CHAPTER 2

使用する前に

この章では、コントローラの初期設定およびログインの方法を説明します。この章の内容は、次のとおりです。

設定ウィザードの使用方法

（注）　基本的な動作ができるようにコントローラを設定する前に、コントローラのクイック スタート ガイドまたはインストレーション ガイドを参照して、ハードウェアに関する作業を完了してください。

設定ウィザードでは、コントローラ上での基本的な設定を行うことができます。このウィザードは、コントローラを購入した直後やコントローラを工場出荷時のデフォルトにリセットした後に実行します。設定ウィザードは、GUI と CLI のどちらの形式でも使用できます。

（注）　Catalyst 3750G Integrated Wireless LAN Controller Switch でコントローラを設定するには、3750 デバイス マネージャから起動される GUI 設定ウィザードを使用することをお勧めします。手順は、『*Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide*』を参照してください。

（注）　コントローラを工場出荷時のデフォルトに戻す手順については、「コントローラのデフォルト設定へのリセット」（P.4-116）を参照してください。

コントローラのコンソール ポートの接続

基本的な動作ができるようにコントローラを設定するには、VT-100 ターミナル エミュレーション プログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行する PC にコントローラを接続する必要があります。

ステップ 1　ヌルモデム シリアル ケーブルの一端をコントローラのコンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。

（注）　5500 シリーズ コントローラでは、RJ-45 コンソール ポートと USB コンソール ポートのどちらでも使用できます。USB コンソール ポートを使用する場合は、5 ピン ミニ タイプ B コネクタをコントローラの USB コンソール ポートに接続し、もう一端を PC の USB タイプ A ポートに接続します。Windows PC を USB ポートに接続するのが初めての場合は、USB コンソール ドライバをインストールするための画面が表示されます。インストール画面の指示に従って、ドライバをインストールしてください。USB コンソール ドライバは PC 上の COM ポートにマッピングされるので、この COM ポートにターミナル エミュレータ アプリケーションをマッピングする必要があります。

ステップ 2　PC の VT-100 ターミナル エミュレーション プログラムを起動します。

ステップ 3　ターミナル エミュレーション プログラムのパラメータを次のとおりに設定します。

- 9600 ボー
- データ ビット 8
- ストップ ビット 1
- パリティなし
- ハードウェア フロー制御なし

ステップ 4　AC 電源コードをコントローラに接続し、アース付き 100 ～ 240 VAC、50/60 Hz の電源コンセントに差し込みます。

ステップ 5　電源を入れます。起動スクリプトによって、オペレーティング システム ソフトウェアの初期化（コードのダウンロードおよび電源投入時自己診断テスト）および基本設定が表示されます。

コントローラの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

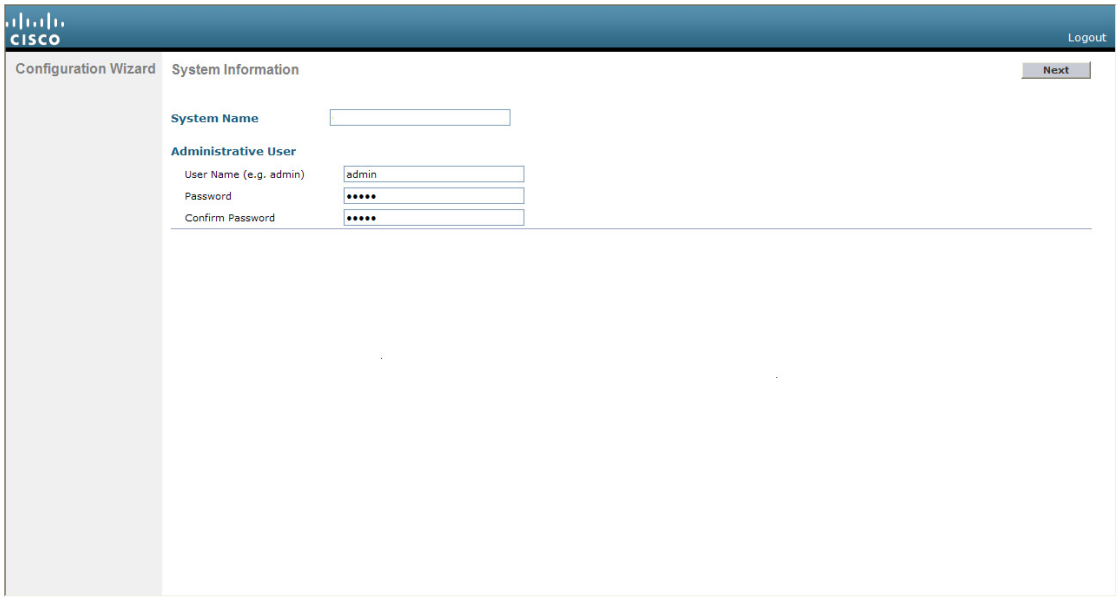
GUI 設定ウィザードの使用方法

GUI 設定ウィザードを使用してコントローラを設定する手順は、次のとおりです。

ステップ 1　コントローラと同じサブネット（たとえば 192.168.10.1）を使用するように PC を設定します。

ステップ 2　PC 上で Internet Explorer 6.0 SP1 以上または Firefox 2.0.0.11 以上を起動して、アドレス行に「http://192.168.1.1」と入力します。設定ウィザードが表示されます（図 2-1 を参照）。

図 2-1　設定ウィザード：[System Information] ページ



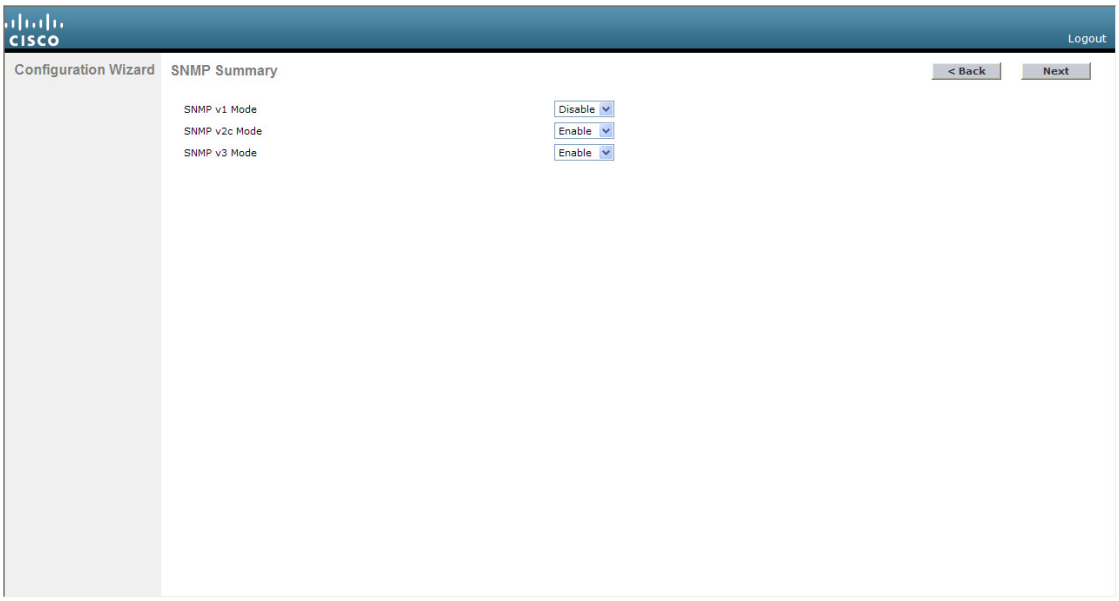
ステップ 3　[System Name] フィールドに、このコントローラに割り当てる名前を入力します。ASCII 文字を最大 31 文字入力できます。

ステップ 4　[User Name] フィールドに、このコントローラに割り当てる管理者ユーザ名を入力します。ASCII 文字を最大 24 文字入力できます。デフォルトのユーザ名は *admin* です。

ステップ 5　[Password] フィールドおよび [Confirm Password] フィールドに、このコントローラに割り当てる管理者パスワードを入力します。ASCII 文字を最大 24 文字入力できます。デフォルトのパスワードは *admin* です。

ステップ 6　[Next] をクリックします。[SNMP Summary] ページが表示されます（図 2-2 を参照）。

図 2-2　設定ウィザード：[SNMP Summary] ページ



ステップ 7　このコントローラに対して SNMP（Simple Network Management Protocol）v1 モードを有効にする場合は、[SNMP v1 Mode] ドロップダウン ボックスから [Enable] を選択します。有効にしない場合は、このパラメータを [Disable] のままにします。

（注）　SNMP とは、IP ネットワーク上のノード（サーバ、ワークステーション、ルータ、スイッチなど）を管理するプロトコルです。現時点では、SNMP のバージョンには SNMPv1、SNMPv2c、SNMPv3 の 3 つがあります。

ステップ 8　このコントローラに対して SNMPv2c モードを有効にするには、このパラメータを [Enable] のままにします。有効にしない場合は、[SNVP v2c Mode] ドロップダウン ボックスから [Disable] を選択します。

ステップ 9　このコントローラに対して SNMPv3 モードを有効にするには、このパラメータを [Enable] のままにします。有効にしない場合は、[SNVP v3 Mode] ドロップダウン ボックスから [Disable] を選択します。

ステップ 10　[Next] をクリックします。

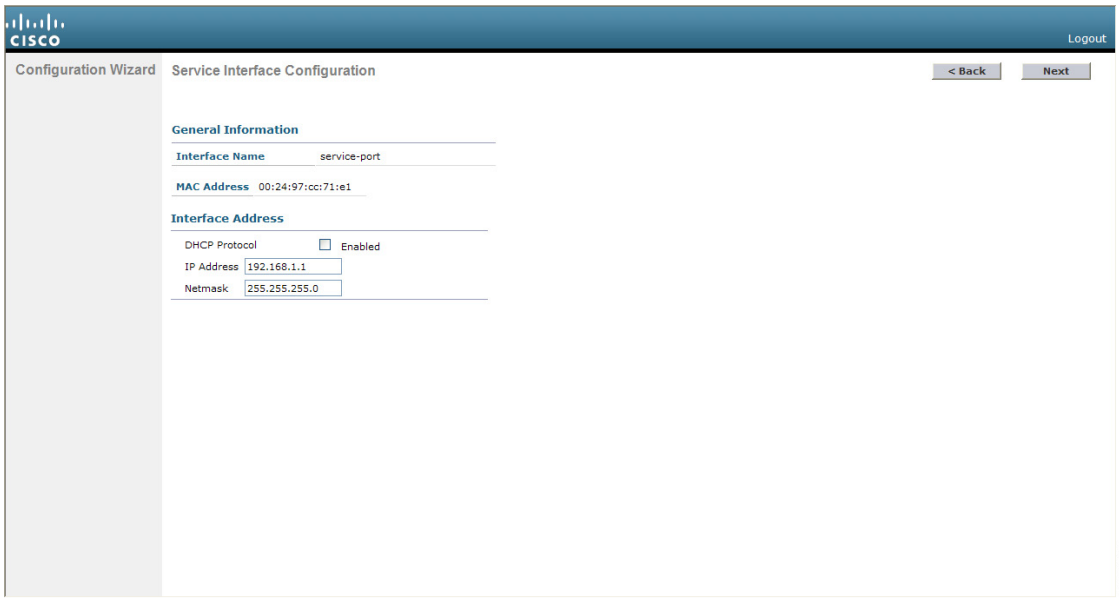
ステップ 11　次のメッセージが表示されたら、[OK] をクリックします。

```
Default values are present for v1/v2c community strings. Please make sure to create new
v1/v2c community strings once the system comes up. Please make sure to create new v3 users
once the system comes up.
```

（注）　手順については、「SNMP コミュニティ文字列のデフォルト値の変更」（P.4-44）および「SNMP v3 ユーザのデフォルト値の変更」（P.4-46）を参照してください。

[Service Interface Configuration] ページが表示されます（図 2-3 を参照）。

図 2-3　設定ウィザード : [Service Interface Configuration] ページ



ステップ 12　コントローラのサービス ポート インターフェイスの IP アドレスを DHCP サーバから取得するように設定するには、[DHCP Protocol Enabled] チェックボックスをオンにします。サービス ポートを使用しない場合、またはサービス ポートに固定 IP アドレスを割り当てる場合は、このチェックボックスをオフのままにします。

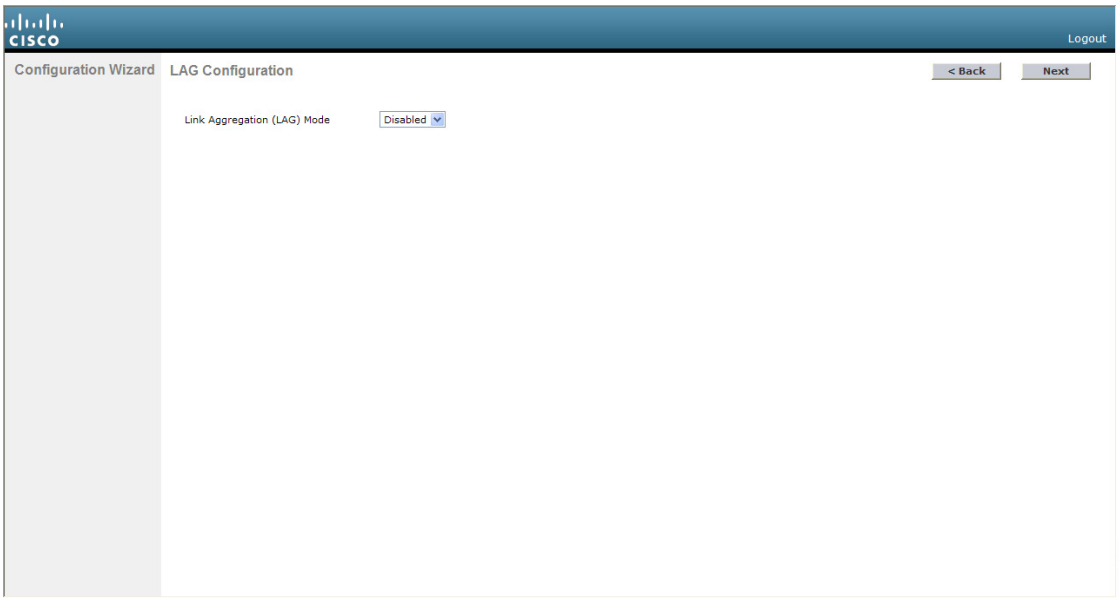
（注）　サービス ポート インターフェイスは、サービス ポートを介した通信を制御します。このインターフェイスの IP アドレスは、管理インターフェイスとは異なるサブネット上のものであることが必要です。このように設定されていれば、コントローラを直接、または専用の管理ネットワーク経由で管理できるので、ネットワークがダウンしているときもサービス アクセスが可能になります。

ステップ 13　次のいずれかの操作を行います。

- ステップ 12 で DHCP を有効にした場合は、[IP Address] フィールドと [Netmask] フィールドの入力内容をクリアして空白にします。
- ステップ 12 で DHCP を無効にした場合は、[IP Address] フィールドと [Netmask] フィールドにサービス ポートの固定 IP アドレスとネットマスクを入力します。

ステップ 14　[Next] をクリックします。[LAG Configuration] ページが表示されます（図 2-4 を参照）。

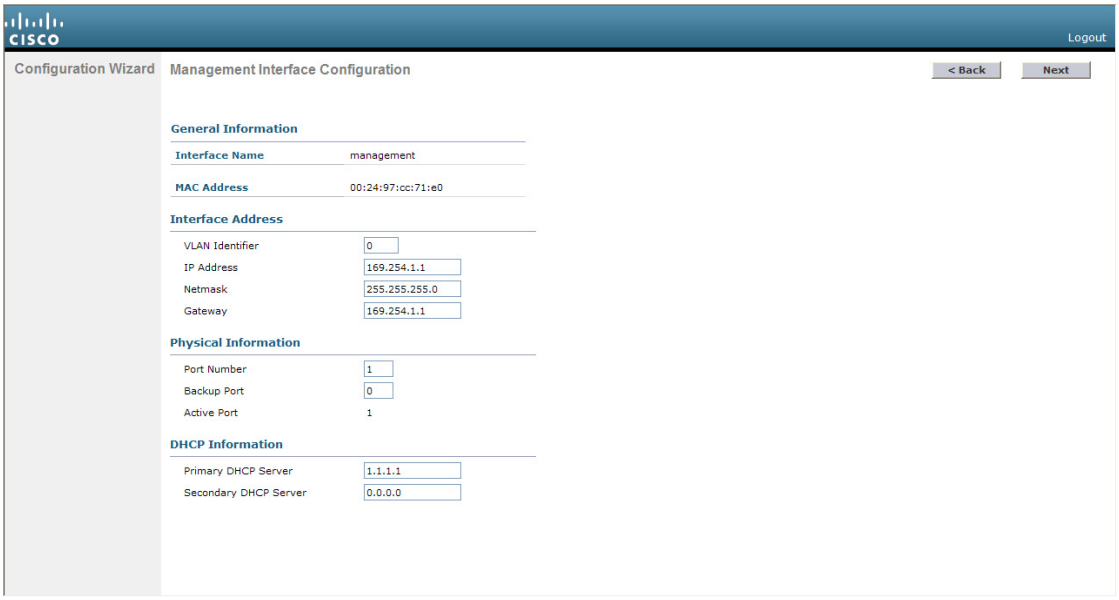
図 2-4　設定ウィザード：[LAG Configuration] ページ



ステップ 15　リンク集約（LAG）を有効にするには、[Link Aggregation (LAG) Mode] ドロップダウン ボックスから [Enabled] を選択します。LAG を無効にするには、このフィールドを [Disabled] のままにします。

ステップ 16　[Next] をクリックします。[Management Interface Configuration] ページが表示されます（図 2-5 を参照）。

図 2-5　設定ウィザード：[Management Interface Configuration] ページ



（注）　管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。

ステップ 17　[VLAN Identifier] フィールドに、管理インターフェイスの VLAN 識別子（有効な VLAN 識別子）を入力します。タグなし VLAN の場合は、**0** を入力します。VLAN 識別子は、スイッチ インターフェイス設定と一致するように設定する必要があります。

ステップ 18　[IP Address] フィールドに、管理インターフェイスの IP アドレスを入力します。

ステップ 19　[Netmask] フィールドに、管理インターフェイス ネットマスクの IP アドレスを入力します。

ステップ 20　[Gateway] フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。

ステップ 21　[Port Number] フィールドに、管理インターフェイスに割り当てられたポート番号を入力します。各インターフェイスは、少なくとも 1 つのプライマリ ポートにマップされます。

ステップ 22　[Backup Port] フィールドに、管理インターフェイスに割り当てられたバックアップ ポートの番号を入力します。管理インターフェイスのプライマリ ポートに障害が発生した場合は、管理インターフェイスは自動的にバックアップ ポートに移動します。

ステップ 23　[Primary DHCP Server] フィールドに、クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイス（使用する場合）の IP アドレスを取得するためのデフォルト DHCP サーバの IP アドレスを入力します。

ステップ 24　[Secondary DHCP Server] フィールドに、クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイス（使用する場合）の IP アドレスを取得するためのセカンダリ DHCP サーバの IP アドレスを入力します（省略可能）。

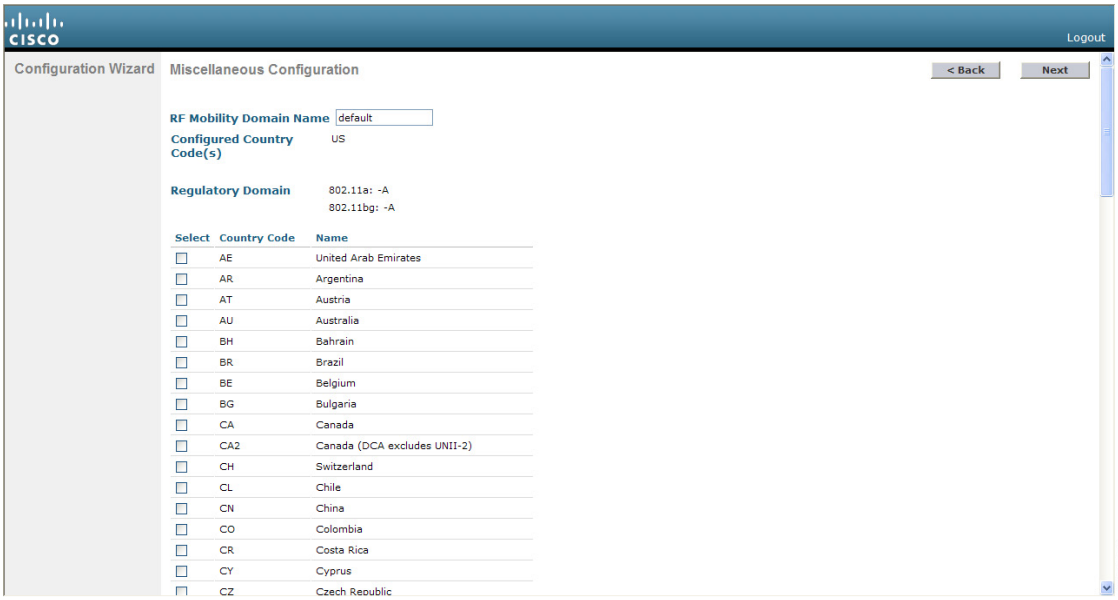
ステップ 25　[Next] をクリックします。[AP-Manager Interface Configuration] ページが表示されます。

（注）　5500 シリーズ コントローラの場合は、このページは表示されません。このシリーズは AP マネージャ インターフェイスの設定が必要ないからです。管理インターフェイスは、デフォルトでは AP マネージャ インターフェイスのように動作します。

ステップ 26　[IP Address] フィールドに、AP マネージャ インターフェイスの IP アドレスを入力します。

ステップ 27　[Next] をクリックします。[Miscellaneous Configuration] ページが表示されます（図 2-6 を参照）。

図 2-6　設定ウィザード：[Miscellaneous Configuration] ページ



ステップ 28　[RF Mobility Domain Name] フィールドに、コントローラが所属するモビリティ グループ/RF グループの名前を入力します。

（注）　ここで入力する名前は、モビリティ グループと RF グループの両方に割り当てられますが、これらのグループは同じではありません。どちらのグループもコントローラの集合を定義するものですが、目的が異なっています。RF グループ内のすべてのコントローラは通常同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラは同じ RF グループに属します。ただし、モビリティ グループはスケーラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現するのに対して、RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現します。詳細は、第 11 章および第 12 章を参照してください。

ステップ 29　[Configured Country Code(s)] フィールドに、コントローラが使用される国のコードが表示されます。別の国で使用する場合は、その国のチェックボックスをオンにします。

（注）　複数の国のアクセス ポイントを 1 つのコントローラで管理する場合は、複数の国コードを選択できます。設定ウィザードの実行後、コントローラに接続している各アクセス ポイントに特定の国を割り当てる必要があります。手順については、「国コードの設定」（P.7-73）を参照してください。

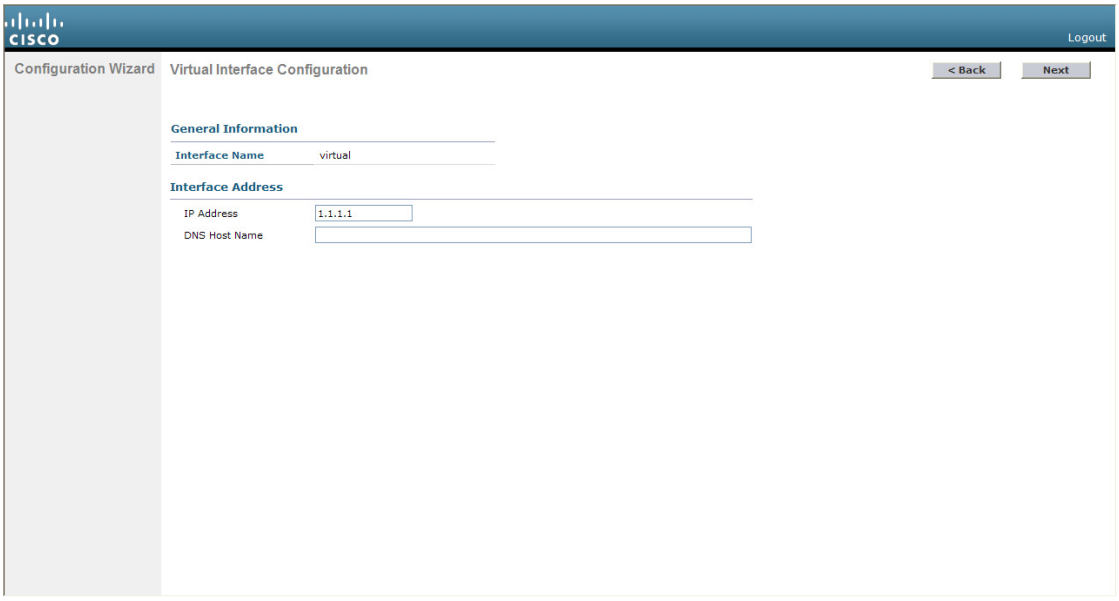
ステップ 30　[Next] をクリックします。

ステップ 31　次のメッセージが表示されたら、[OK] をクリックします。

```
Warning! To maintain regulatory compliance functionality, the country code setting may
only be modified by a network administrator or qualified IT professional. Ensure that
proper country codes are selected before proceeding.
```

[Virtual Interface Configuration] ページが表示されます（図 2-7 を参照）。

図 2-7　設定ウィザード：[Virtual Interface Configuration] ページ



ステップ 32　[IP Address] フィールドに、コントローラの仮想インターフェイスの IP アドレスを入力します。1.1.1.1 のような、架空の、割り当てられていない IP アドレスを入力する必要があります。

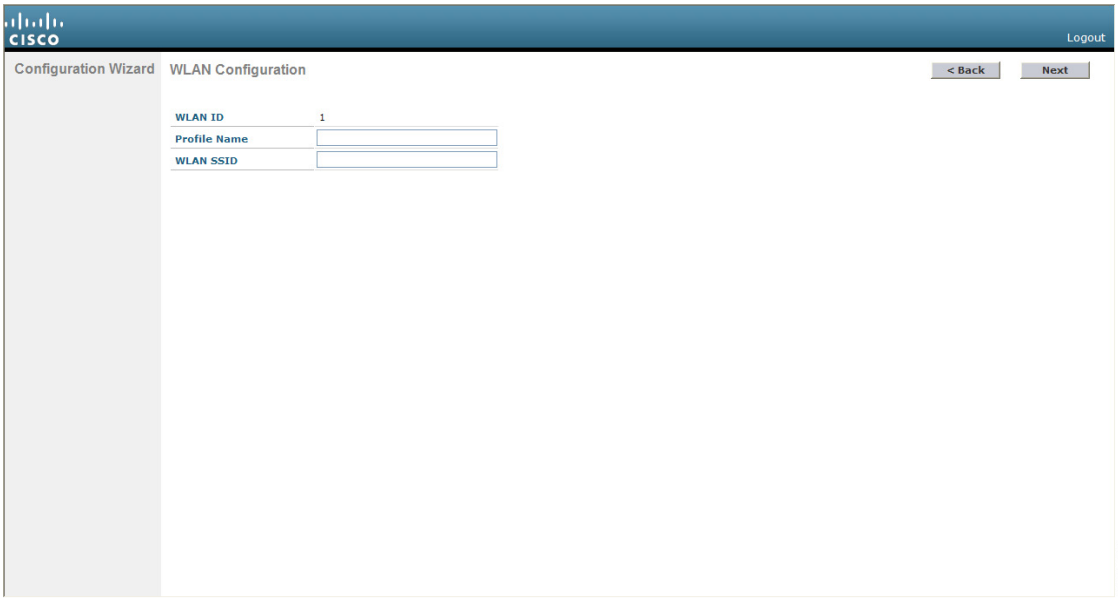
（注）　仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。

ステップ 33　[DNS Host Name] フィールドに、レイヤ 3 Web 認可が有効化されているときの証明書のソース確認に使用される Domain Name System（DNS; ドメイン ネーム システム）ゲートウェイの名前を入力します。

（注）　確実に接続と Web 認証が行われるためには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスの DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

ステップ 34　[Next] をクリックします。[WLAN Configuration] ページが表示されます（図 2-8 を参照）。

図 2-8　設定ウィザード：[WLAN Configuration] ページ



ステップ 35　Profile Name フィールドに、この WLAN に割り当てるプロファイル名に対する最大 32 文字の英数字を入力します。

ステップ 36　[WLAN SSID] フィールドに、ネットワーク名つまりサービス セット ID（SSID）を英数字 32 文字以内で入力します。SSID が設定されると、コントローラの基本機能が使用可能になり、そのコントローラに接続されたアクセス ポイントの無線を有効化できるようになります。

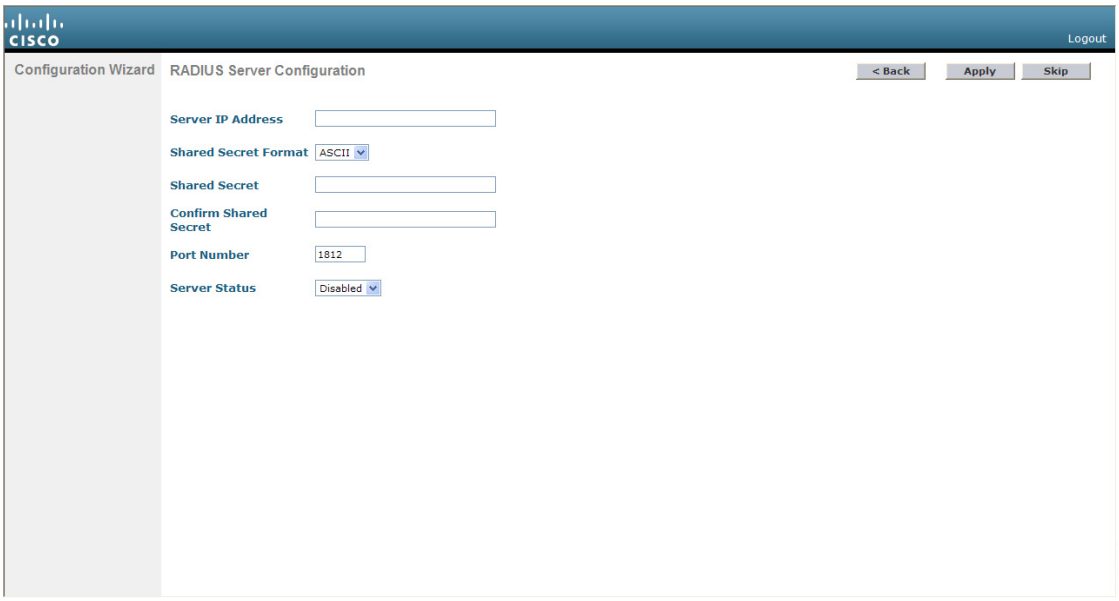
ステップ 37　[Next] をクリックします。

ステップ 38　次のメッセージが表示されたら、[OK] をクリックします。

```
Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change this after
the wizard is complete and the system is rebooted.
```

[RADIUS Server Configuration] ページが表示されます（図 2-9 を参照）。

図 2-9　設定ウィザード：[RADIUS Server Configuration] ページ



ステップ 39　[Server IP Address] フィールドに、RADIUS サーバの IP アドレスを入力します。

ステップ 40　[Shared Secret Format] ドロップダウン ボックスから、共有シークレットの形式として [ASCII] または [Hex] を選択します。

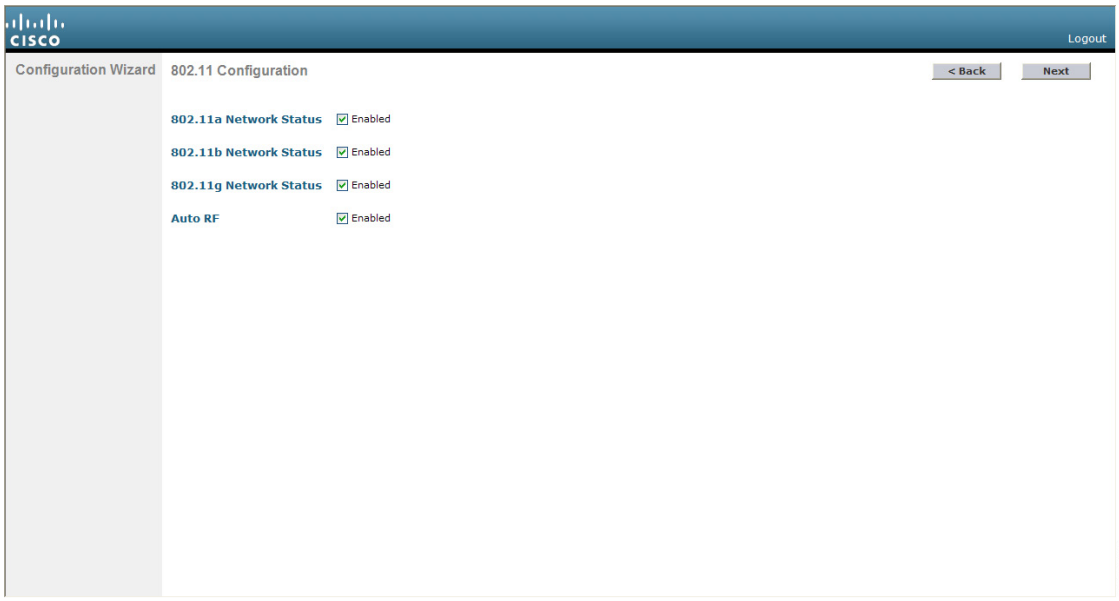
ステップ 41　[Shared Secret] フィールドと [Confirm Shared Secret] フィールドに、RADIUS サーバによって使用される秘密鍵を入力します。

ステップ 42　[Port Number] フィールドに、RADIUS サーバの通信ポートを入力します。デフォルト値は 1812 です。

ステップ 43　RADIUS サーバを有効にするには、[Server Status] ドロップダウン ボックスから [Enabled] を選択します。RADIUS サーバを無効にするには、このフィールドを [Disabled] のままにします。

ステップ 44　[Apply] をクリックします。[802.11 Configuration] ページが表示されます（図 2-10 を参照）。

図 2-10　設定ウィザード：[802.11 Configuration] ページ



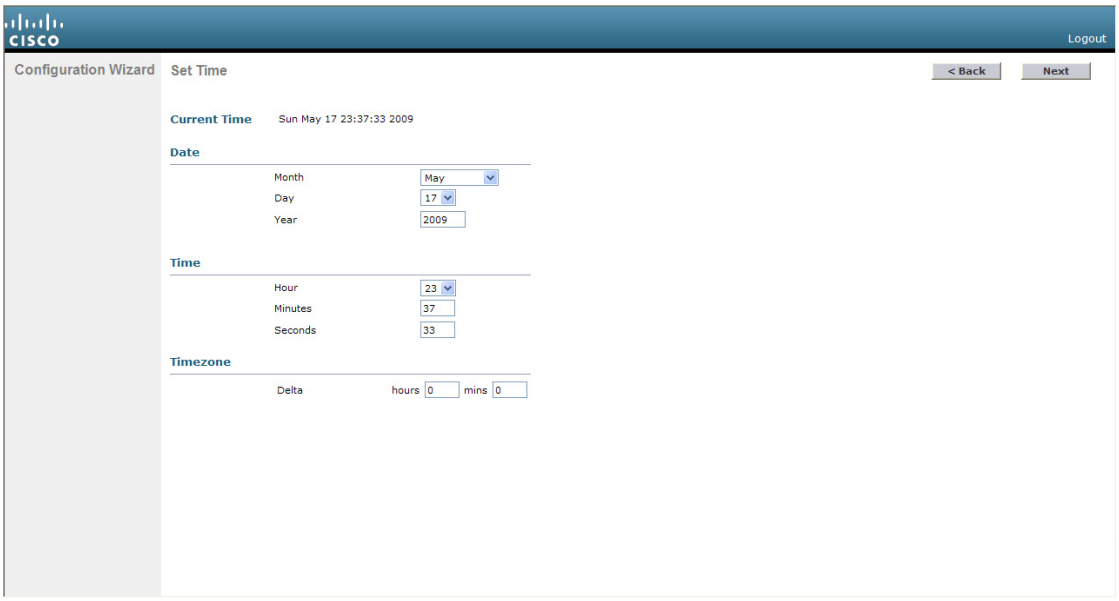
ステップ 45　802.11a、802.11b、および 802.11g の Lightweight アクセス ポイント ネットワークを有効にするには、[802.11a Network Status]、[802.11b Network Status]、および [802.11g Network Status] の各チェックボックスをオンのままにします。これらのネットワークのサポートを無効にするには、チェックボックスをオフにします。

ステップ 46　コントローラの Radio Resource Management（RRM）自動 RF 機能を有効にするには、[Auto RF] チェックボックスをオンのままにします。自動 RF 機能のサポートを無効にするには、このチェックボックスをオフにします。RRM の詳細は、第 11 章を参照してください。

（注）　自動 RF 機能を有効にすると、コントローラが自動的に他のコントローラと RF グループを形成できるようになります。グループでは、チャネルや送信電力の割り当てなど、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。

ステップ 47　[Next] をクリックします。[Set Time] ページが表示されます（図 2-11 を参照）。

図 2-11　設定ウィザード：[Set Time] ページ



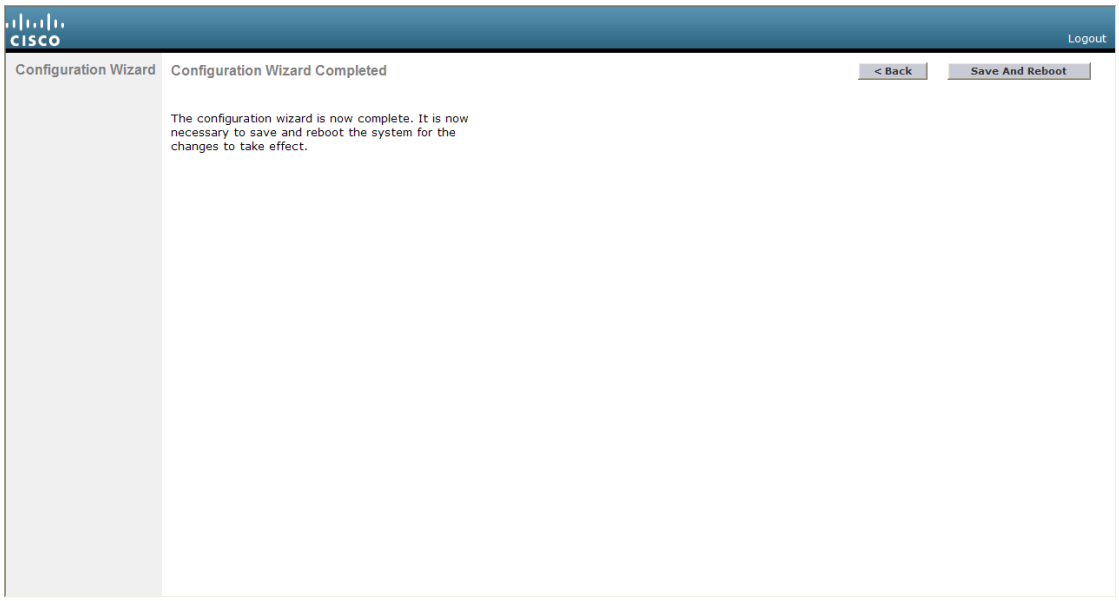
ステップ 48　コントローラのシステム時間を手動で設定するには、現在の日付を Month/DD/YYYY の形式で、現在の時刻を HH:MM:SS の形式で入力します。

ステップ 49　夏時間（DST）が自動的に設定されないように時間帯を手動で設定するには、現地時間とグリニッジ標準時（GMT）との差の時間の部分を [Delta Hours] フィールドに入力し、分の部分を [Delta Mins] フィールドに入力します。

（注）　時間帯を手動で設定するときは、GMT を基準とした現在の時間帯の時差を +/- を付けて入力します。たとえば、米国の太平洋標準時は、GMT の時刻より 8 時間遅れています。したがって、-8 と入力します。

ステップ 50　[Next] をクリックします。[Configuration Wizard Completed] ページが表示されます（図 2-12 を参照）。

図 2-12　設定ウィザード : [Configuration Wizard Completed] ページ



ステップ 51　設定を保存してコントローラをリブートするには、[Save and Reboot] をクリックします。

ステップ 52　次のメッセージが表示されたら、[OK] をクリックします。

```
Configuration will be saved and the controller will be rebooted. Click ok to confirm.
```

ステップ 53　コントローラの設定が保存されてリブートし、ログイン画面が表示されます。「GUI の使用方法」（P.2-16）の説明に従って、コントローラにログインしてください。

CLI 設定ウィザードの使用方法

（注）　利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。

（注）　入力した応答が正しくない場合は、「Invalid Response」などのエラー メッセージが表示され、ウィザードのプロンプトが再び表示されます。

（注）　前のコマンド ラインに戻る必要があるときは、ハイフン キーを押してください。

CLI 設定ウィザードを使用してコントローラを設定する手順は、次のとおりです。

ステップ 1　AutoInstall プロセスを終了するかどうかをたずねるメッセージが表示されたら、「yes」と入力します。「yes」と入力しなかった場合は、30 秒後に AutoInstall プロセスが開始します。

（注）　AutoInstall とは、設定ファイルを TFTP サーバからダウンロードしてから、設定を自動的にコントローラにロードする機能です。詳細は、「設定のないコントローラでの AutoInstall 機能の使用」（P.2-26）を参照してください。

（注）　Cisco WiSM コントローラでは、AutoInstall 機能はサポートされません。

ステップ 2　システム名を入力します。これは、コントローラに割り当てる名前です。ASCII 文字を最大 31 文字入力できます。

ステップ 3　このコントローラに割り当てる管理者のユーザ名およびパスワードを入力します。それぞれ、24 文字までの ASCII 文字を入力できます。デフォルトの管理者ユーザ名およびパスワードは、それぞれ *admin* と *admin* です。

ステップ 4　コントローラのサービス ポート インターフェイスの IP アドレスが DHCP サーバから取得されるように設定する場合は、[DHCP] と入力します。サービス ポートを使用しない場合、またはサービス ポートに固定 IP アドレスを割り当てる場合は、「none」と入力します。

（注）　サービス ポート インターフェイスは、サービス ポートを介した通信を制御します。このインターフェイスの IP アドレスは、管理インターフェイスとは異なるサブネット上のものであることが必要です。このように設定されていれば、コントローラを直接、または専用の管理ネットワーク経由で管理できるので、ネットワークがダウンしているときもサービス アクセスが可能になります。

ステップ 5　ステップ 4 で「none」と入力した場合は、サービス ポート インターフェイスの IP アドレスとネットマスクを次の 2 行で入力します。

ステップ 6　Link Aggregation（LAG; リンク集約）を有効にする場合は「yes」を選択し、無効にする場合は「NO」を選択します。LAG の詳細は、第 3 章を参照してください。

ステップ 7　管理インターフェイスの IP アドレスを入力します。

（注）　管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。

ステップ 8　管理インターフェイス ネットマスクの IP アドレスを入力します。

ステップ 9　デフォルト ルータの IP アドレスを入力します。

ステップ 10　管理インターフェイスの VLAN 識別子（有効な VLAN 識別子）を入力します。タグなし VLAN の場合は 0 を入力します。VLAN 識別子は、スイッチ インターフェイス設定と一致するように設定する必要があります。

ステップ 11　クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイスが IP アドレスを取得するためのデフォルト DHCP サーバの IP アドレスを入力します。

ステップ 12　AP マネージャ インターフェイスの IP アドレスを入力します。

（注）　5500 シリーズ コントローラの場合は、このプロンプトは表示されません。このシリーズは AP マネージャ インターフェイスの設定が必要ないからです。管理インターフェイスは、デフォルトでは AP マネージャ インターフェイスのように動作します。

ステップ 13　コントローラの仮想インターフェイスの IP アドレスを入力します。1.1.1.1 のような、架空の、割り当てられていない IP アドレスを入力する必要があります。

（注）　仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。

ステップ 14　必要に応じて、コントローラを追加するモビリティ グループ/RF グループの名前を入力します。

（注）　ここで入力する名前は、モビリティ グループと RF グループの両方に割り当てられますが、これらのグループは同じではありません。どちらのグループもコントローラの集合を定義するものですが、目的が異なっています。RF グループ内のすべてのコントローラは通常同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラは同じ RF グループに属します。ただし、モビリティ グループはスケーラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現するのに対して、RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現します。詳細は、第 11 章および第 12 章を参照してください。

ステップ 15　ネットワーク名または Service Set Identifier（SSID）を入力します。SSID が設定されると、コントローラの基本機能が使用可能になり、そのコントローラに接続されたアクセス ポイントの無線を有効化できるようになります。

ステップ 16　クライアントに独自の IP アドレス割り当てを許可する場合は「YES」と入力し、クライアントの IP アドレスが DHCP サーバから取得されるようにするには「no」と入力します。

ステップ 17　RADIUS サーバをここで設定するには、「YES」と入力してから、RADIUS サーバの IP アドレス、通信ポート、および秘密鍵を入力します。それ以外の場合は、「no」と入力します。「no」と入力した場合は、「Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.」というメッセージが表示されます。

ステップ 18　コントローラが使用される国のコードを入力します。

（注）　使用可能な国コードの一覧を表示するには、「help」と入力します。

（注）　複数の国のアクセス ポイントを 1 つのコントローラで管理する場合は、複数の国コードを入力できます。複数の国コードを入力するには、国コードをカンマで区切ります（「US,CA,MX」など）。設定ウィザードの実行後、コントローラに接続している各アクセス ポイントに特定の国を割り当てる必要があります。手順については、「国コードの設定」（P.7-73）を参照してください。

ステップ 19　802.11b、802.11a、および 802.11g の Lightweight アクセス ポイント ネットワークを有効にするには「YES」と入力し、無効にするには「no」と入力します。

ステップ 20　コントローラの Radio Resource Management（RRM）自動 RF 機能を有効にするには「YES」と入力し、無効にするには「no」と入力します。RRM の詳細は、第 11 章を参照してください。

（注）　自動 RF 機能を有効にすると、コントローラが自動的に他のコントローラと RF グループを形成できるようになります。グループでは、チャネルや送信電力の割り当てなど、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。

ステップ 21　電源投入時にコントローラの時間設定が外部ネットワーク タイム プロトコル（NTP）サーバから受信されるようにするには、「YES」と入力して NTP サーバを設定します。それ以外の場合は、「no」と入力します。

（注）　Cisco サービス統合型ルータにインストールされるコントローラ ネットワーク モジュールにはバッテリがないため、時間設定を保存することはできません。したがって、電源投入時に外部 NTP サーバから時間設定を受信する必要があります。

ステップ 22　ステップ 21 で「no」と入力した場合に、コントローラのシステム時間をここで手動設定するには、「YES」と入力します。システム時間を後で設定する場合は、「no」と入力します。

ステップ 23　ステップ 22 で「YES」と入力した場合は、現在の日付を MM/DD/YY の形式で、現在の時刻を HH:MM:SS の形式で入力します。

ステップ 24　設定が正しいかどうかをたずねるプロンプトが表示されたら、「yes」または「NO」と入力します。

コントローラの設定が保存されてリブートし、ログイン画面が表示されます。「CLI の使用方法」（P.2-22）の説明に従って、コントローラにログインしてください。

GUI の使用方法

Web ブラウザ、つまり、グラフィカル ユーザ インターフェイス（GUI）は、各コントローラに組み込まれています。最大 5 名のユーザが、コントローラ http または https（http + SSL）管理ページを同時に閲覧して、パラメータを設定し、コントローラとそのアソシエートされているアクセス ポイントの動作ステータスを監視することができます。

（注）　Cisco UWN Solution のセキュリティを強化するために、HTTPS インターフェイスを有効にし、HTTP インターフェイスを無効にすることをお勧めします。

GUI を使用する際の注意事項

GUI を使用するときは、次の点に留意してください。

- GUI を使用する PC では、Windows XP SP1 以降または Windows 2000 SP4 以降が稼働している必要があります。
- この GUI は、Microsoft Internet Explorer バージョン 6.0 SP1 以降および Mozilla Firefox 2.0.0.11 以降に完全に対応しています。

（注）　Opera および Netscape はサポートされていません。

（注）　コントローラ GUI へのアクセスおよび Web 認証がサポートされているブラウザは、Internet Explorer 6.0 SP1 以降および Mozilla Firefox 2.0.0.11 以降だけです。

- サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、サービス ポート インターフェイスの使用をお勧めします。サービス ポート インターフェイスの設定方法については、第 3 章を参照してください。
- GUI のページ上部にある [Help] をクリックすると、オンライン ヘルプが表示されます。オンライン ヘルプを表示するには、ブラウザのポップアップ ブロックを無効にする必要があります。

GUI へのログイン

コントローラ GUI にログインする手順は、次のとおりです。

ステップ 1　ブラウザのアドレス行にコントローラの IP アドレスを入力します。接続をセキュリティで保護するには、**https://*<IP アドレス>*** と入力します。接続をセキュリティで保護しない場合は、**http://*<IP アドレス>*** と入力します。

（注）　HTTPS をセットアップする手順は、「GUI を使用した Web およびセキュア Web モードの有効化」（P.2-18）を参照してください。

ステップ 2　ユーザ名とパスワードを入力する画面が表示されたら、有効な値を入力して [OK] をクリックします。コントローラの [Summary] ページが表示されます。

（注）　設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

GUI からのログアウト

コントローラの GUI からログアウトするには、次の手順に従います。

ステップ 1　画面右上の [Logout] をクリックします。

ステップ 2　[Close] をクリックするとログオフ プロセスが完了し、それ以降は、権限のないユーザはコントローラ GUI にはアクセスできなくなります。

ステップ 3　決定を確認する画面が表示されたら、[Yes] をクリックします。

Web モードおよびセキュア Web モードの有効化

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効化すると、GUI との通信を保護できます。HTTPS では、SSL（Secure Socket Layer）プロトコルを使用することによって、HTTP ブラウザのセッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。また、外部で生成された証明書をダウンロードすることもできます。

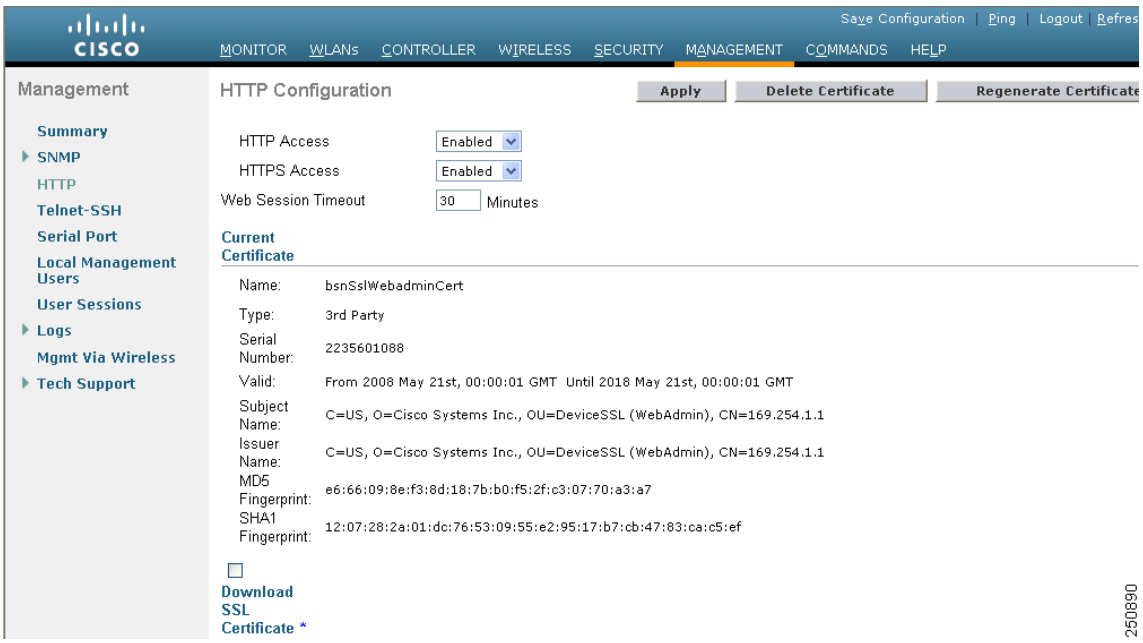
Web モードおよびセキュア Web モードの設定は、コントローラ GUI と CLI のどちらでも実行できます。

GUI を使用した Web およびセキュア Web モードの有効化

コントローラの GUI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　[Management] > [HTTP] の順に選択して [HTTP Configuration] ページを開きます（図 2-13 を参照）。

図 2-13　[HTTP Configuration] ページ



ステップ 2　Web モード（ユーザが「http://*<IP アドレス>*」を使用してコントローラ GUI にアクセスできます）を有効にするには、[HTTP Access] ドロップダウン ボックスから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。デフォルト値は [Disabled] です。Web モードの接続は、セキュリティで保護されません。

ステップ 3　セキュア Web モード（ユーザが「https://*<IP アドレス>*」を使用してコントローラ GUI にアクセスできます）を有効にするには、[HTTPS Access] ドロップダウン ボックスから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。デフォルト値は [Enabled] です。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 4　[Web Session Timeout] フィールドに、Web セッションのアクティビティがない場合にタイムアウトするまでの時間（分単位）を入力します。30 ～ 160 分の範囲内の値を入力できます。デフォルト値は 30 分です。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　ステップ 3 でセキュア Web モードを有効にした場合は、ローカル Web アドミニストレーション SSL 証明書が生成されて自動的に GUI に適用されます。現在の証明書の詳細は、[HTTP Configuration] ページの中央に表示されます（図 2-13 を参照）。

（注）　独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」（P.2-20）の手順を参照してください。

（注）　必要に応じて、現在の証明書を削除することもできます。削除するには、[Delete Certificate] をクリックします。[Regenerate Certificate] をクリックすると、新しい証明書が生成されます。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した Web およびセキュア Web モードの有効化

コントローラの CLI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　Web モードを有効または無効にするには、次のコマンドを入力します。

config network webmode {**enable** | **disable**}

このコマンドを実行すると、ユーザが「http://<*IP アドレス*>」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は disabled です。Web モードの接続は、セキュリティで保護されません。

ステップ 2　セキュア Web モードを有効または無効にするには、次のコマンドを入力します。

config network secureweb {**enable** | **disable**}

このコマンドを実行すると、ユーザが「https://<*IP アドレス*>」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は enabled です。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 3　セキュア Web モードのセキュリティの強化を有効または無効にするには、次のコマンドを入力します。

config network secureweb cipher-option high {**enable** | **disable**}

このコマンドを実行すると、ユーザが「https://<*IP アドレス*>」を使用してコントローラの GUI にアクセスできるようになりますが、ブラウザが 128 ビット（またはそれ以上）の暗号をサポートしている必要があります。デフォルト値は無効（disable）です。

ステップ 4　Web 管理に対して SSLv2 を有効または無効にするには、次のコマンドを入力します。

config network secureweb cipher-option sslv2 {**enable** | **disable**}

SSLv2 を無効にすると、SSLv2 だけを使用するように設定されたブラウザからは接続できなくなります。SSLv3 以降のような、安全性の高いプロトコルを使用するよう設定されたブラウザを使用する必要があります。デフォルト値は有効（enable）です。

ステップ 5　コントローラが証明書を生成したことを確認するには、次のコマンドを入力します。

show certificate summary

次のような情報が表示されます。

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

（注）　独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」（P.2-20）の手順を参照してください。

ステップ 6　（オプション）新しい証明書を生成する場合は、次のコマンドを入力します。

config certificate generate webadmin

数秒後、証明書が生成されたことをコントローラが確認します。

ステップ 7　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM（不揮発性 RAM）に保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラをリブートするには、次のコマンドを入力します。

reset system

外部で生成した SSL 証明書のロード

TFTP サーバを使用して、外部で生成された SSL 証明書をコントローラにダウンロードできます。TFTP を使用する際の注意事項は次のとおりです。

- サービス ポート経由で証明書をロードする場合、サービス ポートはルーティングできないため、TFTP サーバはコントローラと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。また、証明書をディストリビューション システム ネットワーク ポート経由でロードする場合は、TFTP サーバはどのサブネットに存在していてもかまいません。
- サードパーティの TFTP サーバを Cisco WCS と同じ PC 上で実行することはできません。WCS 内蔵型 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。

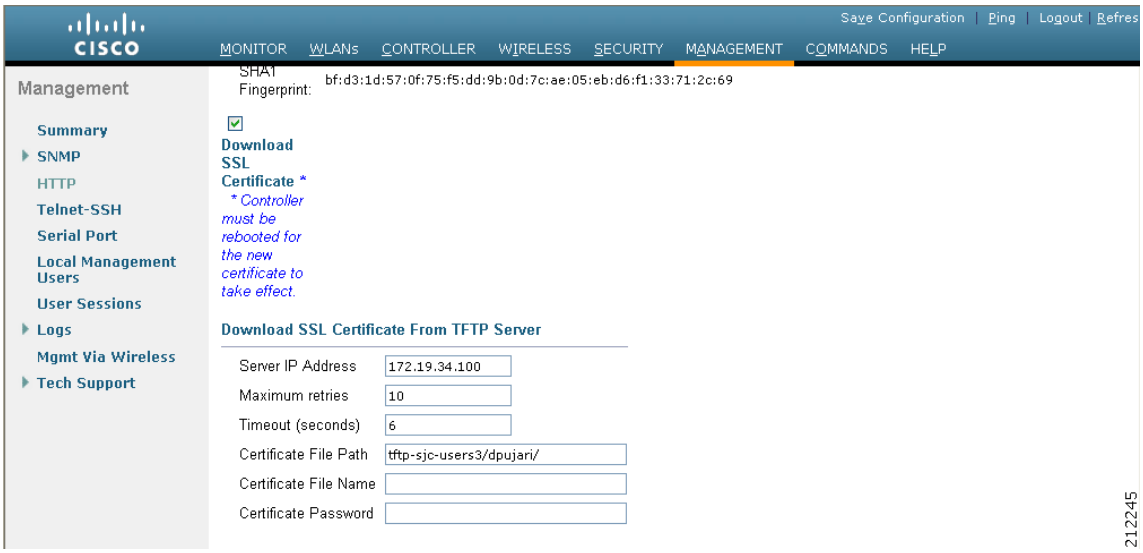
（注）　各 HTTPS 証明書には RSA キーが組み込まれています。キーの長さは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまでさまざまです。認証局から新しい証明書を取得する際、証明書に組み込まれた RSA キーの長さが 768 ビット以上であることを確認してください。

GUI を使用した SSL 証明書のロード

コントローラの GUI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　[HTTP Configuration] ページの [Download SSL Certificate] チェックボックスをオンにします（図 2-14 を参照）。

図 2-14　[HTTP Configuration] ページ



ステップ 2　[Server IP Address] フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 3　[Maximum Retries] フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 4　[Timeout] フィールドに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 5　[Certificate File Path] フィールドに、証明書のディレクトリ パスを入力します。

ステップ 6　[Certificate File Name] フィールドに、証明書の名前を入力します（*webadmincert_name*.pem）。

ステップ 7　（オプション）[Certificate Password] フィールドに、証明書を暗号化するためのパスワードを入力します。

ステップ 8　[Apply] をクリックして、変更を適用します。

ステップ 9　[Save Configuration] をクリックして、変更を保存します。

ステップ 10　コントローラをリブートして変更内容を有効にするには、[Commands] > [Reboot] > [Reboot] > [Save and Reboot] の順に選択します。

CLI を使用した SSL 証明書のロード

コントローラの CLI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　パスワードを使用して、.PEM エンコード ファイル形式の HTTPS 証明書を暗号化します。PEM エンコード ファイルは、Web アドミニストレーション証明書ファイル（*webadmincert_name*.pem）と呼ばれます。

ステップ 2　*webadmincert_name*.pem ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 3　現在のダウンロードの設定を表示するには、次のコマンドを入力してプロンプトに「n」と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename.............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

ステップ 4　次のコマンドを使用して、ダウンロード設定を変更します。

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

ステップ 5　オペレーティング システムが Web アドミニストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、次のコマンドを入力します。

transfer download certpassword *private_key_password*

ステップ 6　現在のダウンロードの設定を確認して証明書とキーのダウンロードを開始するには、次のコマンドを入力して、プロンプトに「y」と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

ステップ 7　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM に保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラをリブートするには、次のコマンドを入力します。

reset system

CLI の使用方法

Cisco UWN Solution のコマンドライン インターフェイス（CLI）は、各コントローラに組み込まれています。CLI では、VT-100 ターミナル エミュレーション プログラムを使用して、個々のコントローラおよび各コントローラにアソシエートされた Lightweight アクセス ポイントをローカルまたはリモー

トで設定、監視、制御することができます。この CLI は、単純なテキスト ベースのツリー構造のインターフェイスです。最大 5 名のユーザが Telnet 対応ターミナル エミュレーション プログラムを使用してコントローラにアクセスできます。

（注）　特定のコマンドの情報は、『*Cisco Wireless LAN Controller Command Reference*』を参照してください。

（注）　XML 設定の文字列を CLI コマンドに入力する場合は、文字列を引用符で囲む必要があります。

CLI へのログイン

コントローラ CLI にアクセスする方法は、次の 2 つがあります。

- コントローラ コンソール ポートへのシリアル直接接続
- 事前設定されたサービス ポートやディストリビューション システム ポートを使用したイーサネット上のリモート コンソール セッション

CLI にログインする前に、使用する接続の種類に基づいて接続および環境変数を設定しておく必要があります。

ローカル シリアル接続の使用方法

シリアル ポートに接続するには次が必要です。

- VT-100 ターミナル エミュレーション プログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行している PC
- ヌルモデム シリアル ケーブル

シリアル ポートを介してコントローラ CLI にログインする手順は、次のとおりです。

ステップ 1　ヌルモデム シリアル ケーブルの一端をコントローラのコンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。

（注）　5500 シリーズ コントローラでは、RJ-45 コンソール ポートと USB コンソール ポートのどちらでも使用できます。USB コンソール ポートを使用する場合は、5 ピン ミニ タイプ B コネクタをコントローラの USB コンソール ポートに接続し、もう一端を PC の USB タイプ A ポートに接続します。Windows PC を USB ポートに接続するのが初めての場合は、USB コンソール ドライバをインストールするための画面が表示されます。インストール画面の指示に従って、ドライバをインストールしてください。USB コンソール ドライバは PC 上の COM ポートにマッピングされるので、この COM ポートにターミナル エミュレータ アプリケーションをマッピングする必要があります。

ステップ 2　PC の VT-100 ターミナル エミュレーション プログラムを起動します。

ステップ 3　ターミナル エミュレーション プログラムのパラメータを次のとおりに設定します。

- 9600 ボー
- データ ビット 8
- ストップ ビット 1
- パリティなし
- ハードウェア フロー制御なし

（注）　コントローラのシリアル ポートは、9600 ボー レートおよび短いタイムアウト用に設定されています。これらの値を変更するには、**config serial baudrate** *baudrate* コマンドおよび **config serial timeout** *timeout* コマンドを使用します。**config serial timeout 0** と入力すると、シリアル セッションはタイムアウトしなくなります。

ステップ 4　プロンプトが表示されたら、有効なユーザ名とパスワードを入力してコントローラにログインします。設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。

（注）　デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

CLI のルート レベル システム プロンプトが表示されます。

```
#(system prompt)>
```

（注）　システム プロンプトは、最大 31 文字の任意の英数字から成る文字列です。システム プロンプトを変更するには、**config prompt** コマンドを入力します。

リモート イーサネット接続の使用方法

リモートでコントローラに接続するには、次が必要です。

- イーサネット ネットワークを介してコントローラにアクセスできる PC
- コントローラの IP アドレス
- Telnet セッション用の VT-100 ターミナル エミュレーション プログラムまたは DOS シェル

（注）　デフォルトでは、コントローラは Telnet セッションをブロックします。Telnet セッションを有効にするには、シリアル ポートへのローカル接続を使用する必要があります。Telnet セッションを有効にする方法は、「Telnet および SSH セッションの設定」（P.2-34）を参照してください。

リモート イーサネット接続を介してコントローラ CLI にログインする手順は、次のとおりです。

ステップ 1　VT-100 ターミナル エミュレーション プログラムまたは DOS シェル インターフェイスのパラメータが次のとおりに設定されていることを確認します。

- イーサネット アドレス
- ポート 23

ステップ 2　コントローラの IP アドレスを使用して CLI に Telnet 接続します。

ステップ 3　プロンプトが表示されたら、有効なユーザ名とパスワードを入力してコントローラにログインします。設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。

（注）　デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

CLI のルート レベル システム プロンプトが表示されます。

```
#(system prompt)>
```

（注）　システム プロンプトは、最大 31 文字の任意の英数字から成る文字列です。システム プロンプトを変更するには、**config prompt** コマンドを入力します。

CLI からのログアウト

CLI での作業が終了したら、ルート レベルに移動して「logout」と入力します。揮発性 Random-Access Memory（RAM; ランダムアクセス メモリ）への変更を保存するかどうかを確認するプロンプトが表示されます。

（注）　アクティビティがない状態が 5 分間続くと、変更を保存せずに自動的に CLI からログアウトされます。**config serial timeout** コマンドを使用すると、自動ログアウト時間を 0（自動ログアウトしない）～ 160 分の範囲内で設定できます。

CLI のナビゲーション

CLI のナビゲーションは、5 つのレベルに分かれています。

ルート レベル

レベル 2

レベル 3

レベル 4

レベル 5

CLI にログインしたときは、ルート レベルです。ルート レベルでは、任意のフル コマンドを、正しいコマンド レベルに移動することなく入力できます。表 2-1 は、CLI のナビゲーションおよび一般的なタスク実行のためのコマンドの一覧です。

表 2-1　CLI のナビゲーションと共通タスクのコマンド

コマンド	操作
help	ルート レベルの場合、システム全体のナビゲーション コマンドが表示されます。
?	現在のレベルで使用できるコマンドが表示されます。

表 2-1　CLI のナビゲーションと共通タスクのコマンド

コマンド	操作
< コマンド> **?**	指定したコマンドのパラメータが表示されます。
exit	1 つ下のレベルに移動します。
Ctrl+Z	ルート レベルに戻ります。
save config	ルート レベルの場合、使用中のアクティブな RAM への変更を、リブート後も維持されるように不揮発性 RAM（NVRAM）に保存します。
reset system	ルート レベルの場合、ログアウトせずにコントローラをリセットします。

設定のないコントローラでの AutoInstall 機能の使用

設定のないコントローラを起動するときに、AutoInstall 機能によって設定ファイルを TFTP サーバからダウンロードして設定をコントローラに自動的にロードすることができます。

（注）　Cisco WiSM コントローラでは、AutoInstall 機能はサポートされません。

AutoInstall の概要

ネットワーク上に（または WCS フィルタを介して）すでに存在するコントローラに設定ファイルを作成する場合は、TFTP サーバに設定ファイルを配置し、DHCP サーバを設定します。これによって新しいコントローラは IP アドレスと TFTP サーバの情報を取得でき、AutoInstall 機能が新しいコントローラの設定ファイルを自動的に取得できます。

コントローラを起動すると、AutoInstall プロセスが開始されます。設定ウィザードが起動したことが AutoInstall へ通知されないかぎり、コントローラは何も処理しません。設定ウィザードが起動しなければ、そのコントローラには有効な設定があります。

AutoInstall は、設定ウィザードが起動したことを通知されると（つまり、コントローラに設定がないときは）、さらに 30 秒間待機します。この間、ユーザは設定ウィザードからの最初のプロンプトに応答できます。

```
Would you like to terminate autoinstall? [yes]:
```

30 秒の中断タイムアウトが経過すると、AutoInstall は DHCP クライアントを起動します。30 秒のタイムアウトが経過した後でも、プロンプトで「Yes」と入力すれば、AutoInstall のタスクを停止できます。ただし、TFTP タスクによってフラッシュがロックされており、有効な設定ファイルのダウンロードとインストールが進行中のときは、AutoInstall を停止することはできません。

DHCP による IP アドレスの入手、および TFTP サーバからの設定ファイルのダウンロード

AutoInstall では次のインターフェイスが使用されます。

- 5500 および 4400 シリーズ コントローラ
  - eth0：サービス ポート（タグなし）

  - dtl0 : NPU を介したギガビット ポート 1（タグなし）
- 2100 シリーズ コントローラ
  - dtl0 : FastEthernet ポート 1（タグなし）

AutoInstall は DHCP プロセスが正常に終了するまで、またはユーザが AutoInstall プロセスを停止するまで DHCP サーバから IP アドレスを取得しようとします。DHCP サーバから IP アドレスを正常に取得するための最初のインターフェイスは、AutoInstall タスクに登録されます。このインターフェイスの登録によって、AutoInstall は TFTP サーバ情報の取得と、設定ファイルのダウンロードのプロセスを開始します。

インターフェイスの DHCP IP アドレスを取得した後、AutoInstall はコントローラのホスト名と TFTP サーバの IP アドレスを決定する短い一連のイベントを開始します。この一連のイベントの各段階では、デフォルト情報または暗黙的情報よりも明示的に設定された情報が優先され、明示的 IP アドレスよりも明示的ホスト名が優先されます。

プロセスは次のとおりです。

- DHCP を介して 1 つ以上の Domain Name System（DNS）サーバ IP アドレスが得られると、AutoInstall は /etc/resolv.conf ファイルを作成します。このファイルにはドメイン名、および受信された DNS サーバのリストが含まれます。Domain Name Server オプションでは、DNS サーバのリストが提供され、Domain Name オプションではドメイン名が提供されます。
- ドメイン サーバがコントローラと同じサブネット上にない場合、静的ルート エントリがドメイン サーバごとにインストールされます。これらの静的ルートは、HDCP Router オプションを介して取得されたゲートウェイをポイントします。
- コントローラのホスト名は、次の順序で決定されます。
  - DHCP Host Name オプションが受信された場合、この情報（最初のピリオド [.] で切り捨てられる）がコントローラのホスト名として使用されます。
  - DNS の逆ルックアップがコントローラの IP アドレスで実行されます。DNS がホスト名を返すと、（最初のピリオド [.] で切り捨てられた）この名前はコントローラのホスト名として使用されます。
- TFTP サーバの IP アドレスは、次の順序で決定されます。
  - AutoInstall が DHCP TFTP Server Name オプションを受信した場合、AutoInstall はこのサーバ名の DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - DHCP Server Host Name（sname）フィールドが有効な場合は、AutoInstall はこの名前に対する DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - AutoInstall が DHCP TFTP Server Address オプションを受信した場合、このアドレスが TFTP サーバの IP アドレスとして使用されます。
  - AutoInstall はデフォルトの TFTP サーバ名（cisco-wlc-tftp）の DNS lookup を実行します。DNS lookup が正常に終了した場合、受信した IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - DHCP サーバの IP アドレス（siaddr）フィールドがゼロ以外の値である場合、このアドレスは TFTP サーバの IP アドレスとして使用されます。
  - 制限されたブロードキャスト アドレス（255.255.255.255）が TFTP サーバの IP アドレスとして使用されます。
- TFTP サーバがコントローラと同じサブセットにない場合、静的ルート（/32）が TFTP サーバの IP アドレスとしてインストールされます。この静的ルートは、DHCP Router オプションを介して取得されたゲートウェイをポイントします。

（注）　コントローラに DHCP を設定する方法の詳細は、「DHCP の設定」（P.6-8）を参照してください。

（注）　コントローラに TFTP サーバを設定する方法の詳細は、第 9 章を参照してください。

（注）　WCS を介して DHCP サーバと TFTP サーバを設定する方法の詳細は、『*Cisco Wireless Control System Configuration Guide, Release 6.0*』の第 10 章を参照してください。

設定ファイルの選択

ホスト名と TFTP サーバが決定されると、AutoInstall は設定ファイルのダウンロードを試行します。AutoInstall は DHCP IP アドレスを取得するインターフェイスごとに 3 回の完全なダウンロードを繰り返します。たとえば、4400 シリーズ コントローラが eth0 と dtl0 の両方で DHCP IP アドレスを取得すると、各インターフェイスは設定のダウンロードを試行します。インターフェイスは、3 回の試行後に設定ファイルを正常にダウンロードできない場合、それ以上のダウンロードを試行しません。

正常にダウンロードおよびインストールされた最初の設定ファイルがコントローラのリブートをトリガーします。リブート後に、コントローラは新しくダウンロードされた設定を実行します。

AutoInstall は、名前がリストアップされる順番で設定ファイルを検索します。

- DHCP Boot File Name オプションによって提供されるファイル名
- DHCP File フィールドで提供されるファイル名
- *host name*-confg
- *host name*.cfg
- *Base MAC Address*-confg（0011.2233.4455-confg など）
- *serial number*-confg
- ciscowlc-confg
- ciscowlc.cfg

AutoInstall は、設定ファイルが見つかるまで、このリストの順にファイルを探します。登録されているインターフェイスごとにこのリストを 3 回サイクルし、設定ファイルが見つからない場合、実行を停止します。

（注）　ダウンロードされる設定ファイルは、完全な設定を行えることもあれば、WCS で管理されるコントローラに十分な程度の情報を持つ最小限の設定のこともあります。完全な設定ファイルは、WCS から直接展開できます。

（注）　AutoInstall が TFTP サーバから取得できる設定ファイルの作成とアップロードの詳細は、第 9 章を参照してください。

（注）　WCS リリース 5.0 以降には、コントローラの AutoInstall 機能があります。WCS 管理者はコントローラのホスト名、MAC アドレス、シリアル番号を含むフィルタを作成し、このフィルタのルールにテンプレートのグループ（設定グループ）を関連付けることができます。WCS は、コントローラの最初の起動時に初期設定をコントローラにコピーします。コントローラが検出された後、WCS は設定グループで定義されているテンプレートをコピーします。AutoInstall 機能と WCS の詳細については、『*Cisco Wireless Control System Configuration Guide, Release 6.0*』の第 15 章を参照してください。

AutoInstall の操作例

次は AutoInstall の全プロセスの一例です。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interation 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ===> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not
found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system
```

システムの日時の管理

設定ウィザードの実行時にシステムの日時を設定しなかった場合や、設定を変更したい場合は、この項で説明する手順に従って、日時をネットワーク タイム プロトコル（NTP）サーバから取得するようにコントローラを設定するか、手動で日時を設定します。コントローラ上の時間帯は、Greenwich Mean Time（GMT; グリニッジ標準時）を基準として設定します。

（注）　日時が正しく設定されていない場合は、Cisco Aironet Lightweight アクセス ポイントがコントローラに接続できなくなる可能性があります。アクセス ポイントからコントローラへの接続を許可する前に、コントローラの日時を設定してください。

日時を取得するための NTP サーバの設定

各 NTP サーバの IP アドレスは、コントローラ データベースに追加されています。すべてのコントローラは NTP サーバを検索して、リブート時およびユーザ定義ポーリング間隔ごとに（毎日から毎週）、現在時刻を取得できます。

NTP サーバから日時を取得するように設定するには、次のコマンドを使用します。

1. コントローラの NTP サーバを指定するには、次のコマンドを入力します。

   config time ntp server *index ip_address*

2. ポーリングの間隔（秒）を指定するには、次のコマンドを入力します。

   config time ntp *interval*

手動による日時の設定

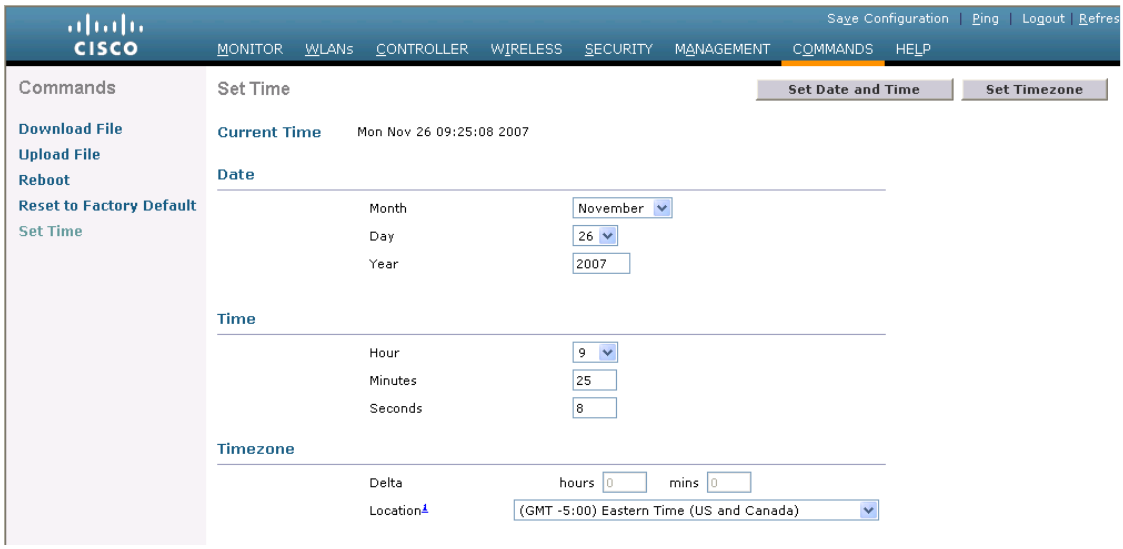
コントローラの GUI または CLI を使用して日時を手動で設定するには、この項の手順に従ってください。

GUI を使用した日時の設定

コントローラの GUI を使用して現地の日時を設定する手順は、次のとおりです。

ステップ 1　[Commands] > [Set Time] の順に選択して [Set Time] ページを開きます（図 2-15 を参照）。

図 2-15　[Set Time] ページ



現在の日時がページ上部に表示されます。

ステップ 2　[Timezone] セクションの [Location] ドロップダウン ボックスから現地の時間帯を選択します。

（注）　Daylight Saving Time（DST; 夏時間）を使用する時間帯を選択すると、DST の発生時の時間変更を反映してコントローラが自動的にそのシステム クロックを設定します。米国では、DST は 3 月の第 2 日曜から始まり、11 月の第 1 日曜日で終わります。

（注）　時間帯デルタをコントローラ GUI で設定することはできません。ただし、コントローラ CLI で設定した場合は、その変更がコントローラ GUI の [Delta Hours] フィールドと [Mins] フィールドに反映されます。

ステップ 3　[Set Timezone] をクリックして、変更を適用します。

ステップ 4　[Date] セクションの [Month] と [Day] のドロップダウン ボックスから現在の現地の月と日を選択し、[Year] フィールドに年を入力します。

ステップ 5　[Time] セクションの [Hour] ドロップダウン ボックスから現在の現地時間を選択し、[Minutes] フィールドと [Seconds] フィールドに分と秒を入力します。

（注）　日時を設定した後に、時間帯のロケーションを変更すると、[Time] セクションの値が更新され、この新しい時間帯のロケーションが反映されます。たとえば、コントローラが東部標準時の正午に設定されていて、時間帯を太平洋標準時に変更すると、時間は自動的に午前 9 時に変更されます。

ステップ 6　[Set Date and Time] をクリックして、変更を適用します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した日時の設定

コントローラの CLI を使用して現地の日時を設定する手順は、次のとおりです。

ステップ 1　コントローラ上の現在の現地日時を GMT で設定するには、次のコマンドを入力します。

config time manual *mm/dd/yy hh:mm:ss*

（注）　時刻を設定するときは、現在の現地時間を GMT で表した時間を 00:00 ～ 24:00 の範囲内の値として入力します。たとえば、米国の太平洋標準時刻の午前 8 時の場合は 16:00 と入力します。太平洋標準時の時間帯は GMT より 8 時間遅れているからです。

ステップ 2　コントローラに時間帯を設定するには、次のいずれかを実行します。

- 夏時間（DST）が発生時に自動的に設定されるように時間帯ロケーションを設定するには、次のコマンドを入力します。

  config time timezone location *location_index*

  location_index は次の時間帯ロケーションの 1 つを表す数字です。

  - 1.（GMT-12:00）国際日付変更線の西側
  - 2.（GMT-11:00）サモア
  - 3.（GMT-10:00）ハワイ
  - 4.（GMT-9:00）アラスカ
  - 5.（GMT-8:00）太平洋標準時（米国およびカナダ）
  - 6.（GMT-7:00）山地標準時（米国およびカナダ）
  - 7.（GMT-6:00）中部標準時（米国およびカナダ）
  - 8.（GMT-5:00）東部標準時（米国およびカナダ）
  - 9.（GMT-4:00）大西洋標準時（カナダ）
  - 10.（GMT-3:00）ブエノスアイレス（アルゼンチン）
  - 11.（GMT-2:00）中央大西洋
  - 12.（GMT-1:00）アゾレス諸島
  - 13.（GMT）ロンドン、リスボン、ダブリン、エジンバラ（デフォルト値）
  - 14.（GMT+1:00）アムステルダム、ベルリン、ローマ、ウィーン
  - 15.（GMT+2:00）エルサレム
  - 16.（GMT+3:00）バクダッド
  - 17.（GMT+4:00）マスカット、アブダビ
  - 18.（GMT+4:30）カブール
  - 19.（GMT+5:00）カラチ、イスラマバード、タシケント
  - 20.（GMT+5:30）コロンボ、コルカタ、ムンバイ、ニューデリー
  - 21.（GMT+5:45）カトマンズ
  - 22.（GMT+6:00）アルマティ、ノボシビルスク
  - 23.（GMT+6:30）ラグーン
  - 24.（GMT+7:00）サイゴン、ハノイ、バンコク、ジャカルタ

- 25.（GMT+8:00）香港、北京、重慶
- 26.（GMT+9:00）東京、大阪、札幌
- 27.（GMT+9:30）ダーウィン
- 28.（GMT+10:00）シドニー、メルボルン、キャンベラ
- 29.（GMT+11:00）マガダン、ソロモン諸島、ニューカレドニア
- 30.（GMT+12:00）カムチャッカ、マーシャル諸島、フィジー

（注）　このコマンドを入力すると、DST に入ったときに、コントローラが自動的にそのシステムクロックを DST に合わせて設定します。米国では、DST は 3 月の第 2 日曜から始まり、11 月の第 1 日曜日で終わります。

- DST が自動的に設定されないように時間帯を手動で設定するには、次のコマンドを入力します。

  config time timezone *delta_hours delta_mins*

  delta_hours は GMT と現地時間の差の時間部分、*delta_mins* は GMT と現地時間の差の分部分です。

  時間帯を手動で設定するときは、GMT を基準とした現在の時間帯の時差を +/- を付けて入力します。たとえば、米国の太平洋標準時は、GMT の時刻より 8 時間遅れています。したがって、-8 と入力します。

（注）　時間帯を手動で設定することで、コントローラ CLI のみで DST が設定されることを回避できます。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　コントローラが現在の現地時間を現地の時間帯で表示していることを確認するには、次のコマンドを入力します。

show time

次のような情報が表示されます。

```
Time.......................................... Mon Nov 26 10:25:33 2007

Timezone delta................................ 0:0
Timezone location............................. (GMT -5:00) Eastern Time (US and Canada)

NTP Servers
    NTP Polling Interval...................... 86400

     Index              NTP Server
    -------  --------------------------------
       1              19.1.1.1
```

（注）　時間帯ロケーションが設定済みの場合は、[Timezone] の [Delta] の値は「0:0」に設定されます。時間帯デルタを使用して時間帯を手動で設定した場合は、[Timezone] の [Location] は空白になります。

Telnet および SSH セッションの設定

Telnet は、コントローラの CLI にアクセスするためのネットワーク プロトコルです。Secure Shell（SSH）は Telnet のセキュリティをさらに強化したプロトコルであり、データ暗号化およびセキュア チャネルを使用してデータを転送します。コントローラ GUI と CLI のどちらでも、Telnet および SSH のセッションを設定できます。

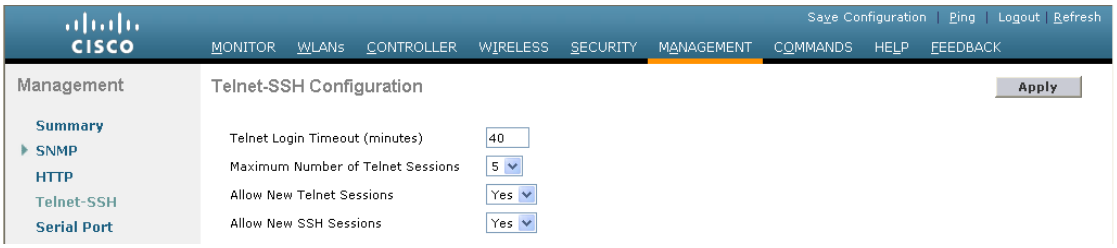
（注）　Telnet または SSH を使用して Lightweight アクセス ポイントのトラブルシューティングを行う手順については、「Telnet または SSH を使用したアクセス ポイントのトラブルシューティング」（P.D-49）を参照してください。

GUI を使用した Telnet/SSH セッションの設定

コントローラの GUI を使用して Telnet および SSH のセッションを設定する手順は、次のとおりです。

ステップ 1　[Management] > [Telnet-SSH] の順にクリックして [Telnet-SSH Configuration] ページを開きます（図 2-16 を参照）。

図 2-16　[Telnet-SSH Configuration] ページ



ステップ 2　[Telnet Login Timeout] フィールドに、非アクティブの Telnet セッションを終了させるまでの時間を分単位で入力します。有効な値の範囲は 0 ～ 160 分で、デフォルト値は 5 分です。値が 0 の場合は、タイムアウトしないことを表します。

ステップ 3　[Maximum Number of Telnet Sessions] ドロップダウン ボックスから、同時 Telnet セッションの最大数を選択します。有効な値の範囲は 0 ～ 5 セッションで、デフォルト値は 5 セッションです。

ステップ 4　コントローラ上での新規 Telnet セッションを許可する場合は [Allow New Telnet Sessions] ドロップダウン ボックスから [Yes] を選択し、許可しない場合は [No] を選択します。デフォルト値は [No] です。

ステップ 5　コントローラ上での新規 SSH セッションを許可する場合は [Allow New SSH Sessions] ドロップダウン ボックスから [Yes] を選択し、許可しない場合は [No] を選択します。デフォルト値は [Yes] です。

ステップ 6　[Apply] をクリックして、変更を適用します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

ステップ 8　Telnet 設定の概要を表示するには、[Management] > [Summary] を選択します。[Summary] ページが表示されます（図 2-17 を参照）。

図 2-17　[Summary] ページ

Telnet および SSH の追加のセッションが許可されるかどうかが、このページに表示されます。

CLI を使用した Telnet/SSH セッションの設定

コントローラの CLI を使用して Telnet および SSH のセッションを設定する手順は、次のとおりです。

ステップ 1　コントローラ上での新規 Telnet セッションを許可または禁止するには、次のコマンドを入力します。

config network telnet {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 2　コントローラ上での新規 SSH セッションを許可または禁止するには、次のコマンドを入力します。

config network ssh {**enable** | **disable**}

デフォルト値は有効（enable）です。

ステップ 3　非アクティブの Telnet セッションを終了させるまでの時間（分単位）を指定するには、次のコマンドを入力します。

config sessions timeout *timeout*

timeout は、0 ～ 160 分の範囲内の値です。デフォルト値は 5 分です。値が 0 の場合は、タイムアウトしないことを表します。

ステップ 4　同時 Telnet セッションの最大数を指定するには、次のコマンドを入力します。

config sessions maxsessions *session_num*

session_num は、0 ～ 5 の範囲内の値です。デフォルト値は 5 セッションです。

ステップ 5　変更を保存するには、次のコマンドを入力します。

save config

ステップ 6　Telnet と SSH の設定を表示するには、次のコマンドを入力します。

show network summary

次のような情報が表示されます。

```
RF-Network Name.............................. TestNetwork1
Web Mode..................................... Enable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh)........................... Enable
```

```
Telnet..................................... Disable
...
```

ステップ 7　Telnet セッションの設定を表示するには、次のコマンドを入力します。

show sessions

次のような情報が表示されます。

```
CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

ステップ 8　アクティブな Telnet セッションをすべて表示するには、次のコマンドを入力します。

show loginsession

次のような情報が表示されます。

```
ID    User Name      Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00      admin           EIA-232     00:00:00      00:19:04
```

ステップ 9　アクティブな Telnet セッションをすべて終了させる、または特定の Telnet セッションを終了させるには、次のコマンドを入力します。

config loginsession close {**all** | *session_id*}

GUI と CLI へのワイヤレス接続の有効化

無線クライアントを使用してコントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード以外のすべての管理タスクでサポートされています。

無線クライアント デバイスから GUI または CLI を開くには、接続が許可されるようにコントローラを設定する必要があります。GUI や CLI への無線接続を有効にする手順は、次のとおりです。

ステップ 1　CLI にログインします。

ステップ 2　**config network mgmt-via-wireless enable** と入力します。

ステップ 3　無線クライアントを使用して、コントローラに接続されている Lightweight アクセス ポイントにアソシエートします。

ステップ 4　無線クライアントで、コントローラの Telnet セッションを開くか、コントローラの GUI にブラウザからアクセスします。

ヒント　コントローラの GUI を使用して無線接続を有効にするには、[Management > Mgmt Via Wireless] ページを選択して、[Enable Controller Management to be accessible from Wireless Clients] チェックボックスをオンにします。