無線デバイスの監視

この章では、WCS を使って無線 LAN を監視する方法について説明します。この章の内容は、次のとおりです。

不正アクセス ポイントの監視

許可されていない不正アクセス ポイントは安価で簡単に利用できることから、従業員は、IT 部門に連絡して同意を得ることなく、それらのアクセス ポイントを既存の LAN やビルディング内のアドホック ネットワークに接続することがあります。これらの不正アクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正アクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、無線ユーザはセキュリティで保護されていないアクセス ポイントの場所を頻繁に公表するため、企業のセキュリティが侵害される危険性も増大します。

Cisco Wireless LAN Solution では、担当者がスキャナを持って不正アクセス ポイントを手作業で検出するのではなく、管理対象のアクセス ポイントに MAC アドレスと IP アドレスによって不正アクセス ポイントを検出させて、その情報を自動的に収集し、システム オペレータがその不正アクセス ポイントの特定、タグ付け、および阻止ができるようになります。また、1 つから 4 つのアクセス ポイントで、不正アクセス ポイントのクライアントに認証解除とアソシエート解除のメッセージを送信することで不正アクセスを防ぐこともできます。

不正アクセス ポイントのロケーション、タギング、および阻止

この組み込み型の検出、タギング、監視、および阻止の機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

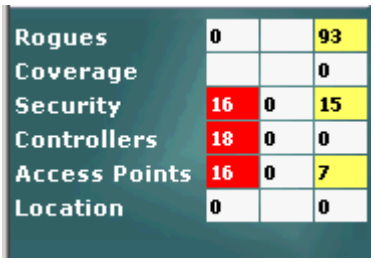
- 不正アクセス ポイントを特定します。
- 新しい不正アクセス ポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 不明な不正アクセス ポイントが削除または認識されるまで監視します。
- 最も近い場所の認可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 つから 4 つのアクセス ポイントで、不正アクセス ポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセス ポイントを阻止します。この阻止は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセス ポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は承諾します。
  - 不正アクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセス ポイントが削除または認識されるまで、不明なアクセス ポイントとしてタグ付けします。
  - 不正アクセス ポイントを阻止済みとしてタグ付けし、1 つから 4 つのアクセス ポイントで、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセス ポイントにアソシエートしないようにします。この機能は、同じ不正アクセス ポイント上のアクティブなチャネルに適用されます。

不正アクセス ポイントの検出と特定

無線 LAN 上のアクセス ポイントで、電源が入りコントローラにアソシエートされると、WCS ではすぐに不正アクセス ポイントのリスニングが開始します。コントローラによって、不正アクセス ポイントが検出されると、すぐに WCS に通知され、WCS によって、不正アクセス ポイントのアラームが作成されます。

WCS が不正アクセス ポイント メッセージをコントローラから受け取ると、すべての WCS ユーザ インターフェイス ページの左下にアラーム ダッシュボードが表示されます。図 6-1 のアラーム ダッシュボードは、93 個の不正アクセス ポイント アラームを示しています。

図 6-1　不正アクセス ポイントを示すアラーム ダッシュボード



不正アクセス ポイントを検出し特定する手順は、次のとおりです。

ステップ 1　**Rogues** インジケータをクリックして、Rogue AP Alarms ページを表示します。このページには、アラームの重大度、不正アクセス ポイントの MAC アドレス、不正アクセス ポイントのタイプ、不正アクセス ポイントが最初に検出された日時、および SSID が表示されます。

ステップ 2　**Rogue MAC Address** リンクをクリックして、それに関連付けられた Alarms > Rogue - AP MAC Address ページを表示します。このページには、不正アクセス ポイントのアラームに関する詳細情報が表示されます。

ステップ 3　アラームを変更するには、Select a command ドロップダウン メニューから次のコマンドのいずれかを選択し、**GO** をクリックします。

- **Assign to me**：選択されたアラームを現在のユーザに割り当てます。
- **Unassign**：選択されたアラームの割り当てを解除します。
- **Delete**：選択されたアラームを削除します。
- **Clear**：選択されたアラームをクリアします。
- **Event History**：不正アラームのイベントを表示できます。
- **Detecting APs**（無線帯域、場所、SSID、チャネル番号、WEP 状態、短いプリアンブルまたは長いプリアンブル、RSSI、および SNR を含む）：不正アクセス ポイントを現在検出しているアクセス ポイントを表示できます。
- **Rogue Clients**：この不正アクセス ポイントとアソシエートしているクライアントを表示できます。
- **Set State to ‘Unknown - Alert’**：不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、阻止機能をオフにします。

  Set State to ‘Known - Internal’：不正アクセス ポイントを内部としてタグ付けして既知の不正アクセス ポイント リストに追加し、阻止機能をオフにします。

Set State to ‘Known - External’：不正アクセス ポイントを外部としてタグ付けして既知の不正アクセス ポイント リストに追加し、阻止機能をオフにします。

- **1 AP Containment ～ 4 AP Containment**：level 1 containment を選択した場合は、不正な機器の近辺にある 1 つのアクセス ポイントが、その不正な機器にアソシエートされたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信します。level 2 containment を選択した場合は、不正な機器の近辺にある 2 つのアクセス ポイントが、その不正な機器のクライアントに認証解除とアソシエート解除のメッセージを送信します。この動作は level 4 まで同様です。

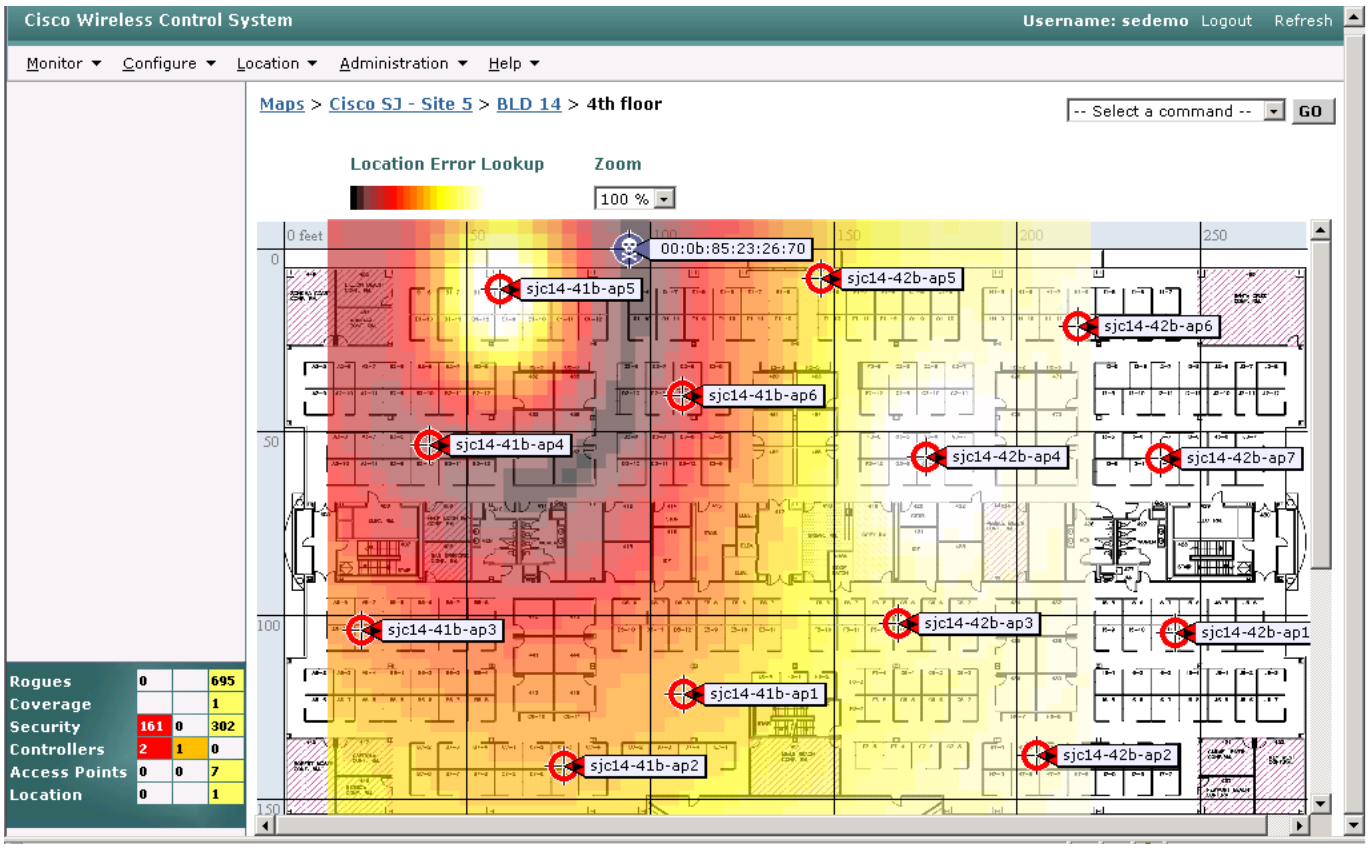
ステップ 4　Select a command ドロップダウン メニューから、**Map (High Resolution)** を選択して、**GO** をクリックし、計算された不正アクセス ポイントの現在位置を Maps > Building Name > Floor Name ページに表示します。

WCS Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較することによって、不正アクセス ポイントが存在する可能性が最も高い位置が特定され、その位置に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。

アクセス ポイント 1 つと全方向性アンテナ 1 つだけの低展開ロケーション ベースのネットワークの場合に、不正アクセス ポイントが存在する可能性が最も高い位置は、不正ではないアクセス ポイントの周辺です。

WCS Base を使用している場合は、不正アクセス ポイントからの RSSI 信号強度を頼りに、不正な機器から最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。図 6-2 は、不正な機器の位置を示すマップを示しています。

図 6-2　不正な機器の位置を示すマップ



不正アクセス ポイントの認識

不正アクセス ポイントを認識する手順は、次のとおりです。

ステップ 1　Rogue AP Alarms ページに移動します。

ステップ 2　認識する不正アクセス ポイントのチェックボックスをオンにします。

ステップ 3　Select a command ドロップダウン メニューから、**Set State to 'Known - Internal'** または **Set State to** 'Known - External' を選択します。いずれの場合も、不正アクセス ポイントの項目が Rogue AP Alarms ページから削除されます。

クライアントの検索

WCS を使用して無線 LAN 上でクライアントを検索する手順は、次のとおりです。

ステップ 1　**Monitor > Devices > Clients** の順にクリックし、Clients Summary ページに移動します。

ステップ 2　サイドバーで、Search For Clients By ドロップダウン メニューの **All Clients** を選択し、**Search** をクリックして Clients ページを表示します。

（注）　WCS Controllers または Location Servers の下でクライアントを検索できます。

ステップ 3　場所を特定したいクライアントの ユーザ名 をクリックします。WCS に、対応する Clients Client Name ページが表示されます。

ステップ 4　クライアントを検索するには、Select a command ドロップダウン メニューから次のオプションのいずれかを選択し、**GO** をクリックします。

- **Recent Map (High Resolution)** : アソシエーションを解除せずにクライアントを検索します。
- **Present Map (High Resolution)** : クライアントとのアソシエーションを解除し再アソシエートしてからクライアントを検索します。この方法を選択した場合は、警告メッセージが表示され、続行するかどうかの確認を求められます。

WCS Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較して、クライアントの最も可能性の高い位置を見つけ、その位置に小さなラップトップ アイコンが表示されます。WCS Base を使用している場合は、クライアントからの RSSI 信号強度を頼りに、クライアントから最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなラップトップ アイコンが表示されます。図 6-3 は、クライアントの位置を示すヒート マップを示しています。

図 6-3　クライアントの位置を示すマップ

カバレッジ ホールの検索

*カバレッジ ホール*とは、クライアントが無線ネットワークから信号を受信できない領域のことです。Cisco Wireless LAN Solution の Radio Resource Management（RRM）によって、これらのカバレッジ ホール領域が特定され WCS に報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。無線 LAN 上でカバレッジ ホールを検索する手順は、次のとおりです。

ステップ 1　WCS ユーザ インターフェイスのページの左下にある **Coverage** インジケータをクリック（または **Monitor > Alarms** の順にクリックして Alarm Category の下で **Coverage** を検索）して、Coverage Hole Alarms ページを表示します。

ステップ 2　**Monitor > Maps** の順にクリックして、access points を name で検索します（この検索ツールでは、大文字と小文字が区別されます）。検索されたアクセス ポイントが設置されているフロアと外部領域を含む Maps > Search Results ページが表示されます。

ステップ 3　フロアまたは屋外領域のリンクをクリックして、関連する **Maps > Building Name > Floor Name** ページを表示します。

ステップ 4　カバレッジ ホールを報告したアクセス ポイントの近辺で信号強度の弱い領域を探します。その領域がカバレッジ ホールの可能性が最も高い領域です。信号強度の弱い領域が表示されない場合は、フロア図面マップが正確であることを確認してください。

コントローラからネットワーク デバイスへの ping

コントローラからネットワーク デバイスを ping する手順は、次のとおりです。

ステップ 1　**Configure** > **Controllers** の順にクリックし、All Controllers ページに移動します。

ステップ 2　目的の IP アドレスをクリックして、**IP Address > Controller Properties** ページを表示します。

ステップ 3　サイドバーで、**System > Commands** の順にクリックして、**IP Address > Controller Commands** ページを表示します。

ステップ 4　Administrative Commands ドロップダウン メニューから、**Ping From Controller** を選択し、**GO** をクリックします。

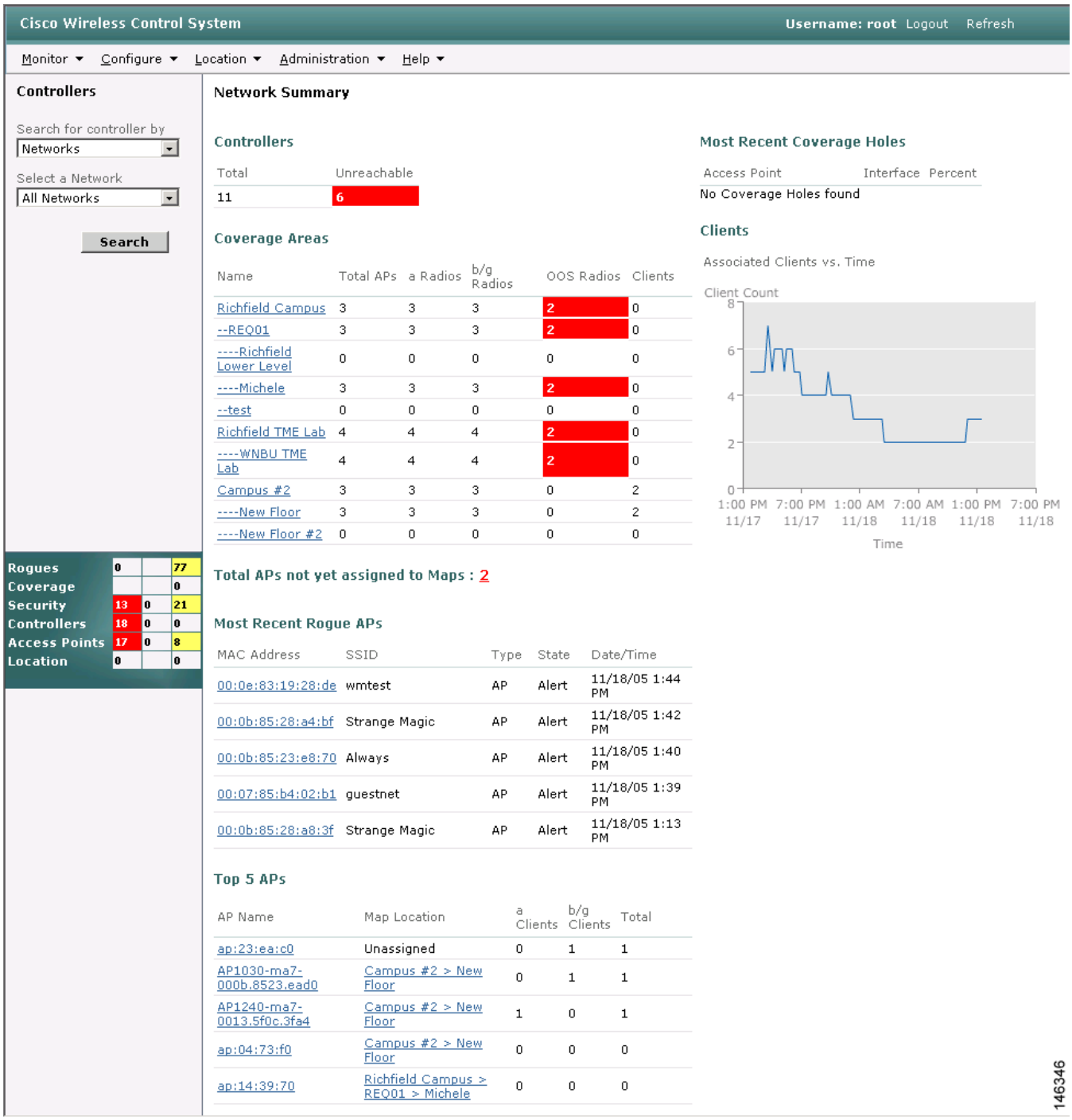
ステップ 5　Enter an IP Address (x.x.x.x) to Ping ウィンドウで、コントローラに ping させるネットワーク デバイスの IP アドレスを入力して、**OK** をクリックします。

Ping Results ウィンドウが開いて、送受信されたパケットが表示されます。ネットワーク デバイスに再度 ping するには、**Restart** をクリックします。または、ネットワーク デバイスへの ping を停止して、Ping Results ウィンドウを終了するには、**Close** をクリックします。

コントローラのステータスと設定の表示

コントローラとアクセス ポイントを WCS データベースに追加すれば、Cisco Wireless LAN Solution のステータスを表示できます。システム ステータスを表示するには、**Monitor > Network Summary** の順にクリックして Network Summary ページを表示します（図 6-4 参照）。

図 6-4　Network Summary ページ



WCS の統計レポートの表示

WCS によって、クライアント カウント、無線の使用状況、送信電力レベルとチャネル情報、プロファイル ステータスなどの統計値が定期的に収集され、レポートにまとめられます。これらのレポートを表示するには、**Monitor** > **Reports** の順にクリックします。

802.11 カウンタ レポート

このレポートは、802.11 カウンタのために選択したパラメータに基づいてグラフを表示します。

ステップ 1　**Monitor > Reports** の順に選択します。

ステップ 2　左側のサイドバーのメニューから、**802.11 Counters** を選択します。

ステップ 3　コントローラ、フロア領域、または屋外領域単位でレポートを表示するかどうかを指定します。

ステップ 4　レポートにおいてすべてのコントローラを表示するかどうか、または特定の IP アドレスを選択するかどうかを指定します。

ステップ 5　レポートにおいてすべてのアクセス ポイントを表示するかどうか、または特定の MAC アドレスを選択するかどうかを指定します。

ステップ 6　レポートにおいて 802.11a または 802.11b/g 無線通信機に重点を置くかどうかを選択します。

ステップ 7　過去 1 時間、過去 6 時間、過去 1 日間、過去 2 日間、過去 3 日間、過去 4 日間、過去 5 日間、過去 6 日間、過去 7 日間のレポートが必要かどうかを指定します。

ステップ 8　**Generate Report** をクリックします。

音声統計レポート

次の手順では、音声統計レポートのパラメータの設定方法について説明します。このレポートでは、音声統計に関して、選択したパラメータに基づいたグラフを表示します。

ステップ 1　**Monitor > Reports** の順に選択します。

ステップ 2　左側のサイドバーのメニューから、**Voice Statistics** を選択します。

ステップ 3　コントローラ、フロア領域、または屋外領域単位でレポートを表示するかどうかを指定します。

ステップ 4　レポートにおいてすべてのコントローラを表示するかどうか、または特定の IP アドレスを選択するかどうかを指定します。

ステップ 5　レポートにおいてすべてのアクセス ポイントを表示するかどうか、または特定の MAC アドレスを選択するかどうかを指定します。

ステップ 6　レポートにおいて 802.11a または 802.11b/g 無線通信機に重点を置くかどうかを選択します。

ステップ 7　過去 1 時間、過去 6 時間、過去 1 日間、過去 2 日間、過去 3 日間、過去 4 日間、過去 5 日間、過去 6 日間、過去 7 日間のレポートが必要かどうかを指定します。

ステップ 8　**Generate Report** をクリックします。また、**Monitor > Devices > Access Points** にアクセスして 1 つまたは複数のアクセス ポイントを選択し、選択した Generate a report for selected AP ドロップダウン メニューから **Voice Statistics** を選択して **GO** をクリックすることもできます。

レポートには、アクセス ポイントの名前と無線通信機、進行中のコール数、進行中のローミング コール数、および使用中の帯域幅の割合が表示されます。

音質メトリック レポート

このレポートを生成するためには、トラフィック ストリーム メトリックが 802.11b/g 音声パラメータのコントローラにおいて有効になっている必要があります。このパラメータの設定の詳細は、「802.11a 音声テンプレートの設定」の項（P. 9-38）を参照してください。このレポートには、音声トラフィック ストリーム メトリックの表が表示されます。

ステップ 1　左側のサイドバーのメニューから、**Monitor > Devices > Access Points** を選択します。

ステップ 2　チェックボックスをクリックして、レポートを実行したいアクセス ポイントを選択します。

ステップ 3　Generate a report for selected AP ドロップダウン メニューから、**Voice Metrics** を選択し、**GO** をクリックします。

このレポートには、次の値が表示されます。

- Time QoS：アクセス ポイントから統計が集められた時間
- % PLR (Downlink)：ダウンリンクでのパケット損失率
- %PLR (Uplink)：アップリンクでのパケット損失率
- Avg Queuing Delay (ms) (Downlink)：ダウンリンクでの平均キューイング遅延時間（ミリ秒）
- Avg Queuing Delay (ms) (Uplink)：アップリンクでの平均キューイング遅延時間（ミリ秒）
- % Packets > 40 ms Queuing Delay：40 ミリ秒を超えるキューイング遅延のパケットの割合
- % Packets > 20 ms Queuing Delay：20 ミリ秒を超えるキューイング遅延のパケットの割合
- Roaming Delay：ローミング遅延時間（ミリ秒）

音声 TSM レポート

このレポートには、このアクセスポイントで有効にできる CCX クライアントが表示されます。トラフィック ストリーム メトリックのテンプレートについては、「QoS テンプレートの設定」の項（P. 9-4）を参照してください。

ステップ 1　左側のサイドバーのメニューから、**Monitor > Devices > Access Points** を選択します。

ステップ 2　チェックボックスをクリックして、レポートを実行したいアクセス ポイントを選択します。

ステップ 3　Generate a report for selected AP ドロップダウン メニューから、**Voice TSM Reports** を選択し、**GO** をクリックします。

このレポートには、次の値が表示されます。

- Avg Queuing Delay (ms)：平均キューイング遅延時間（ミリ秒）
- % Packet with less than 10 ms delay：10 ミリ秒より少ない遅延時間のパケットの割合
- % Packet with more than 10 < 20 ms delay：10 ミリ秒を超えるが 20 ミリ秒より少ない遅延時間のパケットの割合
- % Packet with more than 20 < 40 ms delay：20 ミリ秒を超えるが 40 ミリ秒より少ない遅延時間のパケットの割合
- % Packet with more than 40 ms delay：40 ミリ秒を超える遅延時間のパケットの割合
- Packet Loss Ratio：損失したパケットの割合
- Total Packet Count：合計パケット数
- Roaming Count：この 90 seconds metrics ウィンドウでローミングのネゴシエーションのために交換されたパケット数
- Roaming Delay：ローミング遅延時間（ミリ秒）

メッシュ ツリーの表示

Mesh Tree View では、移動が容易なツリー ビューでアクセス ポイントとの親子関係を確認でき、関心のあるアクセス ポイントだけを選択して、アクセス ポイントが Map ビューに表示する内容をフィルタリングできます。

View Filters の下の黒い四角形のアイコンをクリックして、メッシュ ツリー ビューを表示します。このアイコンは、メッシュ アクセス ポイントがマップ上に存在する場合に利用可能になります。

メッシュ ツリー ビューがマップの上に表示され、次の情報が表示されます。

- 各 PAP アクセス ポイントの隣のアイコンは、親リンクの状態を表します。緑色のアイコンは高い Signal to Noise Ratio（SNR; 信号対雑音比）（25 dB 以上）を表し、黄色のアイコンは許容範囲の SNR（20 ～ 25 dB）を表します。また、赤色のアイコンは低い SNR（20 dB 以下）を表します。メッシュ ツリー ビュー内のアイコンの上にカーソルを移動して、ブリッジ リンク情報を表示します。
- 子アクセス ポイントと親アクセス ポイントの間のリンクです。アクセス ポイントが選択されていない場合は、その子孫はすべて灰色になり選択されません。

Quick Selection ドロップダウン リストからオプションを選択するか、ツリー ビューの適切なチェックボックスをオンにすることにより、マップ ビューの外観を変更できます。子アクセスポイントを表示するには、ルート アクセス ポイントへの親アクセスポイントを選択する必要があります。

次の表は、Mesh Parent-Child Hierarchical ウィンドウのパラメータを示しています。

表 6-1　メッシュの親子階層

パラメータ	説明
Select only Root APs	マップ ビューにルート アクセス ポイントだけを表示したい場合は、この設定を選択します。
Select up to 1st hops	マップ ビューに 1 番目のホップだけを表示したい場合は、この設定を選択します。
Select up to 2nd hops	マップ ビューに 2 番目のホップだけを表示したい場合は、この設定を選択します。
Select up to 3rd hops	マップ ビューに 3 番目のホップだけを表示したい場合は、この設定を選択します。
Select up to 4th hops	マップ ビューに 4 番目のホップだけを表示したい場合は、この設定を選択します。
Select All	マップ ビューにすべてのアクセス ポイントを表示したい場合は、この設定を選択します。

Update Map View をクリックして画面を更新し、選択したオプションでマップ ビューを再表示します。

（注）　マップ ビュー情報は WCS データベースから取得され、15 分おきに更新されます。

アイコンの上にカーソルを移動して、ブリッジ リンク情報を表示します。

表 6-2　ブリッジ リンク情報

パラメータ	説明
Information fetched on	情報を集めた日時
Link SNR	リンクの Signal to Noise Ratio（SNR）
Link Type	階層化されたリンク関係
SNR Up	アップリンクの Signal to Noise Ratio（dB）
SNR Down	ダウンリンクの Signal to Noise Ratio（dB）
Tx Parent Packets	
Rx Parent Packets	
Link State	
Adjusted Link Metric	
Parent Link Metric	
Poor SNR	
Time of Last Hello	最後のハローの日時

リンク テストの実行

リンク テストでは ping を使用してリンク品質をテストします。アクセス ポイントで受信される ping 応答パケットの RF パラメータは、リンク品質を求めるためにコントローラによってポーリングされます。無線通信のリンク品質は方向（クライアントからアクセス ポイントへ、またはアクセス ポイントからクライアントへ）によって異なるため、リンク品質が両方向でテストされるように CCX リンクテストがサポートされていることが重要です。行のステータスが成功または失敗を示すまで、同じ時間おきにコントローラをポーリングします。リンク テストの際は、表が読み込まれます。リンク テストに失敗した場合は、コントローラは ping テストに戻ります。

リンク テストには 2 種類の方法でアクセスできます。1 つ目の方法は、次のとおりです。

ステップ 1　**Monitor > Devices > Clients** の順に選択します。

ステップ 2　左側のサイドバーのメニューから、Search for Clients By ドロップダウン メニューの **All Clients** を選択します。

ステップ 3　Client States ドロップダウン メニューで **All States** を選択します。client list ページが表示されます。

ステップ 4　最後の列の **Link Test** をクリックします。リンク テストが開始されます。図 6-5 はリンク テスト結果のサンプルを示しています。結果は、クライアントがアソシエートされている場合は同じページに表示されます。リンク テストに失敗するとエラー メッセージが表示されます。

リンク テストにアクセスするもう 1 つの方法は、次のとおりです。

ステップ 1　**Monitor > Devices > Clients** の順に選択します。

ステップ 2　ウィンドウの Clients Detected by Location Servers 部分で、Total Clients 列の下の URL をクリックします。

ステップ 3　User 列のリンクをクリックして詳細ページへ進みます。

ステップ 4　Select a command ドロップダウン メニューから、**Link Test** を選択します。

図 6-5 は CCX リンク テスト結果のサンプルを示し、図 6-6 は ping テスト結果のサンプルを示しています。

図 6-5　CCX リンク テスト結果

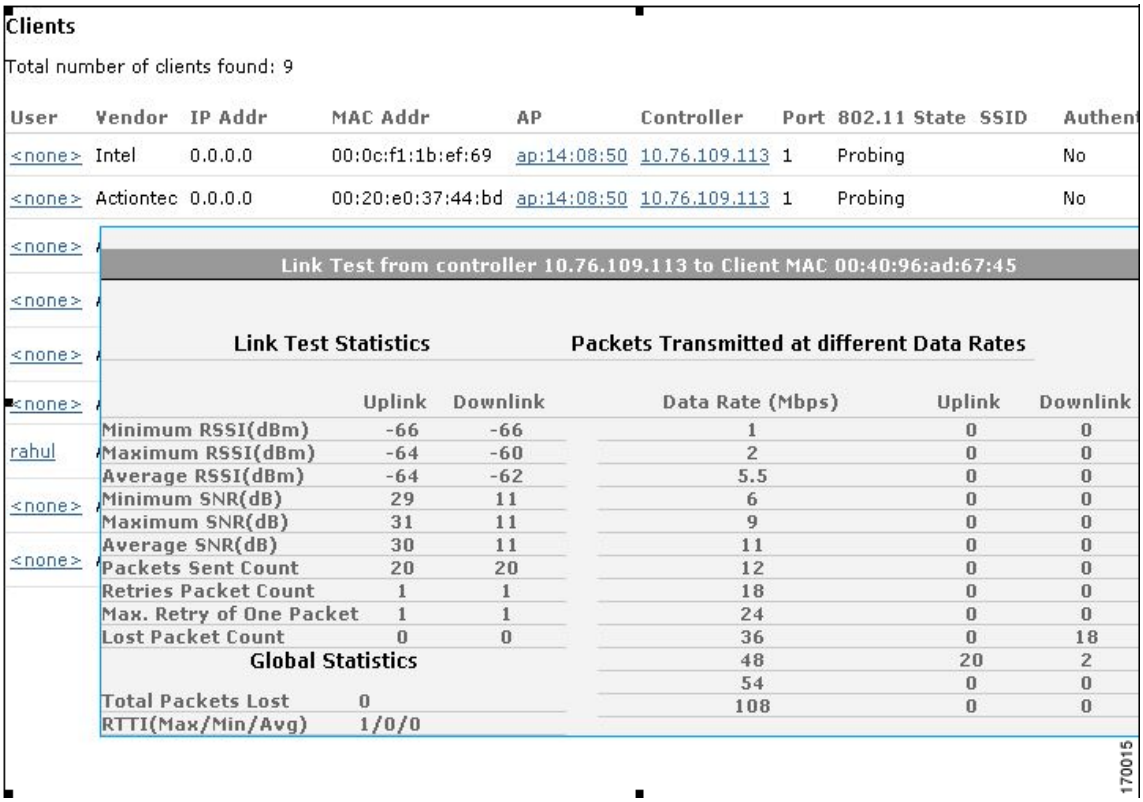
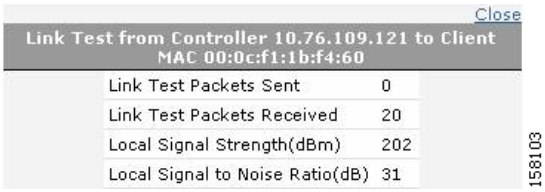


図 6-6　Ping テスト結果



コントローラとアクセス ポイントの Unique Device Identifier の取得

Unique Device Identifier（UDI; 固有デバイス識別情報）の規格は、Cisco のハードウェア製品ファミリ全体で一意的に製品を識別します。また、ユーザがビジネスやネットワーク操作において Cisco 製品を識別し追跡できるようにし、資産管理システムを自動化できるようにします。この規格は、電子的、物理的、および標準的なビジネス コミュニケーションすべてにわたり一貫しています。UDI は次の 5 つのデータ要素で構成されています。

- 整列可能な製品 ID（PID）
- 製品 ID のバージョン（VID）
- シリアル番号（SN）
- エンティティ名
- 製品説明

UDI は工場でコントローラと Lightweight アクセス ポイントの Electrically Erasable Programmable Read-Only Memory（EEPROM; 電気的消去再書き込み可能 ROM）に焼き付けられ、GUI を通して取得できます。

コントローラとアクセス ポイントの UID を取得する手順は、次のとおりです。

ステップ 1　**Monitor > Devices > Controllers** の順にクリックします。

ステップ 2　UDI 情報を取得したいコントローラの IP アドレスの上でクリックします。コントローラの UDI の 5 つのデータ要素がウィンドウに表示されます。