CHAPTER 10

# ワイヤレス デバイスの管理

このモジュールでは、次のワイヤレス デバイス管理タスクについて説明します。

**ワイヤレス デバイスへのアクセスのセキュリティ強化**


- 「モード ボタン機能のディセーブル化」（P.10-2）
- 「アクセス ポイントへの不正アクセスの防止」（P.10-3）
- 「特権 EXEC コマンドへのアクセスの保護」（P.10-3）
- 「RADIUS でのアクセス ポイント アクセスの制御」（P.10-11）
- 「TACACS+ でのアクセス ポイント アクセスの制御」（P.10-16）


**アクセス ポイント ハードウェアおよびソフトウェアの管理**


- 「ワイヤレス ハードウェアおよびソフトウェアの管理」（P.10-19）
  - 「ワイヤレス デバイスの工場出荷時のデフォルト設定へのリセット」（P.10-19）
  - 「ワイヤレス デバイスの再起動」（P.10-19）
  - 「ワイヤレス デバイスのモニタリング」（P.10-20）
- 「システムの時刻と日付の管理」（P.10-20）
- 「システム名およびプロンプトの設定」（P.10-26）
- 「バナーの作成」（P.10-29）


**ワイヤレス デバイス通信の管理**


- 「イーサネットの速度およびデュプレックスの設定」（P.10-31）
- 「ワイヤレス ネットワーク管理のアクセスポイントの設定」（P.10-31）
- 「ローカル認証および許可のアクセス ポイントの設定」（P.10-32）
- 「認証キャッシュおよびプロファイルの設定」（P.10-33）
- 「DHCP サービスを提供するアクセス ポイントの設定」（P.10-36）
- 「セキュア シェルのアクセス ポイントの設定」（P.10-39）
- 「クライアント ARP キャッシングの設定」（P.10-40）
- 「ポイントツーマルチポイント ブリッジの複数の VLAN およびレート制限の設定」（P.10-41）

# モード ボタン機能のディセーブル化

**[no] boot mode-button** コマンドを使用して、ワイヤレス デバイスのモード ボタンをディセーブルにすることができます。

**注意**　このコマンドを使用すると、パスワード回復がディセーブルになります。このコマンドを入力した後で、アクセス ポイントの特権 EXEC モード パスワードを紛失した場合、Cisco Technical Assistance Center（TAC）に問い合せて、アクセス ポイント Command Line Interface（CLI; コマンドライン インターフェイス）へのアクセスを再び取得する必要があります。

**（注）**　ワイヤレス デバイスを再起動するには、ルータの Cisco IOS CLI から **service-module wlan-ap reset** コマンドを使用します。このコマンドについては、「ワイヤレス デバイスの再起動」（P.10-19）を参照してください。

モード ボタンは、デフォルトでイネーブルにされています。アクセス ポイントのモード ボタンをディセーブルにするには、特権 EXEC モードから、次の作業を行います。

| | 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 | **no boot mode-button** | アクセス ポイントのモード ボタンをディセーブルにします。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。<br>**（注）**　コンフィギュレーションを保存する必要はありません。 |

特権 EXEC モードで **show boot** または **show boot mode-button** コマンドを実行して、モード ボタンのステータスをチェックできます。ステータスは、実行コンフィギュレーションには表示されません。次に、**show boot** および **show boot mode-button** コマンドに対する通常の応答を示します。

```
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 パスワードを認識している限り、**boot mode-button** コマンドを使用して、モードボタンを通常の動作に戻すことができます。

# アクセス ポイントへの不正アクセスの防止

不正ユーザが、ワイヤレス デバイスを再設定したり、設定情報を表示したりできないように防止できます。通常、ネットワーク管理者は、ワイヤレス デバイスにアクセスでき、ローカル ネットワーク内から端末またはワークステーションを介して接続するユーザにアクセスを制限します。

ワイヤレス デバイスへの不正アクセスを防止するには、次のいずれかのセキュリティ機能を設定します。

- ワイヤレス デバイスにローカルで保存される、ユーザ名およびパスワードのペア。これらのペアは、ユーザのワイヤレス デバイスへのアクセスを許可する前に、各ユーザを認証します。また、特定の権限レベル（読み取り専用または読み取り / 書き込み）を各ユーザ名とパスワードのペアに割り当てることができます。詳細については、「ユーザ名およびパスワードのペアの設定」（P.10-8）を参照してください。デフォルトのユーザ名は、*Cisco* です。デフォルトのパスワードは、*Cisco* です。ユーザ名およびパスワードは、大文字と小文字が区別されます。

  （注）　TAB、?、$、+ および [ の文字は、パスワードには無効な文字です。

- ユーザ名およびパスワードのペアは、セキュリティ サーバのデータベースに中央で保存されます。詳細については、「RADIUS でのアクセス ポイント アクセスの制御」（P.10-11）を参照してください。

# 特権 EXEC コマンドへのアクセスの保護

ネットワークの端末アクセス制御を提供する簡単な方法は、パスワードを使用して、権限レベルを割り当てることです。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。権限レベルは、ユーザがネットワーク デバイスにログインした後で使用できるコマンドを定義します。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference for Release 12.4*』を参照してください。

ここでは、コンフィギュレーション ファイルおよび特権 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。また、このコンフィギュレーションについても説明します。


- 「デフォルト パスワードおよび権限レベルの設定」（P.10-4）
- 「スタティック イネーブル パスワードの設定または変更」（P.10-5）
- 「暗号化によるイネーブル パスワードおよびイネーブル シークレット パスワードの保護」（P.10-6）
- 「ユーザ名およびパスワードのペアの設定」（P.10-8）
- 「複数の権限レベルの設定」（P.10-9）

# デフォルト パスワードおよび権限レベルの設定

表 1 に、デフォルト パスワードおよび権限レベルのコンフィギュレーションを示します。

**表 1　　デフォルトのパスワードおよび権限レベル**

| 権限レベル | デフォルト設定 |
|---|---|
| ユーザ名およびパスワード | デフォルトのユーザ名は、*Cisco* です。デフォルトのパスワードは、*Cisco* です。 |
| イネーブル パスワードおよび権限レベル | デフォルトのパスワードは、*Cisco* です。デフォルトは、レベル 15 です（特権 EXEC レベル）。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 パスワードおよび権限レベル | デフォルトのイネーブル パスワードは、*Cisco* です。デフォルトは、レベル 15 です（特権 EXEC レベル）。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、*Cisco* 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。 |

# スタティック 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 コンフィギュレーション モードで、**no enable password** コマンドを使用すると、イネーブル パスワードを削除できますが、このコマンドを使用する場合は十分に注意してください。イネーブル パスワードを削除すると、特権 EXEC モードからロックされます。

スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **enable password** *password* | 新しいパスワードを定義するか、特権 EXEC モードにアクセスするための既存のパスワードを変更します。<br>デフォルトのパスワードは、*Cisco* です。<br>*password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行スペースは無視されます。パスワードを作成する場合、疑問符の前にキーの組み合わせを指定すると、疑問符（?）文字を含めることができます。たとえば、abc?123 というパスワードを作成する場合、次のようにします。<br>**1.** **abc** を入力します。<br>**2.** **Crtl-V** を入力します。<br>**3.** **?123** を入力します。<br>イネーブル パスワードを入力するプロンプトが表示された場合、疑問符の前に Ctrl-V を付ける必要はありません。パスワード プロンプトには、**abc?123** とだけ入力できます。<br>（注）　TAB、?、$、+ および [ の文字は、パスワードには無効な文字です。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

イネーブル パスワードは、暗号化されず、ワイヤレス デバイスのコンフィギュレーション ファイルに読み込むことができます。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは、暗号化されず、レベル 15（標準特権 EXEC モード アクセス）のアクセスを提供します。

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

# 暗号化によるイネーブル パスワードおよびイネーブル シークレット パスワードの保護

セキュリティを強化するには、特に、ネットワークを介するパスワード、または TFTP サーバに保存されるパスワードのセキュリティを強化するには、グローバル コンフィギュレーション モードで、**enable password** または **enable secret** コマンドのいずれかを使用できます。これらのコマンドを同じことを実行します。つまり、ユーザが特権 EXEC モード（デフォルト）を開始するときに入力しなければならない暗号化されたパスワード、または指定する任意の権限レベルを確立できます。

改善された暗号化アルゴリズムが使用されるため、**enable secret** コマンドを使用することをお勧めします。

**enable secret** コマンドを設定する場合、**enable password** コマンドより優先されます。これら 2 つのコマンドが同時に有効になることはありません。

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化を設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **enable password** [**level** *level*] {*password* \| *encryption-type encrypted*-password} | 新しいパスワードを定義するか、特権 EXEC モードにアクセスするための既存のパスワードを変更します。 |
| | または | または |
| | **enable secret** [**level** *level*] {*password* \| *encryption-type encrypted*-password} | 元に戻すことができない暗号方式を使用して保存される、シークレット パスワードを定義します。<br>• （任意）*level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。デフォルトのレベルは 15 です（特権 EXEC モード権限）。<br>• *password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行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。<br>• （任意）*encryption-type* には、シスコ社製暗号アルゴリズムである、タイプ 5 だけを使用できます。暗号タイプを指定する場合、暗号化されたパスワードを提供する必要があります。暗号化されたパスワードは、別のアクセス ポイント ワイヤレス デバイス コンフィギュレーションからコピーします。<br>**（注）** 暗号タイプを指定して、クリア テキスト パスワードを入力した場合、特権 EXEC モードを再び開始できません。暗号化されたパスワードを損失した場合、いかなる方法でも回復できません。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **service password-encryption** | （任意）パスワードが定義されるか、コンフィギュレーションが書き込まれるときに、パスワードを暗号化します。<br>暗号化により、パスワードは、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。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

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 パスワードを開始する必要があります。

**level** キーワードを使用して、特定の権限レベルのパスワードを定義します。レベルを指定して、パスワードを設定したら、このレベルでアクセスする必要があるユーザだけに、設定したパスワードを提供します。グローバル コンフィギュレーション モードで、**privilege level** コマンドを使用して、さまざまなレベルでアクセス可能なコマンドを指定します。詳細については、「複数の権限レベルの設定」（P.10-9）を参照してください。

パスワード暗号化をイネーブルにした場合、これは、ユーザ名パスワード、認証鍵パスワード、特権コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

パスワードおよびレベルを削除するには、グローバル コンフィギュレーション モードで、**no enable password** [**level** *level*] コマンドまたは **no enable secret** [**level** *level*] コマンドを使用します。パスワード暗号化をディセーブルにするには、グローバル コンフィギュレーション モードで、**no service password-encryption** コマンドを使用します。

次に、権限レベル 2 の暗号化されたパスワード *$1$FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

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

# ユーザ名およびパスワードのペアの設定

ワイヤレス デバイスにローカルで保存される、ユーザ名およびパスワードのペアを設定できます。これらのペアは、ラインまたはインターフェイスに割り当てられ、ユーザがワイヤレス デバイスにアクセスできるようになる前に各ユーザを認証します。権限レベルを定義した場合、各ユーザ名およびパスワードのペアに、特定の権限レベル（および関連する権利と権限）を割り当てることもできます。

ログイン ユーザ名およびパスワードを要求する、ユーザ名に基づいた認証システムを確立するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **username** *name* [**privilege** *level*] {**password** *encryption-type password*} | 各ユーザのユーザ名、権限レベル、およびパスワードを入力します。<br>• *name* には、ユーザ ID を 1 単語で指定します。スペースおよび引用符は使用できません。<br>• （任意）*level* には、ユーザがアクセス権を取得した後の権限レベルを指定します。範囲は、0 ～ 15 です。レベル 15 は、特権 EXEC モード アクセスを提供します。レベル 1 は、ユーザ EXEC モード アクセスを提供します。<br>• *encryption-type* には、暗号化されていないパスワードを使用する場合は 0 を入力します。非表示パスワードを使用する場合は 7 を入力します。<br>• *password* には、ワイヤレス デバイスへのアクセス権を取得するときにユーザが入力する必要があるパスワードを指定します。パスワードは、1 ～ 25 文字でなければなりません。スペースを含めることができます。また、パスワードは、**username** コマンドで指定される最後のオプションでなければなりません。 |
| ステップ 3 | **login local** | ログイン時にローカル パスワード チェックをイネーブルにします。認証は、手順 2 で指定したユーザ名に基づいて行われます。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| 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** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

特定のユーザのユーザ名認証をディセーブルにするには、グローバル コンフィギュレーション モードで、**no username** *name* コマンドを使用します。

パスワード チェックをディセーブルにし、パスワードなしで接続を許可するには、グローバル コンフィギュレーション モードで、**no login** コマンドを使用します。

**（注）** ユーザ名は少なくとも 1 つ設定しなければなりません。また、login local を設定して、ワイヤレス デバイスに Telnet セッションを開かなければなりません。only username にユーザ名を入力しない場合、ワイヤレス デバイスからロックされます。

# 複数の権限レベルの設定

デフォルトでは、Cisco IOS ソフトウェアは、ユーザ EXEC および特権 EXEC の 2 つのパスワード セキュリティ モードを提供します。各モードのコマンドの階層レベルは 16 まで設定できます。複数のパスワードを設定すると、ユーザのさまざまなセットに指定コマンドへのアクセスを許可できます。

たとえば、多数のユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 セキュリティを割り当て、このレベル 2 セキュリティ パスワードを幅広く配布します。ただし、**configure** コマンドへのアクセスをさらに制限する場合、レベル 3 セキュリティを割り当て、そのパスワードを、より限定したユーザ グループに配布します。

ここでは、次の設定情報について説明します。


- 「コマンドの権限レベルの設定」（P.10-9）
- 「権限レベルへのログインおよび終了」（P.10-10）


## コマンドの権限レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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* | コマンドの権限レベルを設定します。<br>• *mode* 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 **configure**、EXEC モードの場合は **exec**、インターフェイス コンフィギュレーション モードの場合は **interface**、ライン コンフィギュレーション モードの場合は **line** を入力します。<br>• *level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードにより許可されるアクセスのレベルです。<br>• *command* には、アクセスを制限するコマンドを指定します。 |
| ステップ 3 | **enable password level** *level password* | 権限レベルのイネーブル パスワードを指定します。<br>• *level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。<br>• *password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行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。<br>**（注）** TAB、?、$、+ および [ の文字は、パスワードには無効な文字です。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | **show running-config**<br>または<br>**show privilege** | 入力内容を確認します。<br>**show running-config** コマンドは、パスワードおよびアクセス レベル コンフィギュレーションを表示します。<br>**show privilege** コマンドは、権限レベル コンフィギュレーションを表示します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

コマンドを権限レベルに設定すると、構文がそのコマンドのサブセットであるすべてのコマンドも、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、**show** コマンドおよび **show ip** コマンドは、個別に別のレベルに設定していない限り、自動的に権限レベル 15 に設定されます。

特定のコマンドのデフォルト権限に戻すには、グローバル コンフィギュレーション モードで、**no privilege** *mode* **level** *level command* コマンドを使用します。

次に、**configure** コマンドを権限レベル 14 に設定し、ユーザがレベル 14 コマンドを使用するときに入力しなければならないパスワードとして *SecretPswd14* を定義する例を示します。

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

## 権限レベルへのログインおよび終了

指定された権限レベルにログインする、または指定された権限レベルを終了するには、特権 EXEC モードで、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **enable** *level* | 指定された権限レベルにログインします。<br>*level* の範囲は 0 ～ 15 です。 |
| ステップ 2 | **disable** *level* | 指定された権限レベルを終了します。<br>*level* の範囲は 0 ～ 15 です。 |

# RADIUS でのアクセス ポイント アクセスの制御

ここでは、Remote Authentication Dial-In User Service（RADIUS）を使用して、ワイヤレス デバイスへの管理者アクセスを制御する方法について説明します。RADIUS をサポートするようにワイヤレス デバイスを設定する方法の詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章を参照してください。

RADIUS は、詳細なアカウンティング情報、および認証や認可プロセスを介した柔軟な管理制御を提供します。RADIUS は、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）により促進され、AAA コマンドを介してだけイネーブルにできます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ここでは、RADIUS 設定について説明します。

- 「デフォルトの RADIUS 設定」（P.10-11）
- 「RADIUS ログイン認証の設定」（P.10-11）（必須）
- 「AAA サーバ グループの定義」（P.10-13）（任意）
- 「ユーザ権限アクセスおよびネットワーク サービスの RADIUS 許可の設定」（P.10-15）（任意）
- 「RADIUS 設定の表示」（P.10-16）

## デフォルトの RADIUS 設定

RADIUS および AAA は、デフォルトでディセーブルにされています。

セキュリティの欠落を避けるため、ネットワーク管理アプリケーションを介して RADIUS を設定できません。イネーブルにされている場合、RADIUS は、コマンドライン インターフェイス（CLI）を介してワイヤレス デバイス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て、そのリストをさまざまなインターフェイスに適用します。認証方式のリストは、実行される認証のタイプ、およびそれらが実行される順序を定義します。これは、定義される認証方式が実行される前に、特定のインターフェイスに適用しなければなりません。唯一の例外は、デフォルトの認証方式リストです（この名前は *default* です）。デフォルトの認証方式リストは、名前付き認証方式リストが明示的に定義されている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。

認証方式リストは、ユーザの認証に使用される順序と認証方式を記述します。最初の方式が失敗した場合の認証にバックアップ システムが使用されるように、認証に 1 つ以上のセキュリティ プロトコルを指定できます。ソフトウェアは、リストの最初の方式を使用して、ユーザを認証します。この方式が応答しない場合、ソフトウェアは、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、リストの認証方式との通信に成功するまで、または定義されているすべての方式が失敗するまで、続けられます。このサイクルのいずれかの時点で認証が失敗した場合、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 アクセスを拒否することで応答した場合、認証プロセスは停止し、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードから、次の作業を行います。これは必須手順です。

| | 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 をイネーブルにします。 |
| ステップ 3 | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] | ログイン認証方式リストを作成します。<br>• 名前付きリストが **login authentication** コマンドで指定されていないときに使用されるデフォルト リストを作成するには、デフォルト状況で使用される方式リストが後に続く **default** キーワードを使用します。デフォルト方式リストは、すべてのインターフェイスに自動的に適用されます。<br>• *list-name* には、作成するリストに名前を付ける文字ストリングを指定します。<br>• *method1...* 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。認証の追加方式は、直前の方式からエラーが返された場合だけ使用されます。失敗した場合は、使用されません。<br>次のいずれかの方式を選択します。<br>• **local**：認証のローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力しなければなりません。**username** *password* グローバル コンフィギュレーション コマンドを使用します。<br>• **radius**：RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバを設定しなければなりません。詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章の「Identifying the RADIUS Server Host」の項を参照してください。 |
| ステップ 4 | **line** [**console** \| **tty** \| **vty**] *line-number* [*ending-line-number*] | ライン コンフィギュレーション モードを開始して、認証リストを適用するラインを設定します。 |
| ステップ 5 | **login authentication** {**default** \| *list-name*} | 認証リストをラインまたはラインのセットに適用します。<br>• **default** を指定する場合、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。<br>• *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config** | 入力内容を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

AAA をディセーブルにするには、グローバル コンフィギュレーション モードで、**no aaa new-model** コマンドを使用します。AAA 認証をディセーブルにするには、グローバル コンフィギュレーション モードで、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] コマンドを使用します。ログインの RADIUS 認証をディセーブルにするか、デフォルト値に戻すには、ライン コンフィギュレーション モードで、**no login authentication** {**default** | *list-name*} コマンドを使用します。

# AAA サーバ グループの定義

ワイヤレス デバイスを設定して、AAA サーバ グループを使用し、認証に既存のサーバ ホストをまとめることができます。設定されているサーバ ホストのサブセットを選択して、特定のサービスでこれらを使用する必要があります。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。このリストは、選択されたサーバ ホストの IP アドレスを示します。

サーバ グループには、各エントリの ID（IP アドレスと UDP ポート番号の組み合わせ）が一意な場合、同じサーバの複数のホスト エントリを含めることもできます。これにより、異なるポートを、特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。同じサービス（アカウンティングなど）の同じ RADIUS サーバで 2 つの異なるホスト エントリを設定する場合、2 番目に設定されるホスト エントリは、最初のホスト エントリのフェールオーバー バックアップとして機能します。

**server** グループ サーバ コンフィギュレーションコマンドを使用して、特定のサーバと定義済みグループ サーバを関連付けます。サーバをその IP アドレスで識別するか、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識別できます。

AAA サーバ グループを定義して、特定の RADIUS サーバをこれに関連付けるには、特権 EXEC モードから、次の作業を行います。

| | 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 をイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **radius-server host** {*hostname* \| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] | 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。<br>• （任意）**auth-port** *port-number* 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。<br>• （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。<br>• （任意）**timeout** *seconds* には、ワイヤレス デバイスが再転送前に RADIUS サーバの応答を待機する時間を指定します。範囲は、1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンド設定を上書きします。**radius-server host** コマンドで timeout が設定されていない場合、**radius-server timeout** コマンドの設定が使用されます。<br>• （任意）**retransmit** *retries* には、サーバが応答しない場合、またはサーバの応答が遅い場合に RADIUS 要求がサーバに再送信される回数を指定します。範囲は、1 ～ 1000 です。**radius-server host** コマンドで retransmit 値が設定されていない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドが使用されます。<br>• （任意）**key** *string* には、ワイヤレス デバイス、および RADIUS サーバで実行している RADIUS デーモン間で使用される認証と暗号キーを指定します。<br>**（注）** このキーは、RADIUS サーバで使用される暗号鍵と一致しなければならないテキスト ストリングです。常に、**radius-server host** コマンドの最後の項目としてキーを設定します。先行スペースは無視されますが、鍵の中間および後続のスペースは使用されます。キーにスペースを含める場合、引用符がキーの一部でない限り、引用符でキーを囲まないでください。<br>単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにワイヤレス デバイスを設定するには、各 UDP ポート番号が異なるように、このコマンドを必要なだけ使用します。ワイヤレス デバイス ソフトウェアは、指定されている順序でホストを検索します。特定の RADIUS ホストで使用する timeout、retransmit、および encryption key の値を設定します。 |
| ステップ 4 | **aaa group server radius** *group-name* | AAA サーバ グループをグループ名で定義します。<br>このコマンドは、ワイヤレス デバイスをサーバ グループ コンフィギュレーション モードにします。 |
| ステップ 5 | **server** *ip-address* | 特定の RADIUS サーバと定義済みサーバ グループと関連付けます。AAA サーバ グループの各 RADIUS サーバでこの手順を繰り返します。<br>グループの各サーバは、手順 2 で事前に定義されている必要があります。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config** | 入力内容を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |
| ステップ 9 | | RADIUS ログイン認証をイネーブルにします。『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章の「Configuring RADIUS Login Authentication」の項を参照してください。 |

指定した RADIUS サーバを削除するには、グローバル コンフィギュレーション モードで、**no radius-server host** *hostname* | *ip-address* コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、グローバル コンフィギュレーション モードで、**no aaa group server radius** *group-name* コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、sg-radius コンフィギュレーション モードで、**no server** *ip-address* コマンドを使用します。

次の例では、ワイヤレス デバイスは、2 つの異なる RADIUS グループ サーバ（*group1* および *group2*）を認識するように設定されます。group1 には、同じサービスに設定されている同じ RADIUS サーバに 2 つの異なるホスト エントリがあります。2 つめのホスト エントリは、最初のエントリのフェールオーバー 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
```

# ユーザ権限アクセスおよびネットワーク 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 許可がイネーブルの場合、ワイヤレス デバイスは、ユーザのプロファイルから受け取った情報を使用します。これは、ローカル ユーザ データベースまたはセキュリティ サーバにあり、ユーザ セッションを設定します。ユーザには、ユーザ プロファイルにより許可されている場合だけ、要求されたサービスのアクセス権が付与されます。

グローバル コンフィギュレーション モードで、**radius** キーワードを指定した **aaa authorization** コマンドを使用して、ユーザの特権 EXEC モードへのネットワーク アクセスを制限するパラメータを設定できます。

**aaa authorization exec radius** コマンドは、これらの authorization パラメータを設定します。

- 認証が RADIUS を使用して実行された場合、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証が RADIUS を使用して実行されなかった場合、ローカル データベースを使用します。

**（注）** 許可は、許可が設定されている場合でも CLI レベルを介してログインする認証ユーザにバイパスされます。

特権 EXEC アクセスおよびネットワーク サービスに RADIUS 許可を指定する場合、特権 EXEC モードから、次の手順を実行します。

| | 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 authorization network radius** | すべてのネットワーク関連サービス要求に対して、ユーザ RADIUS 許可にワイヤレス デバイスを設定します。 |
| ステップ 3 | **aaa authorization exec radius** | ワイヤレス デバイスをユーザ RADIUS 許可に設定して、ユーザが特権 EXEC アクセス権を持つかどうかを決めます。<br>**exec** キーワードは、ユーザ プロファイル情報（**autocommand** 情報など）を返す場合があります。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |

| | 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** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

許可をディセーブルにするには、グローバル コンフィギュレーション モードで、**no aaa authorization** {**network** | **exec**} *method1* コマンドを使用します。

## RADIUS 設定の表示

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

# TACACS+ でのアクセス ポイント アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）を使用して、ワイヤレス デバイスへの管理者アクセスを制御する方法について説明します。TACACS+ をサポートするようにワイヤレス デバイスを設定する方法の詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章を参照してください。

TACACS+ は、詳細なアカウンティング情報、および認証や認可プロセスを介した柔軟な管理制御を提供します。TACACS+ は、AAA により促進され、AAA コマンドを介してだけイネーブルにできます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ここでは、TACACS+ 設定について説明します。

- 「デフォルトの TACACS+ 設定」（P.10-16）
- 「TACACS+ ログイン認証の設定」（P.10-17）
- 「特権 EXEC アクセスおよびネットワーク サービスの TACACS+ 許可の設定」（P.10-18）
- 「TACACS+ 設定の表示」（P.10-19）

## デフォルトの TACACS+ 設定

TACACS+ および AAA は、デフォルトでディセーブルにされています。

セキュリティの欠落を避けるため、ネットワーク管理アプリケーションを介して TACACS+ を設定できません。イネーブルにされている場合、TACACS+ は、CLI を介してワイヤレス デバイス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て、そのリストをさまざまなインターフェイスに適用します。認証方式のリストは、実行される認証のタイプ、およびそれらが実行される順序を定義します。これは、定義される認証方式が実行される前に、特定のインターフェイスに適用しなければなりません。唯一の例外は、デフォルトの認証方式リストです（この名前は *default* です）。デフォルトの認証方式リストは、名前付き認証方式リストが明示的に定義されている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。

認証方式リストは、ユーザの認証に使用される順序と認証方式を記述します。最初の方式が失敗した場合の認証にバックアップ システムが使用されるように、認証に 1 つ以上のセキュリティ プロトコルを指定できます。ソフトウェアは、リストの最初の方式を使用して、ユーザを認証します。この方式が応答しない場合、ソフトウェアは、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、リストの認証方式との通信に成功するまで、または定義されているすべての方式が失敗するまで、続けられます。このサイクルのいずれかの時点で認証が失敗した場合、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 アクセスを拒否することで応答した場合、認証プロセスは停止し、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードから、次の作業を行います。これは必須手順です。

| | 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 をイネーブルにします。 |
| ステップ 3 | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] | ログイン認証方式リストを作成します。<br>• 名前付きリストが **login authentication** コマンドで指定されていないときに使用されるデフォルト リストを作成するには、デフォルト状況で使用される方式リストが後に続く **default** キーワードを使用します。デフォルト方式リストは、すべてのインターフェイスに自動的に適用されます。<br>• *list-name* には、作成するリストに名前を付ける文字ストリングを指定します。<br>• *method1...* 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。認証の追加方式は、直前の方式からエラーが返された場合だけ使用されます。失敗した場合は、使用されません。<br>次のいずれかの方式を選択します。<br>• **local**：認証のローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力しなければなりません。**username** *password* コマンドをグローバル コンフィギュレーション モードで使用します。<br>• **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、TACACS+ サーバを設定しなければなりません。 |
| ステップ 4 | **line** [**console** \| **tty** \| **vty**] *line-number* [*ending-line-number*] | ライン コンフィギュレーション モードを開始して、認証リストを適用するラインを設定します。 |
| ステップ 5 | **login authentication** {**default** \| *list-name*} | 認証リストをラインまたはラインのセットに適用します。<br>• **default** を指定する場合、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。<br>• *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show running-config** | 入力内容を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

AAA をディセーブルにするには、グローバル コマンド モードで、**no aaa new-model** コマンドを使用します。AAA 認証をディセーブルにするには、グローバル コマンド モードで、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするか、デフォルト値に戻すには、ライン コンフィギュレーション モードで、**no login authentication** {**default** | *list-name*} コマンドを使用します。

# 特権 EXEC アクセスおよびネットワーク 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 許可がイネーブルの場合、ワイヤレス デバイスは、ユーザ プロファイルから受け取った情報を使用します。これは、ローカル ユーザ データベースまたはセキュリティ サーバにあり、ユーザ セッションを設定します。ユーザには、ユーザ プロファイルの情報により許可されている場合だけ、要求されたサービスのアクセス権が付与されます。

グローバル コンフィギュレーション モードで、**tacacs+** キーワードを指定した **aaa authorization** コマンドを使用して、ユーザの特権 EXEC モードへのネットワーク アクセスを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、これらの許可パラメータを設定します。

- 認証が TACACS+ を使用して実行された場合、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証が TACACS+ を使用して実行されなかった場合、ローカル データベースを使用します。

**（注）** 許可は、許可が設定されている場合でも CLI レベルを介してログインする認証ユーザにバイパスされます。

特権 EXEC アクセスおよびネットワーク サービスに TACACS+ 許可を指定する場合、特権 EXEC モードから、次の手順を実行します。

| | 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 authorization network tacacs+** | すべてのネットワーク関連サービス要求に対して、ユーザ TACACS+ 許可にワイヤレス デバイスを設定します。 |
| ステップ 3 | **aaa authorization exec tacacs+** | ワイヤレス デバイスをユーザ TACACS+ 許可に設定して、ユーザが特権 EXEC アクセス権を持つかどうかを決めます。<br>**exec** キーワードは、ユーザ プロファイル情報（**autocommand** 情報など）を返す場合があります。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| 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** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

許可をディセーブルにするには、グローバル コンフィギュレーション モードで、**no aaa authorization** {**network** | **exec**} *method1* コマンドを使用します。

## TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、特権 EXEC モードで、**show tacacs** コマンドを使用します。

# ワイヤレス ハードウェアおよびソフトウェアの管理

ここでは、次の作業の実行について説明します。

- 「ワイヤレス デバイスの工場出荷時のデフォルト設定へのリセット」（P.10-19）
- 「ワイヤレス デバイスの再起動」（P.10-19）
- 「ワイヤレス デバイスのモニタリング」（P.10-20）

## ワイヤレス デバイスの工場出荷時のデフォルト設定へのリセット

ワイヤレス デバイス ハードウェアおよびソフトウェアをその工場出荷時のデフォルト設定にリセットするには、ルータの Cisco IOS 特権 EXEC モードで、**service-module wlan-ap0 reset default-config** コマンドを使用します。

**注意**　データを損失することがあるため、シャットダウンまたは障害状態からの回復には、**service-module wlan-ap0 reset** コマンドだけを使用してください。

## ワイヤレス デバイスの再起動

正規の手順でシャットダウンを実行し、ワイヤレス デバイスを再起動するには、ルータの Cisco IOS 特権 EXEC モードで、**service-module wlan-ap0 reload** コマンドを使用します。確認プロンプトで、**Enter** キーを押してアクションを確認するか、**n** を入力してキャンセルします。

自律モードで実行している場合、reload コマンドを使用する、再起動前に設定が保存されます。これに失敗した場合、次のメッセージが表示されます。

```
Failed to save service module configuration.
```

Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）モードで実行している場合、reload 機能は、通常、Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）により扱われます。**service-module wlan-ap0 reload** コマンドを入力した場合、次のメッセージが表示されます。

```
The AP is in LWAPP mode. Reload is normally handled by WLC controller.

Still want to proceed? [yes]
```

# ワイヤレス デバイスのモニタリング

ここでは、ルータのハードウェアのモニタリング用のコマンドについて説明します。

- 「ワイヤレス デバイス統計情報の表示」（P.10-20）
- 「ワイヤレス デバイス ステータスの表示」（P.10-20）

## ワイヤレス デバイス統計情報の表示

特権 EXEC モードで、**service-module wlan-ap0 statistics** コマンドを使用すると、ワイヤレス デバイス統計情報を表示できます。次に、このコマンドの出力例を示します。

```
  CLI reset count = 0
  CLI reload count = 1
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 10

The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

## ワイヤレス デバイス ステータスの表示

特権 EXEC モードで、**service-module wlan-ap0 status** コマンドを使用すると、ワイヤレス デバイスのステータスおよびその設定情報を表示できます。次に、このコマンドの出力例を示します。

```
Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..

Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Integrated Services
Routers.
```

# システムの時刻と日付の管理

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、またはワイヤレス デバイスの時刻と日付を設定して、手動で、ワイヤレス デバイスのシステムの時刻と日付を管理できます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*』を参照してください。

ここでは、次の設定情報を示します。

- 「簡易ネットワーク タイム プロトコルについて」（P.10-21）
- 「SNTP の設定」（P.10-21）
- 「時刻および日付の手動設定」（P.10-22）

# 簡易ネットワーク タイム プロトコルについて

簡易ネットワーク タイム プロトコル（SNTP）は、NTP の簡素化されたクライアント専用バージョンです。SNTP は、NTP サーバから時刻を受信できるだけで、時刻サービスを他のシステムに提供できません。SNTP は、通常、100 ミリ秒以内の正確な時刻を提供しますが、NTP の複雑なフィルタリングおよび統計メカニズムは提供しません。

設定済みサーバにパケットを要求してこれを受信する、または任意のソースから NTP ブロードキャスト パケットを受信するように、SNTP を設定できます。複数のソースが NTP パケットを送信する場合、最適な層のサーバが選択されます。NTP および層の詳細については、次の URL をクリックしてください。

*http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075*

複数のサーバが同じ層にある場合、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。これらの両方を満たすサーバが複数ある場合、時刻パケットを最初に送信したサーバが選択されます。SNTP が新しいサーバを選択するのは、クライアントが現在選択されているサーバからパケットの受信を停止した場合、または（上記の条件に従って）SNTP がより最適なサーバを検出した場合だけです。

# SNTP の設定

SNTP は、デフォルトでディセーブルにされています。SNTP をアクセス ポイントでイネーブルにするには、グローバル コンフィギュレーション モードで、表 2 にリストされているコマンドのいずれか、または両方を使用します。

**表 2　　SNTP コマンド**

| コマンド | 目的 |
|---|---|
| **sntp server** {*address* \| *hostname*} [**version** *number*] | NTP サーバから NTP パケットを要求するように SNTP を設定します。 |
| **sntp broadcast client** | 任意の NTP ブロードキャスト サーバから NTP パケットを受信するように SNTP を設定します。 |

**sntp server** コマンドは、各 NTP サーバに一度入力します。NTP サーバは、アクセス ポイントから SNTP メッセージに応答するように設定する必要があります。

**sntp server** コマンドおよび **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 サーバから時刻を受信しますが、層が同じ場合、設定済みサーバからの時刻を優先します。SNTP の情報を表示するには、**show sntp** EXEC コマンドを使用します。

# 時刻および日付の手動設定

他の時刻ソースを使用できない場合、システムを再起動してから時刻と日付を手動で設定できます。次にシステムが再起動されるまで、正確な時刻に維持されます。手動での設定は最後の手段とすることをお勧めします。ワイヤレス デバイスが同期化できる外部ソースがある場合、システム クロックを手動で設定する必要はありません。

ここでは、次の設定情報を示します。


- 「システム クロックの設定」（P.10-22）
- 「時刻と日付の設定の表示」（P.10-23）
- 「時間帯の設定」（P.10-23）
- 「夏時間の設定」（P.10-24）


## システム クロックの設定

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

システム クロックを設定するには、特権 EXEC モードから、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **clock set** *hh*:*mm*:*ss day month year*<br>または<br>**clock set** *hh*:*mm*:*ss month day year* | 次のいずれかの形式を使用して、システム クロックを手動で設定します。<br>• *hh*:*mm*:*ss* には、時間（24 時間形式）、分、秒で時刻を指定します。指定された時刻は、設定されている時間帯に関連します。<br>• *day* には、日付を月の日付で指定します。<br>• *month* には、月をその完全な名前で指定します。<br>• *year* には、年度を 4 桁（省略形ではなく）で指定します。 |
| ステップ 2 | **show running-config** | 入力内容を確認します。 |
| ステップ 3 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

次に、システム クロックを 2001 年 7 月 23 日、1:32 p.m. に手動で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

時刻と日付の設定を表示するには、特権 EXEC モードで、**show clock** [**detail**] コマンドを使用します。

システム クロックは、時刻が信頼できるか（正確か）どうかを示す *authoritative* フラグを保持します。システム クロックが、NTP などのタイミング ソースにより設定されている場合、フラグが設定されます。時刻が信頼できない場合、これは、表示目的だけに使用されます。ピアの時刻が無効な場合、クロックが信頼でき、*authoritative* フラグが設定されるまで、このフラグにより、両ピアがクロックと同期化しないようになります。

次に、**show clock** 表示の前に付いているシンボルの意味を示します。

- *****：時刻は信頼できません。
- （ブランク）：時刻は信頼できます。
- **.**：時刻は信頼できますが、NTP は同期化されません。

## 時間帯の設定

時間帯を手動で設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **clock timezone** *zone hours-offset* [***minutes-offset***] | 時間帯を設定します。<br>ワイヤレス デバイスは、Universal Time Coordinated（UTC; 協定世界時）で内部時刻を保持するため、時刻が手動で設定される場合、このコマンドは、表示目的だけに使用されます。<br>• *zone* には、表示時刻が有効な場合に表示される時間帯の名前を入力します。デフォルトは UTC です。<br>• *hours-offset* には、UTC からの時間オフセットを入力します。<br>• （任意）*minutes-offset* には、UTC からの分オフセットを入力します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

グローバル コンフィギュレーション モードの **clock timezone** コマンドの *minutes-offset* 変数は、現地時間帯と UTC との差が分単位である場合に使用できます。たとえば、Atlantic Canada（AST）の一部の地区の時間帯は、UTC-3.5 です。ここで、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは、**clock timezone AST -3 30** です。

時刻を UTC に設定するには、グローバル コンフィギュレーション モードで、**no clock timezone** コマンドを使用します。

## 夏時間の設定

毎年特定の曜日に夏時間が開始し終了する地域に夏時間を設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]] | 毎年指定された日に開始および終了する夏時間を設定します。<br>夏時間は、デフォルトでディセーブルにされています。パラメータを指定せずに、**clock summer-time** *zone* **recurring** を指定する場合、夏時間の規則は米国の規則をデフォルトにします。<br>• *zone* には、夏時間が施行されているときに表示される時間帯の名前（たとえば、PDT）を指定します。<br>• （任意）*week* には、月の何週目か（1 ～ 5 または **last**）を指定します。<br>• （任意）*day* には、曜日（たとえば、Sunday）を指定します。<br>• （任意）*month* には、月（たとえば、January）を指定します。<br>• （任意）*hh*:*mm* には、時間および分で時刻（24 時間形式）を指定します。<br>• （任意）*offset* には、サマー タイム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 です。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

**clock summer-time** グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地時間帯を基準にしています。開始時刻は、標準時刻を基準にしています。終了時間は夏時間を基準にしています。開始月が、終了月前の場合、システムでは、南半球であると想定されます。

次に、夏時間が、4 月の第一日曜日の 02:00 から始まり、10 月の最後の日曜日の 02:00 に終わるように指定する例を示します。

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

現地の夏時間が、定期的なパターンに従わない（次の夏時間のイベントの正確な日付および時刻を設定する）場合、特権 EXEC モードから、次の手順を実行します。

| | 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 | **clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]]<br>または<br>**clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]] | 夏時間が最初の日付で開始し、2 番目の日付で終了するように設定します。<br>夏時間は、デフォルトでディセーブルにされています。<br>• *zone* には、夏時間が施行されているときに表示される時間帯の名前（たとえば、PDT）を指定します。<br>• （任意）*week* には、月の何週目か（1 ～ 5 または **last**）を指定します。<br>• （任意）*day* には、曜日（たとえば、Sunday）を指定します。<br>• （任意）*month* には、月（たとえば、January）を指定します。<br>• （任意）*hh*:*mm* には、時間および分で時刻（24 時間形式）を指定します。<br>• （任意）*offset* には、サマー タイム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 です。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

**clock summer-time** グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地時間帯を基準にしています。開始時刻は、標準時刻を基準にしています。終了時間は夏時間を基準にしています。開始月が、終了月前の場合、システムでは、南半球であると想定されます。

夏時間をディセーブルにするには、グローバル コンフィギュレーション モードで、**no clock summer-time** コマンドを使用します。

次に、夏時間が 2000 年 10 月 12 日 02:00 に始まり、2001 年 4 月 26 日 02:00 に終了するよう設定する例を示します。

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

# システム名およびプロンプトの設定

識別できるようにワイヤレス デバイスのシステム名を設定します。デフォルトでは、システム名およびプロンプトは *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。大なりシンボル（>）が追加されます。グローバル コンフィギュレーション モードで **prompt** コマンドを使用してプロンプトを手動で設定しない限り、プロンプトは、システム名が変更された場合に必ず更新されます。

**（注）** ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP Addressing Services Command Reference*』を参照してください。

ここでは、次の設定情報を示します。


- 「デフォルトのシステム名およびプロンプト設定」（P.10-26）
- 「システム名の設定」（P.10-26）
- 「DNS について」（P.10-27）


## デフォルトのシステム名およびプロンプト設定

デフォルトのアクセス ポイント システム名およびプロンプトは *ap* です。

## システム名の設定

システム名を手動で設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **hostname** *name* | システム名を手動で設定します。<br>デフォルト設定は、*ap* です。<br>**（注）** システム名を変更すると、ワイヤレス デバイス ラジオがリセットされ、関連付けられているクライアント デバイスの関連付けが解除され、その後すぐに再び関連付けられます。<br>**（注）** システム名は最高 63 文字まで入力できます。ただし、ワイヤレス デバイスがそれ自体をクライアント デバイスに識別する場合、システム名の最初の 15 文字だけ使用します。クライアント ユーザがデバイス間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 文字になるようにしてください。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

システム名を設定する場合、名前は、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 コンフィギュレーション モードで、**no hostname** コマンドを使用します。

# DNS について

DNS プロトコルは、ホスト名を IP アドレスにマッピングできる分散データベースである、Domain Name System（DNS; ドメイン ネーム システム）を制御します。ワイヤレス デバイスで DNS を設定する場合、**ping**、**telnet**、**connect**、および関連する Telnet サポート操作など、すべての IP コマンドで、IP アドレスの代わりにホスト名を使用できます。

IP は、位置やドメインによってデバイスを識別できる階層ネーミング スキームを定義します。ドメイン名は、デリミタとしてピリオド（.）を使用して結合されます。たとえば、Cisco Systems は、IP が *com* ドメイン名により識別される営利団体であるため、そのドメイン名は *cisco.com* です。このドメインの、File Transfer Protocol（FTP; ファイル転送プロトコル）システムなど、特定のデバイスは、*ftp.cisco.com* として識別されます。

ドメイン名を追跡するため、IP は、IP アドレスにマッピングされる名前のキャッシュ（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ます。ドメイン名を IP アドレスにマッピングするには、ホスト名を識別し、ネットワークに存在するネーム サーバを指定し、DNS をイネーブルにする必要があります。

ここでは、次の設定情報を示します。


- 「デフォルトの DNS 設定」（P.10-27）
- 「DNS の設定」（P.10-28）
- 「DNS 設定の表示」（P.10-29）


## デフォルトの DNS 設定

表 10-3 では、デフォルトの DNS 設定を示しています。

**表 10-3　デフォルトの DNS 設定**

| 機能 | デフォルト設定 |
|---|---|
| DNS enable state | ディセーブル。 |
| DNS default domain name | 設定されていません。 |
| DNS servers | ネーム サーバ アドレスは設定されていません。 |

## DNS の設定

DNS を使用するようにワイヤレス デバイスを設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **ip domain-name** *name* | 完全修飾でないホスト名（ドット付き 10 進表記ドメイン名を使用しない名前）を完成させるためにソフトウェアが使用するデフォルト ドメイン名を定義します。<br>未修飾名とドメイン名を区切る最初のピリオドを含めないでください。<br>起動時、ドメイン名は設定されません。ただし、ワイヤレス デバイス設定が BOOTP または DHCP サーバに渡される場合、デフォルト ドメイン名が BOOTP または DHCP サーバにより設定されることがあります（この情報でサーバが構成された場合）。 |
| ステップ 3 | **ip name-server** *server-address1* [*server-address2 ... server-address6*] | 1 つ以上のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。<br>ネーム サーバは 6 台まで指定できます。スペースでサーバ アドレスを区切ります。最初に指定されるサーバは、プライマリ サーバです。ワイヤレス デバイスは、DNS 要求を最初にプライマリ サーバに送信します。この要求に失敗すると、バックアップ サーバに要求が送信されます。 |
| ステップ 4 | **ip domain-lookup** | （任意）ワイヤレス デバイスでの DNS に基づいたホスト名からアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。<br>ネットワーク デバイスが、名前割り当てを制御し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 ネーミング スキーム（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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config** | 入力内容を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

ワイヤレス デバイス IP アドレスをそのホスト名として使用する場合、IP アドレスが使用され、DNS 要求は発生しません。ピリオド（.）を含まないホスト名を設定する場合、名前を IP アドレスにマッピングする DNS 要求が行われる前に、デフォルト ドメイン名が続くピリオドが、ホスト名に追加されます。デフォルト ドメイン名は、グローバル コンフィギュレーション モードで **ip domain-name** コマンドを設定される値です。ホスト名にピリオド（.）が含まれる場合、Cisco IOS ソフトウェアは、デフォルト ドメイン名をホスト名に追加せずに、IP アドレスを参照します。

ドメイン名を削除するには、グローバル コンフィギュレーション モードで、**no ip domain-name** *name* コマンドを使用します。ネーム サーバ アドレスを削除するには、グローバル コンフィギュレーション モードで、**no ip name-server** *server-address* コマンドを使用します。ワイヤレス デバイスで DNS をディセーブルにするには、グローバル コンフィギュレーション モードで、**no ip domain-lookup** コマンドを使用します。

## DNS 設定の表示

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

（注）　DNS がワイヤレス デバイスで設定されている場合、**show running-config** コマンドを使用すると、サーバの名前ではなく、IP アドレスが表示されることがあります。

# バナーの作成

Message-of-The-Day（MOTD）およびログイン バナーを設定できます。MOTD バナーは、接続されるすべての端末にログイン時に表示されます。これは、すべてのネットワーク ユーザに影響を与えるメッセージ（間もなくシステムがシャットダウンされるなど）を送信する場合に便利です。

ログイン バナーも接続されているすべての端末に表示されます。これは、MOTD バナーが表示されてから、ログイン プロンプトが表示されるまでに表示されます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報を示します。

- 「デフォルトのバナー設定」（P.10-29）
- 「Message-of-the-Day ログイン バナーの設定」（P.10-29）
- 「ログイン バナーの設定」（P.10-30）

## デフォルトのバナー設定

MOTD およびログイン 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

ワイヤレス デバイスへのログインが発生したときに画面に表示される単一または複数行のメッセージ バナーを作成できます。

MOTD ログイン バナーを設定するには、特権 EXEC モードから、次の作業を行います。

| | 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 | **banner motd** *c message c* | Message-of-the-Day を指定します。<br>*c* には、シャープ記号（#）などの必要なデリミタを入力し、**Enter** キーを押します。デリミタは、バナー テキストの開始および終了を示します。終了デリミタの後の文字は廃棄されます。<br>*message* には、最高 255 文字のバナー メッセージを入力します。メッセージでデリミタを使用できません。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

MOTD バナーを削除するには、グローバル コンフィギュレーション モードで、**no banner motd** コマンドを使用します。

次に、ワイヤレス デバイスの MOTD バナーを設定する例を示します。シャープ記号（#）は、開始および終了デリミタとして使用されます。

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

次の例では、直前の設定のバナーを示します。

```
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

接続されている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 バナーが表示されてから、ログイン プロンプトが表示されるまでに表示されます。

ログイン バナーを設定するには、特権 EXEC モードから、次の作業を行います。

| | 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 | **banner login** *c message c* | ログイン メッセージを指定します。<br>*c* には、シャープ記号（#）などの必要なデリミタを入力し、**Enter** キーを押します。デリミタは、バナー テキストの開始および終了を示します。終了デリミタの後の文字は廃棄されます。<br>*message* には、最高 255 文字のログイン メッセージを入力します。メッセージでデリミタを使用できません。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

ログイン バナーを削除するには、グローバル コンフィギュレーション モードで、**no banner login** コマンドを使用します。

次に、ドル記号（$）を開始および終了デリミタとして使用して、ワイヤレス デバイスのログイン バナーを設定する例を示します。

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

# イーサネットの速度およびデュプレックスの設定

Cisco 1941-W ISR インターフェイスは、デフォルトで 1000 Mbps 速度およびデュプレックス設定だけをサポートします。インターフェイスは常に稼動しています ワイヤレス デバイスがスイッチからインライン電力を受け取る場合、イーサネット リンクをリセットする速度またはデュプレックス設定を変更すると、ワイヤレス デバイスが再起動されます。

**（注）** ワイヤレス デバイス イーサネット ポートの速度またはデュプレックス設定は、ワイヤレス デバイスが接続されているポートのイーサネット設定と一致しなければなりません。ワイヤレス デバイスが接続されているポートの設定を変更する場合、ワイヤレス デバイス イーサネット ポートの設定もこれに一致するように変更します。

イーサネットの速度およびデュプレックスは、デフォルトで **auto** に設定されています。イーサネットの速度およびデュプレックスを設定するには、特権 EXEC モードから、次の作業を行います。

| | 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 | **interface fastethernet0** | コンフィギュレーション インターフェイス モードを開始します。 |
| ステップ 3 | **speed** {**10** \| **100** \| **auto**} | イーサネットの速度を設定します。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 | **duplex** {**auto** \| **full** \| **half**} | デュプレックスを設定します。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 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config** | 入力内容を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

# ワイヤレス ネットワーク管理のアクセスポイントの設定

ワイヤレス デバイスをワイヤレス ネットワーク管理でイネーブルにできます。Wireless Network Manager（WNM; 無線ネットワーク マネージャ）は、ワイヤレス LAN のデバイスを管理します。

次のコマンドを入力して、WNM と相互作用するようにワイヤレス デバイスを設定します。

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

次のコマンドを入力して、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します。

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

可能なステータスは、*not authenticated*、*authentication in progress*、*authentication fail*、*authenticated* および *security keys setup* です。

# ローカル認証および許可のアクセス ポイントの設定

ローカル モードで AAA を実装するようにワイヤレス デバイスを設定して、サーバなしで動作するように AAA を設定できます。ワイヤレス デバイスは、認証および許可を扱います。この設定ではアカウンティングは使用できません。

（注）　ワイヤレス デバイスを 802.1x 対応クライアント デバイスのローカル オーセンティケータとして設定し、メイン サーバのバックアップを提供、または RADIUS サーバなしでネットワークの認証サービスを提供できます。ローカル オーセンティケータとしてワイヤレス デバイスを設定する方法の詳細については、Cisco.com 上のマニュアル『*Using the Access Point as a Local Authenticator*』を参照してください。
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

ワイヤレス デバイスをローカル AAA に設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 をイネーブルにします。 |
| ステップ 3 | **aaa authentication login default local** | ログイン認証を設定して、ローカル ユーザ名データベースを使用します。**default** キーワードは、ローカル ユーザ データベース認証をすべてのインターフェイスに適用します。 |
| ステップ 4 | **aaa authorization exec local** | ユーザ AAA 許可を設定して、ローカル データベースをチェックすることでユーザが EXEC シェルの実行を許可されるかどうかを決定します。 |
| ステップ 5 | **aaa authorization network local** | すべてのネットワーク関連サービス要求に対して、ユーザ AAA 許可を設定します。 |
| ステップ 6 | **username** *name* [**privilege** *level*] {**password** *encryption-type password*} | ローカル データベースを入力し、ユーザ名に基づいた認証システムを確立します。<br>このコマンドを各ユーザに繰り返します。<br>• *name* には、ユーザ ID を 1 単語で指定します。スペースおよび引用符は使用できません。<br>• （任意）*level* には、ユーザがアクセス権を取得した後の権限レベルを指定します。範囲は、0 ～ 15 です。レベル 15 は、特権 EXEC モード アクセスを提供します。レベル 0 は、ユーザ EXEC モード アクセスを提供します。<br>• *encryption-type* には、暗号化されていないパスワードを使用する場合は **0** を入力します。非表示パスワードを使用する場合は **7** を入力します。<br>• *password* には、ワイヤレス デバイスへのアクセス権を取得するときにユーザが入力する必要があるパスワードを指定します。パスワードは、1 ～ 25 文字でなければなりません。スペースを含めることができます。また、パスワードは、**username** コマンドで指定される最後のオプションでなければなりません。<br>（注）　TAB、?、$、+ および [ の文字は、パスワードには無効な文字です。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 8 | **show running-config** | 入力内容を確認します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

AAA をディセーブルにするには、グローバル コマンド モードで、**no aaa new-model** コマンドを使用します。許可をディセーブルにするには、グローバル コンフィギュレーション モードで、**no aaa authorization** {**network** | **exec**} *method1* コマンドを使用します。

# 認証キャッシュおよびプロファイルの設定

認証キャッシュおよびプロファイル機能を使用すると、アクセス ポイントでユーザの認証および許可応答をキャッシュに入れることができます。これにより、これ以降の認証および許可要求を AAA サーバに送信しなくて済みます。

（注）　アクセス ポイントでは、この機能は、Admin 認証だけでサポートされます。

この機能をサポートする次のコマンドは、Cisco IOS リリース 12.3(7) に含まれています。

**cache expiry**
**cache authorization profile**
**cache authentication profile**
**aaa cache profile**

（注）　これらのコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC*』を参照してください。

次に、許可キャッシュがイネーブルにされている、TACACS+ を使用した Admin 認証に設定されたアクセス ポイントの設定例を示します。この例は、TACACS サーバに基づいていますが、アクセス ポイントは、RADIUS を使用した Admin 認証に設定できます。

```
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アクセス ポイントの設定

次の項では、DHCP サーバとして機能するようにワイヤレス デバイスを設定する方法について説明します。


- 「DHCP サーバの設定」（P.10-36）
- 「DHCP サーバ アクセス ポイントのモニタリングおよび保守」（P.10-38）


## DHCP サーバの設定

デフォルトでは、アクセス ポイントは、ネットワークの DHCP サーバから IP 設定を受け取るように設定されています。また、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て、IP 設定を有線およびワイヤレスの両方の LAN に割り当てることもできます。

（注）　アクセス ポイントを DHCP サーバとして設定する場合、IP アドレスは、そのサブネットのデバイスに割り当てられます。デバイスは、サブネット外ではなく、サブネット上の他のデバイスと通信します。データをサブネット外に渡す必要がある場合、デフォルト 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 アドレスは、DHCP サーバとして設定されているアクセス ポイントと同じサブネットになければなりません。

DHCP 関連のコマンドおよびオプションの詳細については、『*Cisco IOS IP Addressing Services Configuration Guide, Release 12.4*』の DHCP パートを参照してください。DHCP パートを参照するには、次の URL をクリックしてください。

*http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html*

アクセス ポイントを設定して、DHCP サービスを提供し、デフォルト ルータを指定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **ip dhcp excluded-address** *low_address* [*high_address*] | ワイヤレス デバイスが割り当てるアドレスの範囲からワイヤレス デバイス IP アドレスを除外します。10.91.6.158 のように 4 つの文字グループで IP アドレスを入力します。<br>ワイヤレス デバイスは、DHCP アドレス プール サブネットのすべての IP アドレスが、DHCP クライアントへの割り当てに使用できると想定します。そのため、DHCP サーバがクライアントへの割り当てに使用しない IP アドレスを指定する必要があります。<br>（任意）除外されたアドレスの範囲を入力するには、範囲のロー エンドのアドレスを入力し、その後で範囲のハイ エンドのアドレスを入力します。 |
| ステップ 3 | **ip dhcp pool** *pool_name* | DHCP 要求に応答してワイヤレス デバイスが割り当てる IP アドレスのプールの名前を作成し、DHCP コンフィギュレーションモードを開始します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **network** *subnet_number* [*mask* \| *prefix-length*] | アドレス プールのサブネット番号を割り当てます。ワイヤレス デバイスは、このサブネット内で IP アドレスを割り当てます。<br>（任意）アドレス プールのサブネット マスクを割り当てるか、アドレス プレフィクスを構成するビット数を指定します。このプレフィクスは、ネットワーク マスクを割り当てる代替方法です。プレフィクス長の前には、スラッシュ（/）を付ける必要があります。 |
| ステップ 5 | **lease** {*days* [*hours*] [*minutes*] \| **infinite**} | ワイヤレス デバイスにより割り当てられる IP アドレスのリース期間を設定します。<br>• days：リース期間を日数で設定します。<br>• （任意）hours：リース期間を時間単位で設定します。<br>• （任意）minutes：リース期間を分単位で設定します。<br>• infinite：リース期間を無限に設定します。 |
| ステップ 6 | **default-router** *address* [*address2 ... address 8*] | サブネットの DHCP クライアントのデフォルト ルータの IP アドレスを指定します。ただし、IP アドレスが必要な場合、1 つのコマンド最高 8 つのアドレスを指定できます。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config** | 入力内容を確認します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

これらのコマンドの **no** 形式を使用すると、デフォルト設定に戻すことができます。

次に、ワイヤレス デバイスを DHCP サーバとして設定する、IP アドレスの範囲を除外する、デフォルト ルータを割り当てる例を示します。

```
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 ポイントのモニタリングおよび保守

次の例では、DHCP サーバ アクセス ポイントのモニタリングおよび保守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.10-38）
- 「clear コマンド」（P.10-38）
- 「debug コマンド」（P.10-39）


## show コマンド

DHCP サーバとしてのワイヤレス デバイスの情報を表示するには、特権 EXEC モードで、表 10-4 のコマンドを入力します。

**表 10-4　DHCP サーバの show コマンド**

| コマンド | 目的 |
|---|---|
| **show ip dhcp conflict** [*address*] | 特定の DHCP サーバにより記録されるすべてのアドレス衝突のリストを表示します。ワイヤレス デバイス IP アドレスを入力して、ワイヤレス デバイスにより記録される衝突を表示します。 |
| **show ip dhcp database** [*url*] | DHCP データベースの最近のアクティビティを表示します。<br>**（注）**　このコマンドは、特権 EXEC モードで使用します。 |
| **show ip dhcp server statistics** | サーバ統計情報および送受信されたメッセージのカウント情報を表示します。 |

## clear コマンド

DHCP サーバ変数をクリアするには、特権 EXEC モードで、表 10-5 のコマンドを使用します。

**表 10-5　DHCP サーバの clear コマンド**

| コマンド | 目的 |
|---|---|
| **clear ip dhcp binding** {*address* \| *}} | DHCP データベースからの自動アドレス 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クリアされます。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クリアされます。 |
| **clear ip dhcp conflict** {*address* \| *}} | DHCP データベースからアドレス衝突をクリアします。address 引数を指定すると、特定の（クライアント）IP アドレスの衝突がクリアされます。アスタリスク（*）を指定すると、すべてのアドレスの衝突がクリアされます。 |
| **clear ip dhcp server statistics** | すべての DHCP サーバ カウンタを 0 にリセットします。 |

### debug コマンド

DHCP サーバ デバッグをイネーブルにするには、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**}

このコマンドの **no** 形式を使用すると、ワイヤレス デバイス DHCP サーバのデバッグをディセーブルにできます。

# セキュア シェルのアクセス ポイントの設定

ここでは、Secure Shell（SSH; セキュア シェル）機能の設定について説明します。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference for Release 12.4*』の「Secure Shell Commands」の項を参照してください。

## SSH について

SSH は、レイヤ 2 またはレイア 3 デバイスへの安全なリモート接続を提供するプロトコルです。SSH バージョン 1 と SSH バージョン 2 の 2 つの SSH バージョンがあります。このソフトウェア リリースは、これら両方の SSH バージョンをサポートしています。バージョン番号を指定しない場合、アクセス ポイントでは、デフォルトで、バージョン 2 が使用されます。

SSH は、デバイスが認証されるときに強力な暗号化を提供することで、Telnet よりも安全なリモート接続を提供します。SSH 機能には、SSH サーバおよび SSH 統合クライアントがあります。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（詳細について、「RADIUS でのアクセス ポイント アクセスの制御」（P.10-11）を参照してください）
- ローカル認証および許可（詳細については、「ローカル認証および許可のアクセス ポイントの設定」（P.10-32）を参照してください）

SSH の詳細については、『*Cisco IOS Security Configuration Guide for Release 12.4*』の第 5 部「Other Security Features」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）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 から暗号化されたソフトウェア イメージをダウンロードしてください。詳細については、このリリースのリリース ノートを参照してください。

SSH の設定および SSH 設定の表示については、『*Cisco IOS Security Configuration Guide for Release 12.4*』の第 6 部「Other Security Features」を参照してください。これは、次のリンクの Cisco.com から利用できます。

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

# クライアント ARP キャッシングの設定

関連するクライアント デバイスの Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュを保守するようにワイヤレス デバイスを設定できます。ワイヤレス デバイスで ARP キャッシュを保守すると、ワイヤレス LAN のトラフィック負荷を軽減できます。ARP キャッシングは、デフォルトでディセーブルにされています。

ここでは、この情報について説明します。


- 「クライアント ARP キャッシングについて」（P.10-40）
- 「ARP キャッシングの設定」（P.10-41）


## クライアント ARP キャッシングについて

ワイヤレス デバイスの ARP キャッシングにより、ワイヤレス デバイスのクライアント デバイスの ARP 要求を停止することでワイヤレス LAN のトラフィックが軽減されます。ARP 要求をクライアント デバイスに転送せずに、ワイヤレス デバイスは、関連付けられているクライアント デバイスに代わり要求に応答します。

ARP キャッシングがディセーブルの場合、ワイヤレス デバイスは、関連付けられているクライアントにラジオ ポートを介してすべての ARP 要求を転送します。ARP 要求を受け取るクライアントはこれに応答します。ARP キャッシングがイネーブルの場合、ワイヤレス デバイスは、関連付けられているクライアントの ARP 要求に応答し、要求をクライアントに転送しません。ワイヤレス デバイスが、キャッシュにない IP アドレスの ARP 要求を受け取ると、ワイヤレス デバイスは、その要求をドロップし、これを転送しません。そのビーコンで、ワイヤレス デバイスは、クライアント デバイスにバッテリ寿命を延ばすためにブロードキャスト メッセージを安全に無視できることを通知する情報要素を含んでいます。

### オプション ARP キャッシング

シスコ以外のクライアント デバイスがアクセス ポイントに関連付けられていて、データを受け渡さない場合、ワイヤレス デバイス は、クライアント IP アドレスを認識できない場合があります。このような状況がワイヤレス LAN で頻繁に発生する場合、オプション ARP キャッシングをイネーブルにできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスは、IP アドレスがワイヤレス デバイスに認識されているクライアントに代わって応答しますが、そのラジオ ポートから、認識されていないクライアントへの ARP 要求を転送します。ワイヤレス デバイスが、関連付けられているすべてのクライアントの IP アドレスを学習すると、関連付けられているクライアントに送信されない ARP 要求をドロップします。

# ARP キャッシングの設定

関連付けられているクライアントの ARP キャッシングを保守するようにワイヤレス デバイスを設定するには、特権 EXEC モードから、次の手順を実行します。

| | 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 | **dot11 arp-cache** [**optional**] | ワイヤレス デバイスで ARP キャッシングをイネーブルにします。<br>• （任意）**optional** キーワードを使用して、IP アドレスがワイヤレス デバイスに認識されているクライアント デバイスだけで ARP キャッシングをイネーブルにします。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 入力内容を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）入力内容をコンフィギュレーション ファイルに保存します。 |

次に、ARP キャッシングをアクセス ポイントで設定する例を示します。

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

# ポイントツーマルチポイント ブリッジの複数の VLAN およびレート制限の設定

この機能は、各 VLAN でのトラフィック レートを制御できる機能により、複数の VLAN で動作するように、ポイントツーマルチポイント ブリッジをどのように設定できるかを変更します。

（注）　レート制限ポリシーは、非ルート ブリッジのファスト イーサネット入力ポートだけに適用できます。

通常、複数の VLAN サポートにより、ユーザは、個々の VLAN に各リモート サイトがある、リモート サイトでの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、トラフィックを各サイトに分割し制御できます。レート制限を設定すると、全体のリンク帯域幅の消費量が指定量を超えるリモート サイトがなくなります。非ルート ブリッジのファスト イーサネット入力ポートを使用して、アップリンク トラフィックだけを制御できます。

クラスベースのポリシー機能を使用することで、レート制限を指定して、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できます。イーサネット インターフェイスの入力でレートを提供すると、すべての着信イーサネット パケットが設定レートに準拠するようになります。