Unified Wireless Network における不正検出

内容

概要

ワイヤレス ネットワークにより、有線ネットワークが拡大され、作業員の生産性と情報へのアクセスが向上します。ただし、認証されていないワイヤレス ネットワークを追加すると、セキュリティの懸念が高まります。有線ネットワークのポート セキュリティについて十分な検討をせずに、安易にワイヤレス ネットワークによって有線ネットワークを拡大させるかもしれません。そのため、適切に保護されているワイヤレス/有線インフラストラクチャに従業員各自の Cisco アクセス ポイント（AP）を持ち込んだ場合、本来はセキュアなネットワークで不正なユーザのセキュア ネットワークへのアクセスを許してしまい、容易に侵害されてしまう結果になるかもしれません。

ネットワーク管理者は不正検出を行うことで、このセキュリティの問題を監視して、解消することができます。Cisco Unified Network アーキテクチャには、不正の特定と抑止を高度に実行するソリューションを提供する 2 とおりの不正検出方法が用意されています。高価で有効性を検証しにくい追加のネットワークとツールは必要ありません。

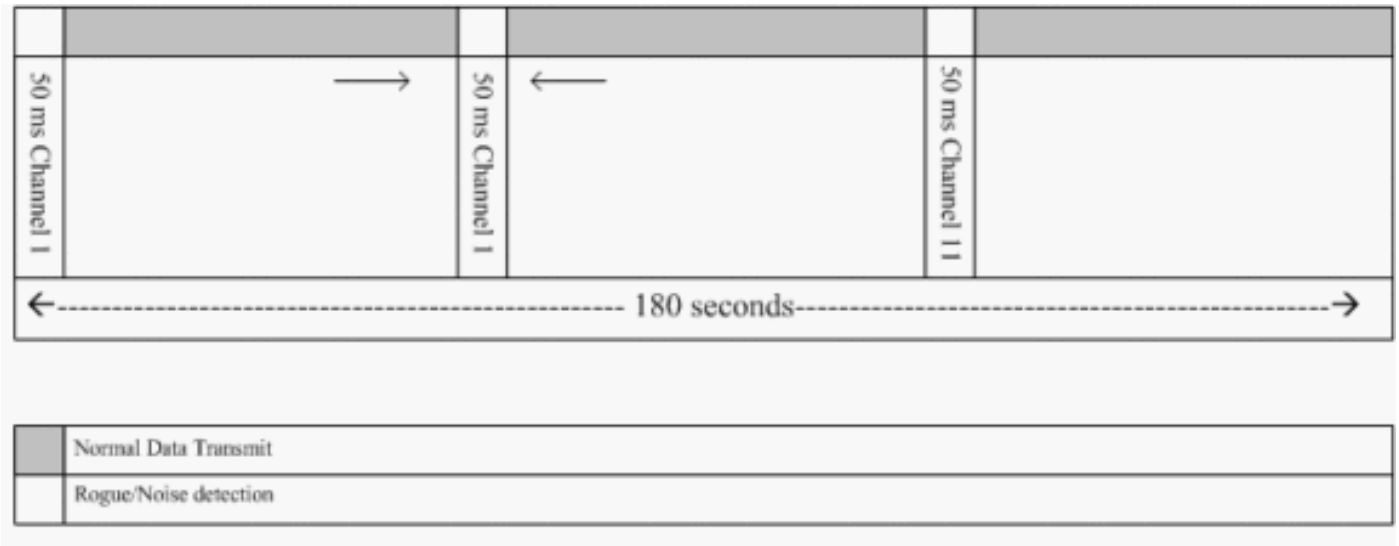
機能の概要

不正検出を義務付ける規制や、不正検出実施に関して遵守する必要がある法律はありません。ただし不正の抑止には法的な課題が伴い、自動実施する場合にはインフラストラクチャ プロバイダーが困難な立場に立たされることがあります。シスコはこのような問題に慎重に対応し、これらのソリューションを提供します。各コントローラには RF グループ名が設定されています。Lightweight AP がコントローラに登録されると、コントローラで設定されている RF グループ固有の**認証情報要素（IE）**がすべてのビーコン/プローブ応答フレームに埋め込まれます。Lightweight AP は、AP から受信したビーコン/プローブ応答フレームにこの **IE** がないかまたは**正しくない IE** が含まれている場合、その AP を不正 AP として報告し、その BSSID を不正テーブルに記録し、不正テーブルをコントローラに送信します。Rogue Location Discovery Protocol（RLDP）とパッシブ オペレーションという 2 つの手法があります。詳細については、「アクティブな不正の判別」で説明します。

インフラストラクチャにおける不正検出

アクティブなワイヤレス環境での不正検出にはコストがかかることがあります。このプロセスでは動作している（またはローカル モードの）AP に対してサービスを停止し、ノイズを監視し、不正検出を実行するように指示します。スキャン対象チャネルと、すべてのステーションをスキャンする期間をネットワーク管理者が設定します。AP は 50 ミリ秒間にわたって不正クライアント ビーコンを監視した後、クライアントに対して再びサービスを提供するために設定されているチャネルに戻ります。このアクティブなスキャンとネイバー メッセージにより、不正な AP とネットワークに接続している有効な AP が特定されます。スキャンされるチャネルとスキャン期間を設定するには、[Wireless] > [802.11b/g Network]（ネットワーク要件に基づいて「**b/g**」または「**a**」）を参照し、ブラウザ ウィンドウの右上隅にある [Auto RF] ボタンを選択します。

[Noise/Interference/Rogue Monitoring Channels] までスクロールし、不正とノイズを検出するためにスキャンするチャネルを設定します。選択可能な項目は[All Channels]（1 ~ 14）、[Country Channels]（1 ~ 11）、[Dynamic Channel Association (DCA) Channels]（デフォルトでは 1、6、11）です。 このようなチャネルのスキャン期間とノイズ測定間隔を、同じウィンドウの [Monitor Intervals (60 to 3600 secs)] で設定できます。デフォルトでは、オフチャネル ノイズと不正の監視間隔は 180 秒です。つまり各チャネルが 180 秒おきにスキャンされます。180 秒ごとにスキャンされる DCA チャネルの例を次に示します。



この図に示すように、スキャン対象として多数のチャネルが設定されており、スキャン間隔が短いため、AP が実際にデータ クライアントにサービスを提供できる期間が短くなります。

Lightweight AP はクライアントと AP が不正であると判断するためにしばらく待機します。これは、別のサイクルが完了するまでこのような不正が別の AP から報告されないためです。不正な AP とクライアント、ノイズ、干渉をモニタするため、同じ AP が同じチャネルに再び移動します。同じクライアントと AP が検出されると、これらのクライアントと AP はコントローラで不正として再びリストされます。コントローラはこれらの不正な AP やクライアントがローカル ネットワークに接続しているか、または単にネイバー AP に接続しているかの確認を開始します。いずれの場合でも、管理対象ローカル ワイヤレス ネットワーク外部の AP は不正として見なされます。

不正の詳細

Lightweight AP は、不正クライアント、ノイズ、チャネル干渉をモニタするために、50 ミリ秒間オフチャネルになります。検出された不正クライアントや不正 AP はコントローラに送信され、次の情報が収集されます。

- 不正 AP の MAC アドレス
- 不正 AP の名前
- 不正な接続クライアントの MAC アドレス
- WPA または WEP でフレームが保護されているかどうか
- プリアンブル
- 信号対雑音比（SNR）
- Receiver Signal Strength Indicator（RSSI）

Rogue Detector アクセス ポイント

AP を Rogue Detector として使用できます。この場合、この AP がすべての有線側接続 VLAN を監視できるように、この AP をトランク ポートに配置できます。次にすべての VLAN の有線サブネット上でクライアントが検索されます。Rogue Detector AP はコントローラから送信される確認済み不正クライアントまたは不正 AP のレイヤ 2 アドレスを確認するため、Address Resolution Protocol（ARP）パケットを監視します。一致するレイヤ 2 アドレスが検出されると、コントローラはこの不正 AP または不正クライアントを脅威として識別するアラームを生成します。このアラームは、有線ネットワーク上で不正が検出されたことを示します。

アクティブな不正の判別

不正 AP がコントローラによって不正として追加されるには、この不正 AP が 2 回「検出」される必要があります。不正 AP が企業ネットワークの有線セグメントに接続していない場合、これは脅威として見なされません。不正がアクティブであるかどうかを判別するため、さまざまな手法が使用されます。このような手法の 1 つとして RLDP があります。

Rogue Location Discovery Protocol（RLDP）

RLDP は、不正 AP で認証（オープン認証）が設定されていない場合に使用されるアクティブな手法です。このモードはアクティブな AP に対し不正チャネルに移動してクライアントとして不正に接続するように指示します（デフォルトではこのモードは無効になっています）。このとき、アクティブな AP はすべての接続クライアントに認証解除メッセージを送信して無線インターフェイスをシャットダウンします。次に、不正 AP にクライアントとして関連付けられます。

AP は不正 AP からの IP アドレスの取得を試行し、ローカル AP と不正接続の情報が含まれている User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP 経由でコントローラに転送します。コントローラがこのパケットを受け取ると、RLDP 機能により有線ネットワークで不正 AP が検出されたことをネットワーク管理者に対して通知するためのアラームが設定されます。

注：debug dot11 rldp enableコマンドを使用して、Lightweight APが不正APとDHCPアドレスを関連付けて受信しているかどうかを確認します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

Lightweight AP から送信される UDP（宛先ポート 6352）の例を以下に示します。

```
0020 0a 01 01 0d 0a 01 ......(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
.....x........ 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

データの先頭 5 バイトには、不正 AP からローカル モード AP に渡された DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレス、その後の 6 バイトは不正 AP の MAC アドレスを示します。その後に 18 バイトの 0 が続きます。

パッシブ オペレーション：

これは、不正 AP に何らかの認証（WEP または WPA）が設定されている場合に使用される手法です。不正 AP で何らかの認証が設定されている場合、Lightweight AP を関連付けることはできません。これは、Lightweight AP は不正 AP で設定されているキーを認識していないためです。このプロセスではまずコントローラが、Rogue Detector として設定されている AP に、不正クライアント MAC アドレスのリストを渡します。Rogue Detector は設定されているすべての接続サブネットをスキャンし、ARP 要求を確認します。次に ARP が一致するレイヤ 2 アドレスを検索します。一致するアドレスが検出されると、コントローラからネットワーク管理者に対し、有線サブネットで不正が検出されたことが通知されます。

アクティブな不正の抑止

有線ネットワーク上で不正クライアントが検出されたら、ネットワーク管理者は不正 AP と不正クライアントの両方を抑止できます。これは、不正 AP に関連付けられているクライアントに 802.11 認証解除パケットが送信され、このようなセキュリティ ホールにより生じる脅威が緩和されることで実現します。不正 AP の抑止が試行されるたびに、Lightweight AP のリソースの約 15 %が使用されます。したがって不正 AP が抑止されたら、その不正 AP を物理的に検出して除外することを推奨します。

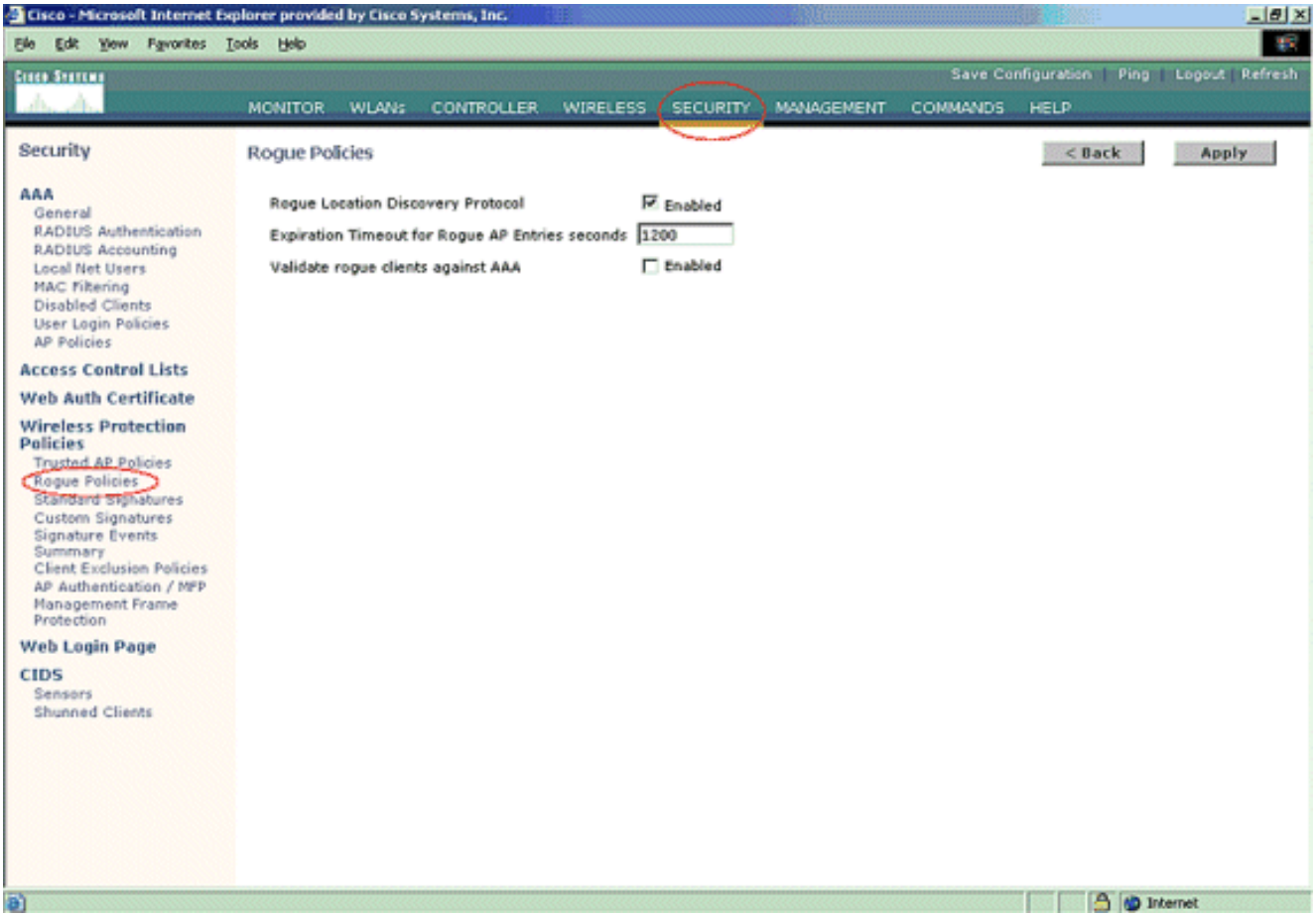
注： WLC リリース 5.2.157.0 以降では、不正の検出後に検出された不正を手動または自動のいずれで抑止するかを選択できます。5.2.157.0 より古いコントロール ソフトウェア リリースでは手動抑止のみ可能です。

不正検出：設定手順

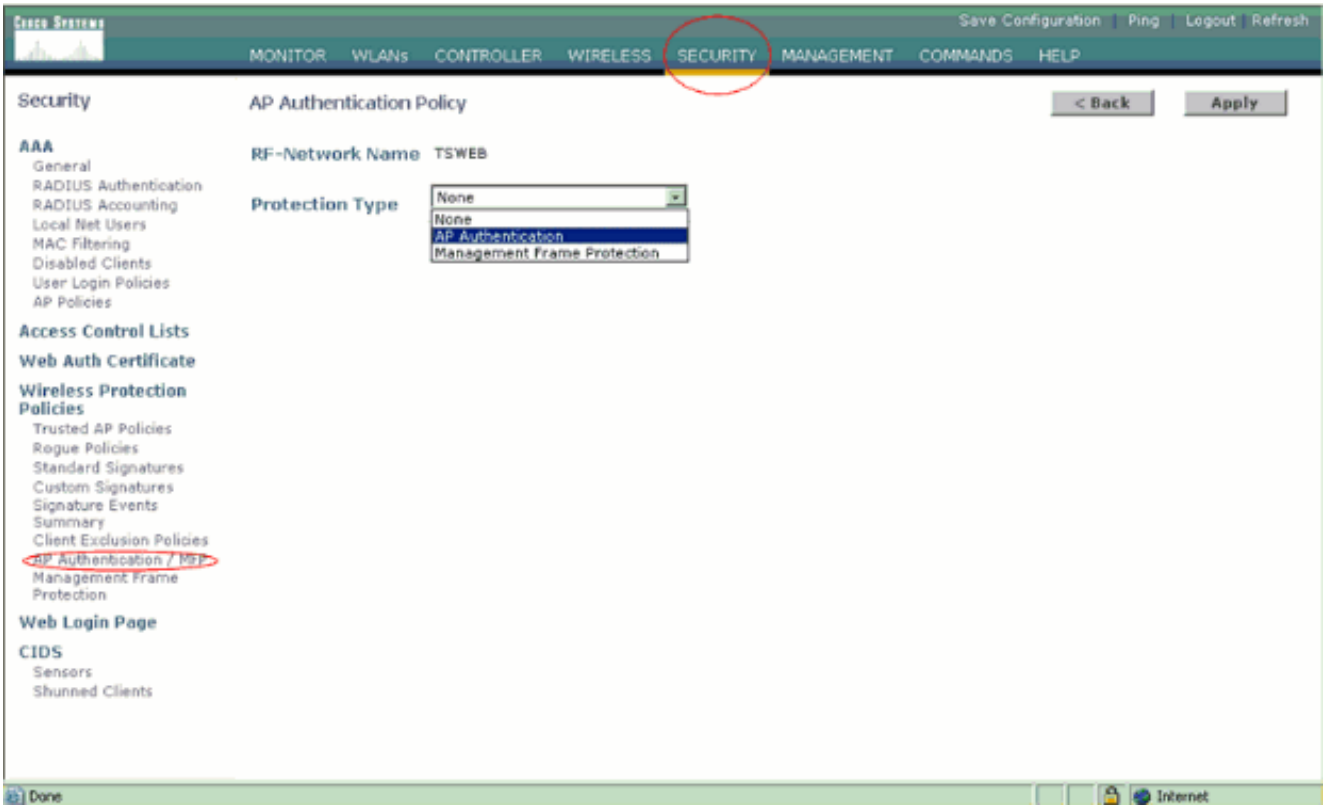
すぐに利用できるネットワーク セキュリティを最大限に活用できるようにするため、デフォルトでは不正検出設定のほとんどが有効になっています。次に示す設定手順では、重要な不正検出情報を具体的に説明する目的で、コントローラで不正検出が設定されていないことを前提としています。

不正検出を設定するには次の手順を実行します。

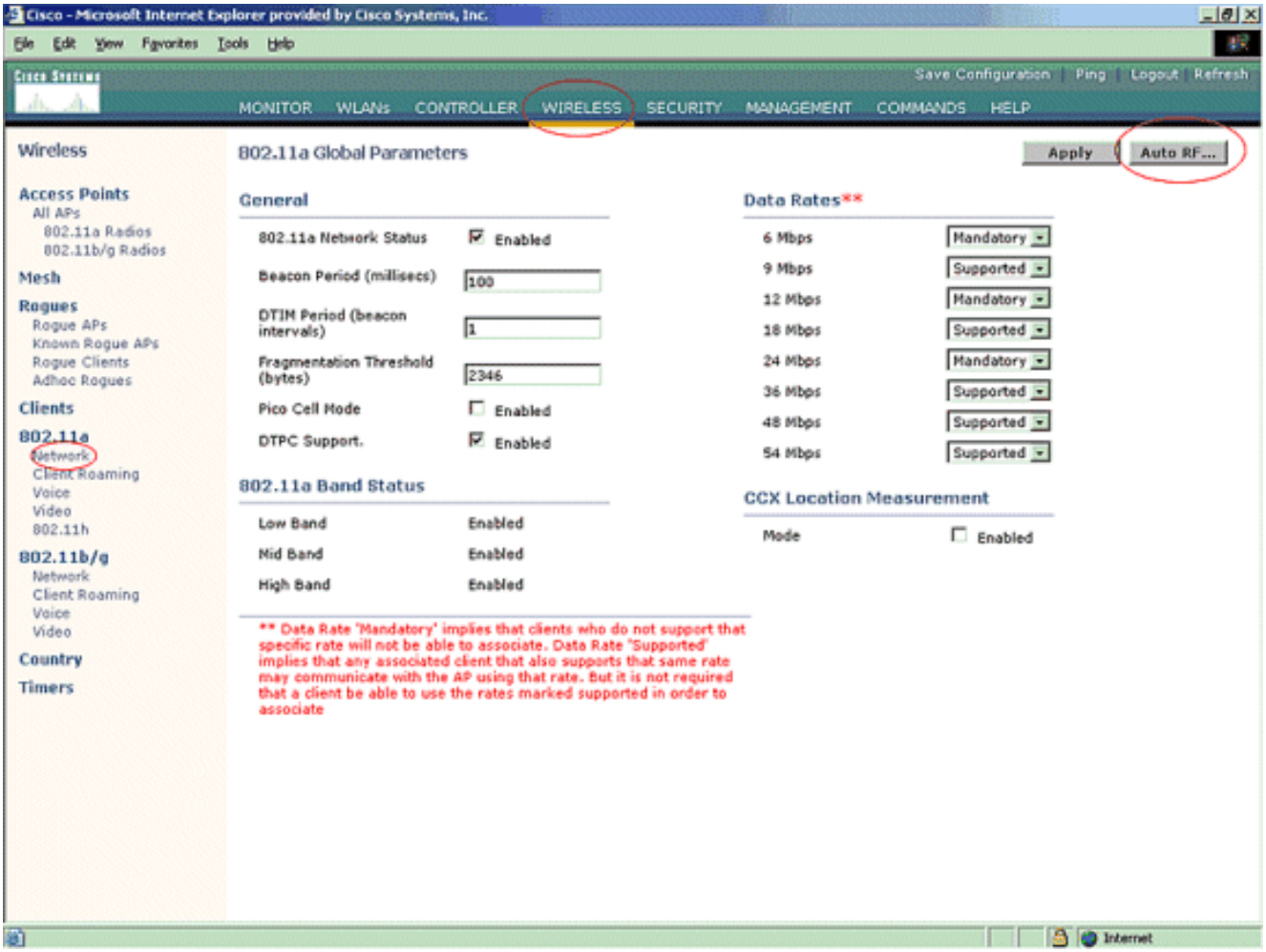
1. Rogue Location Discovery プロトコルがオンになっていることを確認します。このプロトコルをオンにするには、次の図に示すように [Security] > [Rogue Policies] を選択して [Rogue Location Discovery Protocol] の [Enabled] を選択します。**注：不正**APが一定時間聞こえない場合は、コントローラから削除されます。これは不正 AP の**有効期限タイムアウト（Expiration Timeout）**です。これは RLDP オプションの下で設定します。



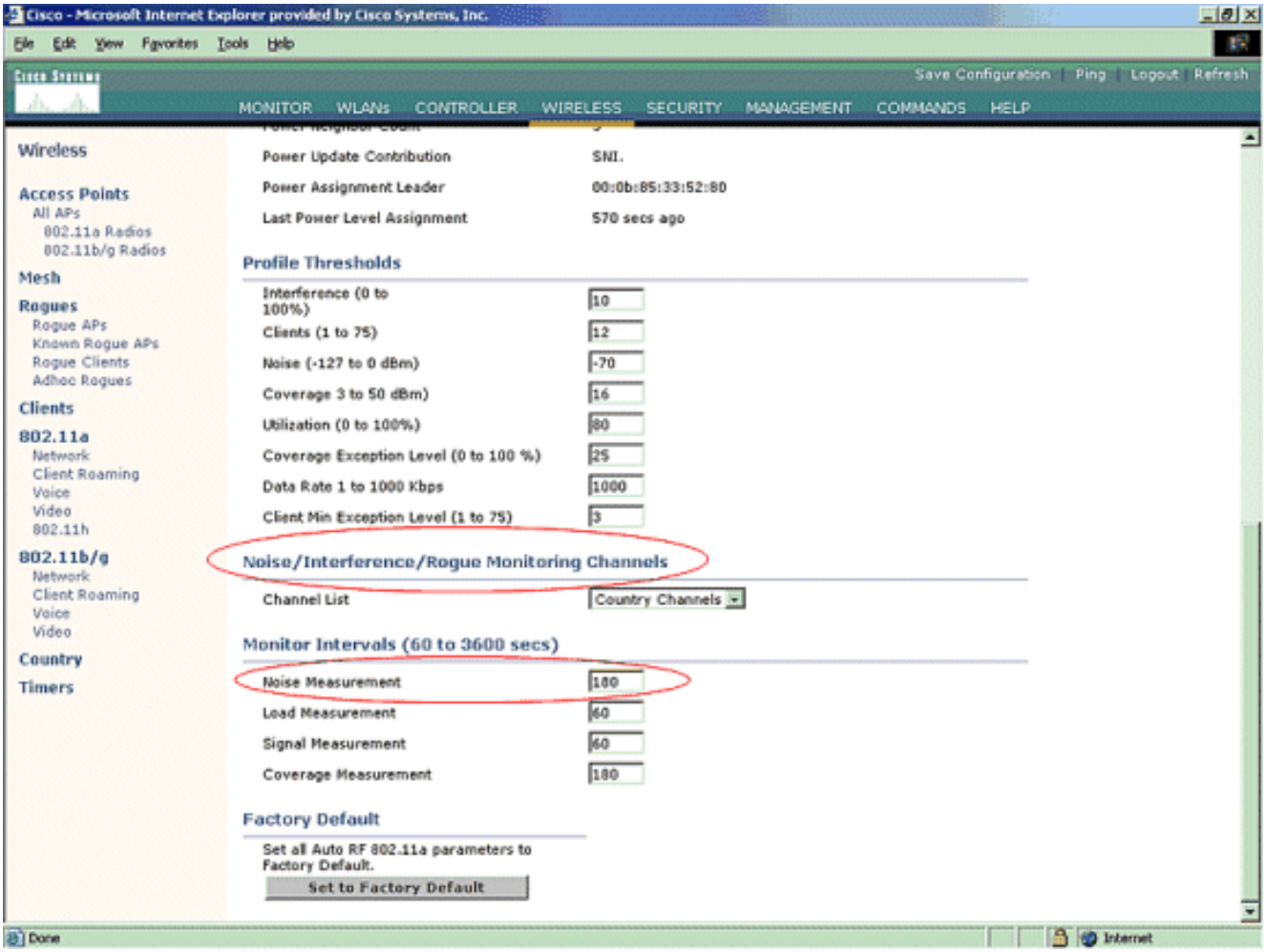
2. このステップは任意で実行します。この機能が有効に設定されていると、異なる **RF グループ**名の RRM ネイバー パケットを送信する AP が不正として報告されます。これは、RF 環境を調べる場合に役立ちます。この機能を有効にするには、[Security] > [AP Authentication] を選択します。次の図に示すように、[Protection Type] として [AP Authentication] を選択します。



3. 次に示す手順でスキャン対象チャネルを確認します。次の図に示すように [Wireless] > [802.11a Network] を選択し、右側の [Auto RF] を選択します。



[Auto RF] ページを下にスクロールし、[Noise/Interference/Rogue Monitoring Channels] を選択します。



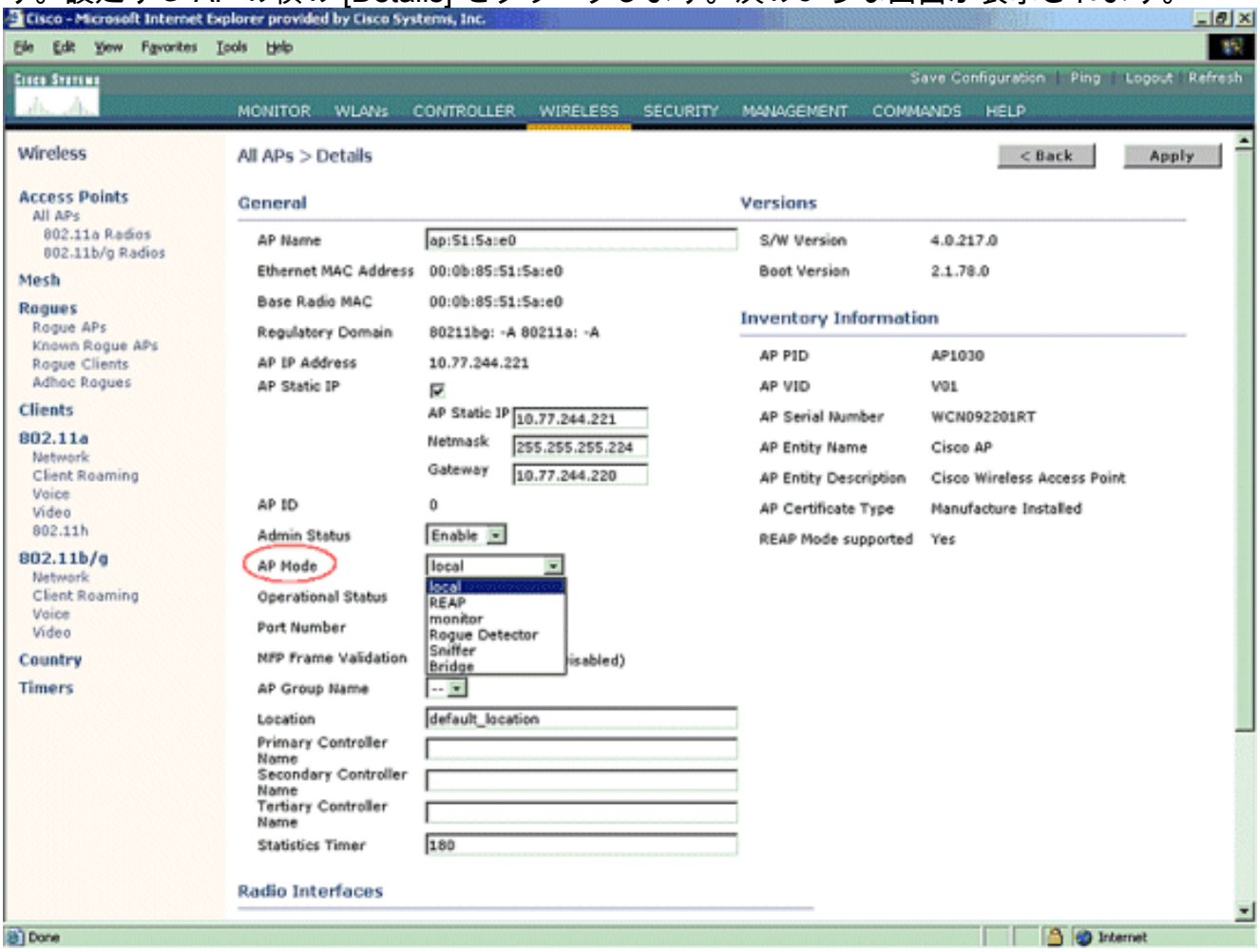
[Channel List] に、他のコントローラや AP 機能に加えて、スキャンして不正をモニタするチャネルの詳細が示されます。Lightweight AP の詳細については『Lightweight Access Point FAQ』を、ワイヤレス コントローラの詳細については『Wireless LAN Controller（WLC）トラブルシューティングの FAQ』を参照してください。

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. 選択したチャネルのスキャン期間を設定します。定義したチャネル グループのスキャン期間は、[Monitor Intervals] > [Noise Measurement] で設定します。設定可能な期間の範囲は 60 ~ 3600 秒です。デフォルトの 180 秒を使用する場合、AP はチャネル グループ内の各チャネルを 180 秒ごとに 1 回 50 ミリ秒にわたってスキャンします。この期間中に AP 無線がサービス チャネルから指定のチャネルに変更され、50 ミリ秒間にわたって監視と値の記録が行われ、その後元のチャネルに戻ります。ホップ タイムと維持期間（50 ミリ秒）により、AP が毎回約 60 ミリ秒間オフチャネルになります。つまり、各 AP は 180 秒のうちの約 840 ミリ秒間、不正を監視します。「監視」時間と「維持」時間は変更できません。また [Noise Measurement] の値を調整してもこれらの値は変更されません。Noise Measurement

タイマーの値を小さくすると、不正検出プロセスではより迅速により多くの不正が検出されます。ただしこのように機能が向上する一方で、データ統合性とクライアント サービスが低下します。またこの値を大きくすると、データ統合性は向上しますが、不正の迅速な検出機能が低くなります。

5. AP の運用モードを設定します。Lightweight AP 運用モードにより AP の役割が決定します。このドキュメントで説明する情報に関連するモードを次に示します。**Local**：これは通常の AP 運用モードです。このモードでは、ノイズと不正を検出するために設定されているチャネルをスキャンする間に、データ クライアントにサービスが提供されます。この運用モードでは、AP は 50 ミリ秒にわたってオフチャネルになり、不正を監視します。Auto RF 設定で指定されている期間にわたり、各チャネルで 1 回ずつ行われます。**Monitor**：これは無線受信専用モードであり、AP がすべての設定チャネルを 12 秒おきにスキャンできます。このように設定された AP には認証解除パケットだけが無線で送信されます。monitor モードの AP は不正を検出できますが、RLDP パケットを送信するために疑わしい不正にクライアントとして接続することはできません。**注：DCAは**、デフォルトのモードで設定可能なオーバーラップしないチャネルを指します。**Rogue Detector**：このモードでは、AP 無線がオフであり、AP は有線トラフィックのみを監視します。コントローラは Rogue Detector として設定されている AP と、疑わしい不正クライアントおよび AP の MAC アドレスのリストを渡します。Rogue Detector は ARP パケットのみを監視します。Rogue Detector は必要に応じてトランク リンクを介してすべてのブロードキャスト ドメインに接続できます。Lightweight AP がコントローラに接続したら、個々の AP モードを設定できます。AP モードを変更するには、コントローラ Web インターフェイスに接続して [Wireless] に移動します。設定する AP の横の [Details] をクリックします。次のような画面が表示されます。



[AP Mode] ドロップダウン メニューを使用して適切な AP 運用モードを選択します。

トラブルシューティングのためのコマンド

AP の設定のトラブルシューティングには次のコマンドも使用できます。

- **show rogue ap summary**：このコマンドは、Lightweight AP により検出された不正 AP のリストを表示します。
- **show rogue ap detailed** ***<不正apのMACアドレス>：個々の不正APの詳細を表示するには、このコマンドを使用します。***これは、不正 AP が有線ネットワークに接続しているかどうかを判別する場合に役立つコマンドです。

結論

シスコの中央集中型コントローラ ソリューションの不正検出と抑止は、業界でも最も効果的で影響の少ない不正検出/抑止手法です。ネットワーク管理者はさらに柔軟にソリューションをカスタマイズして、ネットワークの要件に対応できます。

関連情報

- RF グループの概要
- テクニカル サポートとドキュメント – Cisco Systems