



アクセス ポイントの管理

この章では、wireless device の管理方法について説明します。この章の内容は、次のとおりです。

- [モード ボタンの無効化 \(P. 5-2\)](#)
- [アクセス ポイントへの不正アクセスの防止 \(P. 5-3\)](#)
- [特権 EXEC コマンドへのアクセス防止 \(P. 5-4\)](#)
- [RADIUS によるアクセス ポイントへのアクセスの制御 \(P. 5-10\)](#)
- [TACACS+ によるアクセス ポイントへのアクセスの制御 \(P. 5-15\)](#)
- [イーサネットの速度およびデュプレックスの設定 \(P. 5-18\)](#)
- [アクセス ポイントの無線ネットワーク管理の設定 \(P. 5-19\)](#)
- [アクセス ポイントのローカル認証および許可の設定 \(P. 5-19\)](#)
- [認証キャッシュとプロファイルの設定 \(P. 5-21\)](#)
- [DHCP サービスを提供するためのアクセス ポイントの設定 \(P. 5-24\)](#)
- [アクセス ポイントの Secure Shell の設定 \(P. 5-27\)](#)
- [クライアント ARP キャッシングの設定 \(P. 5-28\)](#)
- [システムの日時の管理 \(P. 5-30\)](#)
- [HTTP アクセスの定義 \(P. 5-35\)](#)
- [HTTP アクセスの定義 \(P. 5-35\)](#)
- [バナーの作成 \(P. 5-39\)](#)
- [Autonomous Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードする方法 \(P. 5-41\)](#)
- [日本の W52 ドメインへの移行方法 \(P. 5-41\)](#)
- [ポイントツーマルチポイントブリッジにおける複数の VLAN とレート制限の設定 \(P. 5-43\)](#)

モード ボタンの無効化


コンソール ポートを搭載したアクセス ポイントのモード ボタンは、`[no] boot mode-button` コマンドで無効にできます。このコマンドを使用するとパスワードによるリカバリを防ぎ、権限のないユーザがアクセス ポイントの CLI にアクセスできないようにします。



注意

このコマンドは、パスワードによるリカバリを無効にします。このコマンドを入力した後、アクセス ポイントの特権 EXEC モードのパスワードを紛失してしまうと、アクセス ポイントの CLI にアクセスしなおすには、シスコの Technical Assistance Center (TAC) に連絡する必要があります。

モード ボタンはデフォルトで有効に設定されています。特権 EXEC モードから、次の手順に従ってアクセス ポイントのモード ボタンを無効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no boot mode-button</code>	アクセス ポイントのモード ボタンを無効にします。
ステップ 3	<code>end</code>	 (注) この設定は保存する必要はありません。

モード ボタンのステータスをチェックするには、特権 EXEC モードから `show boot` または `show boot mode-button` コマンドを実行します。設定の実行時には、ステータスが表示されません。`show boot` と `show boot mode-button` コマンドを実行すると、通常次のような応答が表示されます。

```
ap#show boot
BOOT path-list:
flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap#show boot mode-button
on
ap#
```



(注)

特権 EXEC のパスワードがわかっている場合は、`boot mode-button` コマンドを使用して、モード ボタンを通常動作に復旧できます。

アクセスポイントへの不正アクセスの防止

権限のないユーザが wireless device の設定を変更したり、設定情報を表示したりするのを防ぐことができます。通常は、ネットワーク管理者から wireless device へのアクセスを許可し、ローカルネットワーク内の端末またはワークステーションから接続するユーザのアクセスは制限します。

wireless device への不正なアクセスを防ぐには、次のいずれかのセキュリティ機能を設定してください。

- wireless device でローカルに保存されるユーザ名とパスワードの組み合わせ。この組み合わせによって、各ユーザは wireless device にアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り / 書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細は、「[ユーザ名とパスワードの組み合わせの設定](#)」の項（P. 5-7）を参照してください。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。ユーザ名とパスワードでは、大文字と小文字が区別されます。



(注) TAB、?、\$、+、および [は、パスワードには無効な文字です。

- セキュリティ サーバのデータベースに集中的に保存されたユーザ名とパスワードの組み合わせ。詳細は、「[RADIUS によるアクセスポイントへのアクセスの制御](#)」の項（P. 5-10）を参照してください。

特権 EXEC コマンドへのアクセス防止

ネットワークで端末のアクセスを制御する簡単な方法として、パスワードの使用と特権レベルの割り当てがあります。パスワード保護は、ネットワークまたはネットワーク デバイスへのアクセスを制限します。特権レベルは、ユーザがネットワーク デバイスにログインした後に発行できるコマンドを定義します。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Security Command Reference』を参照してください。

この項では、コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。内容は次のとおりです。

- デフォルト パスワードと特権レベルの設定 (P. 5-4)
- 静的イネーブル パスワードの設定または変更 (P. 5-4)
- 暗号化によるイネーブル パスワードとイネーブル シークレット パスワードの保護 (P. 5-6)
- ユーザ名とパスワードの組み合わせの設定 (P. 5-7)
- 複数の特権レベルの設定 (P. 5-8)

デフォルト パスワードと特権レベルの設定

表 5-1 にデフォルト パスワードと特権レベルの設定を示します。

表 5-1 デフォルト パスワードと特権レベル

機能	デフォルト設定
ユーザ名とパスワード	デフォルトのユーザ名は <i>Cisco</i> 、デフォルトのパスワードは <i>Cisco</i> です。
イネーブル パスワードと特権レベル	デフォルトのパスワードは <i>Cisco</i> です。デフォルトはレベル 15 (特権 EXEC レベル) です。パスワードはコンフィギュレーション ファイルで暗号化されます。
イネーブル シークレット パスワードと特権レベル	デフォルトの特権 パスワードは <i>Cisco</i> です。デフォルトはレベル 15 (特権 EXEC レベル) です。パスワードはコンフィギュレーション ファイルに書き込まれる前に暗号化されます。
回線パスワード	デフォルトのパスワードは <i>Cisco</i> です。パスワードはコンフィギュレーション ファイルで暗号化されます。

静的イネーブル パスワードの設定または変更


イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。



(注)

グローバル設定コマンド `no enable password` は、イネーブル パスワードを削除しますが、このコマンドを使用する場合は十分な注意が必要です。イネーブル パスワードを削除すると、EXEC モードからロックアウトされます。

特権 EXEC モードから、次の手順に従って静的イネーブルパスワードを設定または変更します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>enable password <i>password</i></code>	<p>特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>デフォルトのパスワードは <i>Cisco</i> です。</p> <p><i>password</i> には 1 ~ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。パスワードにクエスチョン マーク (?) を含めることができます。その場合はパスワードを作成するとき、クエスチョン マークを入力する前に Ctrl+V キーを押してください。たとえば、パスワード abc?123 を作成する場合は、次のように入力します。</p> <ol style="list-style-type: none"> 1. abc を入力します。 2. Ctrl+V を入力します。 3. ?123 を入力します。 <p>イネーブルパスワードの入力を求められたときは、クエスチョン マークの前で Ctrl+V キーを押す必要はありません。パスワード プロンプトで単純に abc?123 と入力します。</p> <p> (注) TAB、?、\$、+、および [は、パスワードには無効な文字です。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	<p>(オプション) コンフィギュレーション ファイルに入力内容を保存します。</p> <p>イネーブルパスワードは暗号化されず、wireless device のコンフィギュレーション ファイルで読み取ることができます。</p>

次の例は、イネーブルパスワードを *l1u2c3k4y5* に変更する方法を示しています。パスワードは暗号化されず、レベル 15 へのアクセス (従来の特権 EXEC モードへのアクセス) を可能にします。

```
AP(config)# enable password l1u2c3k4y5
```


暗号化によるイネーブルパスワードとイネーブルシークレットパスワードの保護

セキュリティレベルを強化するために、特にネットワークを越えるパスワードや Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバに保存されたパスワードについて、グローバル設定コマンド `enable password` または `enable secret` を使用できます。どちらのコマンドを使っても、ユーザが特権 EXEC モード (デフォルト) または指定した特権レベルにアクセスする場合に入力が要求される暗号化パスワードを設定できます。

より高度な暗号化アルゴリズムを使用しているため、`enable secret` コマンドの使用をお勧めします。

`enable secret` コマンドを設定する場合、`enable password` コマンドよりも優先されます。2つのコマンドを同時に有効にはできません。

特権 EXEC モードから、次の手順に従ってイネーブルパスワードとイネーブルシークレットパスワードに暗号化を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>enable password [level level] {password encryption-type encrypted-password}</code> または <code>enable secret [level level] {password encryption-type encrypted-password}</code>	<p>特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>または</p> <p>シークレットパスワードを定義します。これは非可逆的暗号化方式を使用して保存されます。</p> <ul style="list-style-type: none"> (オプション) <code>level</code> の指定範囲は 0 ~ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。デフォルトのレベルは 15 (特権 EXEC モードの特権) です。 <code>password</code> には 1 ~ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。 (オプション) <code>encryption-type</code> には、タイプ 5 (シスコ独自の暗号化アルゴリズム) だけが指定できます。暗号化タイプを指定する場合は、別のアクセスポイントの設定からコピーした暗号化パスワードを指定する必要があります。 <p> (注) 暗号化タイプを指定し、クリアテキストパスワードを入力すると、特権 EXEC モードを再開できません。失われた暗号化パスワードはどのような方法でも復元できません。</p>
ステップ 3	<code>service password-encryption</code>	<p>(オプション)パスワードの定義時または設定の書き込み時にパスワードを暗号化します。</p> <p>暗号化により、パスワードをコンフィギュレーション ファイルで読み取ることができなくなります。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

イネーブルパスワードとイネーブルシークレットパスワードが両方とも定義されている場合、ユーザはイネーブルシークレットパスワードの方を入力する必要があります。

特定の特権レベル用のパスワードを定義するには、level キーワードを指定します。レベルを指定し、パスワードを設定した後、このレベルでアクセスする必要のあるユーザだけにパスワードを与えてください。任意のレベルでアクセスできるコマンドを指定する場合は、グローバル設定コマンド `privilege level` を使用します。詳細は、「複数の特権レベルの設定」の項 (P. 5-8) を参照してください。

パスワードの暗号化を有効にすると、ユーザ名パスワード、認証キーパスワード、特権コマンドパスワード、コンソールと仮想端末の回線パスワードを含むすべてのパスワードに適用されます。

パスワードとレベルを削除するには、グローバル設定コマンド `no enable password [level level]` または `no enable secret [level level]` を使用します。パスワードの暗号化を無効にするには、グローバル設定コマンド `no service password-encryption` を使用します。

次の例は、特権レベル 2 の暗号化パスワード `1FaD0$Xyti5Rkls3LoyxzS8` を設定する方法を示しています。

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

ユーザ名とパスワードの組み合わせの設定

ユーザ名とパスワードの組み合わせを設定できます。これは、wireless device でローカルに保存されます。ユーザ名とパスワードの組み合わせは、回線またはインターフェイスに割り当てられ、各ユーザが wireless device にアクセスする際の認証に使用されます。特権レベルを定義している場合、ユーザ名とパスワードのそれぞれの組み合わせに特定の特権レベル(アソシエートされている権利と特権を含む)を割り当てることができます。

特権 EXEC モードから、次の手順に従って、ログイン ユーザ名とパスワードを要求するユーザ名ベースの認証システムを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>username name [privilege level]</code> <code>{password encryption-type password}</code>	各ユーザのユーザ名、特権レベル、パスワードを入力します。 <ul style="list-style-type: none"> <code>name</code> には、ユーザ ID を 1 ワードで指定します。空白と引用符は使用できません。 (オプション) <code>level</code> には、ユーザがアクセス後に取得する特権レベルを指定します。指定範囲は 0 ~ 15 です。レベル 15 は特権 EXEC モードのアクセスを許可します。レベル 1 はユーザ EXEC モードのアクセスを許可します。 <code>encryption-type</code> には、後ろに暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。非表示のパスワードが続くことを指定するには 7 を入力します。 <code>password</code> には、wireless device へアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ~ 25 文字の間で指定します。空白を入れることもできます。また、パスワードは必ず <code>username</code> コマンドの最後のオプションとして指定してください。
ステップ 3	<code>login local</code>	ログイン時にローカルパスワードのチェック機能を有効にします。認証はステップ 2 で指定したユーザ名に基づいて実行されます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

■ 特権 EXEC コマンドへのアクセス防止

	コマンド	目的
ステップ 5	show running-config	入力内容を確認します。
ステップ 6	copy running-config startup-config	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

特定のユーザに対してユーザ名の認証を無効にするには、グローバル設定コマンド `no username name` を使用します。

パスワードチェック機能を無効にし、パスワードを指定しない接続を許可する場合は、回線設定コマンド `no login` を使用します。



(注) ユーザ名は 1 つ以上設定しなければなりません。また、`login local` を `wireless device` との Telnet セッションを開くように設定する必要があります。ユーザ名が 1 つだけの場合にそのユーザ名を入力しないと、`wireless device` からロックアウトされることがあります。

複数の特権レベルの設定

デフォルトでは、Cisco IOS ソフトウェアにはユーザ EXEC モードと特権 EXEC モードという 2 つのパスワードセキュリティのモードがあります。各モードにコマンドの階層を最大 16 レベルまで設定できます。複数のパスワードを設定すると、ユーザグループ別に特定のコマンド群へのアクセスを許可できます。

たとえば、`clear line` コマンドへのアクセスを多くのユーザに許可する場合は、このコマンドにレベル 2 のセキュリティを指定し、レベル 2 のパスワードを広く配布します。一方、`configure` コマンドについては、アクセスをもう少し制限する場合は、このコマンドにレベル 3 のセキュリティを指定し、より限られたユーザグループにレベル 3 のパスワードを配布します。


この項では設定情報を扱います。

- [コマンドに対する特権レベルの設定 \(P. 5-8\)](#)
- [特権レベルへのログインと終了 \(P. 5-9\)](#)

コマンドに対する特権レベルの設定

特権 EXEC モードから、次の手順に従って特定のコマンドモードに特権レベルを設定します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	privilege mode level level command	コマンドに特権レベルを設定します。 <ul style="list-style-type: none"> • <i>mode</i> には、グローバル コンフィギュレーション モードの場合は <code>configure</code> を、EXEC モードの場合は <code>exec</code> を、インターフェイス設定モードの場合は <code>interface</code> を、回線設定モードの場合は <code>line</code> を入力します。 • <i>level</i> の指定範囲は 0 ~ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。レベル 15 はイネーブルパスワードで許可されるアクセスレベルです。 • <i>command</i> にはアクセスを制限するコマンドを指定します。

	コマンド	目的
ステップ 3	<code>enable password level level password</code>	<p>特権レベルにイネーブルパスワードを指定します。</p> <ul style="list-style-type: none"> <code>level</code> の指定範囲は 0 ~ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。 <code>password</code> には 1 ~ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。 <p> (注) TAB、?、\$、+、および [は、パスワードには無効な文字です。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code> または <code>show privilege</code>	<p>入力内容を確認します。</p> <p>最初のコマンドは、パスワードとアクセスレベルの設定を表示します。2 番目のコマンドは、特権レベルの設定を表示します。</p>
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

コマンドに特権レベルを設定すると、そのコマンドの一部を構文とするコマンドもすべてそのレベルに設定されます。たとえば、`show ip route` コマンドをレベル 15 に設定すると、個別に異なるレベルに設定しない限り、`show` コマンドと `show ip` コマンドも自動的にレベル 15 に設定されます。

特定のコマンドについてデフォルトの特権に戻すには、グローバル設定コマンド `no privilege mode level level command` を使用します。

次の例は、`configure` コマンドを特権レベル 14 に設定し、ユーザがレベル 14 のコマンドを使用する場合に入力するパスワードとして `SecretPswd14` を定義する方法を示しています。

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

特権レベルへのログインと終了

特権 EXEC モードから、次の手順に従って、指定された特権レベルにログインし、指定された特権レベルに出ます。

	コマンド	目的
ステップ 1	<code>enable level</code>	<p>指定した特権レベルにログインします。</p> <p><code>level</code> の指定範囲は 0 ~ 15 です。</p>
ステップ 2	<code>disable level</code>	<p>指定した特権レベルに出ます。</p> <p><code>level</code> の指定範囲は 0 ~ 15 です。</p>

RADIUS によるアクセスポイントへのアクセスの制御

この項では、Remote Authentication Dial-In User Service (RADIUS) を使用して、wireless device の管理者アクセス権を制御する手順について説明します。RADIUS をサポートするように wireless device を設定する手順の詳細は、第13章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

RADIUS は詳細なアカウント情報を提供し、認証と許可のプロセスを柔軟に管理します。RADIUS は AAA を通じて効率化され、AAA コマンドでのみ有効に設定できます。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Security Command Reference for Release 12.3』を参照してください。

次の各項で RADIUS の設定について説明します。

- [デフォルトの RADIUS 設定 \(P. 5-10\)](#)
- [RADIUS ログイン認証の設定 \(P. 5-10\)](#) (必須)
- [AAA サーバグループの定義 \(P. 5-12\)](#) (オプション)
- [ユーザ特権アクセスとネットワークサービスの RADIUS 許可の設定 \(P. 5-14\)](#) (オプション)
- [RADIUS 設定の表示 \(P. 5-14\)](#)

デフォルトの RADIUS 設定

RADIUS と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから RADIUS を設定することはできません。RADIUS を有効にすると、Command-Line Interface (CLI; コマンドライン インターフェイス) 経由で wireless device にアクセスするユーザを認証できます。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト(名前は、*default*)です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストには、ユーザの認証時に照会されるシーケンスと認証方式が記述されています。認証に使用するセキュリティプロトコルを1つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップシステムが確実に機能します。ソフトウェアは、まずリストの最初の方法を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、つまりセキュリティサーバまたはローカルユーザ名データベースがユーザアクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

特権 EXEC モードから、次の手順に従ってログイン認証を設定します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。
ステップ 3	<code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドで名前付きリストの指定をしない場合、使用されるデフォルトのリストを作成する場合は、default キーワードの後に、デフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • <i>list-name</i> には、作成するリストに付ける名前の文字列を指定します。 • <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • local : 認証にローカル ユーザー名データベースを使用します。データベースにユーザー名情報を入力する必要があります。これには、グローバル設定コマンド <code>username password</code> を使用します。 • radius : RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細は、「RADIUS サーバホストの識別」の項 (P. 13-5) を参照してください。
ステップ 4	<code>line [console tty vty] line-number [ending-line-number]</code>	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	<code>login authentication {default list-name}</code>	<p>認証リストを 1 つまたは複数の回線に適用します。</p> <ul style="list-style-type: none"> • default を指定すると、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストが使用されます。 • <i>list-name</i> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド `no aaa new-model` を使用します。AAA 認証を無効にするには、グローバル設定コマンド `no aaa authentication login {default | list-name} method1 [method2...]` を使用します。ログインの RADIUS 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド `no login authentication {default | list-name}` を使用します。

AAA サーバグループの定義


認証時に AAA サーバグループを使用して既存のサーバホストをグループ化するように wireless device を設定できます。設定されたサーバホストのサブセットを選択して、特定のサービスに使用します。このサーバグループは、グローバルサーバホストリストで使用されます。このリストには、選択されたサーバホストの IP アドレスのリストが示されています。

各ホストエントリが一意的識別子 (IP アドレスと UDP ポート番号の組み合わせ) を持っていれば、同一サーバに対する複数のホストエントリをサーバグループに含めることも可能です。それによって、特定の AAA サービスを提供する RADIUS ホストとして、異なるポートを個別に定義できます。同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホストエントリを設定すると、2 番目に設定されたホストエントリは最初のホストエントリの故障時のバックアップとして機能します。

特定のサーバを定義済みグループサーバにアソシエートするには、グループサーバ設定コマンド `server` を使用します。IP アドレスでサーバを特定するか、オプションの `auth-port` および `acct-port` キーワードを使用して複数のホストインスタンスまたはエントリを特定できます。

特権 EXEC モードから、次の手順に従って、AAA サーバグループを定義し、特定の RADIUS サーバをそのグループにアソシエートします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。
ステップ 3	<code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> (オプション) <code>auth-port port-number</code> には、認証要求の User Datagram Protocol (UDP; ユーザ データグラム プロトコル) 宛先ポートを指定します。 (オプション) <code>acct-port port-number</code> には、アカウントリング要求の UDP 宛先ポートを指定します。 (オプション) <code>timeout seconds</code> には、wireless device が RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定範囲は 1 ~ 1000 です。この設定はグローバル設定コマンド <code>radius-server timeout</code> の設定よりも優先されます。<code>radius-server host</code> コマンドでこのタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。 (オプション) <code>retransmit retries</code> には、サーバが応答しない場合または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド <code>radius-server retransmit</code> の設定が使用されます。 (オプション) <code>key string</code> には、wireless device と RADIUS サーバで動作する RADIUS デーモンの間で使用される認証と暗号キーを指定します。

コマンド	目的
	 <p>(注) このキーはテキスト文字列で、その文字列はRADIUSサーバで使用される暗号キーと一致しなければなりません。キーは必ず <code>radius-server host</code> コマンドの最後に設定してください。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。</p> <p>wireless device が単一の IP アドレスと関連付けられた複数のホストエントリを認識するように設定するには、このコマンドを必要な回数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。wireless device ソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用されるタイムアウト、再送信、暗号キーの値を設定します。</p>
ステップ 4 <code>aaa group server radius group-name</code>	AAA サーバグループをグループ名で定義します。 このコマンドを実行すると、wireless device はサーバグループ設定モードへ移行します。
ステップ 5 <code>server ip-address</code>	特定の RADIUS サーバを定義されたサーバグループにアソシエートします。この手順を、AAA サーバグループの各 RADIUS サーバについて繰り返します。 グループ内の各サーバは、手順 2 であらかじめ定義されている必要があります。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code>	入力内容を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。
ステップ 9	RADIUS ログイン認証を有効にします。「 RADIUS ログイン認証の設定 」の項 (P. 13-8) を参照してください。

特定の RADIUS サーバを削除するには、グローバル設定コマンド `no radius-server host hostname | ip-address` を使用します。設定リストからサーバグループを削除する場合は、グローバル設定コマンド `no aaa group server radius group-name` を使用します。また、RADIUS サーバの IP アドレスを削除するには、サーバグループ設定コマンド `no server ip-address` を使用します。

次の例では、wireless device は異なる 2 つの RADIUS グループサーバ (`group1` と `group2`) を認識するように設定されます。group1 には、同じ RADIUS サーバで同じサービス用に設定された異なる 2 つのホストエントリがあります。2 番目のホストエントリは、最初のエントリに対して故障時のバックアップとして機能します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

ユーザ特権アクセスとネットワーク サービスの RADIUS 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可が有効の場合、wireless device は、ローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザが要求したサービスへのアクセスを許可されるのは、ユーザ プロファイル内の情報により許可された場合だけです。

グローバル設定コマンド `aaa authorization` と `radius` キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec radius local` コマンドは次の許可パラメータを設定します。

- 認証に RADIUS が使用された場合は、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS が使用されなかった場合は、ローカル データベースを使用します。



(注) CLI を通してログインした認証済みユーザは、許可が設定されていても許可が省略されます。

特権 EXEC モードから、次の手順に従って特権 EXEC アクセスとネットワーク サービスに RADIUS 許可を指定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるように wireless device を設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、wireless device を設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド `no aaa authorization {network | exec} method1` を使用します。

RADIUS 設定の表示

RADIUS 設定を表示するには、特権 EXEC コマンド `show running-config` を使用します。

TACACS+ によるアクセスポイントへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus (TACACS+) を使用して wireless device の管理者アクセス権を制御する手順について説明します。TACACS+ をサポートするように wireless device を設定する手順の詳細は、第13章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

TACACS+ は詳細なアカウント情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は AAA を通じて効率化され、AAA コマンドでのみ有効に設定できます。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Security Command Reference for Release 12.3』を参照してください。

次の項で TACACS+ の設定について説明します。

- [デフォルトの TACACS+ 設定 \(P. 5-15\)](#)
- [TACACS+ ログイン認証の設定 \(P. 5-15\)](#)
- [特権 EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定 \(P. 5-17\)](#)
- [TACACS+ 設定の表示 \(P. 5-17\)](#)

デフォルトの TACACS+ 設定

TACACS+ と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 経由で wireless device にアクセスする管理者を認証できます。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト(名前は、*default*)です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義された方式リストは、デフォルトの方式リストよりも優先されます。

方式リストには、ユーザの認証時に照会されるシーケンスと認証方式が記述されています。認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップシステムが確実に機能します。ソフトウェアは、まずリストの最初の方法を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースがユーザ アクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

特権 EXEC モードから、次の手順に従ってログイン認証を設定します。この手順は必須です。

■ TACACS+ によるアクセスポイントへのアクセスの制御

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。
ステップ 3	<code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • <code>login authentication</code> コマンドで名前付きリストの指定をしない場合に使用されるデフォルトのリストを作成する場合は、<code>default</code> キーワードの後に、デフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • <code>list-name</code> には、作成するリストに付ける名前の文字列を指定します。 • <code>method1...</code> には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • <code>local</code> : 認証にローカル ユーザー名データベースを使用します。データベースにユーザー名情報を入力する必要があります。これには、グローバル設定コマンド <code>username password</code> を使用します。 • <code>tacacs+</code> : TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。
ステップ 4	<code>line [console tty vty] line-number [ending-line-number]</code>	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	<code>login authentication {default list-name}</code>	<p>認証リストを 1 つまたは複数の回線に適用します。</p> <ul style="list-style-type: none"> • <code>default</code> を指定すると、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストが使用されます。 • <code>list-name</code> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド `no aaa new-model` を使用します。AAA 認証を無効にするには、グローバル設定コマンド `no aaa authentication login {default | list-name} method1 [method2...]` を使用します。ログインの TACACS+ 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド `no login authentication {default | list-name}` を使用します。

特権 EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可が有効の場合、wireless device は、ローカル ユーザ データベースかセキュリティ サーバ上にあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザが要求したサービスへのアクセスを許可されるのは、ユーザ プロファイル内の情報により許可された場合だけです。

グローバル設定コマンド `aaa authorization` と `tacacs+` キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec tacacs+ local` コマンドは次の許可パラメータを設定します。

- 認証に TACACS+ が使用された場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用していない場合、ローカル データベースを使用します。



(注) CLI を通してログインした認証済みユーザは、許可が設定されていても許可が省略されます。

特権 EXEC モードから、次の手順に従って特権 EXEC アクセスとネットワーク サービスに TACACS+ 許可を指定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network tacacs+</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが TACACS+ 許可を受けるように <code>wireless device</code> を設定します。
ステップ 3	<code>aaa authorization exec tacacs+</code>	ユーザの TACACS+ 許可でユーザの特権 EXEC アクセス権の有無を判断するように、 <code>wireless device</code> を設定します。 <code>exec</code> キーワードを指定すると、ユーザ プロファイル情報 (<code>autocommand</code> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド `no aaa authorization {network | exec} method1` を使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計を表示するには、特権 EXEC コマンド `show tacacs` を使用します。

イーサネットの速度およびデュプレックスの設定

wireless device のイーサネット ポートに速度およびデュプレックスの設定を割り当てることができます。wireless device のイーサネット ポート上の速度設定とデュプレックス設定のどちらについても、デフォルト設定の **auto** を使用することをお勧めします。wireless device がスイッチからインライン電源を受け取ったときに、速度設定またはデュプレックス設定が変更されるとイーサネットリンクがリセットされ、wireless device がリブートします。wireless device の接続先のスイッチのポートが **auto** に設定されていない場合、wireless device のポートを **half** または **full** に変更してデュプレックスの不一致を修正することができます。これによってイーサネットリンクはリセットされなくなります。ただし、**half** または **full** から **auto** に戻すと、リンクがリセットされ、wireless device がスイッチからインライン電源を受け取ると、その wireless device はリブートします。



(注) wireless device のイーサネット ポート上の速度およびデュプレックスの設定は、wireless device の接続先のポート上のイーサネット設定と一致させる必要があります。wireless device の接続先のポート上の設定を変更する場合は、これと一致するように wireless device のイーサネット ポート上の設定も変更します。

イーサネットの速度とデュプレックスは、デフォルトでは **auto** に設定されています。特権 EXEC モードから、次の手順に従ってイーサネットの速度とデュプレックスを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface fastethernet0</code>	インターフェイス設定モードを開始します。
ステップ 3	<code>speed { 10 100 auto }</code>	イーサネット速度を設定します。デフォルト設定の auto を使用することをお勧めします。
ステップ 4	<code>duplex { auto full half }</code>	デュプレックス設定を行います。デフォルト設定の auto を使用することをお勧めします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

アクセスポイントの無線ネットワーク管理の設定

wireless device を無線ネットワーク管理に対して有効にできます。Wireless Network Manager (WNM; 無線ネットワーク マネージャ) は無線 LAN 上のデバイスを管理します。

wireless device が WNM と対話するように設定するには、次のコマンドを入力します。

```
AP(config)# wlccp wnm ip address ip-address
```

WDS アクセスポイントと WNM の間の認証ステータスをチェックするには、次のコマンドを入力します。

```
AP# show wlccp wnm status
```

not authenticated、*authentication in progress*、*authentication fail*、*authenticated*、*security keys setup* のいずれかのステータスをとります。

アクセスポイントのローカル認証および許可の設定

サーバを介さずに AAA を操作できるように設定するには、ローカル モードで AAA を実装するように wireless device を設定します。wireless device は、認証と許可を処理します。この設定ではアカウントリングは使用できません。




(注) wireless device を 802.1x 対応のクライアント デバイス用のローカル認証サーバとして設定し、メインサーバのバックアップを提供したり、RADIUS サーバのないネットワーク上で認証サービスを提供したりできます。wireless device をローカル認証サーバとして設定する方法の詳細は、[第9章「ローカル認証サーバとしてのアクセスポイントの設定」](#)を参照してください。

特権 EXEC モードから、次の手順に従ってローカル AAA に wireless device を設定します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA を有効にします。
ステップ 3	aaa authentication login default local	ローカル ユーザ名データベースを使用するログイン認証を設定します。default キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	aaa authorization exec local	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	aaa authorization network local	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。

■ アクセスポイントのローカル認証および許可の設定

	コマンド	目的
ステップ 6	<code>username name [privilege level] {password encryption-type password}</code>	<p>ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。</p> <p>このコマンドを各ユーザについて繰り返します。</p> <ul style="list-style-type: none"> <code>name</code> には、ユーザ ID を 1 ワードで指定します。空白と引用符は使用できません。 (オプション) <code>level</code> には、ユーザがアクセス後に取得する特権レベルを指定します。指定範囲は 0 ~ 15 です。レベル 15 は特権 EXEC モードのアクセスを許可します。レベル 0 はユーザ EXEC モードのアクセスを許可します。 <code>encryption-type</code> には、後ろに暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。非表示のパスワードが続くことを指定するには 7 を入力します。 <code>password</code> には、wireless device へアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ~ 25 文字の間で指定します。空白を入れることもできます。また、パスワードは必ず <code>username</code> コマンドの最後のオプションとして指定してください。 <p> (注) TAB、?、\$, +、および [は、パスワードには無効な文字です。</p>
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド `no aaa new-model` を使用します。許可を無効にするには、グローバル設定コマンド `no aaa authorization {network | exec} method1` を使用します。

認証キャッシュとプロファイルの設定

認証キャッシュとプロファイル機能を使用すると、アクセスポイントがユーザのために認証 / 許可応答をキャッシュできるようになります。このため、次回の認証 / 許可要求を AAA サーバに送信しなくて済むようになります。



(注) この機能は、アクセスポイントの Admin 認証にのみサポートされています。

この機能をサポートする次のコマンドが、Cisco IOS リリース 12.3(7) に用意されています。

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```



(注) このコマンドについては、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.3(7)JA』を参照してください。

次の例は、Admin 認証用に設定したアクセスポイントの設定例です。認証キャッシュを有効に設定した状態の TACACS+ を使用しています。この例では TACACS サーバを使用していますが、アクセスポイントは RADIUS を使用して Admin 認証用に設定できます。

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
```

```

cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache

!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908

```

```
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7
111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

DHCP サービスを提供するためのアクセスポイントの設定

次の項では、wireless device を DHCP サーバとして機能させる方法について説明します。

- DHCP サーバの設定 (P. 5-24)
- DHCP サーバ アクセスポイントの監視と維持 (P. 5-25)

DHCP サーバの設定

デフォルトでは、アクセスポイントは、ネットワーク上の DHCP サーバから IP 設定を受信するように設定されています。アクセスポイントを DHCP サーバとして機能するように設定し、IP 設定を、有線 LAN と無線 LAN 両方のデバイスに割り当てることもできます。

1100 シリーズのアクセスポイントは、デフォルト設定ではミニ DHCP サーバとして機能し、DHCP サーバから IP 設定を受信できません。ミニ DHCP サーバとして、1100 シリーズのアクセスポイントは、そのイーサネットポートに接続されている 1 台の PC と無線クライアントデバイスに 10.0.0.11 ~ 10.0.0.30 の範囲の最大 20 個の IP アドレスを提供します。無線クライアントデバイスについては、Service Set Identifier (SSID; サービスセット ID) を使用しないように設定され、すべてのセキュリティ設定が無効になるものが対象となります。このミニ DHCP サーバの機能は、1100 シリーズのアクセスポイントに静的 IP アドレスを割り当てると、自動的に無効になります。初期セットアップを簡単にするためのコンソールポートがあるので、1200 シリーズのアクセスポイントは自動的に DHCP サーバにはなりません。



(注)

アクセスポイントを DHCP サーバとして設定すると、IP アドレスがそのサブネット上のアクセスポイントに割り当てられます。このアクセスポイントは、サブネット上の他のアクセスポイントと通信しますが、それ以上先とは通信しません。サブネットより先にデータを送信する必要がある場合は、デフォルトのルータを割り当てる必要があります。デフォルトルータの IP アドレスには、DHCP サーバとして設定したアクセスポイントと同じサブネット上のものを設定してください。

DHCP 関連のコマンドとオプションの詳細は、『Cisco IOS IP Configuration Guide for Release 12.3』の「Configuring DHCP」の章を参照してください。次のリンクをクリックすると、「Configuring DHCP」の章を参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

特権 EXEC モードから、次の手順に従って、アクセスポイントが DHCP サービスを提供するように設定し、デフォルトルータを指定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dhcp excluded-address low_address [high_address]</code>	wireless device が割り当てるアドレス範囲から、wireless device の IP アドレスを除外します。アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。 wireless device では、DHCP アドレス プール サブネット中のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定されます。DHCP サーバがクライアントに割り当てるべきでない IP アドレスを指定する必要があります。 (オプション)除外するアドレスの範囲を指定するには、範囲の下限のアドレスの後に、範囲の上限のアドレスを入力します。

	コマンド	目的
ステップ 3	<code>ip dhcp pool pool_name</code>	DHCP 要求に応じて wireless device が割り当てる IP アドレスのプールの名前を生成し、DHCP 設定モードを開始します。
ステップ 4	<code>network subnet_number</code> [<i>mask</i> <i>prefix-length</i>]	アドレス プールにサブネット番号を割り当てます。wireless device は、このサブネット内の IP アドレスを割り当てます。 (オプション) アドレス プールにサブネット マスクを割り当てるか、アドレス接頭辞を構成するビット数を指定します。接頭辞はネットワーク マスクを割り当てる代替法です。接頭辞の長さの前には必ずスラッシュ (/) を入力してください。
ステップ 5	<code>lease { days [hours] [minutes] infinite }</code>	wireless device によって割り当てられた IP アドレスのリース期間を設定します。 <ul style="list-style-type: none"> days : 日数でリース期間を設定します。 (オプション) hours : 時間数でリース期間を設定します。 (オプション) minutes : 分数でリース期間を設定します。 infinite : リース期間を無限に設定します。
ステップ 6	<code>default-router address [address2 ... address 8]</code>	サブネット上の DHCP クライアントに対し、デフォルト ルータの IP アドレスを指定します。求められるのは 1 つの IP アドレスですが、コマンド行 1 行につき最大 8 つまでのアドレスを指定できます。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

デフォルト設定に戻すには、これらのコマンドの `no` フォームを使用します。

この例では、wireless device を DHCP サーバとして設定する方法を示しています。IP アドレスの範囲は省略し、デフォルト ルータを割り当てています。

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

DHCP サーバ アクセスポイントの監視と維持

次の項では、DHCP サーバ アクセスポイントの監視と維持に使用できるコマンドについて説明します。


- [Show コマンド \(P. 5-26\)](#)
- [Clear コマンド \(P. 5-26\)](#)
- [Debug コマンド \(P. 5-26\)](#)

■ DHCP サービスを提供するためのアクセスポイントの設定

Show コマンド

DHCP サーバとしての wireless device に関する情報を表示するには、EXEC モードで表 5-2 中のコマンドを入力します。

表 5-2 DHCP サーバ用の Show コマンド

コマンド	目的
<code>show ip dhcp conflict [address]</code>	特定の DHCP サーバによって記録されているすべてのアドレス競合のリストを表示します。wireless device の IP アドレスを入力すると、wireless device によって記録されている競合が表示されます。
<code>show ip dhcp database [url]</code>	DHCP データベースでの最近のアクティビティを表示します。  (注) このコマンドは特権 EXEC モードで使用してください。
<code>show ip dhcp server statistics</code>	送受信されたサーバの統計情報やメッセージに関するカウント情報を表示します。

Clear コマンド

DHCP サーバ変数を消去するには、特権 EXEC モードで表 5-3 中のコマンドを使用します。

表 5-3 DHCP サーバ用の Clear コマンド

コマンド	目的
<code>clear ip dhcp binding { address * }</code>	DHCP データベースから自動アドレスバインディングを削除します。address 引数を指定すると、特定の(クライアント)IPアドレスの自動バインディングが消去されます。アスタリスク(*)を指定すると、すべての自動バインディングが消去されます。
<code>clear ip dhcp conflict { address * }</code>	DHCP データベースからアドレス競合を消去します。address 引数を指定すると、特定の IP アドレスの競合が消去されます。アスタリスク(*)を指定すると、すべてのアドレスの競合が消去されます。
<code>clear ip dhcp server statistics</code>	すべての DHCP サーバのカウントを 0 にリセットします。

Debug コマンド

DHCP サーバのデバッグを有効にするには、特権 EXEC モードで次のコマンドを使用します。

```
debug ip dhcp server { events | packets | linkage }
```

wireless device DHCP サーバのデバッグを無効にするには、このコマンドの no フォームを使用します。

アクセスポイントの Secure Shell の設定

この項では、Secure Shell (SSH) 機能の設定方法について説明します。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Security Command Reference for Release 12.3』の「Secure Shell Commands」の項を参照してください。

SSH の概要

SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。SSH には、SSH バージョン 1 と SSH バージョン 2 の 2 種類のバージョンがあります。このソフトウェア リリースでは、どちらの SSH バージョンもサポートします。バージョン番号を指定しないと、アクセスポイントがデフォルトのバージョン 2 になります。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりリモート接続の安全性が高くなります。SSH 機能では SSH サーバと SSH 統合クライアントを使用します。クライアントは次のユーザ認証方式をサポートしています。

- RADIUS (詳細は、「[RADIUS によるアクセスポイントへのアクセスの制御](#)」の項 (P. 5-10) を参照)
- ローカル認証と許可 (詳細は、「[アクセスポイントのローカル認証および許可の設定](#)」の項 (P. 5-19) を参照)

SSH の詳細は、『Cisco IOS Security Configuration Guide for Release 12.3』の「Other Security Features」のパート 5 を参照してください。



(注)

このソフトウェア リリースの SSH 機能は IP Security (IPSec; IP セキュリティ) をサポートしていません。

SSH の設定

SSH を設定する前に、Cisco.com から暗号ソフトウェア イメージをダウンロードします。詳細は、このリリースのリリース ノートを参照してください。

SSH の設定方法と SSH 設定の表示方法については、『Cisco IOS Security Configuration Guide for Release 12.3』の「Other Security Features」のパート 5 を参照してください。次の Cisco.com から入手できます。

http://cisco.com/en/US/products/sw/iosswrel/ps5187/products_installation_and_configuration_guides_list.html

クライアント ARP キャッシングの設定

アソシエートされたクライアント デバイスの Address Resolution Protocol (ARP; アドレス レゾリューション プロトコル) キャッシュを保持するように、wireless device を設定できます。wireless device で ARP キャッシュを保持すると、無線 LAN のトラフィック負荷が軽減されます。ARP キャッシングはデフォルトで無効に設定されています。

この項で説明する内容は次のとおりです。

- [クライアント ARP キャッシングの概要 \(P. 5-28\)](#)
- [ARP キャッシングの設定 \(P. 5-28\)](#)

クライアント ARP キャッシングの概要

wireless device での ARP キャッシングは、クライアント デバイスへの ARP 要求を wireless device で止めることによって、無線 LAN 上のトラフィックを軽減します。wireless device は、ARP 要求をクライアント デバイスへ転送する代わりに、アソシエートされたクライアント デバイスに代わって ARP 要求に応答します。

ARP キャッシングを無効にすると、wireless device はすべての ARP 要求をアソシエートされたクライアントに無線ポート経由で転送し、ARP 要求を受け取ったクライアントが応答します。一方、ARP キャッシングを有効にすると、wireless device はアソシエートされたクライアントに代わって ARP 要求に応答し、クライアントへは要求を転送しません。キャッシュにない IP アドレスに向けた ARP 要求を受け取ると、wireless device はその要求を廃棄して転送しません。wireless device は、ビーコンに情報エレメントを追加して、バッテリーの寿命を延ばすためのブロードキャスト メッセージを安全に無視できることをクライアント デバイスに通知します。

オプションの ARP キャッシング

アクセス ポイントにシスコ製以外のクライアント デバイスがアソシエートされ、そのデバイスがデータを通さない場合、wireless device がそのクライアントの IP アドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、wireless device は既知の IP アドレスのクライアントについては、その代理として応答しますが、不明なクライアント宛での ARP 要求はすべて無線ポートから転送します。アソシエートされた全クライアントの IP アドレスを記憶すると、wireless device はそれらのアソシエートされたクライアント以外に対する ARP 要求を廃棄します。

ARP キャッシングの設定

特権 EXEC モードから、次の手順に従って、アソシエートされたクライアントの ARP キャッシュを保持するように wireless device を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 arp-cache [optional]</code>	wireless device での ARP キャッシングを有効にします。 <ul style="list-style-type: none"> • (オプション) wireless device が認識している IP アドレスのクライアント デバイスに限って ARP キャッシングを有効にするには、<code>optional</code> キーワードを使用します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

次の例に、アクセスポイントで ARP キャッシングを設定する方法の例を示します。

```
AP# configure terminal  
AP(config)# dot11 arp-cache  
AP(config)# end
```

システムの日時の管理

wireless device のシステムの時刻と日付は、Simple Network Time Protocol (SNTP; 簡易ネットワークタイム プロトコル) を使用して自動的に管理することも、wireless device に時刻と日付を設定して手動で管理することもできます。



(注) この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Configuration Fundamentals Command Reference for Release 12.3』を参照してください。

この項で説明する設定の内容は次のとおりです。

- [Simple Network Time Protocol の概要 \(P. 5-30 \)](#)
- [SNTP の設定 \(P. 5-30 \)](#)
- [時刻と日付の手動設定 \(P. 5-31 \)](#)

Simple Network Time Protocol の概要

Simple Network Time Protocol (SNTP) とは、クライアント専用バージョンの簡易版 Network Time Protocol (NTP; ネットワーク タイム プロトコル) です。SNTP は、NTP サーバから時間を受信のみできます。他のシステムに時刻サービスを提供することはできません。SNTP は通常、100 ミリ秒単位で正確な時間を提供しますが、NTP のように複雑なフィルタリングや統計メカニズムはありません。

SNTP は、設定済みサーバからパケットを要求して受け付けるよう設定することも、任意のソースからの NTP ブロードキャスト パケットを受け付けるよう設定することもできます。複数のソースから NTP パケットが送信された場合は、ストラタムが最良のサーバが選択されます。NTP とストラタムの詳細は、次の URL をクリックしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001131

複数のサーバのストラタムが同じだった場合は、ブロードキャスト サーバよりも設定済みサーバが優先されます。基準を両方とも満たすサーバが複数ある場合は、最初に時間パケットを送信する方が選択されます。現在選択中のサーバからパケット受信が途絶えたり、または上記の基準に基づいてより最適なサーバが検出されたりしない限り、SNTP が新たにサーバを選択することはありません。

SNTP の設定

デフォルトでは、SNTP は無効に設定されています。アクセスポイントで SNTP を有効にするには、グローバル コンフィギュレーション モードで次のいずれかまたは両方のコマンドを使用します。

表 5-4 SNTP コマンド

コマンド	目的
<code>sntp server {address hostname} [version number]</code>	NTP サーバから NTP パケットを要求するよう SNTP を設定します。
<code>sntp broadcast client</code>	どの NTP ブロードキャスト サーバからも NTP パケットを受け付けるよう SNTP を設定します。

NTP サーバごとに `sntp server` コマンドを 1 回ずつ入力してください。NTP サーバは、アクセスポイントからの SNTP メッセージに応答できるように設定しておく必要があります。

`sntp server` コマンドと `sntp broadcast client` コマンドの両方を入力した場合、アクセスポイントはブロードキャストサーバからの時間を受け付けますが、同一のストラタムと判断して設定済みサーバからの時間の方を優先します。SNTP に関する情報を表示するには、`show sntp EXEC` コマンドを使用します。

時刻と日付の手動設定

時刻ソースが利用できない場合は、システムの再起動後に手動で時刻と日付を設定できます。時刻は次のシステム再起動まで正確に維持されます。手動設定は最後の手段として行うことをお勧めします。wireless device が同期できる外部ソースがある場合は、システムクロックを手動で設定する必要はありません。

この項で説明する設定の内容は次のとおりです。

- システムクロックの設定 (P. 5-31)
- 時刻と日付の設定の表示 (P. 5-32)
- タイムゾーンの設定 (P. 5-32)
- サマータイム (夏時間) の設定 (P. 5-33)

システムクロックの設定

ネットワークに NTP サーバなどの時刻サービスを提供する外部ソースがある場合は、システムクロックを手動で設定する必要はありません。

特権 EXEC モードから、次の手順に従ってシステムクロックを設定します。

	コマンド	目的
ステップ 1	<code>clock set hh:mm:ss day month year</code> または <code>clock set hh:mm:ss month day year</code>	次のいずれかの書式を使ってシステムクロックを手動で設定します。 <ul style="list-style-type: none"> • <code>hh:mm:ss</code> には、時間 (24 時間形式)、分、秒を指定します。設定されたタイムゾーンを基準に時間を指定します。 • <code>day</code> には、日にちを指定します。 • <code>month</code> には、月を名前で指定します。 • <code>year</code> には、年を 4 桁で指定します。
ステップ 2	<code>show running-config</code>	入力内容を確認します。
ステップ 3	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーションファイルに入力内容を保存します。

次に、システムクロックを手動で 2001 年 7 月 23 日 午後 1 時 32 分に設定する例を示します。

```
AP# clock set 13:32:00 23 July 2001
```

時刻と日付の設定の表示

日付と時刻の設定を表示するには、`show clock [detail]` 特権 EXEC コマンドを使用します。

システム クロックは、時間の信頼性（正確性）を示す *authoritative* フラグを表示し続けます。システム クロックが NTP などの時刻ソースで設定されている場合は、このフラグが設定されます。信頼できない場合、時刻は表示のみに使用されます。ピアの時刻が無効になった場合、クロックが信頼でき、*authoritative* フラグが設定されるまで、このフラグがピアのクロックとの同期を防ぎます。

`show clock` の前に表示される記号には次のような意味があります。

- * : 時刻が信頼できません。
- (空白) : 時刻が信頼できます。
- . : 時刻は信頼できますが、NTP は同期が行われていません。

タイムゾーンの設定

特権 EXEC モードから、次の手順に従ってタイムゾーンを手動で設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clock timezone zone hours-offset [minutes-offset]</code>	タイムゾーンを設定します。 wireless device は内部時間を Universal Time Coordinated (UTC; 協定世界時) で維持するため、このコマンドは表示専用で、時刻を手動で設定するときのみ使用されます。 <ul style="list-style-type: none"> • <i>zone</i> には、標準時間が有効な場合に表示されるタイムゾーンの名前を入力します。デフォルトは UTC です。 • <i>hours-offset</i> には、UTC との時差を時間単位で入力します。 • (オプション) <i>minutes-offset</i> には、UTC との時差を分単位で入力します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

グローバル設定コマンド `clock timezone` の *minutes-offset* 変数は、ローカル タイムゾーンの UTC との時差が 1 時間未満の単位である場合に使用できます。たとえば、大西洋沿岸カナダの一部地域のタイムゾーン (AST) は UTC-3.5 です。3 は 3 時間を、5 は 50 パーセントを意味します。この場合、コマンドを `clock timezone AST -3 30` と指定することになります。

時刻を UTC に設定するには、グローバル設定コマンド `no clock timezone` を使用します。

サマー タイム (夏時間) の設定

特権 EXEC モードから、次の手順に従って、毎年、特定の日付 (曜日) に開始および終了するサマータイム (夏時間) を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</code>	<p>毎年指定された日付に開始および終了するサマー タイムを設定します。</p> <p>サマー タイムはデフォルトでは無効になっています。パラメータを指定しないで <code>clock summer-time zone recurring</code> を指定した場合、サマー タイムのルールは米国のルールをデフォルトとします。</p> <ul style="list-style-type: none"> • <code>zone</code> には、サマー タイムが有効なときに表示されるタイムゾーンの名前 (PDT など) を指定します。 • (オプション) <code>week</code> には、月の第何週かを指定します (1 ~ 5 または <code>last</code>) 。 • (オプション) <code>day</code> には、曜日を指定します (Sunday、Monday など) 。 • (オプション) <code>month</code> には、月を名前で指定します (January、February など) 。 • (オプション) <code>hh:mm</code> には、時刻 (24 時間形式) を時間と分の単位で指定します。 • (オプション) <code>offset</code> には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

グローバル設定コマンド `clock summer-time` の最初の部分は、サマー タイムの開始時を、2 番目の部分は終了時を指定します。すべての時間は ローカル タイム ゾーンを基準にします。開始時間は標準時が基準になります。終了時間はサマー タイムが基準になります。開始月が終了月より後の場合、自動的に南半球であると解釈されます。

次の例では、4 月の第 1 日曜日の 02:00 に開始し、10 月の最終日曜日の 02:00 に終了するサマータイムの指定方法を示します。

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

ユーザ居住地域のサマー タイムが定期的なパターンに従わない場合、特権 EXEC モードから、次の手順に従って、次のサマー タイム イベントの日付と時間を正確に設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]</code> または <code>clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</code>	最初の日付に開始し、2 番目の日付に終了するサマー タイムを設定します。 サマー タイムはデフォルトでは無効になっています。 <ul style="list-style-type: none"> • <i>zone</i> には、サマー タイムが有効なときに表示されるタイムゾーンの名前 (PDT など) を指定します。 • (オプション) <i>week</i> には、月の第何週かを指定します (1 ~ 5 または last) • (オプション) <i>day</i> には、曜日を指定します (Sunday、Monday など) • (オプション) <i>month</i> には、月を名前で指定します (January、February など) • (オプション) <i>hh:mm</i> には、時刻 (24 時間形式) を時間と分の単位で指定します。 • (オプション) <i>offset</i> には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

グローバル設定コマンド `clock summer-time` の最初の部分は、サマー タイムの開始時を、2 番目の部分は終了時を指定します。すべての時間は ローカル タイムゾーンを基準にします。開始時間は標準時が基準になります。終了時間はサマー タイムが基準になります。開始月が終了月より後の場合、自動的に南半球であると解釈されます。

サマー タイムを無効にするには、グローバル設定コマンド `no clock summer-time` を使用します。

次の例では、2000 年 10 月 12 日 02:00 に開始し、2001 年 4 月 26 日 02:00 に終了するサマー タイムの設定方法を示します。

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

HTTP アクセスの定義

デフォルトでは、80 が HTTP アクセスに使用され、ポート 443 が HTTPS アクセスに使用されます。この値は、ユーザがカスタマイズできます。HTTP アクセスの定義方法は、次のとおりです。

- ステップ 1** アクセスポイントの GUI から、**Services > HTTP** の順にクリックします。Service: HTTP-Web サーバ画面が表示されます。
- ステップ 2** この画面に、目的の HTTP と HTTPS のポート番号を入力します。このポート番号フィールドに値を入力しないと、デフォルト値が使用されます。
- ステップ 3** **Apply** をクリックします。

システム名とプロンプトの設定

wireless device を識別するシステム名を設定します。デフォルトでは、システム名とプロンプトは *ap* です。

システムプロンプトを設定しない場合、システム名の最初の 20 文字がシステムプロンプトとして使用されます。大なり記号 (>) が追加されます。プロンプトは、システム名が変更されると必ず更新されますが、グローバル設定コマンド `prompt` を使用して手動でプロンプトを設定している場合は更新されません。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Configuration Fundamentals Command Reference』、および『Cisco IOS IP and IP Routing Command Reference for Release 12.3』を参照してください。

この項で説明する設定の内容は次のとおりです。

- [デフォルトのシステム名とプロンプトの設定 \(P. 5-35\)](#)
- [システム名の設定 \(P. 5-35\)](#)
- [DNS の概要 \(P. 5-36\)](#)



デフォルトのシステム名とプロンプトの設定

アクセスポイントのデフォルトのシステム名とプロンプトは *ap* です。

システム名の設定

特権 EXEC モードから、次の手順に従ってシステム名を手動で設定します。

■ システム名とプロンプトの設定

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>hostname name</code>	システム名を手動で設定します。 デフォルト設定は <i>ap</i> です。  (注) システム名を変更する場合、wireless deviceの無線はリセットされ、アソシエートしているクライアント デバイスはアソシエーションが解除され、ただちに再アソシエートされます。  (注) システム名には、63 文字まで入力することができます。しかし、wireless device では、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。クライアント ユーザがアクセス ポイントどうしを区別することが重要な場合、システム名の一意の部分が最初の 15 文字に現れるようにしてください。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

システム名を設定すると、その名前がシステム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、グローバル設定コマンド `no hostname` を使用します。

DNS の概要

DNS プロトコルは Domain Name System (DNS; ドメイン ネーム システム) を制御します。これはホスト名を IP アドレスにマッピングする際に使用する分散型データベースです。wireless device に DNS を設定すると、`ping`、`telnet`、`connect`、および関連する Telnet サポート操作で、IP アドレスの代わりにホスト名を使用できます。

IP は階層命名方式を定義します。この方式では場所またはドメインでデバイスを特定することができます。ドメイン名はピリオド (.) を区切り文字として連結できます。たとえば、シスコ システムズは IP ではドメイン名 *com* で特定される民間組織です。このためドメイン名は *cisco.com* になります。このドメイン内の File Transfer Protocol (FTP; ファイル転送プロトコル) システムなどの個々のデバイスは *ftp.cisco.com* のように識別されます。

ドメイン名を追跡するために、IP は IP アドレスにマッピングされた名前のキャッシュ(またはデータベース)を保持するドメイン ネーム サーバの概念を定義しています。ドメイン名を IP アドレスにマッピングするには、まずホスト名を特定し、ネットワーク上に存在するネーム サーバを特定し、DNS を有効にします。

この項で説明する設定の内容は次のとおりです。

- [デフォルトの DNS 設定 \(P. 5-37\)](#)
- [DNS の設定 \(P. 5-37\)](#)
- [DNS 設定の表示 \(P. 5-38\)](#)

デフォルトの DNS 設定

表 5-5 にデフォルトの DNS 設定を示します。

表 5-5 デフォルトの DNS 設定

機能	デフォルト設定
DNS の有効 / 無効	無効
DNS デフォルト ドメイン名	設定されていません。
DNS サーバ	ネーム サーバ アドレスは設定されていません。

DNS の設定

特権 EXEC モードから、次の手順に従って DNS を使用するように wireless device を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip domain-name name</code>	ソフトウェアが未修飾ホスト名(ドット付き 10 進ドメイン名を含まない名前)を作成する場合に使用するデフォルトのドメイン名を定義します。 未修飾名をドメイン名と区切るピリオドを先頭に使用しないでください。 ブート時にはドメイン名は設定されていませんが、wireless device の設定が BOOTP または Dynamic Host Configuration Protocol (DHCP)サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります(この情報がサーバに設定されている場合)。
ステップ 3	<code>ip name-server server-address1 [server-address2 ... server-address6]</code>	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバのアドレスは空白で区切ります。最初に指定するサーバがプライマリ サーバになります。wireless device は、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合、バックアップサーバが照会されます。
ステップ 4	<code>ip domain-lookup</code>	(オプション) wireless device で DNS ベースのホスト名からアドレスへの変換を有効にします。この機能はデフォルトで有効に設定されています。 ネットワークのデバイスが名前の割り当てを制御できないネットワークのデバイスとの接続を要求する場合、グローバル インターネット命名方式 (DNS) を使用して、デバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

■ システム名とプロンプトの設定

wireless device の IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため DNS クエリは作成されません。ピリオド (.) を含まないホスト名を設定すると、名前を IP アドレスにマッピングする DNS クエリが作成される前に、ホスト名の後にピリオドとデフォルトのドメイン名が追加されます。デフォルトのドメイン名は、グローバル設定コマンド `ip domain-name` で設定される値です。ホスト名にピリオド (.) が含まれている場合、Cisco IOS ソフトウェアはホスト名にデフォルトのドメイン名を追加せずに、IP アドレスを検索します。

ドメイン名を削除するには、グローバル設定コマンド `no ip domain-name name` を使用します。ネームサーバアドレスを削除するには、グローバル設定コマンド `no ip name-server server-address` を使用します。wireless device で DNS を無効にする場合は、グローバル設定コマンド `no ip domain-lookup` を使用します。

DNS 設定の表示

DNS 設定情報を表示するには、`show running-config` 特権 EXEC コマンドを使用します。



(注)

wireless device で DNS が設定されていると、`show running-config` コマンドはサーバの名前でなく IP アドレスを表示することがあります。

バナーの作成

message-of-the-day (MOTD) バナーとログイン バナーを設定できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ (差し迫ったシステム シャットダウンの通知など) を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。これは MOTD バナーの後、ログイン プロンプトの前に表示されます。



(注) この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Configuration Fundamentals Command Reference for Release 12.3』を参照してください。

この項で説明する設定の内容は次のとおりです。

- [デフォルトのバナー設定 \(P. 5-39 \)](#)
- [Message-of-the-Day ログイン バナーの設定 \(P. 5-39 \)](#)
- [ログイン バナーの設定 \(P. 5-40 \)](#)

デフォルトのバナー設定

デフォルトでは、MOTD バナーとログイン バナーは設定されていません。

Message-of-the-Day ログイン バナーの設定

wireless device にログインしたときに画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

特権 EXEC モードから、次の手順に従って MOTD ログイン バナーを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>banner motd c message c</code>	message-of-the-day (今日のメッセージ) を指定します。 <i>c</i> にはシャープ記号 (#) など希望する区切り文字を入力し、Return キーを押します。区切り文字は、バナー テキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 <i>message</i> には、最大 255 文字のバナー メッセージを入力します。メッセージ内で区切り文字は使用できません。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

MOTD バナーを削除するには、グローバル設定コマンド `no banner motd` を使用します。

■ バナーの作成

次の例は、開始および終了区切り文字にシャープ記号 (#) を使用して、wireless device に MOTD バナーを設定する方法を示しています。

```
AP(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

次の例は、上記の設定で表示されるバナーを示しています。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

ログインバナーの設定

接続したすべての端末に表示されるログインバナーを設定できます。このバナーは MOTD バナーの後、ログインプロンプトの前に表示されます。

特権 EXEC モードから、次の手順に従ってログインバナーを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>banner login c message c</code>	ログインメッセージを指定します。 <i>c</i> にはシャープ記号 (#) など希望する区切り文字を入力し、Return キーを押します。区切り文字は、バナーテキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 <i>message</i> には、最大 255 文字のログインメッセージを入力します。メッセージ内で区切り文字は使用できません。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

ログインバナーを削除するには、グローバル設定コマンド `no banner login` を使用します。

次の例は、開始および終了区切り文字にドル記号 (\$) を使用して、wireless device にログインバナーを設定する方法を示しています。

```
AP(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
AP(config)#
```

Autonomous Cisco Aironet アクセスポイントを Lightweight モードにアップグレードする方法

ネットワーク上で無線 LAN コントローラと通信できるよう、Autonomous Cisco Aironet アクセスポイントを Lightweight モードにアップグレードするユーティリティが用意されています。このアップグレードユーティリティの使用の詳細は、次の URL をご覧ください。

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html#wp156967

日本の W52 ドメインへの移行方法

このユーティリティは、802.11a 無線を J52 から W52 ドメインに移行する際に使用します。このユーティリティは、1130 と 1240 アクセスポイントで動作するほか、RM20、RM21 および RM22A 無線を装備した 1200 アクセスポイントで動作します。802.11a 無線が付属していないアクセスポイントには、この移行はサポートされていません。

次のインターフェイスのグローバル コンフィギュレーション モードの CLI コマンドを使用して、アクセスポイントの 802.11a 無線を W52 ドメインに移行します。

```
dot11 migrate j52 w52
```

警告メッセージが表示されたら、y を入力します。移行プロセスが始まり、アクセスポイントが 2 回リブートしたら完了です。無線ハードウェアをリセットすると、ファームウェア初期化コードが規制ドメインを読み取って初期化します。ハードウェアをリセットすると、ファームウェアをリロードし、無線のイメージをフラッシュしてから初期化処理を進めます。無線が規制ドメインを選択していることを確認するため、アクセスポイントが 2 回目のリブートを開始します。

次の例は移行の完了方法を示しています。

```
ap>enable
Password:
ap#config terminal
ap(config)interface dot11radio0
ap(config-if)#dot11 migrate j52 w52
Migrate APs with 802.11A Radios in the "J"
Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies

WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated, the 802.11A radios will not operate with previous OS versions.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
This AP is eligible for migration:
ap      AIR-AP1242AG-A-K9      0013.5f0e.d1e0  "J" Regulatory Domain
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue ?
(yes/[no]):yes
Burning cookie into serial eeprom:
Reading cookie from system serial eeprom...done.
Editing copy...done.
Writing cookie into system serial eeprom...done.

*Mar 1 00:09:13.844: %DOT11-4-UPGRADE: **** Send your company name and the following
report to:  migrateapj52w52@cisco.com

The following AP has been migrated from J(J52) to U(W52) Regulatory Domain:
AP Name      AP Model      Ethernet MAC
ap           AIR-AP1242AG-A-K9      0013.5f0e.d1e0 "U" Regulatory Domain
*Mar 1 00:09:13.844: Convert Regulatory Domain from J (J52) to U (W52). Writing AP
nvram.
```

```
*Mar 1 00:09:14.060: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: CONVERT
REGULATORY DOMAIN FROM J to U
```

no を選択すると、次の例に示すように操作が停止します。

```
...
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue ?
(yes/[no]):no
AP not migrated.

ap(config-if)#
```

移行の確認

show controllers コマンドを使用して、次の例に示すように移行を確認します。

```
ap#show controllers dot11Radio 1
!
interface Dot11Radio1
Radio AIR-AP1242A, Base Address 0013.5f0e.d1e0, BBlock version
0.00, Software version 5.95.7
Serial number: ALP0916W015
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Japan (UNI1) (JP )
Uniform Spreading Required: No
Current Frequency: 0 MHz Channel 0
Allowed Frequencies: 5180(36) 5200(40) 5220(44) 5240(48)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 5180(36)
5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64)
5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5600(120)
5620(124) 5640(128) 5660(132) 5680(136) 5700(140) 5745(149)
5765(153) 5785(157) 5805(161) 5825(165)
Beacon Flags: 0; Beacons are disabled; Probes are disabled High Density mode disabled
  Local Rx sensitivity (Config -127, Max -57, Min -17, Active 0) dBm
    CCA Sensitivity -64 dBm
  Cell Rx sensitivity -80 dBm, CCA Sensitivity -60 dBm, Tx Power 127 dBm
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
Current Rates: basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Active Rates:
Allowed Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: basic-6.0 basic-9.0 basic-12.0 basic-
18.0 basic-24.0 basic-36.0 basic-48.0 basic-54.0
```



(注) 移行後は、国コードが JP から JU にアップデートされます。移行されていない無線は、まだ国コード JP で表示されます。

ポイントツーマルチポイントブリッジにおける複数のVLANとレート制限の設定

この機能は、ポイントツーマルチポイントブリッジング方法を変更したもので、複数のVLANで動作しながら各VLANでトラフィックレートを管理できるように設定するものです。この機能は、ブリッジ(1240シリーズ)と1300シリーズアクセスポイント/ブリッジとして設定した32MBアクセスポイントで利用できます。16MBアクセスポイント(1100、1200、350シリーズ)では利用できません。



(注)

レート制限ポリシーは、非ルートブリッジのファーストイーサネット入力ポートの入力ポートにのみ適用できます。

通常、複数のVLANをサポートしていると、別々のVLAN上にある各リモートサイトでポイントツーマルチポイントブリッジリンクを設定できます。この設定では、各サイトへのトラフィックを切り分けて管理できてしまいます。レート制限機能は、リンク帯域幅全体のうち指定した量以上を消費しないようリモートサイトに設定するものです。アップリンクトラフィックを管理できるのは、非ルートブリッジのファーストイーサネット入力ポートからのみです。

クラスベースのポリシング機能を使用すると、レート制限を指定して、これを非ルートブリッジのイーサネットインターフェイスの入力に適用できます。イーサネットインターフェイスの入力にレートを適用すると、すべての受信イーサネットパケットが設定したレートに適合します。

次の設定は、**class-map** コマンドを使用したトラフィッククラスの定義方法を示しています。また**policy-map** コマンドで、サービスポリシングに設定したトラフィックポリシング設定をトラフィッククラスの基準と関連付ける方法を示しています。この例では、ファーストイーサネット0インターフェイスの受信パケットすべてに対して、トラフィックポリシングは平均レートの8000ビット/秒、および通常バーストサイズの1000バイトで設定されています。

```
AP enable
AP#config terminal
AP(config)#class-map sample_class
AP(config-cmap)#match any
AP(config-cmap)#exit
AP(config)#policy-map police setting
AP(config-pmap)#class sample_class
AP(config-pmap)#police 8000 1000 conform-action transmit exceed-action drop
AP(config-pmap-c)#exit
AP(config-pmap)#exit
AP(config)#interface fa0
AP(config-if)#service-policy input police-setting
```



(注)

class-map policy コマンドには多数のオプションが用意されていますが、このリリースでサポートされているのは、**match any** オプションだけです。

CLI コマンド

802.11Q タグを受信イーサネットパケットすべてに追加するには、**bridge non-root client vlan <vlan id>** コマンドを使用します。このコマンドは、非ルートブリッジだけに適用できます。

■ ポイントツーマルチポイント ブリッジにおける複数の VLAN とレート制限の設定