CHAPTER 10

Cisco Unified Wireless Network ゲスト アクセス サービス

企業が無線 LAN（WLAN）テクノロジーを導入することにより、従業員やネットワーク リソースが固定ネットワーク接続の制約から解放され、大企業や中小企業の行動の取り方に変化が生じてきました。

また、WLAN によって、個人が公共の場所からインターネットや会社のネットワークにアクセスする方法も変化しました。公衆 WLAN（ホットスポット）の出現により、モバイル ワーカーは、事実上どこからでも会社のネットワークにアクセスできることが当たり前だと考えています。

概要

パブリック アクセスのパラダイムは、企業にも広がってきています。移動性の高い情報オンデマンド文化には、オンデマンド ネットワーク接続が必要です。このような理由から、エンタープライズ ゲスト アクセス サービスは、重要性を増し、企業環境に不可欠のものとなっています。

ゲスト ネットワーキングが重要性を増していることが広く知られている一方で、社内情報やインフラストラクチャ資産の安全性に対する不安があることも事実です。実装が適切であれば、たいていのゲスト アクセス ソリューションを実装した企業では、実装プロセスに関連したネットワーク監査によって、全体的なセキュリティ状況が改善されます。

全体的なセキュリティの改善に加えて、ゲスト アクセス ネットワークの実装によって、次のような全般的メリットが得られます。

- 日付、期間、帯域幅などの変数に基づく、ゲストの認証と権限付与の制御
- ネットワークを使用中または使用したことのあるユーザをトラックする監査メカニズム

さらに、無線ベースのゲスト アクセスのメリットには、次のものが含まれます。

- かつては有線によるネットワーク接続もなかったロビーや共有施設などのエリアを含め、より広範なカバレッジを提供します。
- ゲスト アクセスの領域や部屋を設定する必要がなくなります。

スコープ

企業でゲスト アクセスを提供する際、複数のアーキテクチャを実装できます。この章の目的は、考えられるソリューションをすべて紹介することではありません。その代わりに、この章では、Cisco Unified Wireless Network ソリューションを使用した無線ゲスト ネットワーキングの実装を中心に説明します。その他のトポロジ シナリオにおける有線および無線ゲスト アクセス サービスの展開に関する詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

無線ゲスト アクセスの概要

理想としては、無線ゲスト ネットワークの実装で、企業の既存の無線および有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲスト アクセスを必要とするあらゆる場所で、キャンパス無線ネットワークを介して実装されます。
- ゲスト トラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ 2 またはレイヤ 3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲスト アクセスを制御する外部プラットフォームの実装を伴います。
- ゲスト ユーザ資格情報の管理：スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロール プラットフォーム内に常駐している場合と、AAA またはその他の管理システムのコンポーネントになっている場合があります。

Cisco Unified Wireless Network ソリューションを使用したゲスト アクセス

Cisco Unified WLAN ソリューションは、中央集中型アーキテクチャ内で Ethernet in IP（RFC3378）を使用することにより、柔軟で簡単な実装方法で無線ゲスト アクセスの展開を提供します。Ethernet in IP は、2 つの WLC エンドポイント間にあるレイヤ 3 トポロジ上のトンネルを作成する際に使用されます。このアプローチのメリットは、ゲスト トラフィックを企業から分離するために実装が必要となる、プロトコルやセグメンテーション テクニックを追加しなくていいことです。

中央集中型 WLAN アーキテクチャを使用したゲスト アクセス トポロジの例については、図 10-1 を参照してください。

図 10-1　中央集中型コントローラのゲスト アクセス

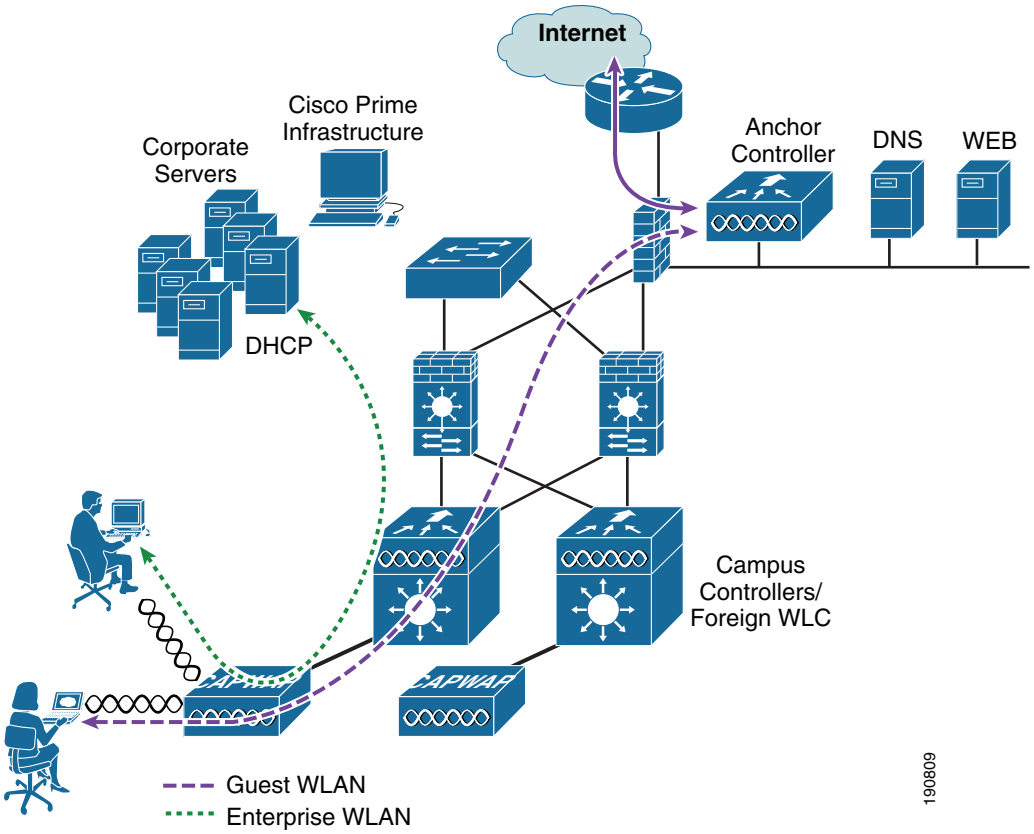


図 10-1 に示すように、アンカー コントローラが企業 DMZ 内に配置され、「アンカー」機能を実行します。アンカー コントローラは、ネットワーク上のその他のキャンパス コントローラを起点とする EoIP トンネルの終端処理に関与します。これらの「外部」コントローラは、企業全体にプロビジョンされたさまざまな WLAN（1 つ以上のゲスト WLAN を含む）の終端、管理、および標準の動作に関与します。ゲスト WLAN は EoIP トンネルを経由してアンカー コントローラに転送されます。具体的には、ゲスト WLAN のデータ フレームが、CAPWAP を使用して AP から外部コントローラにカプセル化されてから、外部管理システムからアンカー WLC で定義されたゲスト VLAN に EoIP でカプセル化されます。このように、ゲスト ユーザ トラフィックは、社内の他のトラフィックによって認識されることなく、また相互作用することなく、透過的にインターネットに転送されます。

WLAN コントローラ ゲスト アクセス

ゲスト アクセス ソリューションは、内蔵型であり、アクセス コントロール、Web ポータル、または AAA サービスを実行するための外部プラットフォームを必要としません。これらの機能はすべて、アンカー コントローラ内で構成および実行されます。ただし、これらの機能のうち 1 つまたはすべてを外部で実装するためのオプションがあり、これについてはこの章の後半で説明します。

サポートされるプラットフォーム

トンネル終端、Web 認証、およびアクセス コントロールを含むアンカー機能が、次の WLC プラットフォームでサポートされています（バージョン 6.0 以降を使用した場合）。

- WLC 2504
- WLC 5508
- WiSM-2
- WLC 7500

次の WLC プラットフォームは、アンカー機能に使用 *できませんが*、標準のコントローラ展開と指定したアンカー コントローラへのゲスト モビリティ トンネルの起点（外部 WLC）として使用できます。

- サービス統合型ルータ用 Cisco WLAN コントローラ モジュール（ISR-SM）
- Cisco 2504

無線ゲスト アクセスをサポートする自動アンカー モビリティ

自動アンカー モビリティ、つまりゲスト WLAN モビリティは、Cisco Unified Wireless Network ソリューションの主要な機能です。EoIP トンネルを使用して、プロビジョンされたゲスト WLAN を 1 つ以上の（アンカー）WLC にマップできます。自動アンカー モビリティによって、ゲスト WLAN と関連するすべてのゲスト トラフィックを、インターネット DMZ に常駐するアンカー コントローラに企業ネットワークを通して透過的に転送できます（図 10-2 を参照）。

図 10-2　自動アンカー EoIP トンネル

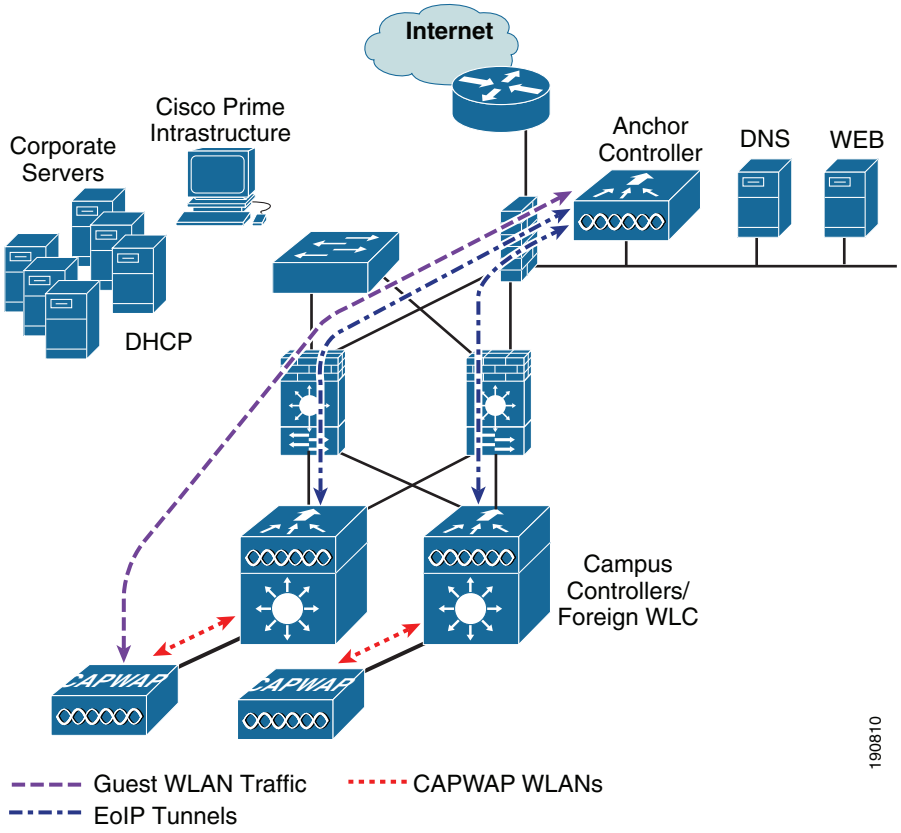
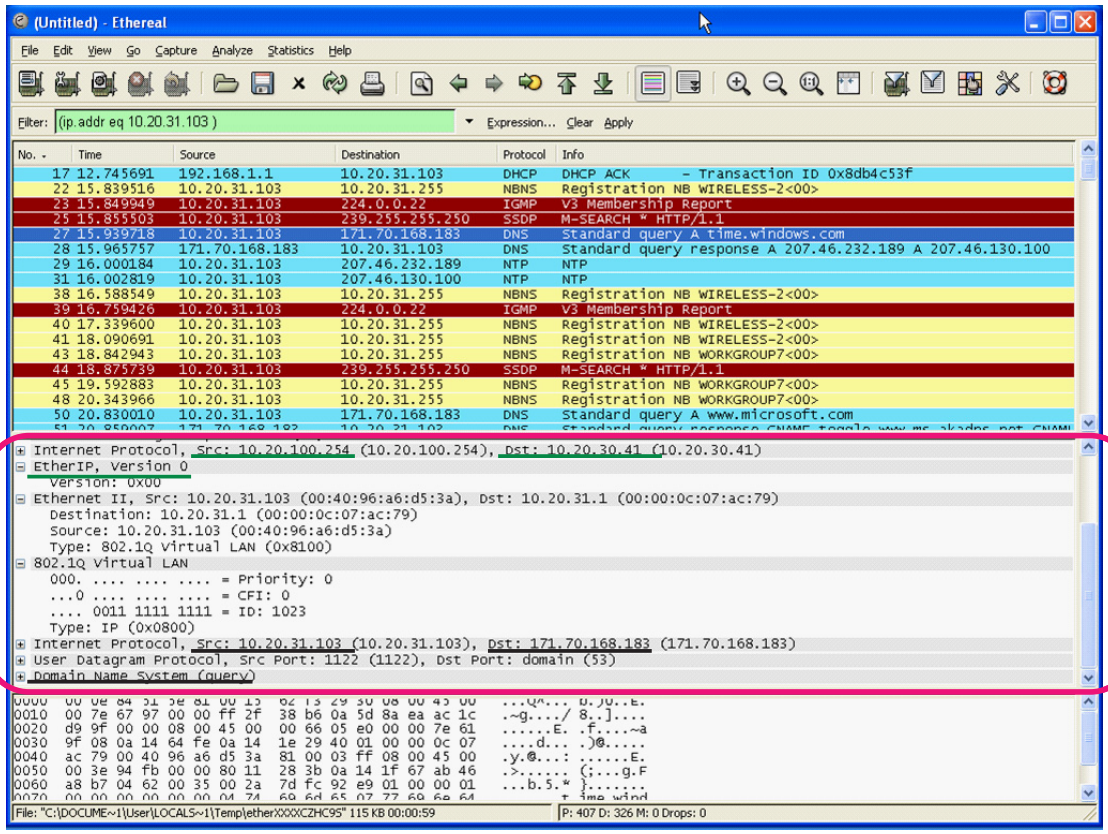


図 10-3 は、ゲスト WLAN がプロビジョンされた外部コントローラとローカル Web 認証を実行しているアンカー コントローラ間の Ethernet in IP トンネル（強調表示部分）のスニファ トレースを示しています。図中の最初の IP 詳細は、外部コントローラとアンカー コントローラ間の Ethernet in IP トンネルを示しています。2 番目の IP 詳細は、ゲスト トラフィックの詳細です（この場合は、DNS クエリー）。

図 10-3　Ethernet in IP スニファ トレースのサンプル



アンカー コントローラ展開ガイドライン

この項では、無線ゲスト アクセスをサポートするためのアンカー コントローラの展開に関するガイドラインを提供します。

アンカー コントローラの位置決め

アンカー コントローラは、ゲスト WLAN トラフィックの終端とそれに続くインターネットへのアクセスに関与するため、通常は企業のインターネット DMZ 内に配置されます。これによって、社内の認証されたコントローラとアンカー コントローラ間の通信を的確に管理するためのルールをファイアウォール内に確立できます。このルールには、送信元または送信先のコントローラのアドレス、WLC 間通信用の UDP ポート 16666、およびクライアント トラフィック用の IP プロトコル ID 97 Ethernet in IP に対するフィルタリングが含まれます。その他に必要なルールは次のとおりです。

- SNMP 用の TCP 161 と 162
- TFTP 用の UDP 69
- HTTP 用または GUI アクセスの HTTPS 用の TCP 80 または 443
- Telnet 用、または CLI アクセスの SSH 用の TCP 23 または 22

トポロジによっては、ファイアウォールを使用して、外部の脅威からアンカー コントローラを保護できます。

最大のパフォーマンスを引き出すために、また、ネットワーク内の位置決めが推奨されていることから、ゲスト アンカー コントローラをゲスト アクセス機能のサポートに専念させることを強く推奨します。つまり、アンカー コントローラを、ゲスト アクセスの他に、社内の他の CAPWAP AP の制御や管理に使用しないようにします。

DHCP サービス

前述したように、ゲスト トラフィックは、EoIP を経由してレイヤ 2 に転送されます。したがって、DHCP サービスを実装できる最初のポイントは、ローカルのアンカー コントローラ上か、クライアントの DHCP 要求を外部サーバに中継できるコントローラ上になります。設定例については、「ゲスト アクセスの設定」（P.10-13）を参照してください。

ルーティング

ゲスト トラフィックは、アンカー コントローラで出力されます。ゲスト WLAN は、アンカー上の動的なインターフェイスまたは VLAN にマッピングされます。トポロジによって、このインターフェイスが、ファイアウォール上のインターフェイスに接続される場合と、インターネット境界ルータに直接接続される場合があります。したがって、クライアントのデフォルト ゲートウェイ IP は、ファイアウォールの IP か、または最初のホップ ルータ上の VLAN またはインターフェイスのアドレスになります。入力ルーティングの場合は、ゲスト VLAN が直接、ファイアウォール上の DMZ インターフェイスに接続されるか、境界ルータ上のインターフェイスに接続されることが考えられます。いずれの場合も、ゲスト（VLAN）サブネットは、直結ネットワークと認識され、それに応じてアドバタイズされます。

アンカー コントローラのサイジングとスケーリング

企業における展開の多くで、ゲスト ネットワーキングを最も効率的にサポートするプラットフォームは、Cisco 5508 シリーズ コントローラです。このコントローラを EoIP トンネル終端によるゲスト アクセスのサポートに限定して展開する場合、コントローラはネットワーク内の AP の管理に使用されないと考えられるため、12 個の AP をサポートする 5508 で十分です。

1 台の 5508 シリーズ コントローラで、社内にある最大 71 台の外部コントローラからの EoIP トンネルをサポートできます。さらに、5508 コントローラは、同時に最大 7,000 ユーザをサポートし、8 Gbps の転送能力があります。

ゲスト アンカー コントローラの選択は、アクティブなゲスト クライアント セッションの数によって定義されているか、またはコントローラ上のアップリンク インターフェイスの容量によって定義されているか、あるいはその両方で定義されたとおりのゲスト トラフィック量に依存します。

ゲスト アンカー コントローラあたりの総スループットとクライアントの制限は次のとおりです。

- Cisco 2504 ワイヤレス LAN コントローラ:4 個の 1 Gbps インターフェイスと 1000 個のゲスト クライアント
- Cisco 5508 ワイヤレス LAN コントローラ（WLC）: 8 Gbps と 7,000 個のゲスト クライアント
- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM-2）: 20 Gbps と 15,000 個のクライアント
- Cisco 7500 ワイヤレス LAN コントローラ（WLC）: 10 Gbps と 20,000 個のクライアント

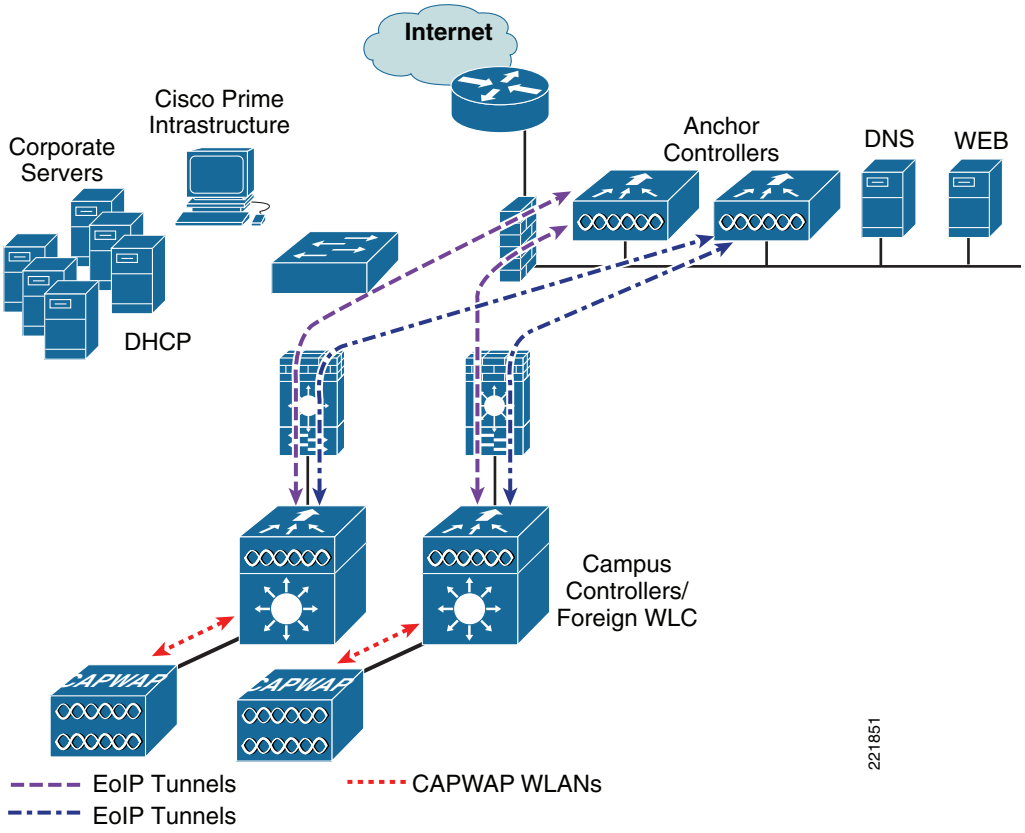
アンカー コントローラの冗長性

Cisco Unified Wireless ソリューション ソフトウェアのリリース 4.1 からは、「ゲスト N+1」冗長性機能が自動アンカー / モビリティ機能に追加されました。この機能には、自動 ping 機能が導入されています。この機能によって、外部コントローラが積極的に ping をアンカー コントローラに送信して、コントロールとデータ パスの接続を確認できます。障害が発生したり、アクティブなアンカーに到達できなくなった場合には、外部コントローラが次のことを行います。

- アンカーが到達できなくなっていることを自動的に検出
- 到達できないアンカーに以前にアソシエートされた無線クライアントを自動的に解除
- 無線クライアントを代替アンカー WLC に自動的に再びアソシエート

ゲスト N+1 冗長性により、所定のゲスト WLAN に 2 つ以上のアンカー WLC を定義できます。図 10-4 は、アンカー コントローラの冗長性を備えた、一般的なゲスト アクセス トポロジを示しています。

図 10-4　ゲスト アンカーの N+1 冗長性を備えたゲスト アクセス トポロジ



ゲスト N+1 冗長性については、次のことに留意してください。

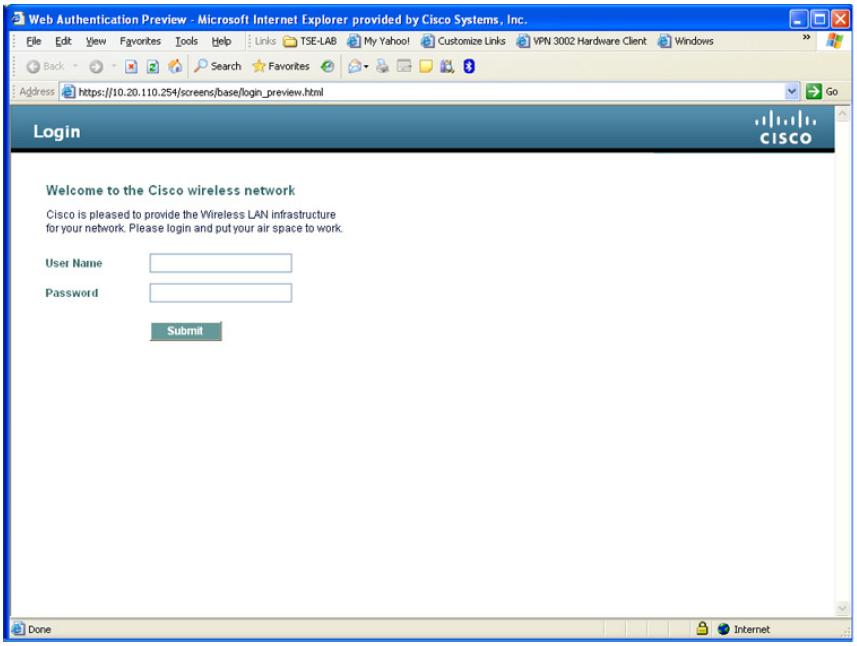
- 所定の外部コントローラの負荷は、ゲスト WLAN に設定されたアンカー コントローラのリスト全体で無線クライアント接続のバランスを取ります。1 つのアンカーを、1 つ以上のセカンダリ アンカーを持つプライマリ アンカーとして指定する方法は、現在のところありません。
- 到達できなくなっているアンカー WLC にアソシエートされた無線クライアントは、WLAN 用に定義された別のアンカーに再びアソシエートされます。これが発生し、Web 認証が使用されている場合には、クライアントは Web ポータル認証ページにリダイレクトされ、資格情報の再送信が要求されます。

（注）　Cisco Unified Wireless Network でマルチキャストが有効でも、ゲスト トンネルではマルチキャスト トラフィックはサポートされません。

Web ポータル認証

Cisco Centralized Guest Access ソリューションは、組み込み型の Web ポータルを備えています。このポータルは、認証用のゲスト資格情報を要求するのに使用され、免責条項または利用規定情報の表示機能と単純なブランディング機能を備えています（図 10-5 を参照）。

図 10-5　コントローラの Web 認証ページ



Web ポータル ページは、すべての Cisco WLAN Controller プラットフォーム上で使用でき、WLAN がレイヤ 3 Web ポリシーベースの認証用に設定された場合にデフォルトで呼び出されます。

よりカスタマイズされたページが必要な場合は、管理者が、カスタマイズされたページをインポートしてローカルに保存するオプションが用意されています。また、会社で外部 Web サーバを使用する場合は、内部サーバを使用せずに外部サーバにリダイレクトするようにコントローラを設定できます。Web ページの設定に関するガイドラインについては、「ゲスト アクセスの設定」（P.10-13）を参照してください。

ユーザ リダイレクション

たいていの Web ベースの認証システムでは一般的なことですが、ゲスト クライアントを WLC の Web 認証ページにリダイレクトする場合は、ゲスト クライアントが Web ブラウザ セッションを起動して、対象 URL を開く必要があります。リダイレクションが正常に動作するには、次の条件を満たす必要があります。

- DNS 解決：ゲスト アクセス トポロジでは、有効な DNS サーバが DHCP 経由で割り当てられ、認証前のユーザからその DNS サーバへアクセスできるようにする必要があります。クライアントが認証で Web ポリシー WLAN にアソシエートすると、DHCP と DNS を除くすべてのトラフィックがブロックされます。そのため、DNS サーバは、アンカー コントローラから到達可能にする必要があります。トポロジによっては、DNS を許可するためにファイアウォールを通してコンジットを開く必要がある場合と、インターネット境界ルータ上の ACL を変更する必要がある場合があります。

（注） 静的 DNS 設定のクライアントは、設定された DNS サーバがゲスト ネットワークからアクセスできるかどうかによって、機能しない場合があります。

- 解決可能なホームページ URL：ゲスト ユーザのホームページ URL は、DNS によってグローバルに解決可能である必要があります。たとえば、ユーザのホームページが、会社のイントラネットの外側では解決できない社内用ホームページである場合、そのユーザはリダイレクトされません。この場合、ユーザは www.yahoo.com や www.google.com などの一般サイトへの URL を開く必要があります。
- HTTP ポート 80：ユーザのホームページは解決可能ですが、HTTP ポート 80 以外のポート上にある Web サーバに接続された場合、ユーザはリダイレクトされません。また、ユーザが WLC の Web 認証ページにリダイレクトされるには、ポート 80 を使用する URL を開く必要があります。

（注） ポート 80 に加え、コントローラがリダイレクションを監視できるように、追加ポート番号を 1 つ設定するオプションは次のとおりです。この設定は、コントローラの CLI を通してのみ使用可能です。<*controller_name*> config> **network web-auth-port** <*port*>

ゲスト資格情報の管理

ゲスト資格情報は、リリース 4.0 以降の管理システムを使用して、一元的に作成および管理できます。ネットワーク管理者は、管理システム内に限定的な特権アカウントを作成し、ゲスト資格情報を作成する目的の Lobby Ambassador アクセスを許可します。このようなアカウントでは、Lobby Ambassador に許可されている機能は、ゲスト資格情報を作成して、Web ポリシーが WLAN に設定されたコントローラに割り当てることだけです。

管理システム内の多くの設定タスクと同様に、ゲスト資格情報はテンプレートを使用して作成されます。次にいくつかの新しいゲストユーザ テンプレートのオプションおよび機能を示します。

- ゲスト テンプレートには、2 種類あります。1 つは、有効期間を制限するかまたは無制限にした、即時のゲスト アクセスをスケジューリングするためのゲスト テンプレートです。もう 1 つは、管理者が「将来の」ゲスト アクセスをスケジューリングして、曜日と時間帯によるアクセス制限を提供します。
- このソリューションにより、管理者はゲスト ユーザに資格情報を E メールで送信できるようになります。さらに、「スケジュール」ゲスト テンプレートが使用されると、アクセスが提供される新しい日（間隔）ごとに、資格情報が自動的に E メールで送信されます。

- （ゲスト）WLAN SSID および管理システムのマッピング情報（キャンパス / ビルディング / フロアの場所）に基づくか、または WLAN SSID および特定のコントローラまたはコントローラのリストに基づいて、ゲスト資格情報を WLC に適用できます。後者の方法は、この章で説明するように、ゲスト モビリティ アンカー方式でゲスト アクセスを展開する場合に使用されます。

Lobby Ambassador がゲスト テンプレートを作成すると、ゲスト アクセス トポロジに応じて 1 つ以上のコントローラに適用されます。*「Web」ポリシーで設定した WLAN* を持つコントローラだけが、適用可能なテンプレートの候補コントローラとして一覧表示されます。これは、ゲスト テンプレートを管理システムのマップ ロケーションの基準に基づいてコントローラに適用する場合にも当てはまります。

適用されたゲスト資格情報は、（アンカー）WLC 上にローカルに保存され（[Security] > [Local Net Users]）、ゲスト テンプレートで定義された「ライフタイム」変数の期限までそこで保持されます。資格情報の有効期限が切れている場合でも、無線ゲストがアソシエートされアクティブな場合は、WLC がトラフィック転送を停止してそのユーザの WEBAUTH_REQD ポリシー状態に戻ります。ゲスト資格情報が（コントローラに）再適用されない場合、そのユーザは二度とネットワークにアクセスすることができません。

（注） ゲスト資格情報に関連付けられたライフタイム変数は、WLAN セッション タイムアウト変数とは無関係です。WLAN セッション タイムアウトの時間を過ぎてもユーザが接続したままの場合は、認証が解除されます。その後、ユーザは、Web ポータルにリダイレクトされ、資格情報の有効期限が切れていない場合には、再度アクセスするためにログインをやり直す必要があります。面倒な認証のリダイレクトを避けるには、ゲスト WLAN セッション タイムアウト変数を適切に設定する必要があります。

ローカル コントローラのロビー管理者のアクセス

中央集中型 WCS 管理システムが展開されていないか使用できない場合、ネットワーク管理者は、ロビー管理者の特権だけを付与したローカル管理者のアカウントをアンカー コントローラ上に設定できます。ロビー管理者のアカウントを使用してコントローラにログインしたユーザは、ゲスト ユーザ管理機能にアクセスできます。ローカル ゲスト管理で使用可能な設定オプションは、管理システムを通して使用可能な機能とは対照的に、限られています。次のオプションが含まれます。

- ユーザ名
- 生成パスワード
- 管理者割り当てパスワード
- 確認パスワード
- 有効期間：日 : 時 : 分
- SSID
- レイヤ 3 Web ポリシー認証用に設定された WLAN だけを表示
- 説明

管理システムによってコントローラに適用された資格情報は、管理者がコントローラにログインしたときに表示されます。ローカルのロビー管理者のアカウントには、管理システムによって以前に作成されたゲスト資格情報を変更または削除する特権が与えられます。WLC 上でローカルに作成されるゲスト資格情報は、コントローラの設定が管理システムで更新されない限り、管理システムに自動的に表示されません。WLC 設定の更新の結果として管理システムにインポートされる、ローカルに作成されるゲスト資格情報は、編集して WLC に再適用できる、新しいゲスト テンプレートとして表示されます。

ゲスト ユーザの認証

「ゲスト資格情報の管理」（P.10-10）で説明したように、管理者が管理システムまたはコントローラ上でローカルのアカウントを使用してゲスト ユーザ資格情報を作成した場合は、それらの資格情報は、コントローラ上でローカルに保存されます。そのコントローラは、中央集中型ゲスト アクセス トポロジの場合、アンカー コントローラとなります。

無線ゲストが Web ポータルを通してログインした場合、コントローラは次の順番で認証を処理します。

1. コントローラが、ユーザ名とパスワードをローカル データベースでチェックし、そこに存在すれば、アクセスを許可します。

ユーザ資格情報が見つからなかった場合は、次のように処理されます。

2. コントローラが、外部 RADIUS サーバがゲスト WLAN 用に設定されているかどうかチェックします（WLAN 構成設定の下）。そのように設定されている場合は、コントローラが、そのユーザ名とパスワードで RADIUS アクセス要求パケットを作成し、選択された RADIUS サーバに転送して認証します。

特定の RADIUS サーバがゲスト WLAN 用に設定されていない場合は、次のように処理されます。

3. コントローラが、グローバルな RADIUS サーバの設定をチェックします。「ネットワーク」ユーザを認証するように設定されたすべての外部 RADIUS サーバは、ゲスト ユーザ資格情報を使用して照会されます。それ以外では、どの RADIUS サーバでも「ネットワーク ユーザ」がオンになっておらず、また上記 1 または 2 でユーザが認証されていない場合、認証は失敗します。

（注）　RADIUS サーバは、[WLC Security] > [AAA] > [RADIUS] 設定でネットワーク ユーザのチェックボックスがオフになっている場合でも、ネットワーク ユーザ認証をサポートするために使用できます。ただし、これを実現するには、サーバが特定の WLAN の [Security] > [AAA Servers] 設定で明示的に選択されている必要があります。

外部認証

WLC およびゲスト アカウント管理（Lobby Ambassador）機能は、WLC 上のローカル認証用にゲスト ユーザ資格情報を作成して適用するためだけに使用できます。ただし、既存のゲスト管理/認証ソリューションが、有線ゲスト アクセスまたは NAC ソリューションの一部として、すでに企業に展開されている場合があります。その場合は、ゲスト ユーザの認証で説明したように、Web ポータル認証を外部 RADIUS サーバに転送するようにアンカー コントローラ/ゲスト WLAN を設定できます。

コントローラが Web ユーザを認証するために使用するデフォルトのプロトコルは、パスワード認証プロトコル（PAP）です。外部 AAA サーバに対して Web ユーザを認証している場合は、そのサーバがサポートしているプロトコルを確認する必要があります。また、Web 認証に CHAP または MD5-CHAP を使用するようにアンカー コントローラを設定できます。Web 認証プロトコル タイプは、WLC のコントローラ設定で設定されます。

Cisco Secure ACS と Microsoft ユーザ データベースを使用した外部認証

ゲスト アクセスの展開で、ゲスト ユーザの認証に Cisco ACS とともに Microsoft ユーザ データベースの使用を検討している場合は、次の Cisco ACS 設定に関する注意事項を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html

特に、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html#wp1041223

ゲスト パススルー

無線ゲスト アクセスのもう 1 つの形態は、ユーザ認証をすべて省略して、オープン アクセスを可能にすることです。ただし、企業は、アクセスを許可する前に利用規定または免責条項のページをユーザに表示することが必要になる場合があります。そのような場合は、Web ポリシーをパススルーするようにゲスト WLAN を設定できます。このシナリオでは、ゲスト ユーザが、免責情報を含むポータル ページにリダイレクトされます。

また、パススルー モードには、ユーザが接続する前に E メール アドレスを入力するオプションもあります（サンプル ページについては、図 10-6 および図 10-7 を参照）。設定例については、「ゲスト アクセスの設定」（P.10-13）を参照してください。

図 10-6　Welcome AUP ページのパススルー

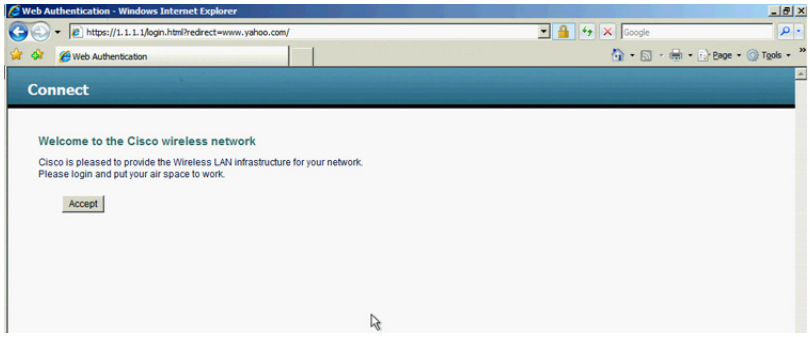
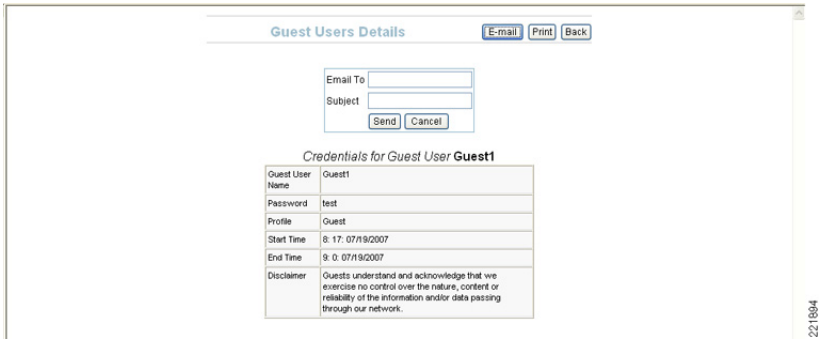


図 10-7　E メールを含むページのパススルー



ゲスト アクセスの設定

この項では、Cisco Unified Wireless Network ソリューション内で無線ゲスト アクセス サービスを有効にする方法について説明します。設定作業では、Web ブラウザを使用する必要があります。コントローラとの Web セッションは、次のコントローラの管理 IP アドレスへの HTTPS セッションを開くことによって、確立されます。**https://***management_IP* またはオプションでコントローラのサービス ポート IP アドレス。

次の手順では、アンカー WLC を除き、コントローラと LAP のインフラストラクチャがすでに展開されているものとします。詳細については、「アンカー コントローラ展開ガイドライン」（P.10-6）を参照してください。

（注）　この項で説明する設定手順は、記載された順序に従って実行することを推奨します。

設定セクション全体を通じて、次の用語が使用されます。

- 外部 WLC：企業のキャンパス全体またはブランチ ロケーションに展開され、AP のグループの管理および制御に使用される 1 つ以上の WLC を指します。外部コントローラが、ゲスト WLAN をゲスト モビリティ EoIP トンネルにマッピングします。
- アンカー WLC：企業 DMZ 内に展開され、ゲスト モビリティ EoIP トンネル終端、Web リダイレクション、およびユーザ認証を実行するために使用される 1 つ以上の WLC を指します。

（注）　この項では、特定の設定画面キャプチャの関連する部分だけを示します。

Cisco Unified Wireless Network ゲスト アクセス ソリューションの実装は、次の設定カテゴリに分類できます。

- アンカー WLC の設置およびインターフェイス設定：ここでは、1 つ以上のアンカー WLC の実装に関する設置の要件、手順、および注意点について簡単に説明します。既存の Cisco Unified Wireless Network 展開にゲスト アクセスを初めて実装する場合、アンカー WLC は通常、企業ネットワークのインターネット エッジに設置される新しいプラットフォームです。
- モビリティ グループの設定：ここでは、外部 WLC が、1 つ以上のゲスト アンカー WLC への EoIP トンネルの起点となるように設定する必要があるパラメータについて説明します。モビリティ グループの設定自体で EoIP トンネルが作成されるわけではなく、ゲスト アクセス WLAN サービスをサポートするために、外部 WLC とアンカー WLC 間のピア関係が確立されます。
- ゲスト WLAN の設定：ゲスト WLAN（外部 WLC を起点とする）をアンカー WLC にマッピングするのに必要な WLAN 固有の設定パラメータに焦点を当てます。ゲスト アクセス ソリューションの設定のこの部分において、外部 WLC とアンカー WLC 間に EoIP トンネルが作成されます。ここでは、Web ベースの認証のレイヤ 3 リダイレクションを起動するために必要な設定についても説明します。
- ゲスト アカウント管理：ここでは、コントローラまたはアンカー WLC のロビー管理者インターフェイスを使用して、アンカー WLC でローカルにゲスト ユーザ資格情報を設定および適用する方法の概要について説明します。
- その他の機能とソリューション オプション：次のような、設定が可能なその他の機能について説明します。
  - Web ポータル ページの設定と管理
  - 外部 Web リダイレクションのサポート
  - 事前認証 ACL
  - アンカー WLC DHCP の設定
  - 外部 RADIUS 認証
  - 外部アクセス コントロール

アンカー WLC の設置およびインターフェイスの設定

「アンカー コントローラの位置決め」（P.10-6）で説明したように、アンカー WLC は、ゲスト アクセスだけに使用して、社内の LAP の制御および管理には使用しないことを推奨します。

この項では、アンカー WLC 上のインターフェイス設定のすべてを扱っているわけではありません。読者は、初期ブート時に必要な、シリアル コンソール インターフェイスを使用した WLC の初期化と設定プロセスに精通していることを前提とします。

この項では、ゲスト アクセス トポロジ内にアンカーとして展開する WLC 上でのインターフェイスの設定に関する特定の情報と注意事項を記載します。

シリアル コンソール インターフェイスを使用した初期設定の一環として、次の 3 つの静的インターフェイスを定義する必要があります。

- コントローラ管理：このインターフェイス/IP は、ネットワーク上の他のコントローラとの通信に使用されます。また、外部コントローラを起点とする EoIP トンネルの終端にも使用されるインターフェイスです。
- AP マネージャ インターフェイス：AP 管理にコントローラを使用しない場合でも、このインターフェイスは設定する必要があります。シスコでは、管理インターフェイスと同じ VLAN およびサブネット上に、AP マネージャ インターフェイスを設定することを推奨します。
- 仮想インターフェイス：コントローラのクイックスタート インストール マニュアルでは、1.1.1.1 などのアドレスの仮想 IP を定義するように推奨されています。このアドレスは、同じモビリティ グループのメンバであるすべてのコントローラで同じアドレスにする必要があります。また、仮想インターフェイスは、コントローラがクライアントを Web 認証のためにリダイレクトするときのソース IP アドレスとしても使用されます。

ゲスト VLAN インターフェイスの設定

前述したインターフェイスは、コントローラに関連付けられた動作と管理機能に使用されます。ゲスト アクセス サービスを実装するには、もう 1 つのインターフェイスを定義する必要があります。これは、ゲスト トラフィックをインターネットにルーティングするためのインターフェイスです。「アンカー コントローラの位置決め」（P.10-6）で説明したように、ゲスト インターフェイスは、ファイアウォール上のポートに接続される場合と、インターネット境界ルータ上のインターフェイスに切り替えられる場合があります。

新しいインターフェイスの定義

次の手順を実行して、ゲスト トラフィックをサポートするインターフェイスを定義および設定します。

ステップ 1　[Controller] タブをクリックします。

ステップ 2　左側のペインで、[Interfaces] をクリックします（図 10-8 を参照）。

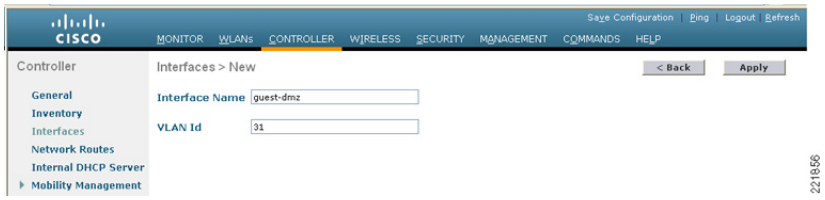
図 10-8　コントローラ インターフェイス

ステップ 3　[New] をクリックします。

インターフェイス名と VLAN ID の定義

ステップ 4　インターフェイス名と VLAN ID を入力します。（図 10-9 を参照）。

図 10-9　　インターフェイス名と VLAN ID



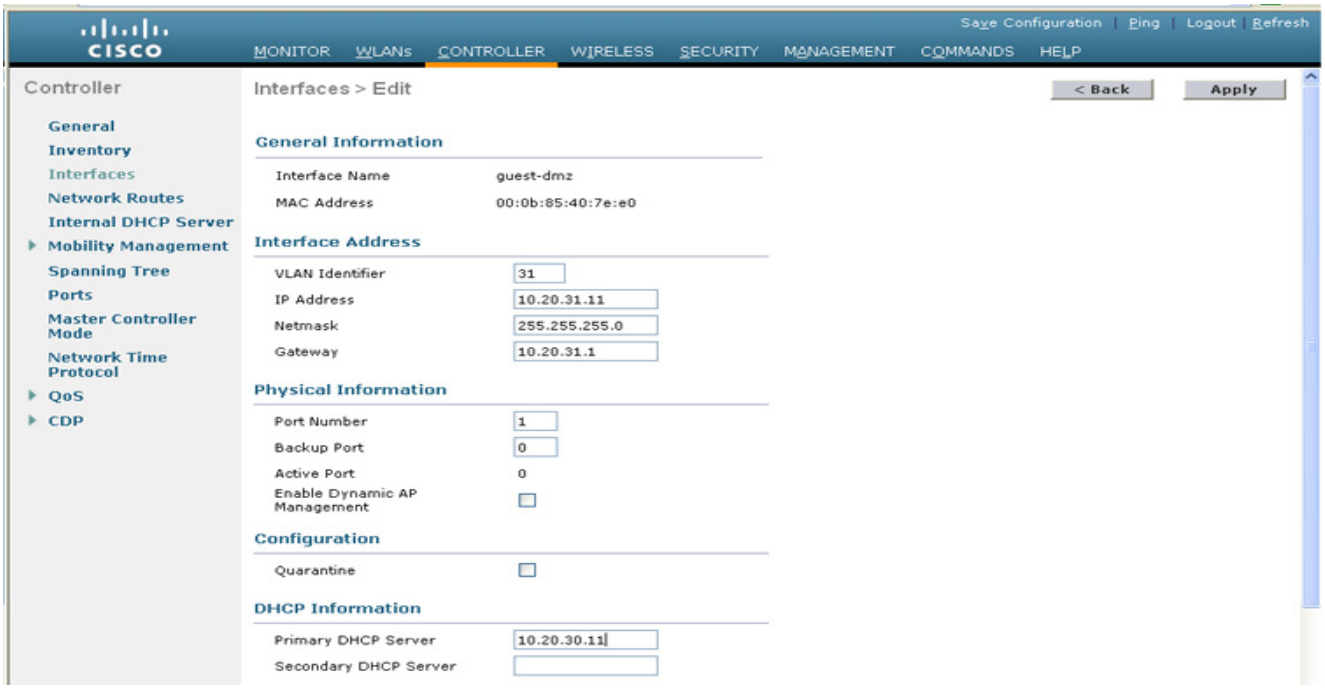
インターフェイス プロパティの定義

ステップ 5　次のプロパティを定義します。

- インターフェイス IP
- マスク
- ゲートウェイ（アンカー コントローラに接続されたファイアウォールまたはネクスト ホップ ルータの場合）
- DHCP サーバ IP（外部 DHCP サーバを使用している場合は、[Primary DHCP Server] フィールドのそのサーバの IP アドレスを使用します）。

  図 10-10 を参照してください。

図 10-10　インターフェイス プロパティの定義



（注）　DHCP サービスをアンカー コントローラ上でローカルに実装する必要がある場合は、[Primary DHCP Server] フィールドにコントローラの管理 IP アドレスを入力します。ゲスト N+1 冗長性が DMZ に実装されている場合、展開されている追加のアンカー WLC ごとに、上記のインターフェイス設定を繰り返します。

モビリティ グループの設定

次のデフォルトのモビリティ グループ パラメータは、標準の中央集中型 WLAN 展開の一部として、外部 WLC に定義しておく必要があります。ゲスト アクセスの自動アンカー モビリティをサポートするには、モビリティ グループ ドメイン名でアンカー WLC も設定する必要があります。

アンカー WLC のデフォルト モビリティ ドメイン名の定義

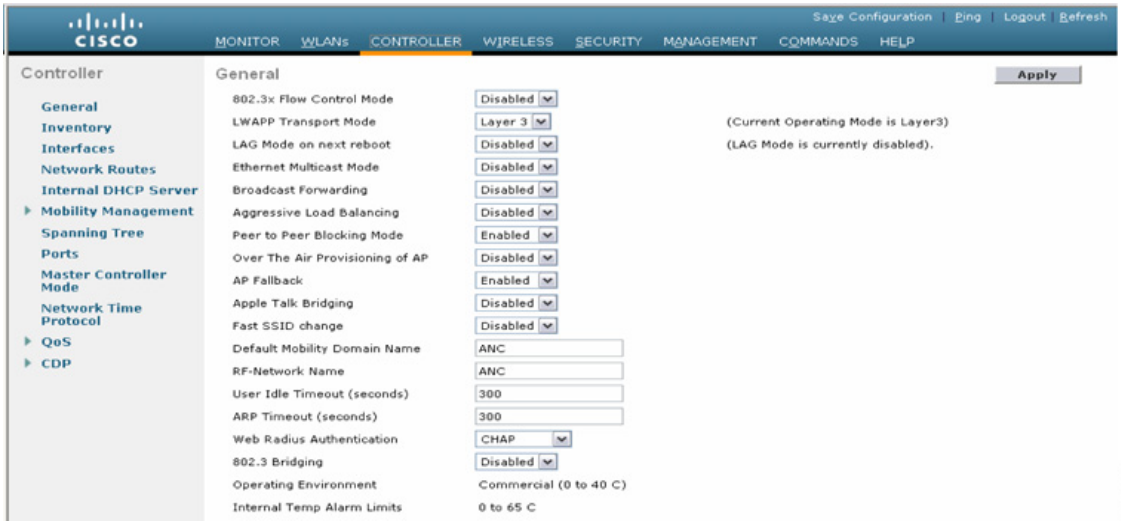
アンカー WLC のデフォルト モビリティ ドメイン名を設定します。アンカーのモビリティ ドメイン名は、外部 WLC に設定した名前と異なる必要があります。以下の例では、企業の無線展開にアソシエートされている WLC（外部コントローラ）は、すべてモビリティ グループ「SRND」のメンバです。一方、ゲスト アンカー WLC は、別のモビリティ グループ名「ANC」で設定されます。これは、企業の無線展開にアソシエートされているプライマリ モビリティ ドメインから、アンカー WLC を論理的に区別しておくために行われます。

ステップ 1　[Controller] タブをクリックします。

ステップ 2　[Default Mobility Domain Name] フィールドに名前を入力します。

ステップ 3　[Apply] をクリックします。（図 10-11 を参照）。

図 10-11　アンカー WLC 上のデフォルト モビリティ ドメイン名の定義



アンカー WLC のモビリティ グループ メンバの定義

ゲスト WLAN をサポートする企業での展開内のすべての外部 WLC は、ゲスト アンカー WLC のモビリティ グループ メンバとして定義する必要があります。

ステップ 1　[Controller] タブをクリックします。

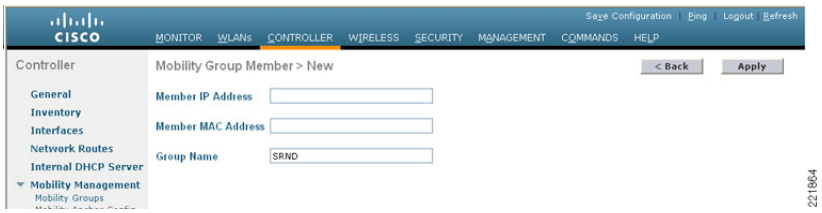
ステップ 2　左側のペインで、[Mobility Management] をクリックし、[Mobility Groups] をクリックします。（図 10-12 を参照）。

図 10-12　モビリティグループメンバの定義

モビリティ グループ メンバとして外部コントローラを追加

ステップ 3　[New] をクリックして、ゲスト アクセス WLAN をサポートする各外部コントローラの MAC と IP アドレスを定義します。（図 10-13 を参照）。

図 10-13　アンカー WLC への外部コントローラの追加



（注）　上に示した図 10-13 の [Group Name] は、外部 WLC の [Default Mobility Domain Name] で設定される名前です。これは、アンカー WLC に使用される名前と異なる必要があります。メンバの IP アドレスと MAC アドレスは、外部 WLC の管理インターフェイスにアソシエートされたアドレスです。ゲスト WLAN をサポートする追加の各外部 WLC に対して、上記の手順を繰り返します。複数のアンカーが展開されている場合（ゲスト N+1 冗長性）、アンカー WLC のデフォルト モビリティ ドメイン名の定義とアンカー WLC のモビリティ グループ メンバの定義の手順を繰り返します。

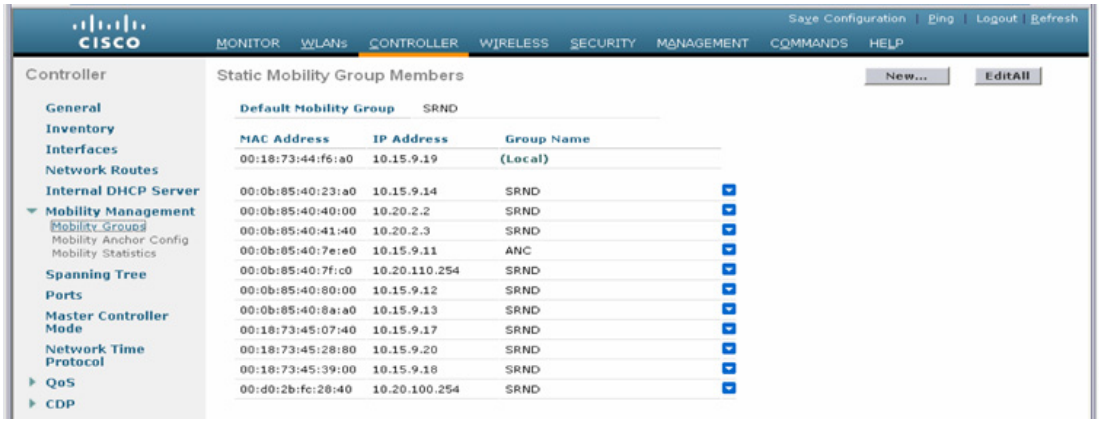
外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加

無線ゲスト アクセスをサポートする自動アンカー モビリティで説明したように、各外部 WLC は、アンカー WLC 上で終端する EoIP トンネルにゲスト WLAN をマッピングします。そのため、アンカー WLC は、各外部コントローラのモビリティ グループのメンバとして定義する必要があります。下の例で、アンカー WLC のグループ名エントリが「ANC」で（「アンカー WLC のモビリティ グループ メンバの定義」（P.10-18）を参照）、企業の無線展開を構成しているもう一方の WLC がモビリティ グループ「SRND」のメンバであることに注意してください。

ステップ 1　[New] をクリックして、アンカー WLC の IP、MAC アドレス、およびグループ名をモビリティ メンバ テーブルに追加します。

ステップ 2　追加の外部コントローラごとにこの手順を繰り返します （図 10-14 を参照）。

図 10-14　外部 WLC へのアンカー コントローラの追加



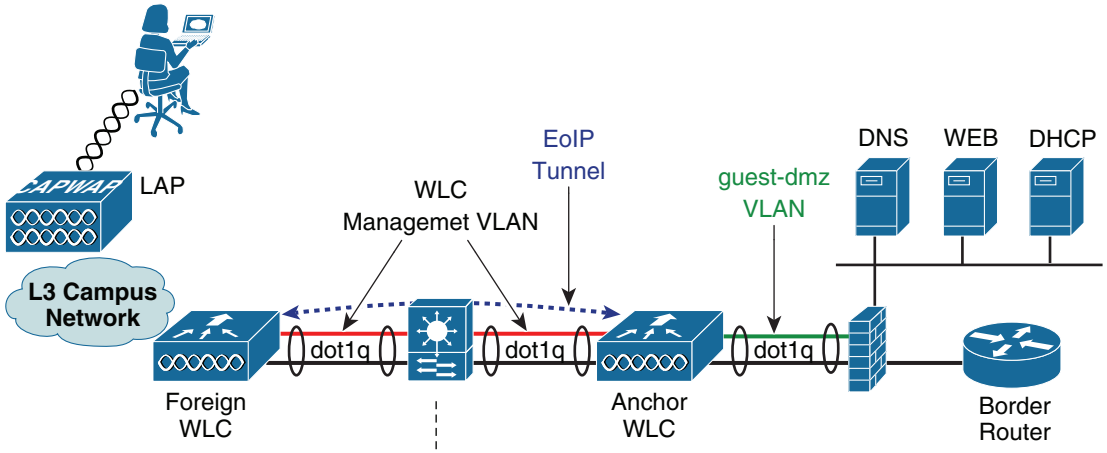
（注）　ゲスト N+1 冗長性機能が展開されている場合、2 つ以上のアンカー WLC エントリが各外部 WLC のモビリティ グループ メンバ リストに追加されます。

ゲスト WLAN の設定

この項では、単一のゲスト WLAN の設定方法について説明します。ゲスト WLAN は、ゲスト アクセスが必要な AP を管理するすべての外部 WLC 上で設定します。アンカー WLC が明らかにゲスト WLAN にアソシエートされた LAP の管理に使用されない場合でも、アンカー WLC は、ゲスト WLAN を使用して設定する必要があります。なぜならば、アンカー WLC は、WLAN の論理拡張機能で、そこでユーザ トラフィックがアンカー WLC 上のインターフェイス /VLAN に最終的にブリッジされるためです（AP と外部コントローラ間では CAPWAP、外部コントローラとアンカー コントローラ間では EoIP を使用）。

（注）　[WLAN Security]、[QoS]、および [Advanced] 設定タブで定義するすべてのパラメータは、アンカーおよび外部 WLC の両方で*同じ設定にする必要があること*に注意することが非常に重要です。図 10-15 は、以下で説明する WLAN 設定のハイレベルの概略図を示しています。

図 10-15　　WLAN の設定



Foreign WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = 802.11b/g only
Interface = Management
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

Mobility Config
Default Mobility Group Name = **SRND**
Static Mobility Members:
00:0b:85:40:7e:e0 10.15.9.11 ANC

Anchor WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = 802.11b/g only
Interface = guest-dmz
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

Mobility Config
Default Mobility Group Name = **ANC**
Static Mobility Members:
00:18:73:44:f6:a0 10.15.9.19 SRND

222545

（注）　[WLAN Security]、[QoS]、および [Advanced] 設定タブで定義するパラメータは、アンカーおよび外部コントローラの両方で*同じ設定にする必要があります*。

外部 WLC：ゲスト WLAN の設定

ステップ 1　[WLANs] タブをクリックして、[New] をクリックします。（図 10-16 を参照）。

図 10-16　ゲスト WLAN の設定

ゲスト WLAN SSID の定義

ステップ 2　将来のゲスト ユーザが、直感的に理解できるか、または認識しやすい SSID を定義します。

コントローラで自動的に VLAN ID を割り当てます。管理者は、他の SSID/WLAN で使用されていなければ、1 ～ 16 の ID を選択できます。

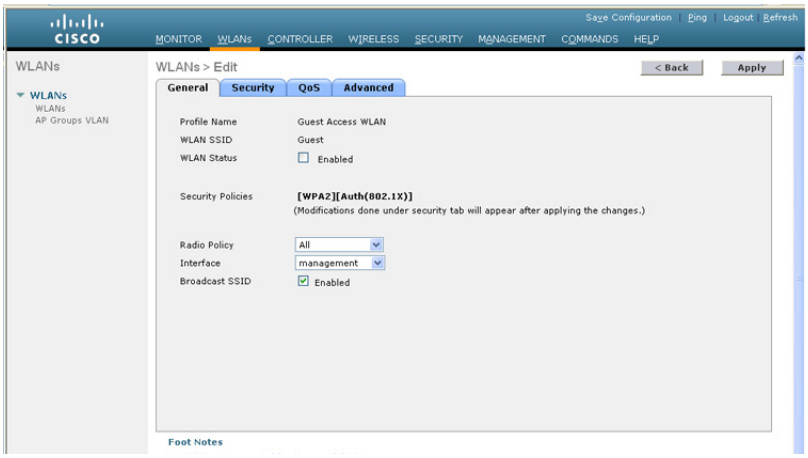
ステップ 3　[Profile Name] を指定します。

ステップ 4　[Apply] をクリックします。（図 10-17 を参照）。

図 10-17　ゲスト WLAN SSID の定義

新しい WLAN の作成後に、図 10-18 に示すように、設定ページが表示されます。

図 10-18　WLAN の設定ページ



（注） ゲスト WLAN のために外部 WLC によって使用されるデフォルト インターフェイスは、管理インターフェイスです。EoIP トンネルがアンカーによって確立できない場合、外部コントローラは、以前に到達不能なアンカーとアソシエートされていた無線クライアントのアソシエーションを解除してから新しいクライアントを割り当て、外部ゲスト WLAN 自体の下で設定されたインターフェイスにクライアントを再度アソシエートします。このため、外部のゲスト WLAN をルーティング不可能なネットワークにリンクするか、あるいは到達不能 IP アドレスを持つ管理インターフェイスの DHCP サーバを設定することを推奨します。アンカーが到達不能になった場合、管理ネットワークへのゲスト クライアントのアクセスを防止します。

ゲスト WLAN のパラメータおよびポリシーの定義

[General Configuration] タブで、次の手順を実行します。

ステップ 1　[WLAN Status] の隣のボックスをクリックして WLAN を有効にします。

ステップ 2　ゲスト アクセスをサポートする帯域を制限する場合は、必要に応じて、無線ポリシーを設定します。

a. [Broadcast SSID] はデフォルトで有効になるので、有効なままにします。

b. デフォルトでは、WLAN は WLC の [management] インターフェイスに割り当てられます。これは変更しないでください。

ステップ 3　[Security] タブをクリックします （図 10-19 を参照）。

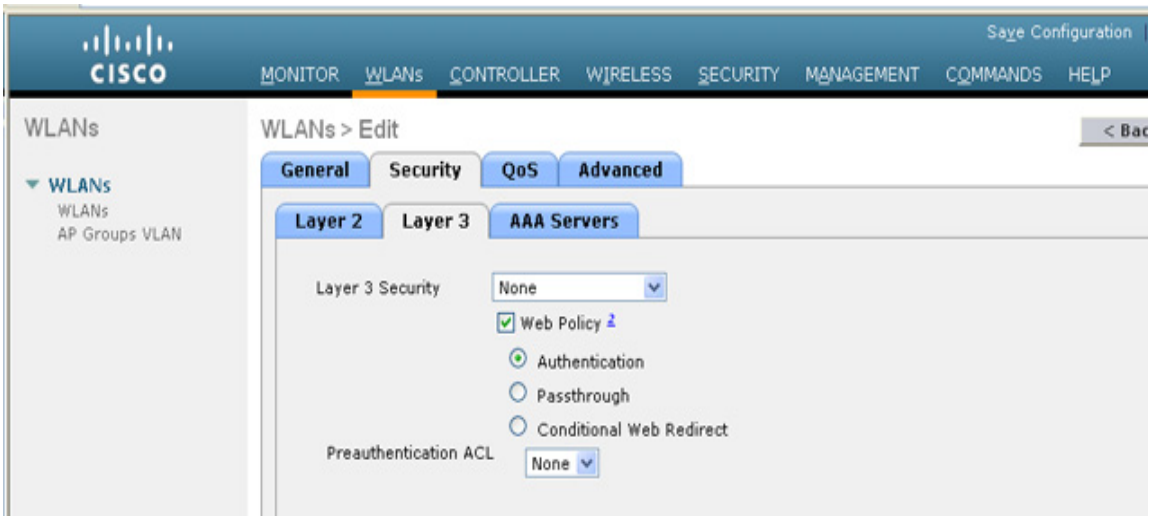
図 10-19　ゲスト WLAN の一般ポリシーの定義

ステップ 4　レイヤ 2 セキュリティを、デフォルトの設定（802.1x WPA/WPA2）から [none] に設定します（図 10-20 を参照）。

図 10-20　WLAN のレイヤ 2 セキュリティ設定

ステップ 5　[Layer 3] タブをクリックします（図 10-21 を参照）。

図 10-21　ゲスト WLAN のレイヤ 3 セキュリティ設定



ステップ 6　[Web Policy] チェックボックスをオンにします（追加オプションのリストが表示されます）。

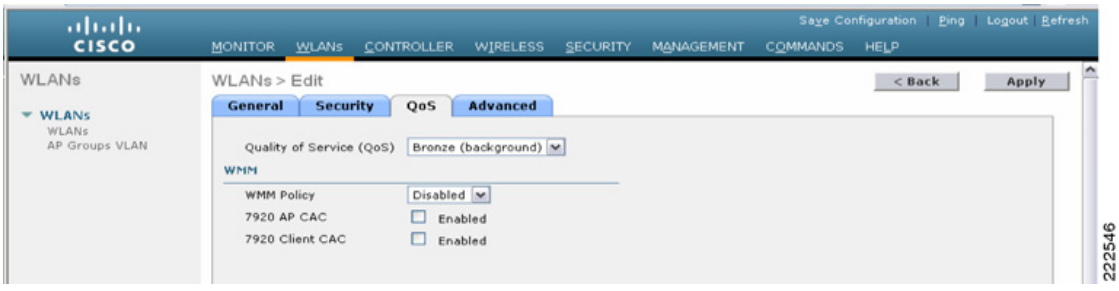
WLC が認証前にクライアント間で DNS トラフィックを受け渡しすることを示す、警告のダイアログボックスが表示されます。

ステップ 7　Web ポリシーに [Authentication] または [Pass-through] を選択します（「ゲスト ユーザの認証」（P.10-12）を参照）。

（注）　事前認証 ACL は、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続することを許可する ACL を適用するために使用できます。ACL は、[Security] > [Access Control Lists] で設定されます。事前認証 ACL が Web 認証ポリシーとともに使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト /URL に解決して接続することができなくなります。

ステップ 8　[QoS] タブを選択します（図 10-22 を参照）。

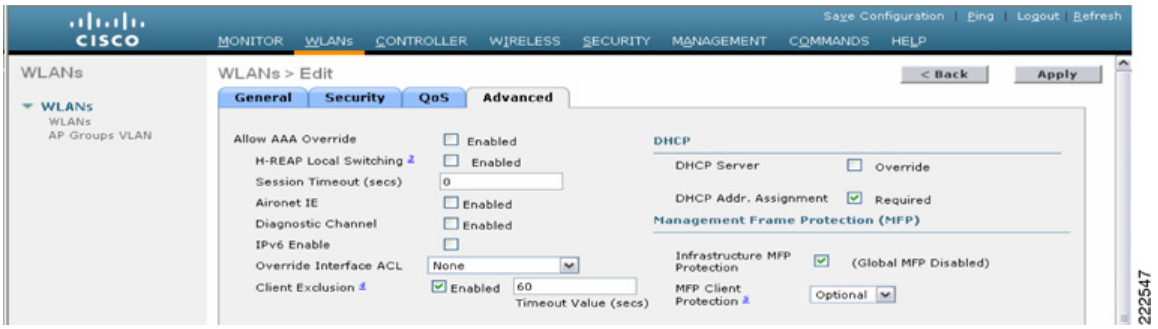
図 10-22　ゲスト WLAN QoS 設定



ステップ 9　オプションで、ゲスト WLAN にアップストリーム QoS プロファイルを設定します。デフォルトは「Silver (Best Effort)」です。この例では、ゲスト WLAN は最低の QoS クラスに再割り当てされています。

ステップ 10　[Advanced] タブをクリックします。（図 10-23 を参照）。

図 10-23　　ゲスト WLAN の高度な設定



ステップ 11　セッション タイムアウトを設定します（オプション）。

（注）　セッション タイムアウトが 0（デフォルト）より大きくなると、有効期限後に強制的に認証が解除され、ユーザは Web ポータルで再認証を要求されます。

ステップ 12　[DHCP Addr. Assignment] を [Required] に設定します。

（注）　ゲスト ユーザが、静的 IP 設定を使用してゲスト ネットワークの使用を試みるのを防ぐため、[DHCP Addr. Assignment] を [Required] に設定することを推奨します。

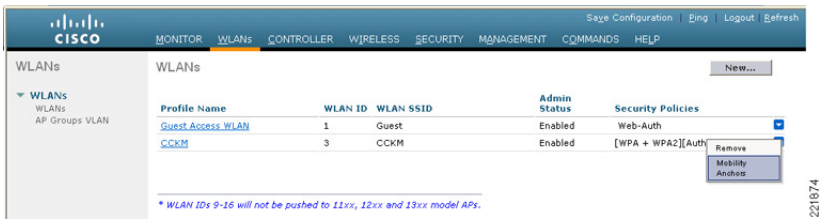
ステップ 13　最後に、[Apply] をクリックします

ゲスト WLAN モビリティ アンカーの設定

ステップ 1　外部 WLC 上の [WLAN] メニューから、新しく作成されたゲスト WLAN を探します。

ステップ 2　右側のプルダウン選択リストから、[Mobility Anchors] を強調表示してクリックします （図 10-24 を参照）。

図 10-24　　WLAN モビリティ アンカー



ステップ 3　[Switch IP Address (Anchor)] プルダウン選択リストで、ネットワーク DMZ 内で展開されたアンカー WLC の管理インターフェイスに対応する IP アドレスを選択します。これは、「外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加」（P.10-19）で設定されたものと同じ IP アドレスです。

ステップ 4　[Mobility Anchor Create] をクリックします （図 10-26 を参照）。

図 10-25　[Switch IP Address (Anchor)] からの管理インターフェイスの選択

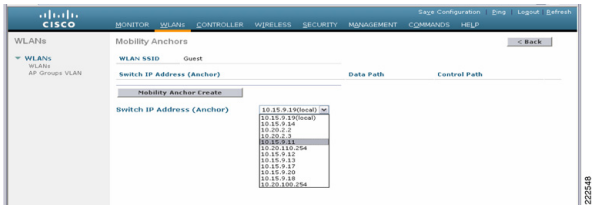
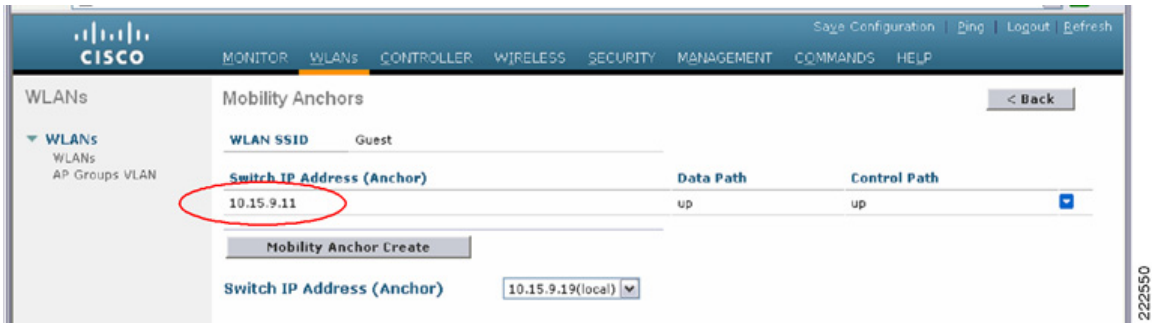


図 10-26　WLAN モビリティ アンカーの選択

ゲスト WLAN モビリティ アンカーの確認

設定されると、図 10-27 に示す画面には、ゲスト WLAN に割り当てられたモビリティ アンカー（上記で選択）が表示されます。

図 10-27　ゲスト WLAN モビリティ アンカーの確認



確認作業を容易にするために、ページには、モビリティ トンネル データ パスと CAPWAPP 制御パスがアンカーで設定されているかどうかが表示されます。両方または片方が「down」と表示されている場合には、「ゲスト アクセスのトラブルシューティング」（P.10-57）でトラブルシューティングのヒントを参照してください。右側のプルダウン選択リストには、宛先アンカー WLC に ping を送信するオプションがあります。

ステップ 5　終了する場合は、[Back] をクリックします。

ステップ 6　展開されている追加の各アンカー WLC（ゲスト N+1 冗長性）に対して、上記の手順を繰り返します。

これで、ゲスト WLAN の設定は終了です。ゲスト WLAN をサポートする追加の各外部 WLC に対して、外部 WLC：ゲスト WLAN の設定からゲスト WLAN モビリティ アンカーの確認のすべての手順を繰り返します。

アンカー WLC 上でのゲスト WLAN の設定

アンカー コントローラ上でのゲスト WLAN の設定は、WLAN インターフェイスおよびモビリティ アンカー設定（以下で詳細を説明）で多少の違いがある点を除き、外部コントローラの設定と同じです。

（注）　ゲスト WLAN に定義する SSID は、外部 WLC 上で定義される SSID とまったく同じにする必要があります。

アンカー WLC：ゲスト WLAN インターフェイス

上記のように、アンカー WLC 上でゲスト WLAN に設定するパラメータは、WLAN がマッピングされるインターフェイスを除いて同じです。この場合、ゲスト WLAN はアンカー WLC 上でインターフェイスまたは VLAN に割り当てられ、アンカー WLC によってファイアウォール上のインターフェイスまたはインターネット境界ルータに接続されます。

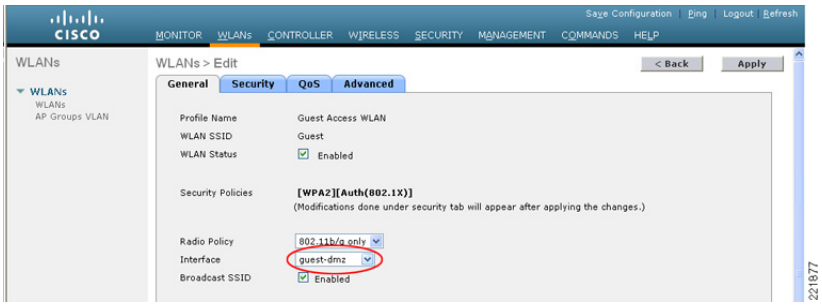
ステップ 1　[WLANs] タブをクリックします。

ステップ 2　次の点を除いて、外部 WLC 上で設定した場合と同様に、ゲスト WLAN を作成、設定、および有効化します。

WLAN の一般的な設定の [Interface] で、ゲスト VLAN インターフェイスの設定で作成されたインターフェイス名を選択します （図 10-28 を参照）。

ステップ 3　[Apply] をクリックします。

図 10-28　アンカー WLC ゲスト WLAN インターフェイスの設定



アンカー WLC：ゲスト WLAN モビリティ アンカーの定義

外部 WLC とは設定が異なる 2 つ目のパラメータは、WLAN モビリティ アンカー設定です。ゲスト WLAN モビリティ アンカーは、アンカー WLC 自体です。

ステップ 1　[WLANs] タブをクリックします。

ステップ 2　ゲスト WLAN を探して、[Mobility Anchors] をクリックします。

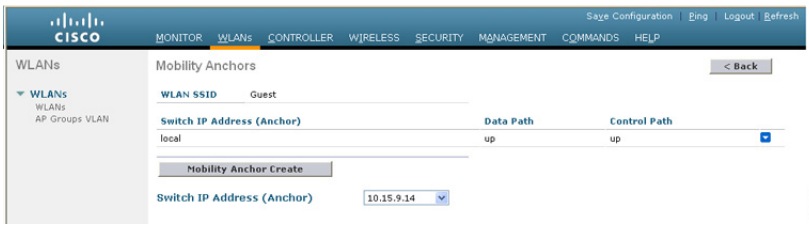
ステップ 3　プルダウン選択リストから、アンカー コントローラを表す IP アドレスを選択します。この IP アドレスの隣に「(Local)」と表示されています。

ステップ 4　[Mobility Anchor Create] をクリックします。（図 10-29 を参照）。

図 10-29　ゲスト WLAN モビリティ アンカーの定義

ゲスト WLAN モビリティ アンカーは、*ローカル*であることに注意してください（図 10-30 を参照）。

図 10-30　ゲスト モビリティ アンカーの確認



ゲスト WLAN のモビリティ アンカーはアンカー WLC 自体なので、データとコントロール パスのステータスは常に「up」と表示されます。「up」と表示されない場合、ローカル WLC をアンカーとして [Switch IP Address (Anchor)] ドロップダウン メニューから選択したことを確認します。

ステップ 5　ゲスト N+1 冗長性を実装している場合、展開されている追加のアンカー WLC ごとに WLAN の設定を繰り返します。それ以外の場合、これでゲスト WLAN をアンカー WLC 上で作成するのに必要な設定手順が完了します。

ゲスト アカウント管理

- ゲスト資格情報をローカルのアンカー コントローラ上で管理する場合は、次のいずれかの方法で資格情報を作成して適用できます。
- Lobby Ambassador 管理者またはスーパー ユーザ / ルート管理者アカウントを使用する
- コントローラ上で直接、ローカルのロビー管理者アカウントまたは読み取り / 書き込みアクセスできるその他の管理アカウントを使用する

管理システムを使用したゲスト管理

次の設定例では、管理システム 4.1.83 以降がインストールおよび設定され、Lobby Ambassador のアカウントが作成されているものとします。

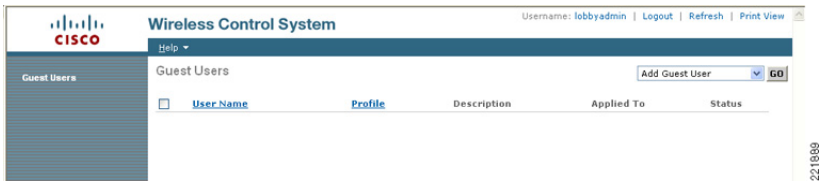
（注）　ゲスト テンプレートを作成する前に、個々の WLC 設定が管理システムと同期していることを確認してください。

システム管理者が割り当てた Lobby Ambassador の資格情報を使用して管理システムにログインします（図 10-31 を参照）。

図 10-31　Lobby Ambassador

ログインすると、図 10-32 に示すような画面が表示されます。

図 10-32　Cisco Prime Infrastructure のロビー管理者インターフェイス



（注）　Cisco Prime Infrastructure は、正式には WCS および NCS と呼ばれていました。

ゲスト テンプレートには、次の 2 種類があります。

- [Add Guest User] テンプレートを使用すると、管理者がゲスト資格情報を作成し、ただちに 1 つ以上のアンカー WLC に適用できます。
- [Schedule Guest User] テンプレートを使用すると、管理者が将来の月、日、時刻に 1 つ以上のアンカー WLC に適用されるゲスト資格情報を作成できます（図 10-33 を参照）。

図 10-33　ゲスト ユーザ テンプレート オプション

ゲスト ユーザの追加テンプレートの使用

ステップ 1　プルダウン選択リストから、[Add Guest User] を選択して [GO] をクリックします。

ステップ 2　図 10-34 に示すようなテンプレートが表示されます。

図 10-34　　ゲスト ユーザの追加テンプレート

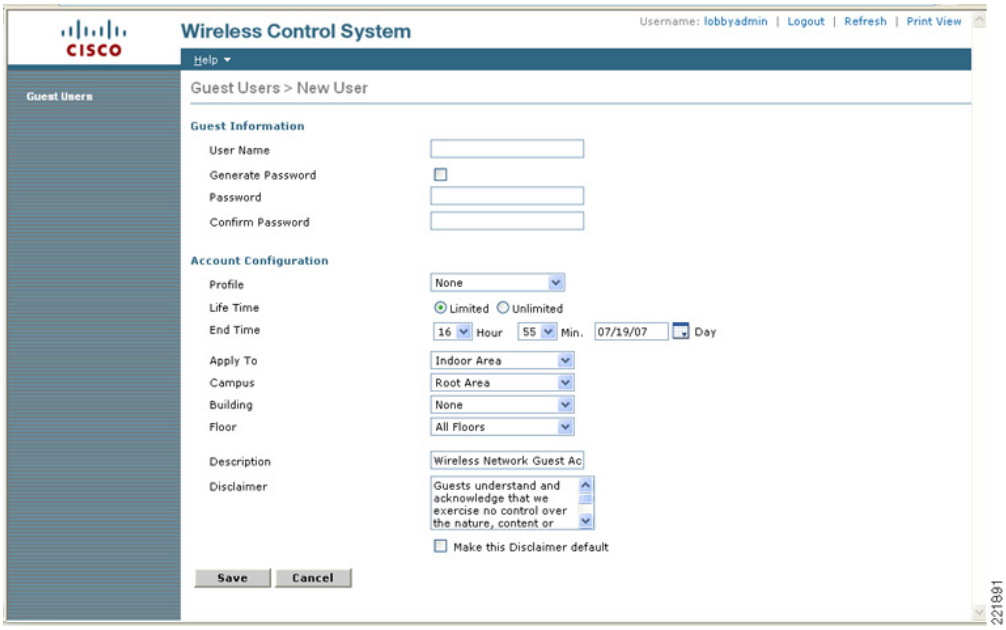
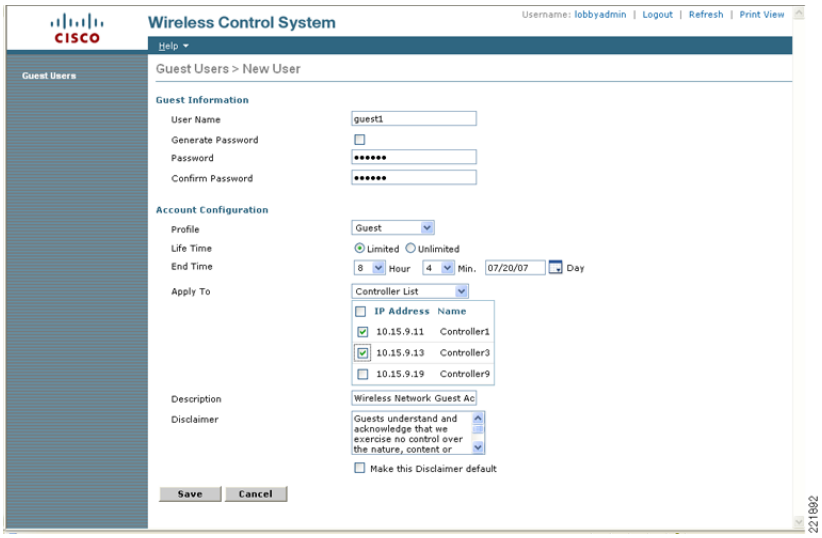


図 10-35 は、ゲスト ユーザ アカウント作成の例を示しています。

図 10-35　ゲスト ユーザ アカウントの作成



ステップ 3　[Guest Information] にユーザ名とパスワードを入力します。

パスワードは大文字と小文字が区別されます。ユーザ名は、24 文字以下に制限されています。管理者には、[Generate Password] チェックボックスをオンにすることによって、パスワードの自動生成を許可するオプションもあります。

ステップ 4　[Account Configuration] で、次の項目を選択します。

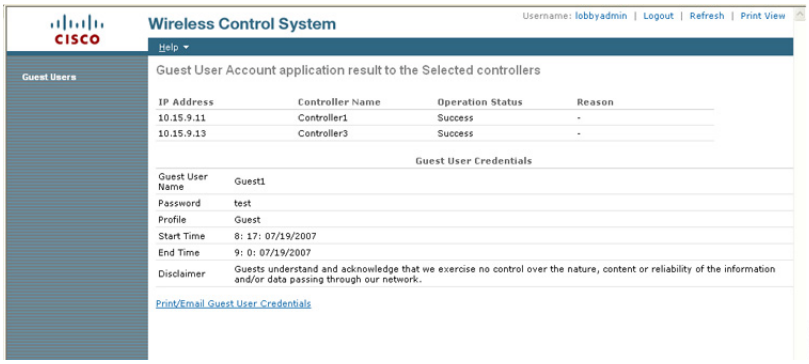
- [Profile]：プルダウン選択リストに、L3 Web ポリシーが設定された WLAN（SSID）のリストが表示されます。
- [Life Time]：[Limited] または [Unlimited] を選択します。
- [End Time]：ゲスト アカウントが [Limited] の場合、資格情報の有効期限が切れる月、日、時刻を選択します。
- [Apply To]：プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。

（注）　図 10-35 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的/地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1）WLAN 展開が管理システム マッピング データベースに統合されている場合、2）ゲスト WLAN（Web ポリシーが設定された WLAN）がモビリティ アンカーを使用しない場合に限られます。

- [Description]：説明を入力します 説明は、[Security] > [Local Net Users] で資格情報を適用する WLC に表示されます。これはゲストに送信できる E メールにも含まれ、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。
- [Disclaimer]：ゲスト ユーザに送信できる E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

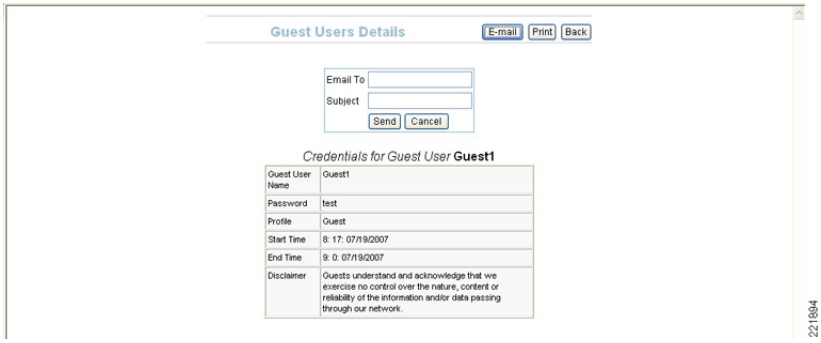
ステップ 5　完了したら、[Save] をクリックします。図 10-36 に示すサマリ画面が表示され、資格情報がアンカー コントローラに適用されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

図 10-36　ゲスト アカウントの正常な作成



ステップ 6　[Print/Email Guest User Credentials] をクリックします。図 10-37 に示すような画面が表示されます。

図 10-37　ゲスト ユーザ詳細の印刷または E メールでの送信



（注）　ゲスト アカウント情報のユーザへの E メール送信をサポートするように SMTP メール サーバを設定する方法の詳細は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html）を参照してください。

アカウントの詳細を印刷または E メールで送信すると、図 10-38 に示すような画面が表示されます。[User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、[User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択することにより、ゲスト アカウントを削除できます。

図 10-38　Cisco Prime Infrastructure ゲスト ユーザのサマリ

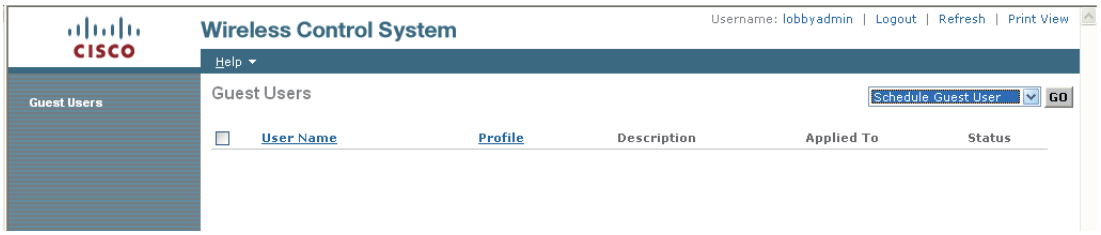
（注）　ユーザがアクティブな状態で Cisco Prime Infrastructure からユーザ テンプレートを削除すると、そのユーザの認証が解除されます。

ゲスト ユーザのスケジュール テンプレートの使用

ゲスト アカウントの設定の詳細は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html）を参照してください。

図 10-39 は、ゲスト ユーザ テンプレート オプションを示しています。

図 10-39　ゲスト ユーザ テンプレート オプション



ステップ 1　プルダウン選択リストから、[Schedule Guest User] を選択して [Go] をクリックします。

図 10-40 に示すようなテンプレートが表示されます。

図 10-40　ゲスト ユーザのスケジュール テンプレート

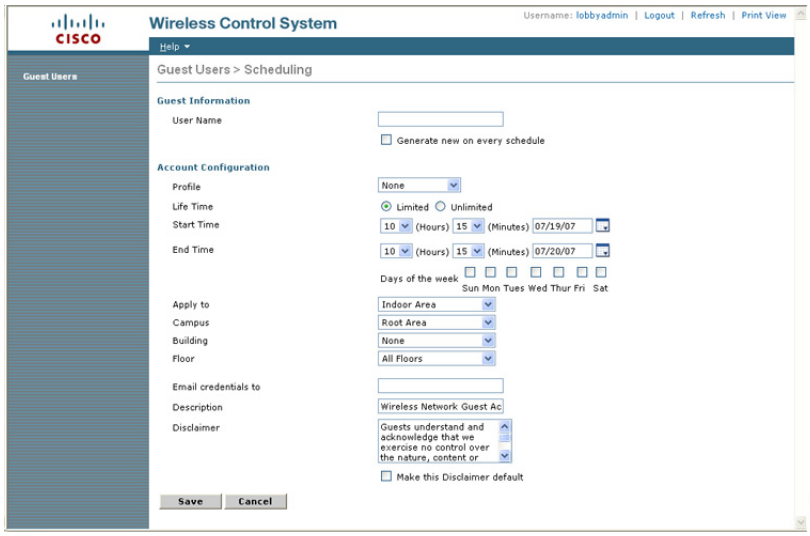
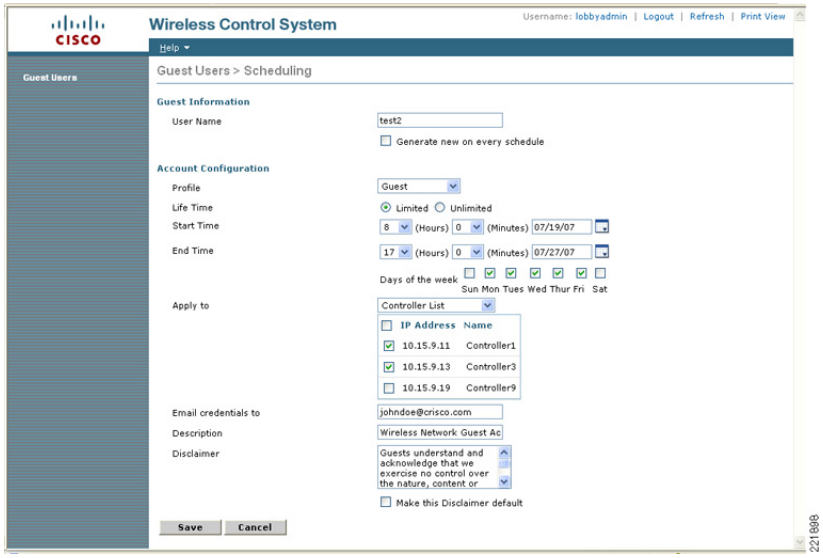


図 10-41 は、ゲスト ユーザ アカウントのスケジュールの作成例を示しています。

図 10-41　ゲスト ユーザ アカウントのスケジュールの作成



ステップ 2　[Guest Information] にユーザ名を入力します。ユーザ名の長さは、24 文字まで可能です。スケジュールベースのテンプレートを使用する場合、管理者には、アクセスが提供される新しい日ごとに、ユーザ名が自動生成できるようになるオプションもあります。また、このテンプレートを使用する場合、ユーザ パスワードが自動生成されます。手動でパスワードを割り当てるオプションはありません。

ステップ 3　[Account Configuration] で、次の項目を選択します。

- [Profile]：プルダウン選択リストに、L3 Web ポリシーが設定された WLAN（SSID）のリストが表示されます。
- [Life Time]：[Limited] または [Unlimited] を選択します。
- [Start Time]：アカウントがアクティブになる時刻、月、日を選択します。

（注）　開始時刻は、アカウントが作成される当日に開始することはできません。開始日は、アカウントが作成される日から 1 日以上過ぎている必要があります。

- [End Time]：アカウントが制限されている場合、終了時刻、月、日を選択します。

（注）　開始日から終了日までの期間は、30 日を超えることはできません。

- [Days of Week]：アカウントの有効期間に応じて、管理者はアクセスできる曜日を管理できます。アクセスが許可される曜日の隣のチェックボックスをクリックします。

（注）　[Days of the Week] が選択されている場合、開始および終了時刻は、それぞれの日のうちでアクセス可能な期間を表します。有効期限が切れるとその日のうちに、Cisco Prime Infrastructure は適用可能なコントローラから資格情報を削除します。アクセスが許可される新しい日 / 間隔ごとに、Cisco Prime Infrastructure によって新しいパスワード（必要に応じてユーザ名）が自動生成され、ゲスト ユーザに E メールで送信され、新しい資格情報が適用可能な WLC に再適用されます。[Days of the Week] が定義されていない場合、開始日時に基づいてアクセスが開始され、終了日時まで常にアクティブになります。

- [Apply To]：プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。

（注）　図 10-41 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的 / 地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1）WLAN 展開が Cisco Prime Infrastructure マッピング データベースに統合されている場合、2）ゲスト WLAN（Web ポリシーが設定された WLAN）がモビリティ アンカーを使用しない場合に限られます。

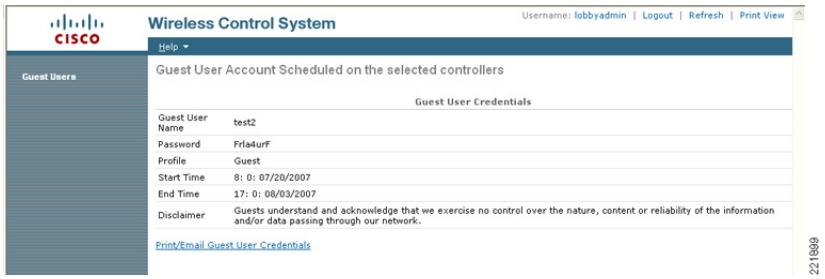
- [E-mail Credentials to]：アカウントを設定するユーザの E メール アドレスを入力します。これは必須フィールドです。

（注）　SMTP メール サーバは、ゲスト アカウント情報の送信に使用できるように、Cisco Prime Infrastructure で設定する必要があります。詳細については、次の項を参照してください。
http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0admin.html

- [Description]：説明を入力します。説明は、[Security] > [Local Net Users] で資格情報を適用する WLC に表示されます。説明は、ゲストに送信できる E メールにも含まれ、どのような資格情報をネットワークへのアクセスに使用するかを知らせます。
- [Disclaimer]：ゲスト ユーザに送信される E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

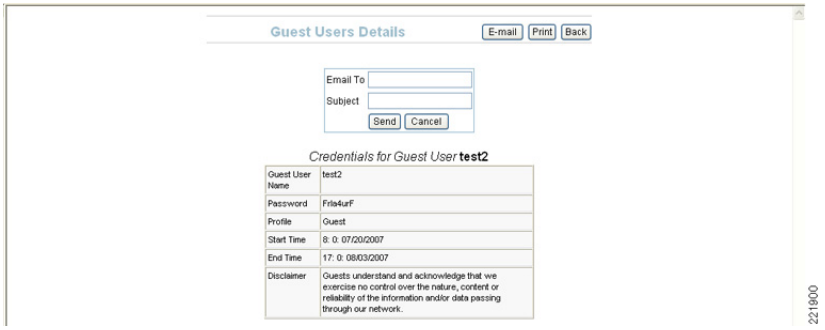
ステップ 4　完了したら、[Save] をクリックします。図 10-42 に示す画面が表示され、スケジュールされたアカウントが作成されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

図 10-42　スケジュールされたアカウントの正常な作成



ステップ 5　必要に応じて、[Print/Email Guest User Credentials] をクリックします。図 10-43 に示すような画面が表示されます。

図 10-43　ゲスト ユーザ詳細の印刷または E メールでの送信



アカウントの詳細を印刷または E メールで送信すると、図 10-44 に示すようなサマリ画面が表示されます。[User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、[User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択することにより、ゲスト アカウントを削除できます。

図 10-44　Cisco Prime Infrastructure ゲスト ユーザのサマリ

（注）　ユーザがアクティブな状態で Cisco Prime Infrastructure からユーザ テンプレートを削除すると、そのユーザの認証が解除されます。

これで、Cisco Prime Infrastructure の Lobby Ambassador インターフェイスを使用したゲスト アカウントの作成に必要な手順は終了です。

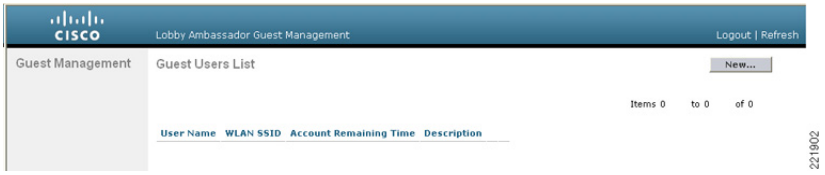
アンカー コントローラ上でのゲスト資格情報の直接管理

次の手順では、ネットワーク管理者が、ロビー管理者の特権を使用して 1 つ以上のアンカー コントローラ上にローカル管理アカウントを設定しているものとします。

ステップ 1　システム管理者が割り当てたロビー管理者の資格情報を使用してアンカー コントローラにログインします。コントローラの Web 管理に対して HTTP/HTTPS を許可するには、ファイアウォールを通してコンジットを開く必要があります。「アンカー コントローラの位置決め」（P.10-6）を参照してください。

ログインすると、図 10-53 に示すような画面が表示されます。

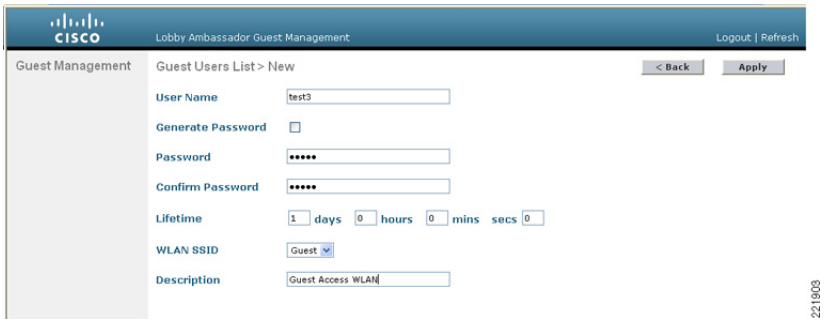
図 10-45　アンカー コントローラのログイン



ステップ 2　[New] をクリックします。

図 10-46 に示すような画面が表示されます。

図 10-46　ローカル WLC ゲスト資格情報の作成



ステップ 3　ユーザ資格情報を作成するには、次の手順を実行します。

a. ユーザ名とパスワードを入力します（手動または自動）。

b. ゲスト アカウントを適用する WLAN/SSID を選択します。その際、L3 Web ポリシーが設定された WLAN だけが表示されます。

c. 資格情報の有効期間を入力します。

d. ユーザの説明を入力します。

ステップ 4　[Apply] をクリックします。

図 10-47 に示すような画面に、新しく追加されたゲスト ユーザが表示されます。

図 10-47　アンカー WLC ゲスト ユーザのリスト

この画面では、次の機能を実行できます。

- 既存のユーザの編集（右端のリンク。非表示）
- 既存のユーザの削除（右端のリンク。非表示）
- 新規ユーザを追加します。

ユーザ アカウントの最大数の設定

コントローラ上で指定可能なゲスト ユーザ アカウントのデフォルト数は 512 です。この値は、次の手順を実行することによって変更できます。

ステップ 1　[Security] タブをクリックします。（図 10-48 を参照）。

図 10-48　ユーザ アカウントの最大数の設定

ステップ 2　左側のペインで、AAA プロパティの下の [General] をクリックします。

ステップ 3　ユーザ データベース エントリの最大数を設定します（512 ～ 2,048 の間）。

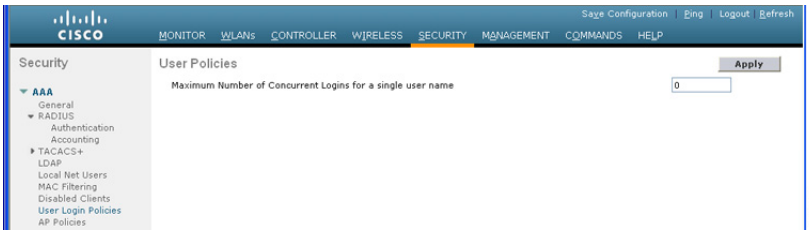
ステップ 4　[Apply] をクリックします。

最大同時ユーザ ログイン

WWLC 上のローカル ユーザ アカウントの同時ログインの最大数は、設定が可能です。同時ログイン数を無制限にする場合は、値を 0 にします。値を 1 ～ 8 に制限することもできます。ユーザ ログインの最大数は、次の手順で設定されます。

ステップ 1　[Security] タブをクリックします。（図 10-49 を参照）。

図 10-49　　ユーザ ログイン ポリシー



ステップ 2　左ペインで、[AAA] の [User Login Policies] をクリックします。

ステップ 3　同時ユーザ ログインの最大数を設定します（0 ～ 8 の間）。

ステップ 4　[Apply] をクリックします。

ゲスト ユーザの管理に関する注意事項

次の警告に注意してください。

- ゲスト アカウントは、上記の方法か、2 つの方法を同時に使用して追加できます。
- Cisco Prime Infrastructure の使用時に、コントローラの設定が最近 Cisco Prime Infrastructure と同期されていない場合、ロビー管理者はローカルのアンカー コントローラ上で作成された可能性のあるユーザ アカウントを表示できないことがあります。この場合に、すでに WLC で設定されているユーザ名で Cisco Prime Infrastructure のロビー管理者がアカウントを追加しようとすると、ローカル設定が Cisco Prime Infrastructure 設定で上書きされます。
- ローカル管理者がユーザ アカウントをローカルのコントローラ上に追加するときには、Cisco Prime Infrastructure 経由で作成されたものも含めて、作成されたすべてのアカウントを表示できます。
- ゲスト ユーザが WLAN に対して認証された状態で、資格情報が Cisco Prime Infrastructure またはローカルのコントローラ上から削除されると、ユーザ トラフィックのフローが停止し、ユーザの認証が解除されます。

その他の機能とソリューション オプション

Web ポータル ページの設定と管理

内部 Web サーバと関連機能は、ローカルのアンカー コントローラ上でホストされます。認証またはパススルー用の Web ポリシーを使用するように WLAN を設定した場合は、デフォルトで内部 Web サーバが呼び出されます。それ以上の設定は必要ありません。内部ポータルには、オプションの設定パラメータがいくつか用意されています。

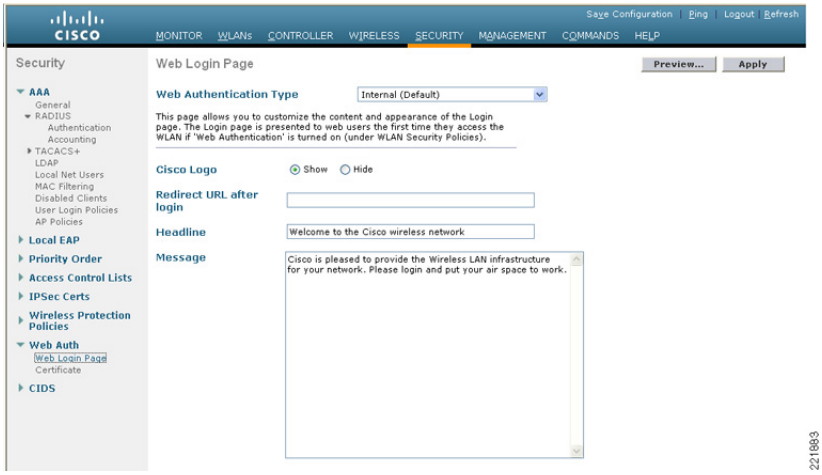
内部 Web ページの管理

ステップ 1　[Security] タブをクリックします。

ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。

図 10-50 に示すような設定画面が表示されます。ポータル ページに表示される見出しとメッセージ情報を変更できます。また、認証後のリダイレクト URL を選択することもできます。

図 10-50　Web ログイン ページ設定画面



ステップ 3　[Apply] をクリックします。

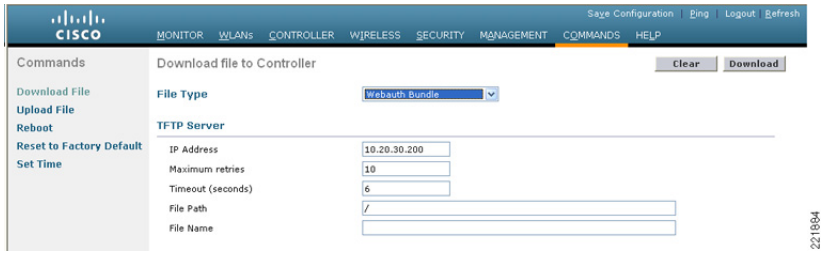
ステップ 4　必要に応じて、[Preview] をクリックして、ユーザに表示されるリダイレクト先のページを確認します。

Web ページのインポート

カスタマイズされた Web ページをダウンロードして、ローカルのアンカー コントローラ上に保存できます。カスタマイズされた Web ページをインポートするには、次の手順を実行します。

ステップ 1　[Commands] タブをクリックします（図 10-51 を参照）。

図 10-51　Web ページのインポート



ステップ 2　[File Type] で [Web Auth Bundle] を選択します。

ステップ 3　ファイルが存在する TFTP サーバの IP アドレスとファイル パスを指定します。

ステップ 4　[Download] をクリックして、ダウンロードを開始します。

Web 認証バンドルをダウンロードする際には、次の点に注意してください。

- プルダウン選択リストから [Web Auth Bundle] を選択して、ファイルがコントローラ上の正しいディレクトリに保存されるようにします。
- [Web Auth Bundle] は、カスタム Web ログイン ページにアソシエートされている、HTML ファイルとイメージ ファイルの **.tar** ファイルである必要があります。ダウンロード後に、WLC によってファイルが untar され、適切なディレクトリに格納されます。
- [Web Auth Bundle]（**.tar** ファイル）は、1MB より大きくてはなりません。
- HTML ログイン ページのファイル名は、**login.html** にする必要があります。

カスタマイズされた Web ページのダウンロードと使用方法の詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcssol.html#wp1065703

インポートした Web 認証ページの選択

コントローラにダウンロードしたカスタマイズ済みの Web 認証ページを使用するには、次の手順を実行します。

ステップ 1　[Security] タブをクリックします。

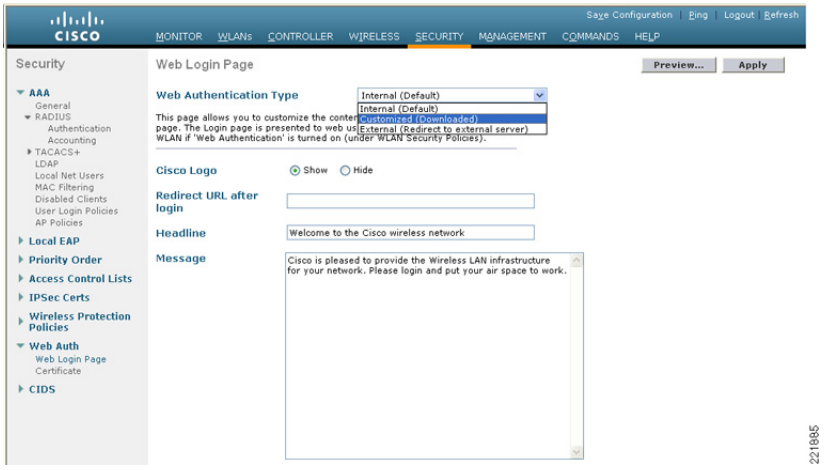
ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。

ステップ 3　[Web Authentication Type] プルダウン選択リストから [Customized (Downloaded)] を選択します。

ステップ 4　[Preview] をクリックして、ダウンロードしたページを表示します。

ステップ 5　最後に、[Apply] をクリックします（図 10-52 を参照）。

図 10-52　インポートした Web 認証ページの選択



内部 Web 証明書の管理

Web 認証ログイン ページでは、ユーザ資格情報を保護するために SSL が使用されます。コントローラでは、簡単な自己署名証明書が使用されます。証明書が自己署名されたものであるため、ゲスト ユーザが図 10-53 に示すような認証ページにリダイレクトされると、次のようなポップアップ アラートが表示されます。

図 10-53　Web 証明書セキュリティ アラート（IE6）

この時点で、[Yes] をクリックして先に進むか、[View Certificate] を選択してそのページを信頼されたサイトとして手動でインストールできます。Web サーバでは、「アンカー WLC の設置およびインターフェイスの設定」（P.10-14）で設定された仮想インターフェイスの IP アドレスが発信元アドレスとして使用されます。ホスト名を IP アドレスと共に指定する場合は、ホスト名が DNS によって解決されるときに、次の条件を満たすようにする必要があります。

- クライアントが Web 認証ページにリダイレクトされる。
- ユーザが、ホスト名とホスト IP アドレスの矛盾が原因の Web 認証エラーに遭遇しない。

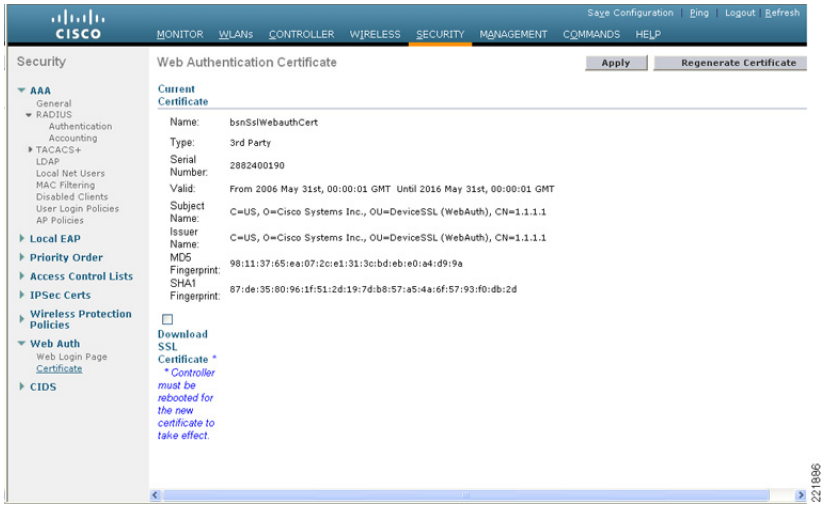
外部 Web 証明書のインポート

信頼できるルート CA によって発行された正式な Web 証明書が必要な場合は、次の手順を実行することによって、コントローラにダウンロードできます。

ステップ 1　[Security] タブをクリックします。

左側のペインで、[Web Auth] をクリックして、[Certificate] をクリックします （図 10-54 を参照）。

図 10-54　外部 Web 証明書のインポート



ステップ 2　[Download SSL Certificate] チェックボックスをオンにします。

ステップ 3　証明書のダウンロードに必要な情報を各フィールドに入力します。

ステップ 4　[Apply] をクリックします。

ステップ 5　証明書をダウンロードしたら、サーバを再起動します。

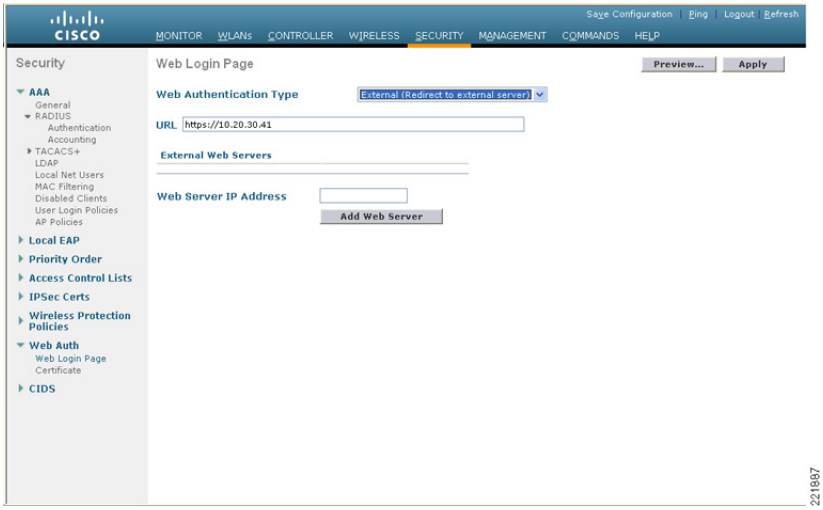
外部 Web リダイレクションのサポート

企業では、有線のゲスト アクセスまたは NAC 機能をサポートする Web ポータル システムがすでに展開されている場合があります。そのような場合は、無線ゲスト ユーザを外部 Web ポータルにリダイレクトするように、アンカー コントローラを次の手順で設定できます。

ステップ 1　[Security] タブをクリックします。

ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。（図 10-55 を参照）。

図 10-55　外部 Web リダイレクションのサポート



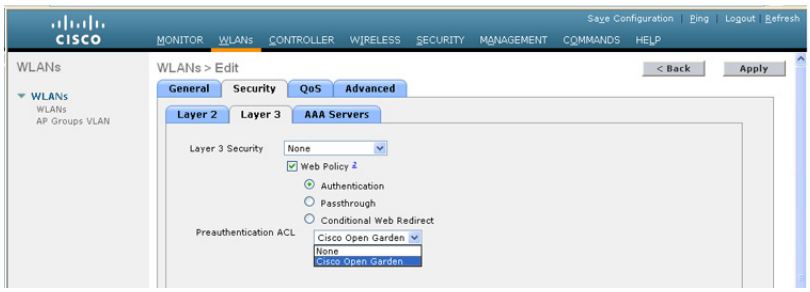
ステップ 3　[Web Server IP] フィールドと [URL] フィールドに入力します。

ステップ 4　[Apply] をクリックします。

アンカー WLC 事前認証 ACL

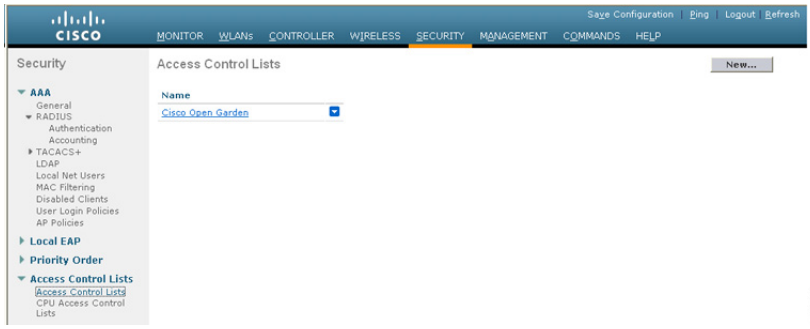
事前認証 ACL は、ゲスト WLAN に適用できます。これにより、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続できます。事前認証 ACL はゲスト WLAN のレイヤ 3 セキュリティ設定で適用されます。有効になっている場合、アンカー WLC 上でのみ実行されます（図 10-56 を参照）。

図 10-56　WLAN 事前認証 ACL



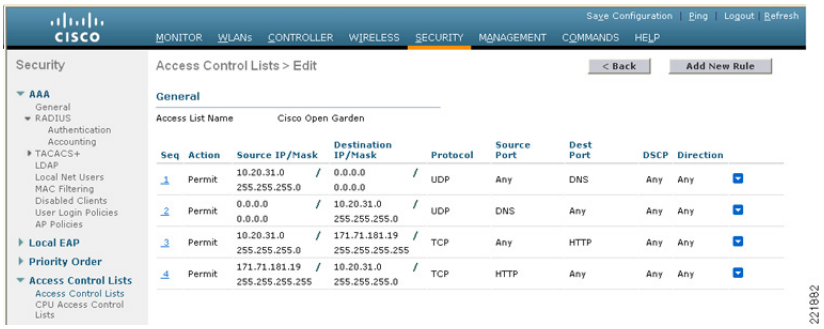
特定の ACL は、[Security] > [Access Control Lists] で設定されます（図 10-57 および図 10-58 を参照）。

図 10-57　WLC アクセス コントロール リスト



（注）　事前認証 ACL が Web 認証ポリシーと共に使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト /URL に解決して接続することができません。

図 10-58　事前認証 ACL の例



アンカー コントローラ DHCP 設定

アンカー コントローラがゲスト アクセス WLAN の DHCP サービスを管理する場合は、次の手順を実行します。

（注）　アンカー コントローラは、ゲスト N+1 冗長性を実装している場合、DHCP サービスを管理するために使用することはできません。なぜなら、2 つ以上の WLC 間で単一のゲスト VLAN/ サブネットのアドレス リースを同期するメカニズムがないからです。

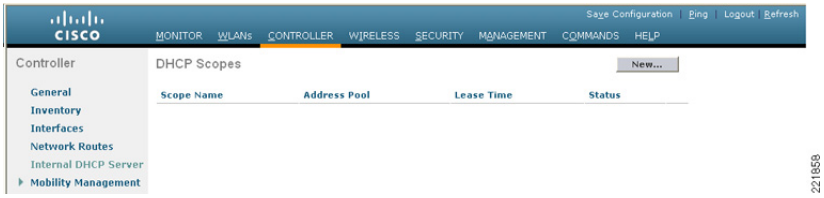
新しい DHCP スコープのアンカー コントローラへの追加

ステップ 1　[Controller] タブをクリックします。

ステップ 2　左側のペインで、[Internal DHCP Server] をクリックします。

ステップ 3　[New] をクリックします。（図 10-59 を参照）。

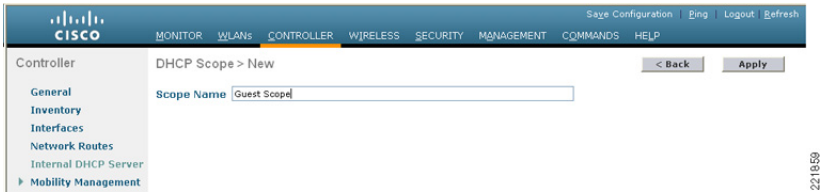
図 10-59　新しい DHCP スコープの追加



スコープ名の定義

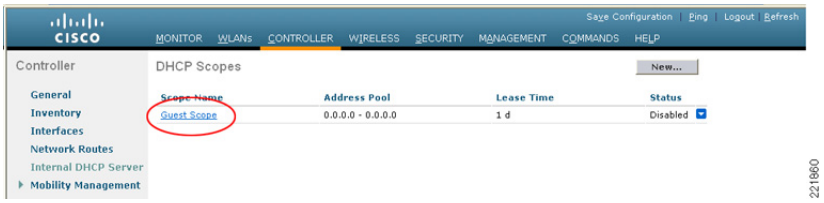
ステップ 4　スコープ名を定義して、[Apply] をクリックします。（図 10-60 を参照）。

図 10-60　スコープ名の定義



ステップ 5　[Scope Name] をクリックして、編集します （図 10-61 を参照）。

図 10-61　DHCP スコープの編集



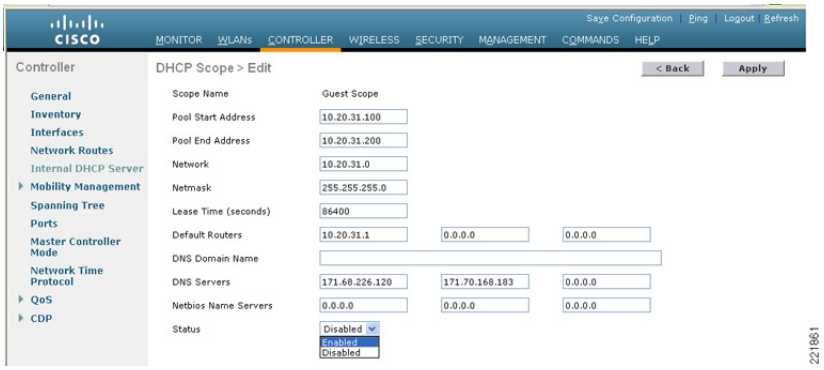
スコープ プロパティの定義

ステップ 6　最低限必要な次の情報を定義します。

- プールの開始と終了
- ネットワーク
- マスク
- デフォルト ルータ
- DNS サーバ

ステップ 7　[Status] として [Enabled] を選択し、[Apply] をクリックします （図 10-62 を参照）。

図 10-62　スコープ プロパティの設定と有効化



外部 RADIUS 認証

ゲスト ユーザの認証で説明したように、ゲスト資格情報をローカルのアンカー コントローラ上に作成して保存する代わりに、外部 RADIUS サーバを使用してゲスト ユーザを認証できます。この方法を使用する場合は、ゲスト アカウント管理で説明したロビー管理機能は使用できません。その他のいくつかのゲスト管理システムと外部 RADIUS サーバの併用が考えられます。

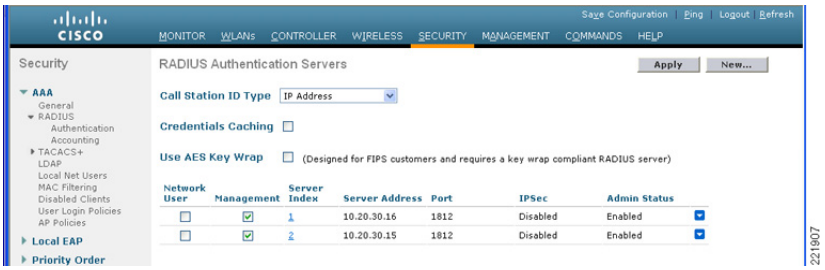
外部 RADIUS サーバを使用するようにゲスト WLAN を設定するには、アンカー コントローラ上で次の設定手順を実行します。

RADIUS サーバの追加

ステップ 1　[Security] タブをクリックします。

サマリ画面が表示されます （図 10-63 を参照）。

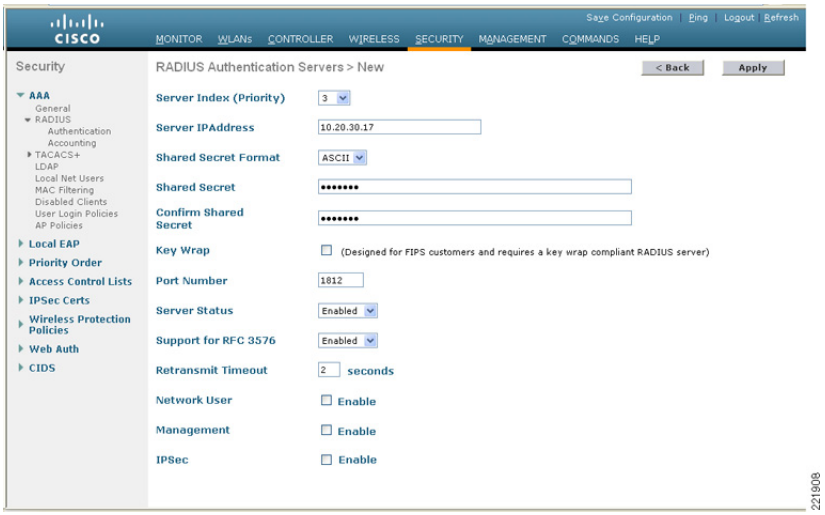
図 10-63　[Summary] 画面



ステップ 2　[New] をクリックします。

図 10-64 に示すような画面が表示されます。

図 10-64　RADIUS サーバ設定の定義



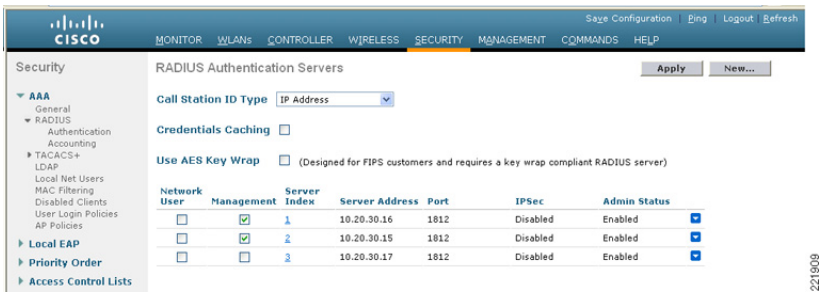
ステップ 3　RADIUS サーバの設定を定義するには、RADIUS サーバ上で指定したように、IP アドレス、共有秘密、および認証ポート番号を設定します。

[Network User] チェックボックスがオフになっていると、RADIUS サーバは、特定の WLAN の RADIUS 設定でそのサーバが明示的に選択されているときにだけユーザ認証に使用されます。また、[Network User] チェックボックスがオンになっていると、RADIUS サーバが、そのサーバの優先順位に基づいて、すべてのユーザ認証に使用されます。

ステップ 4　[Apply] をクリックします。

図 10-65 に示すサマリ画面には、新しく追加されたサーバが表示されます。

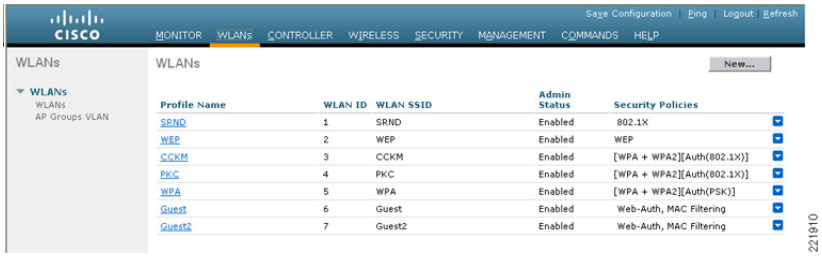
図 10-65　[Summary] 画面



ステップ 5　RADIUS サーバを選択するには、[WLANs] タブをクリックします。

図 10-66 に示すような画面が表示されます。

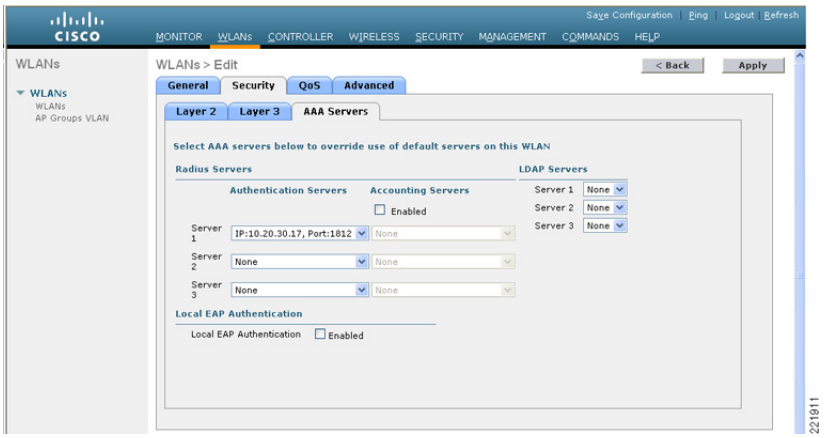
図 10-66　[WLANs] タブ



ステップ 6　ゲスト WLAN を探して、その [Profile Name] をクリックします。

図 10-67 に示すように、ゲスト WLAN の設定画面が表示されます。

図 10-67　ゲスト WLAN の設定画面



ステップ 7　[WLAN Security] タブで [AAA Servers] を選択します。

ステップ 8　[Authentication Servers] のプルダウン選択リストから、Web 認証に使用する RADIUS サーバを選択します。

外部アクセス コントロール

この章で説明した中央集中型ゲスト アクセス トポロジは、Cisco NAC Appliance などの外部アクセス コントロール プラットフォームと統合できます。

このシナリオでは、企業で、有線ゲスト アクセス サービスをサポートするためのアクセス コントロール プラットフォームがインターネットの DMZ に展開されているものとします（図 10-68 を参照）。

図 10-68　外部アクセス コントロールを使用した無線ゲスト アクセス

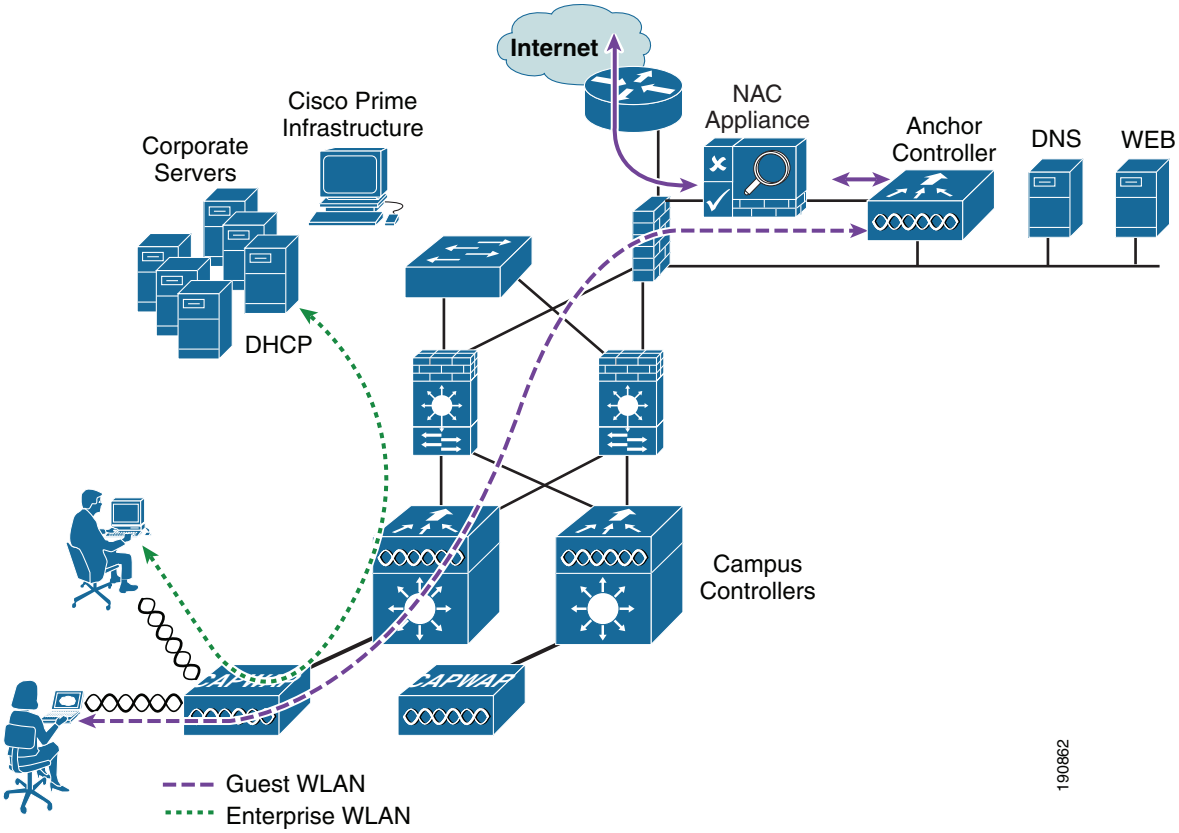


図 10-68 に示すように、無線ゲスト アクセス トポロジは、アンカー コントローラ上のゲスト VLAN インターフェイスが、ファイアウォールや境界ルータに接続する代わりに Cisco NAC Appliance などのアクセス コントロール プラットフォームの inside インターフェイスに接続する点を除いて同じです。

このシナリオでは、NAC Appliance が、リダイレクション、Web 認証、およびその後のインターネットへのアクセスを処理します。キャンパス コントローラとアンカー コントローラは、NAC アプライアンスまたはその他のいくつかのプラットフォームを使用してゲスト アクセスを制御している DMZ に全社的なゲスト WLAN トラフィックをトンネルするためだけに使用されます。

ゲスト WLAN、キャンパス、およびアンカー コントローラの設定は、上記の例と同じです。

唯一の違いは、ゲスト WLAN のセキュリティ設定でレイヤ 3 Web ポリシーが有効になっていない点です（図 10-69 および図 10-70 を参照）。

図 10-69　　ゲスト WLAN のレイヤ 3 セキュリティ ポリシー

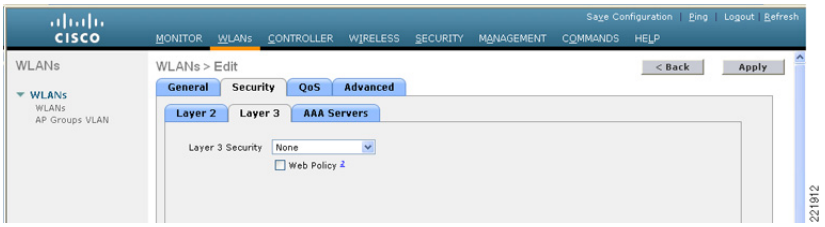
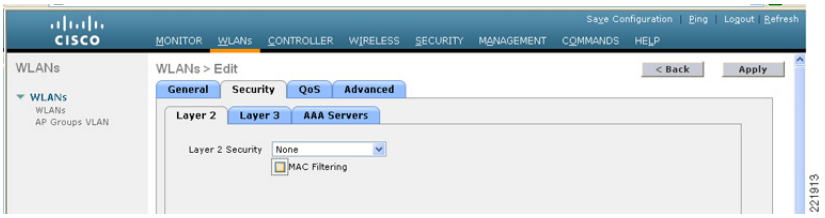


図 10-70　　ゲスト WLAN L2 セキュリティ設定



上記の設定では、セキュリティ ポリシーを使用せずに WLAN が設定されます。ゲスト トラフィックは、アンカー コントローラを通過して、Cisco NAC Appliance の inside インターフェイスまたは信頼されていないインターフェイスに到達し、ユーザが認証されるまでブロックされます。

DHCP は、ローカルのコントローラ上でホストするか、外部の NAC Appliance または専用サーバ経由でホストできます。

Cisco NAC Appliance またはその他の外部アクセス コントロール プラットフォーム固有の設定については、この章では説明しません。詳しい設定ガイドラインについては、プラットフォーム固有のマニュアルを参照してください。

ゲスト アクセス機能の確認

ゲスト アクセス サービスは、ユーザが次の条件を満たしている場合に正しく機能します。

- ゲスト WLAN にアソシエートできる。
- DHCP 経由で IP アドレスを受信する。
- ブラウザを開くと、Web 認証ページにリダイレクトされる。
- 資格情報を入力して、インターネット（またはその他の許可されたアップストリーム サービス）に接続する。

ゲスト アクセスのトラブルシューティング

以降の確認作業とトラブルシューティング作業は、次のことを前提としています。

- このソリューションでは、アンカー コントローラ上の Web 認証機能が使用されている。
- ユーザ資格情報が、ローカルのアンカー コントローラ上で作成および保存されている。

次のようなさまざまな症状のトラブルシューティングを実行するには、少なくとも、外部のキャンパス コントローラからアンカー コントローラに ping できる必要があります。それが不可能な場合は、ルーティングを確認します。

その次に、次の高度な ping コマンドを実行できる必要があります。これらのコマンドは、コントローラのシリアル コンソール インターフェイスを通してだけ実行できます。

- **mping** *neighbor WLC ip*

  このコマンドは、CAPWAP 制御チャネルを通して近隣のコントローラに ping します。

- **eping** *neighbor WLC ip*

  このコマンドは、CAPWAP データ チャネルを通して近隣のコントローラに ping します。

標準の ICMP ping が通っても mping が通らない場合は、各 WLC のデフォルトのモビリティ グループ名が同じであることと、各 WLC の IP、MAC、およびモビリティ グループ名がすべての WLC のモビリティ メンバ リストに入力されていることを確認します。

ping と mping は通っても eping が通らない場合は、ネットワークで IP プロトコル 97（Ethernet-over-IP）がブロックされていないことを確認します。

ユーザがゲスト WLAN に接続できない

- ゲスト WLAN をサポートするアンカー コントローラとすべての外部コントローラでゲスト WLAN が有効になっていることを確認します。
- ゲスト WLAN SSID がブロードキャストされていることを確認します。
- クライアント アダプタまたはソフトウェアの設定を確認します。

ユーザが DHCP 経由で IP アドレスを取得できない

- WLAN の設定がアンカー コントローラ上と外部コントローラ上で同じであることを確認します（WLAN インターフェイスおよびモビリティ アンカーを除く。「アンカー WLC 上でのゲスト WLAN の設定」（P.10-28）を参照）。
- ゲスト WLAN がアンカー WLC 上で有効になっていることを確認します。
- アンカー コントローラのゲスト VLAN インターフェイスの設定で、DHCP サーバのアドレスが適切かどうかをチェックします。
  - 外部 DHCP サーバを使用している場合は、IP アドレスが外部サーバのアドレスになっている必要があります。
  - アンカー コントローラから外部 DHCP サーバにアクセスできることを確認します。
  - DHCP サービスにアンカー コントローラを使用している場合は、DHCP サーバの IP アドレスがコントローラの管理 IP アドレスになっている必要があります。
  - コントローラ上で DHCP スコープが設定され有効になっていることを確認します。
  - DHCP スコープのネットワーク マスクとゲスト VLAN インターフェイスのマスクが一致していることを確認します。

– DHCP スコープが、ネットワーク インフラストラクチャに割り当てられたすべてのアドレスと重複していないことを確認します。

ユーザが Web 認証ページにリダイレクトされない

次の解決方法では、ユーザがゲスト WLAN にアソシエートして IP アドレスを取得できることを想定しています。

- 有効な DNS サーバが DHCP を介してクライアントに割り当てられていることを確認します。
- DNS サーバがアンカー コントローラから接続可能なことを確認します。
- Web ブラウザで開かれている URL が解決可能なことを確認します。
- Web ブラウザで開かれている URL が HTTP ポート 80 に接続していることを確認します。

（注）　内部 Web 認証サーバは、80 およびユーザが定義したもう 1 つのポート番号以外のポート上の入力要求をリダイレクトしません（「ユーザ リダイレクション」（P.10-10）参照）。

ユーザが認証されない

- アンカー コントローラ上のユーザ資格情報がアクティブなことを確認します。

  通常は、ゲスト資格情報に対して有効期間が設定されます。資格情報は、期限が切れていると、アンカー コントローラ上の [Security] > [Local Net Users] リストに表示されません。Cisco Prime Infrastructure を使用して、ローカルのコントローラ上でユーザ テンプレートを適用し直すか、ユーザ資格情報を作成し直してください。管理システムを使用したゲスト管理およびゲスト資格情報の管理を参照してください。
- ユーザ パスワードを確認します。

ユーザがインターネットまたはアップストリーム サービスに接続できない

- アンカー コントローラと、アンカー コントローラに接続されているファイアウォールまたは境界ルータ間のルーティングを確認します。
- 必要に応じて、ファイアウォールまたはインターネット境界ルータの NAT 設定を確認します。

システム モニタリング

以降では、トラブルシューティングに役立つ可能性のあるいくつかの監視コマンドについて説明します。

アンカー コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

```
Cisco Controller) >show client summary
Number of Clients................................ 1
MAC Address       AP Name            Status         WLAN  Auth  Protocol  Port
----------------  -----------------  -------------  ----  ----  --------  ----
00:40:96:ac:5f:f8  10.15.9.19         Associated     3     Yes   Mobile    1
```

プロトコルが Mobile になっていることに注目してください。Auth フィールドには、実際のユーザの状態が反映されます。ユーザが Web 認証をパスすると、このフィールドに YES と表示されます。パスしなかった場合は、このフィールドに NO と表示されます。

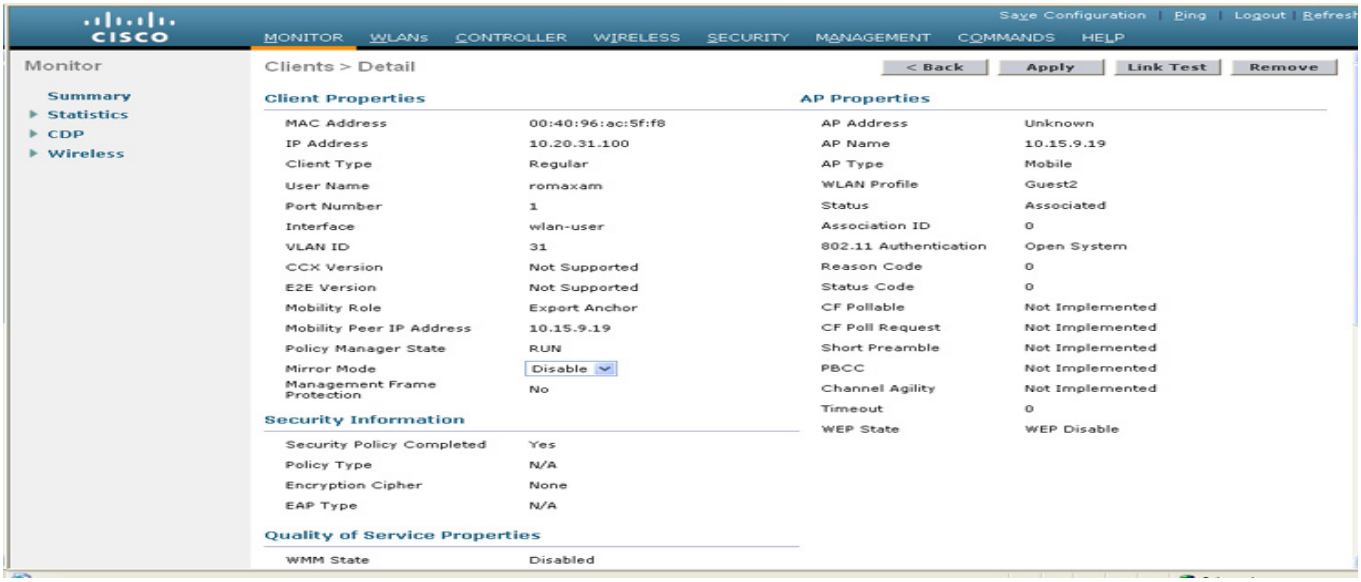
AP 名にも注目してください。これは、外部コントローラ（起点コントローラ）の管理 IP アドレスです。

サマリ情報に示されたクライアントの MAC アドレスを使用して、詳細を表示します。

```
(Cisco Controller) >show client detail 00:40:96:ac:5f:f8
Client MAC Address.............................. 00:40:96:ac:5f:f8
Client Username ................................ romaxam
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 3
BSSID........................................... 00:00:00:00:00:02
Channel......................................... N/A
IP Address...................................... 10.20.31.100
Association Id.................................. 0
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 86316
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.15.9.19
Mobility Move Count............................. 1
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... wlan-user
VLAN............................................ 31
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 0
      Number of Bytes Sent...................... 0
      Number of Packets Received................ 0
      Number of Packets Sent.................... 0
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... Unavailable
      Signal to Noise Ratio..................... Unavailable
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
```

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を得ることができます （図 10-71 を参照）。

図 10-71　[Anchor WLC Monitor] > [Client Detail]



外部のキャンパス コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

```
(WiSM-slot3-1) >show client summary
Number of Clients.............................. 2
MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port
-----------------  -----------------  -------------  ----  ----  --------  ----
00:40:96:ac:5f:f8  AP3_.18e5.7fdc     Associated     1     Yes   802.11g   29
```

アンカー コントローラでは Protocol フィールドが Mobile になっていましたが、同じクライアントに対してこの Protocol フィールドは 802.11g になっていることに注目してください。外部のキャンパス コントローラでは、必ずユーザが Authenticated として表示され、AP name にはクライアントがアソシエートされている実際の AP が反映されます。

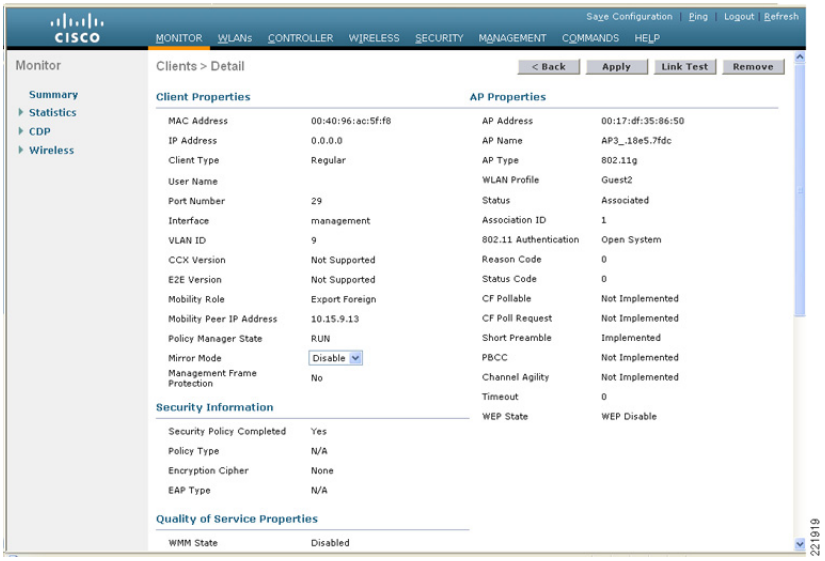
次のコマンドを実行すると、さらに詳しい情報を得られます。

```
(WiSM-slot3-1) >show client detail 00:40:96:ac:5f:f8
Client MAC Address............................. 00:40:96:ac:5f:f8
Client Username ............................... N/A
AP MAC Address................................. 00:17:df:35:86:50
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:17:df:35:86:50
Channel........................................ 11
IP Address..................................... Unknown
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. No CCX support
Mirroring...................................... Disabled
QoS Level...................................... Silver
```

```
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.15.9.13
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... management
VLAN............................................ 9
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 308244
      Number of Bytes Sent...................... 700059
      Number of Packets Received................ 2527
      Number of Packets Sent.................... 1035
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... -75 dBm
      Signal to Noise Ratio..................... 25 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      AP3_.18e5.7fdc(slot 0) .....................
antenna0: 37 seconds ago -73 dBm................. antenna1: 4294510568 seconds ago
-128 dBm
```

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を取得できます（図 10-72 を参照）。

図 10-72　[Foreign WLC Monitor] > [Client Detail]



debug コマンド

シリアル コンソールからは、次のデバッグ コマンドも使用できます。

```
debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable
```