netsh ras set tracing * enabled** コマンドを使用し、WZC のデバッグをオンにします。**netsh ras set tracing * disabled** コマンドを使用し、WZC のデバッグをオフにします。ログは *C:\Windows\tracing* に書き込まれます。 *eapol.log*、*rastls.log*、および *wzctrace.log* が最も重要なログです。**注:** 詳細については、Wireless Diagnostics and Troubleshooting を参照してください。

3. クライアントの設定は、WLC の設定と一致する必要があります。 これは、主にクライアントの SSID とセキュリティ設定に適用されます クライアントの設定に Cisco ユーティリティを使用する場合は、『Cisco Aironet 340、350、および CB20A ワイヤレス LAN クライアント アダプタ インストレーション コンフィギュレーション ガイド Windows 版』ドキュメントの「プロファイル マネージャの使用」セクションを参照してください。
4. ワイヤレスが正しく関連付けられていてもデータを転送できない場合は、VPN のアダプタや有線アダプタに加えて他のすべてのアダプタを無効にします。 マシンに複数のワイヤレス アダプタがある場合は、競合を避けるために他のアダプタを無効にします。
5. 1 台のクライアントのみで接続の問題が発生する場合は、その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。 ほとんどのクライアントで接続の問題が発生し、他に問題がない場合は、WLC のアップグレードを選択します。
6. セキュリティと操作に関連する相互運用性の問題を避けるため、デバイス、つまり、クライアントと WLC が Wi-Fi 認定されていることを確認します。
7. Windows マシンを使用する場合は、Microsoft からの最新のセキュリティ更新プログラムと修正プログラムがすべてインストール済みであることを確認します。 Windows のクライアント ユーティリティを使用する場合は、Microsoft からの最新の修正プログラムがインストール済みであることを確認します。
8. 一部のクライアントでは、EAP 認証に時間がかかります。 この結果、WLC のタイムアウトが発生し、WLC で次のエラー メッセージが受信されます。

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

このメッセージに応じて、クライアントの認証に十分な時間を確保するために WLC で EAP タイムアウト値を増やします。 WLC で EAP タイマーを調整するには、次のコマンドを使用します。

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>

Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>

Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

RF の問題

RF 干渉は脆弱な接続の主な理由の 1 つです。 同じ周波数で動作する電子レンジやコードレス電話など、近くにある 802.11 のネットワークまたはその他のソースが原因で干渉が起きる可能性があります。 近くにある 802.11 ネットワークによる干渉には、次の 2 種類があります。

- **同一チャネル干渉**： カバレッジ エリアが重複するアクセス ポイントがオーバーラップする周波数の同じチャネルまたは複数のチャネルで設定されている場合、重複するカバレッジ エリア内のクライアント接続の問題が生じる原因となります。 この問題を回避するには、オーバーラップしないチャネルにチャネル番号を変更するか、アクセス ポイントを遠くに離してカバレッジ エリアが重複しないようにします。 たとえば、802.11b/g の場合、ネットワーク チャネル 1、6、および 11 がオーバーラップしないチャネルです。
- **隣接チャネル干渉**： 複数のアクセス ポイントが互いに近すぎる位置に設置されたり、高出力の電力レベルを使用したりすると、アクセス ポイントがオーバーラップしないチャネルで設定されている場合でも、干渉が発生します。 この問題を修正するには、アクセス ポイントの電力を下げます。**注:** オーバーラップしないチャネルは、隣接チャネルとも呼ばれます。これは、*隣接チャネル干渉*という名前を説明します。

スペクトル アナライザを使用し、2.4 GHz の範囲で動作する電子レンジやコードレス電話などの干渉源、または 5 GHz の範囲で動作するデバイスを探します。 特定された干渉源を排除します。 また、干渉を回避するためにワイヤレス ネットワークが動作する標準を、802.11b/g から 802.11a などに変更できます。

効果的な RF 通信のもう一つの重要な点は、信号強度です。 弱い信号強度は、接続が断続する原因となります。 壁、金属などの障害物は、RF エネルギーを吸収して反射し、信号強度を減らします。 十分なカバレッジを提供するには、アクセス ポイントの電力を必要なレベルに増やします。 また、範囲と信号強度を拡大するために高ゲイン アンテナを使用できますが、デバイスで動作するために FCC 認定されたアンテナであることを確認します。

注: 信号強度と RF ノイズ（ワイヤレス ネットワークと同じ周波数で動作するその他のソースからの RF 信号またはエネルギー）の差異である信号対雑音比（SNR）は、リンクの品質を評価するための重要な要素です。 高い SNR は、より速いデータ転送をもたらす優れたリンク品質を示します。 小さい値は、断続的な接続またはパフォーマンス低下の原因となる低品質を示します。 ワイヤレス パケット アナライザやサイト調査ソフトウェアは、特定の場所の SNR とスループットを表示できます。

シスコの統合環境では、WLC に実装されている無線の Radio Resource Management（RRM）と呼ばれる概念があります。 RRM はコントローラに組み込まれたソフトウェアで、ワイヤレス ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。 このソフトウェアは、上述の RF に関する問題をすべて解決します。 RRM の詳細については、『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.0』ドキュメントの「Radio Resource Management の設定」セクションを参照してください。

エラー メッセージ

クライアント接続の過程で、WLC とクライアント側の両方の複数のエラー メッセージを受信する場合があります。

- **クライアントが IP アドレスを取得できないか、DHCP から IP アドレスを取得する際に遅延が発生しています。 コントローラの debug dhcp には、次が表示されます。**

  ```
  Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK
  ```

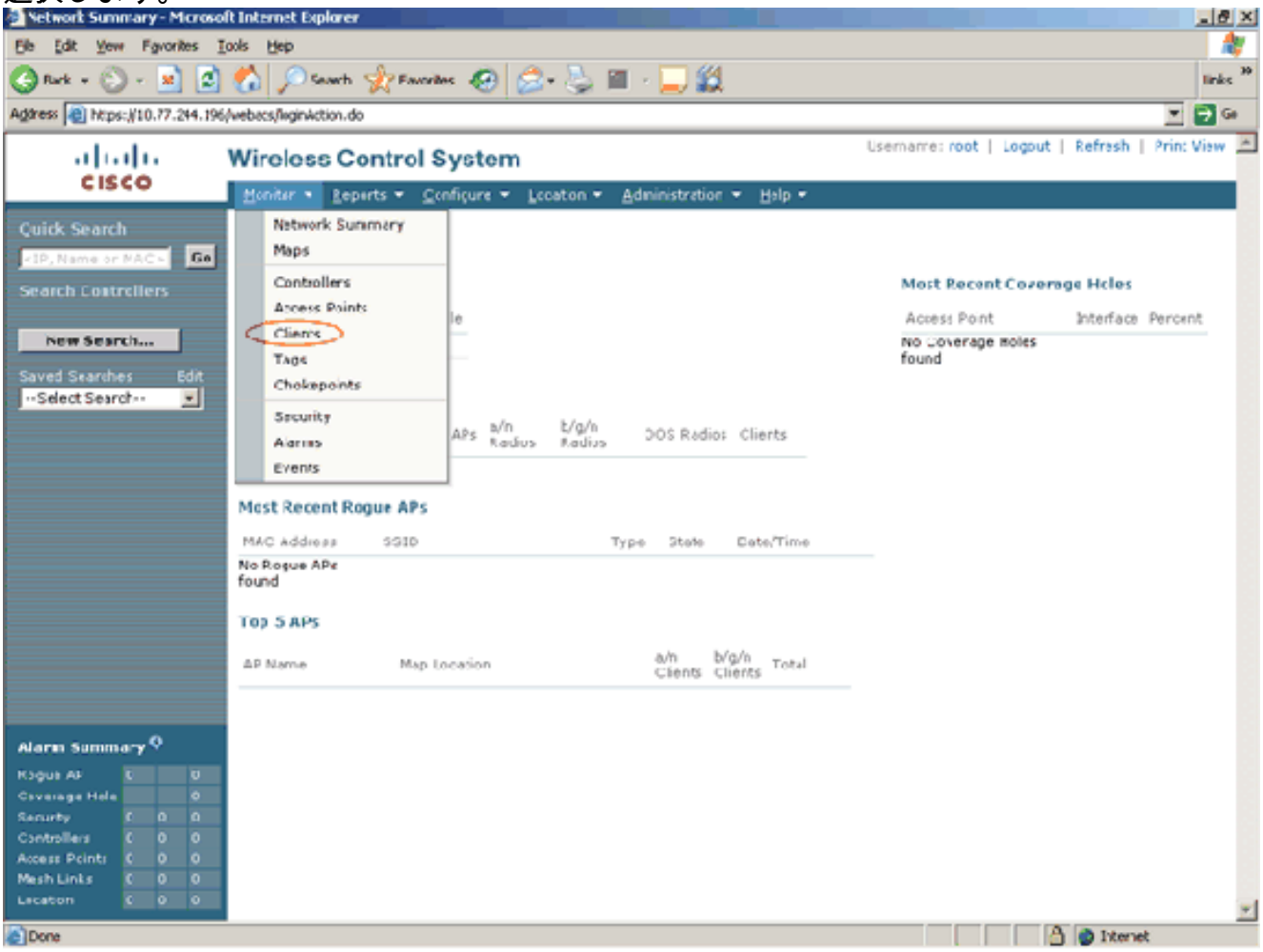
  DHCP NAK は通常、クライアントが属していないサブネットから IP アドレスを取得しようとするクライアントの試みを示すために DHCP サーバから送信されます。 この問題は、同じ WLAN に異なる VLAN が割り当てられた 1 つの WLC から別の WLC にクライアントがローミングされると発生します。これに問題を修正するには、WLC で DHCP プロキシを設定し

ます。

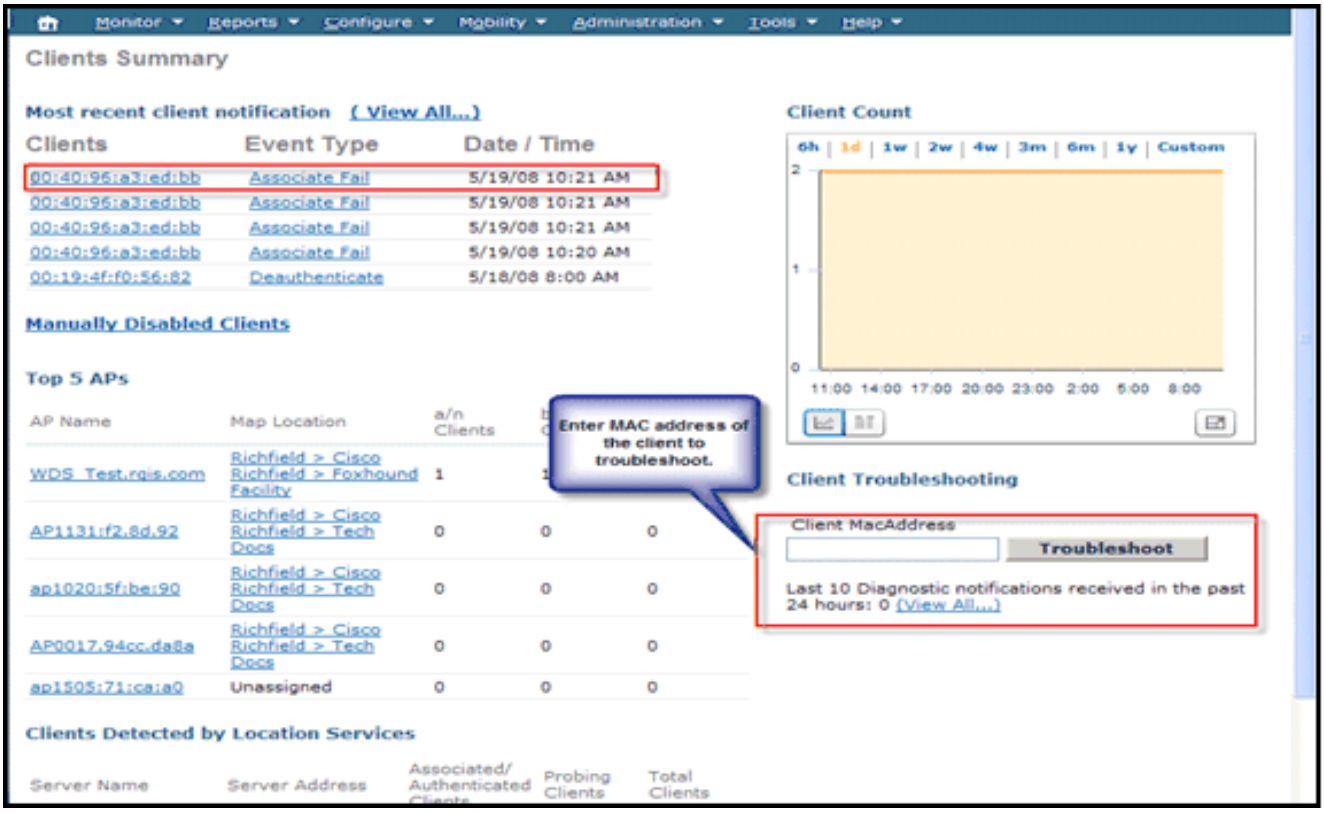
WCS で発生するクライアントに関する問題のトラブルシューティング

WCS は、ワイヤレス環境のクライアント関連の問題を修復するために使用できます。 これは、WCS に組み込まれているトラブルシューティング ツールを使用することによって行われます。 WCS を介してクライアントを修復するには、次の手順を実行する必要があります

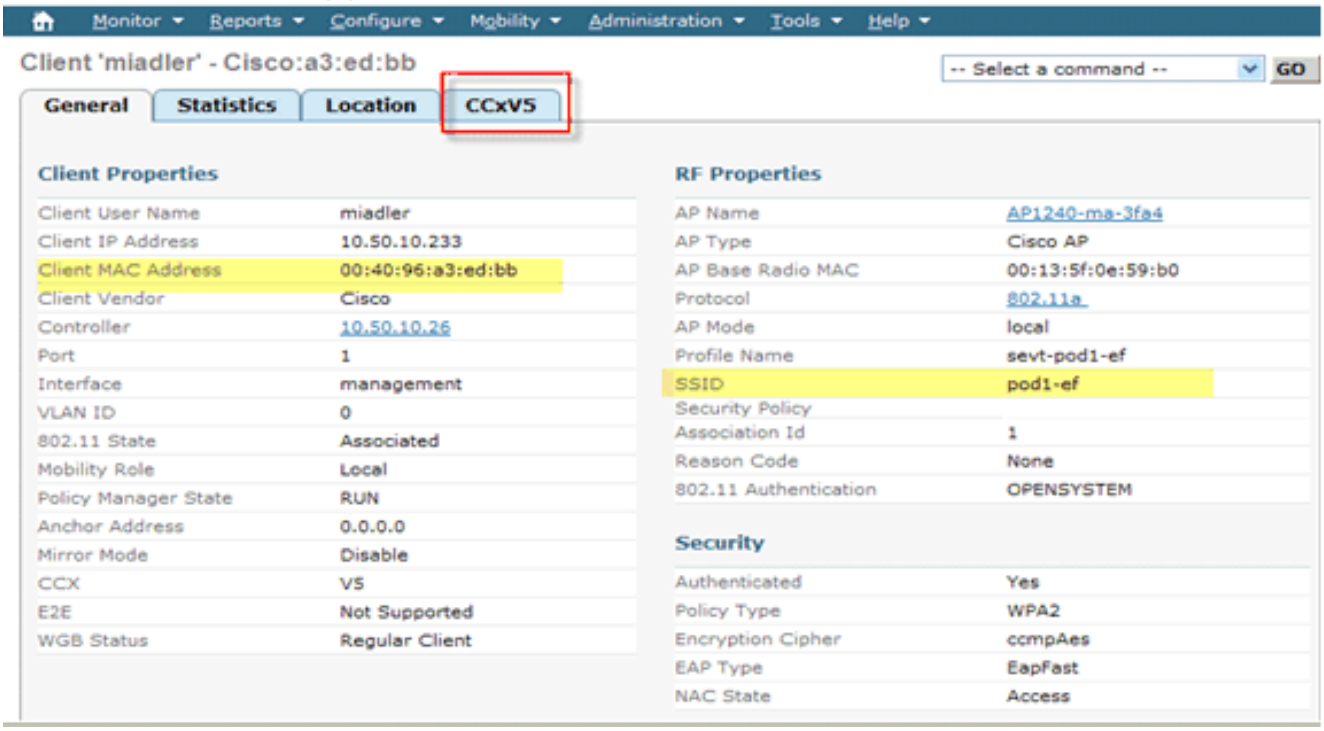
1. WCS の [Dashboard] ページから、[Monitor] メニューをクリックし、リストから [Clients] を選択します。



2. これにより、図 1 に示すように、ワイヤレス ネットワーク上のクライアントのリストを表示する [Client Summary] ページが開きます。**図 1**



3. 特定のクライアントの SSID や認証方式のような詳細情報を表示するには、クライアントをクリックします。 図 2 に、例を示します。 図 1 に示す [Client Summary] ページの右側の下部にある [Troubleshoot] ダイアログボックスでは、トラブルシューティングするデバイスの MAC アドレスを入力できます。 図 3 に示すように、[Troubleshooting Tool] のページが開きます。トラブルシューティングするクライアントの識別と選択によって、[Client Details] ページが表示されます。**図 2**



WEP に関するトラブルシューティング

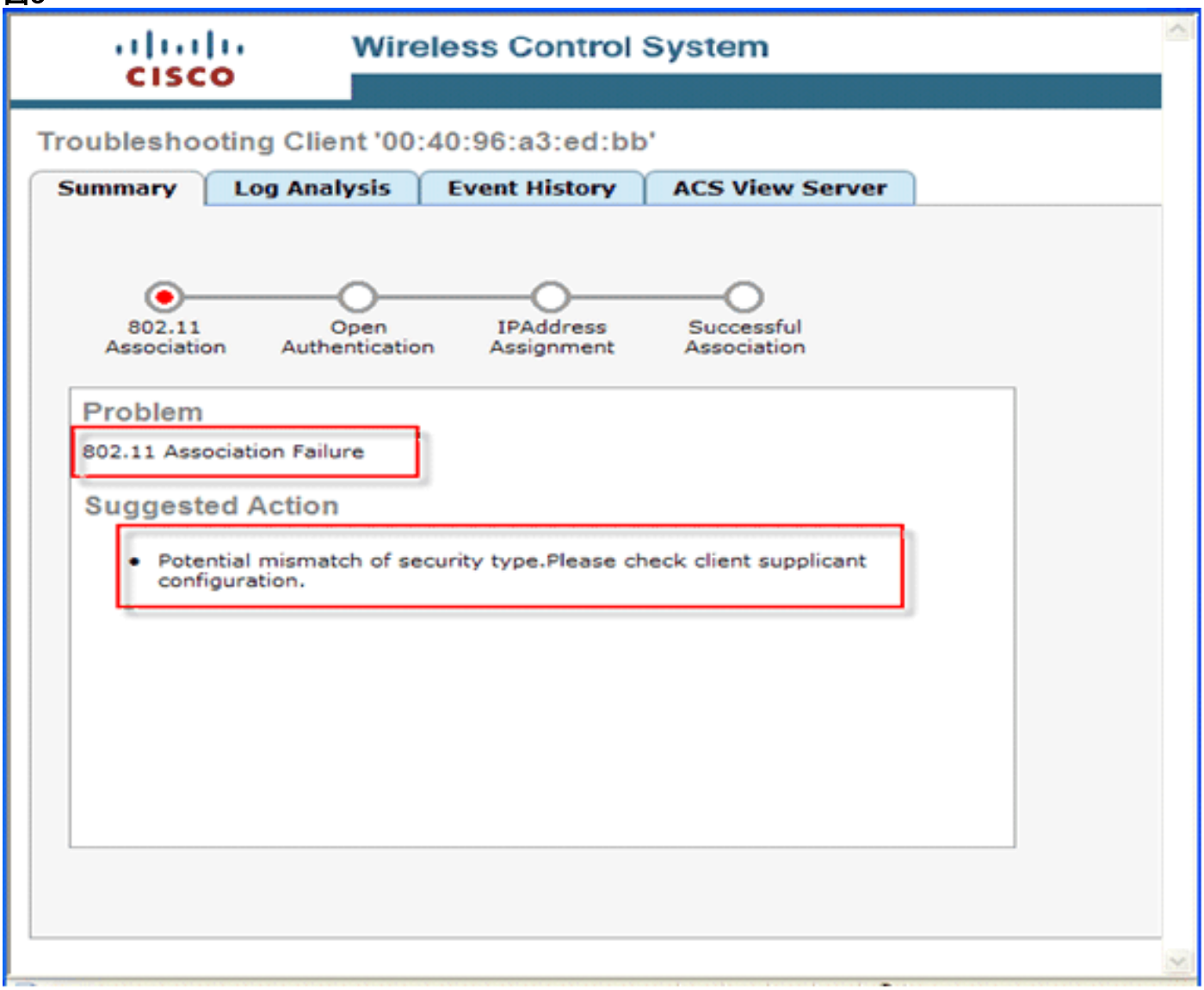
WEP セキュリティ メカニズムを使用するレガシー ワイヤレス クライアントは、多くの場合トラブルシューティングが困難です。 クライアントと AP で次を確認します。

- WEP キーの長さ（およびキーの不一致）
- WEP キー インデックス（およびキーの不一致）
- 設定された認証方式（公開キーと共有キー）

認証の不一致

パケットのキャプチャは手間のかかるプロセスではありますが、WCS クライアントのトラブルシューティング ツールは問題がどこにあるのかを簡単に示すのに役立ちます。 多くの場合、この小さな「ヒント」はトラブルシューティングにかかる時間を短縮します。 図 2 は、[WCS troubleshooting tool] を示します。 図に示すように、問題のあるステージが特定されて表示されるため、そのステージが詳細な分析のために設定されます。

図3



WEP キー インデックスの不一致

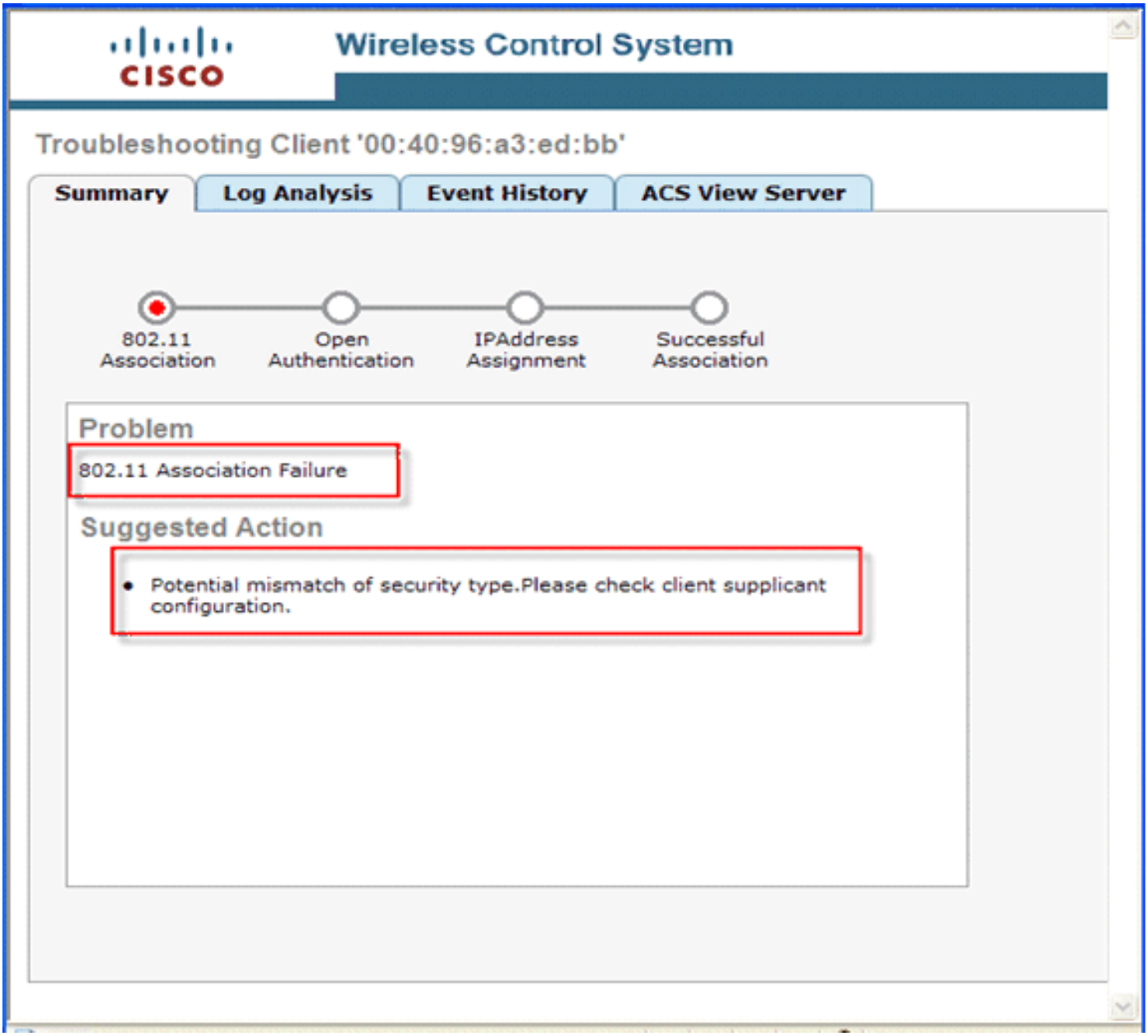
通常、クライアントと AP では最大 4 個の WEP キーを設定できます。 いずれかのキーが演奏キーとして選択されます。 このキーは、クライアントと AP の間で一致する必要があります。 たとえば、クライアントでキー 2 が転送キーとして選択された場合、これは AP のキー 2 と一致する必要があります。ただし、AP では転送キーとは異なるキーがある場合があります。 よくある別の問題は、次の問題です。 クライアントおよびインフラストラクチャのベンダーの仕様の解釈が異なるため、製品での実装が異なる原因となります。 1 つの一般的な例は、0 ~ 3 のキー インデ

ックスと 1 ~ 4 のキー インデックスの使用です。 この結果、設定の不一致と接続試行に失敗する可能性があります。 その時点で、問題の根本原因であるかどうかを示すパケットのデコードにファイルされる [Key ID] フィールドを注意深く確認してください。

WPA-PSK に関するトラブルシューティング

WPA-PSK のトラブルシューティングは、多くの点で WEP に似ています。 ほとんどの試行の失敗は、キーの設定ミスが原因です。 WCS クライアントのトラブルシューティング ツールを使用すると、管理者は WPA のトランザクションの口グを収集できます。 次でハイライトされているように、口グは潜在的な問題のある場所 (*この例では、クライアントの不適切な事前共有キーの設定*) を示します。口グは、WCS クライアントのトラブルシューティング ツールの [Log Analysis] タブから取得されます。 WPA-PSK をレイヤ 2 セキュリティ ポリシーとする WLAN を設定し、誤った PSK を使用してクライアント サプリカントを設定します。 以下は、PSK キーが間違って設定されたイベントの口グです。

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Client 802.1x authentication failure exceeded the limit.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key has possible incorrect psk configuration.
```

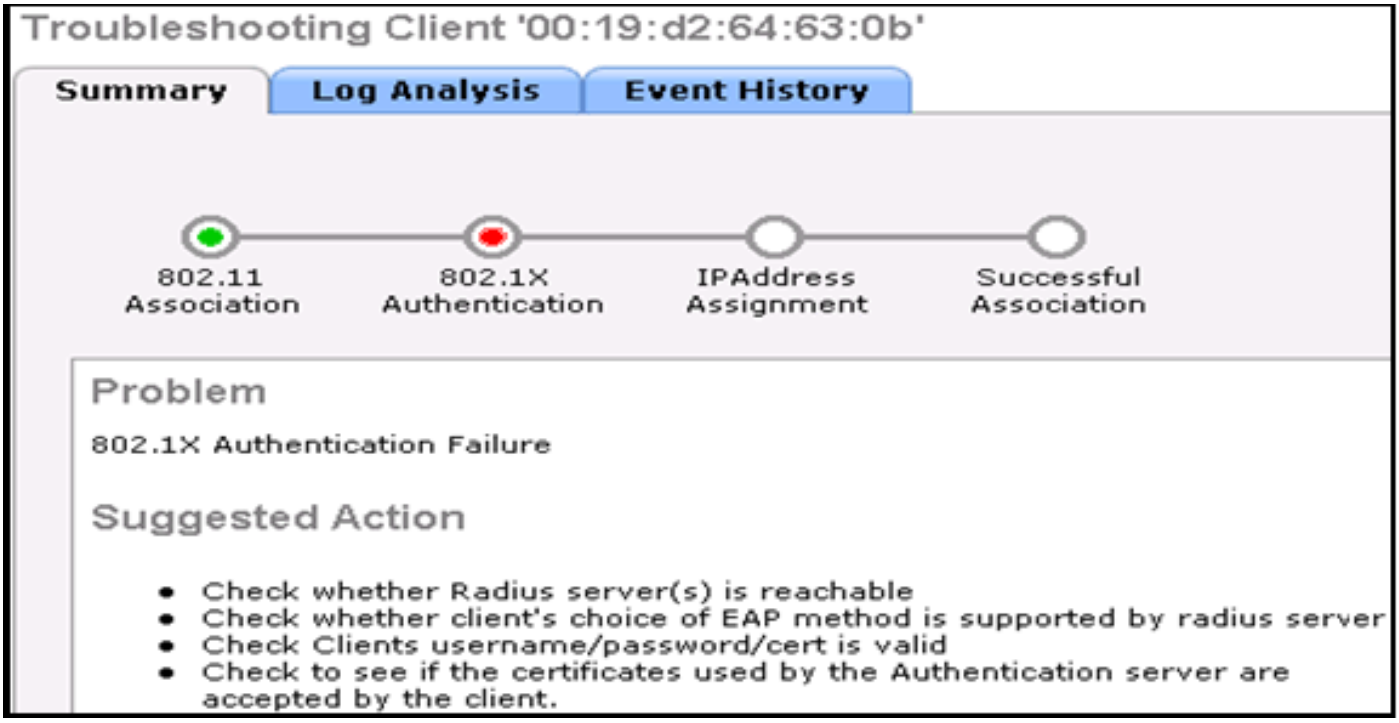


802.1X に関するトラブルシューティング

WLAN の普及に伴い、レガシー クライアントは段階的に廃止されます。 今後の展開では、802.1x が優勢な方向性です。 一連のチェーン (クライアント <> AP <> WLC <> L2/L3 ネットワーク <> AAA サーバ) には、さまざまな設定ミス関連の問題がある可能性があります。 ここでは、WLC と AAA サーバの間が適切に配置されていると仮定します。 サプリカント (クライアント) と AAA サーバの間で発生する問題は、概して次のような問題です。

- 正しくない EAP の種類
- 正しくないクレデンシャルや期限切れの証明書
- 正しくない内部 EAP 方式

クライアント側のセキュリティ設定でユーザのクレデンシャルを変更します。 たとえば、正しくないパスワードを入力し、同じテストを実行します。 トラブルシューティング ツールは問題のある箇所を正確に指摘し、推奨される対応を示します。



上の図に示す [Log Analysis] タブをクリックし、ログに失敗した 802.1x 認証の兆候がないかどうかを確認します。

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2
   Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2
   Received eap failurefrom the client.
```

Web-Auth に関するトラブルシューティング

一般に、推奨されるトラブルシューティング手法では、問題のあるクライアントの「ポリシー マネージャの状態」の検査を含める必要があります。 下の WCS のスクリーン ショットで確認できるように、問題のクライアントは *WEBAUTH_REQD* の状態にとどまっています。 これは、802.11 プロセスがエラーなしで完了し、次の問題が発生する可能性があることを意味します。

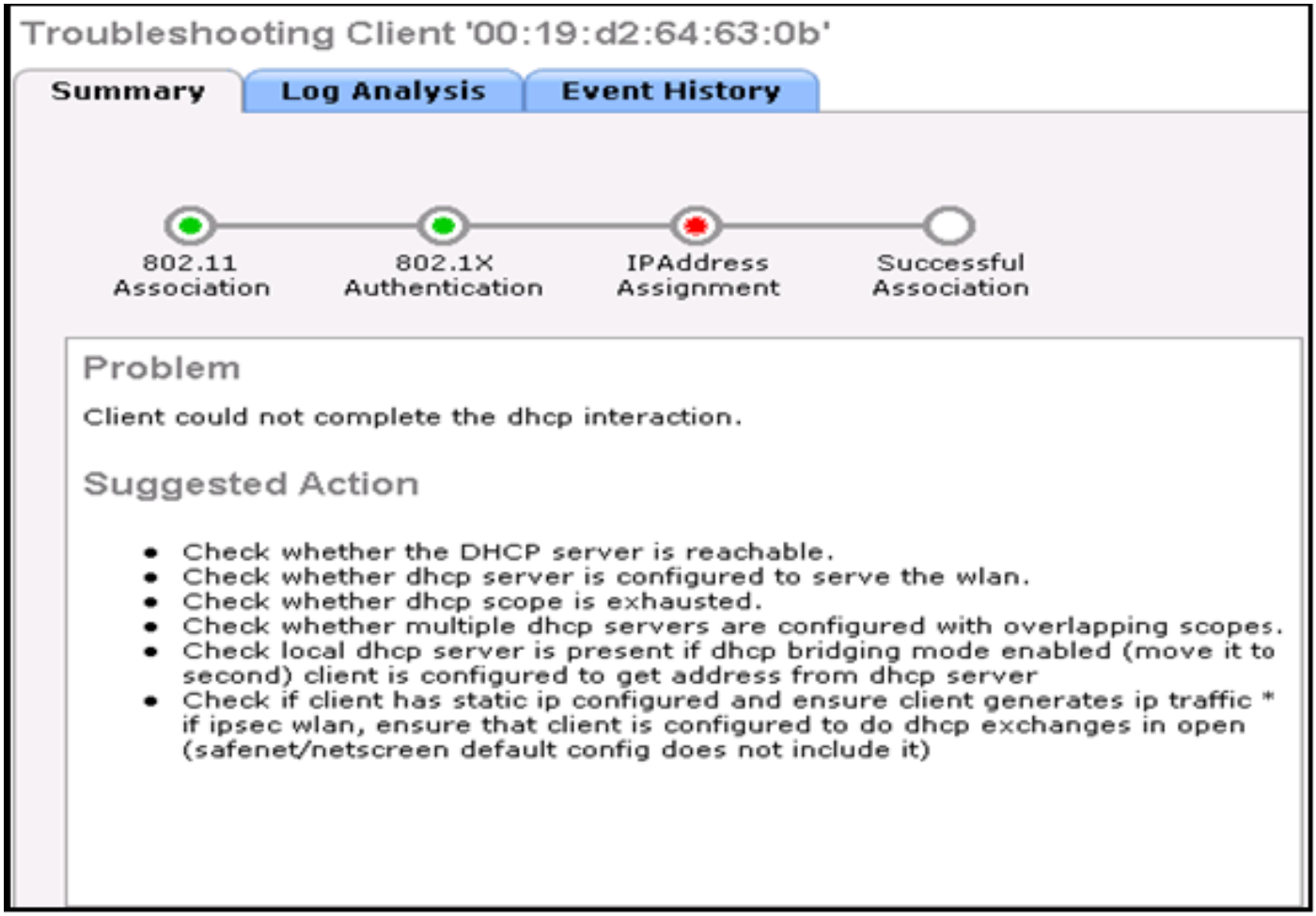
- 正しくないユーザ名とパスワード
- 正しくない ACL の実装（存在する場合は、外部の Web-Auth サーバに接続する）
- DNS が正しく設定されていない等**注:** Web 認証に関するトラブルシューティングの詳細については、『コントローラの Web 認証の設定例』ドキュメントを参照してください。

WCS から収集されたログには、Web-Auth プロセスが失敗したことが表示されます。 このような状況は、WLAN レイヤ 3 ポリシーを Web-Auth に設定し、Web-Auth プロセスを完了しないか、不正確または存在しないログイン クレデンシャルを入力することによってラボでシミュレートできます。 クライアントのトラブルシューティング ツールの概要セクションを確認し、問題が発生した場所を調べます。 WCS に次のログが表示されます。

```
 <TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
```

DHCP および IP アドレスのトラブルシューティング

多くの場合、クライアント デバイスは複数の無線ネットワークで使用されます。 一例として、ホームまたはパブリック ネットワークにある企業デバイスの従業員による使用が挙げられます。 ある従業員にホーム ネットワークの固定 IP アドレスが割り当てられているとします。 その従業員は、知らずに以前に割り当てられた固定 IP アドレスを使用して企業ネットワークに接続します。 これは、WCS クライアントのトラブルシューティング スイートを使用して簡単に指摘できる接続の問題の原因になります。 この分野での問題のほとんどはワイヤレス クライアントにありますが、枯渇したスコープや間違ったスコープなど、有線インフラストラクチャの潜在的な問題が指摘される場合があります。クライアントで正しくない固定 IP アドレスを割り当てた場合や、スイッチで DHCP スコープのパラメータを変更する場合、このシナリオの作成を試みてください。



関連情報

- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.1
- Unified Wireless Network における Radio Resource Management (RRM)
- テクニカル サポートとドキュメント – Cisco Systems