CHAPTER 10

認証タイプの設定

この章では、ブリッジに認証タイプを設定する方法について説明します。この章の内容は、次のとおりです。

認証タイプの概要

この項ではブリッジに設定できる認証タイプについて説明します。認証タイプはブリッジに設定する SSID に関連付けられます。

ブリッジ間で通信するには、Open 認証または Shared Key 認証を使用してブリッジが互いに認証し合う必要があります。最大限のセキュリティを確保するために、ブリッジは Extensible Authentication Protocol（EAP）認証を使用してネットワークからも認証を得る必要があります。この認証タイプではネットワーク上の認証サーバが使用されます。

ブリッジは、次の 4 つの認証メカニズム（タイプ）を使用します。同時に複数の認証を使用することもできます。次の項でそれぞれの認証タイプについて説明します。

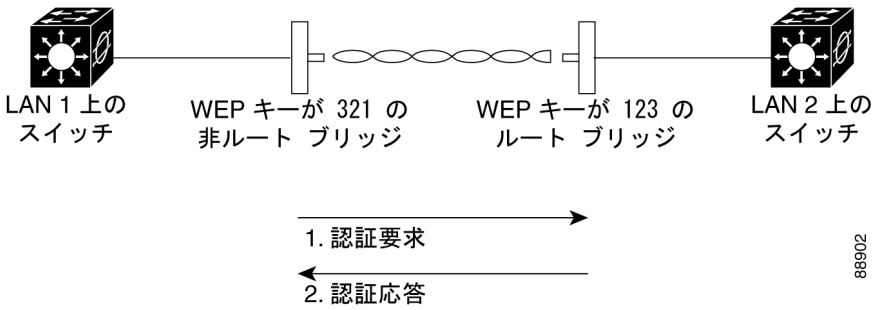
- ブリッジに対する Open 認証（P.10-2）
- ブリッジに対する Shared Key 認証（P.10-2）
- ネットワークに対する EAP 認証（P.10-3）

ブリッジに対する Open 認証

Open 認証では、すべての 1300 シリーズ ブリッジに対して、認証および別の 1300 シリーズ ブリッジとの通信の試みを許可します。Open 認証を使用すると、非ルート ブリッジはルート ブリッジに対して認証できますが、非ルート ブリッジが通信できるのは WEP キーがルート ブリッジの WEP キーに一致する場合のみです。WEP を使用していないブリッジは WEP を使用しているブリッジに対して認証を試みません。Open 認証では、ネットワーク上の RADIUS サーバは使用されません。

図 10-1 は、認証を試みる非ルート ブリッジと、Open 認証を使用しているルート ブリッジとの認証シーケンスを示しています。この例では、デバイスの WEP キーがブリッジのキーと一致しないため、認証はできても、データを転送することができません。

図 10-1　Open 認証のシーケンス



ブリッジに対する Shared Key 認証

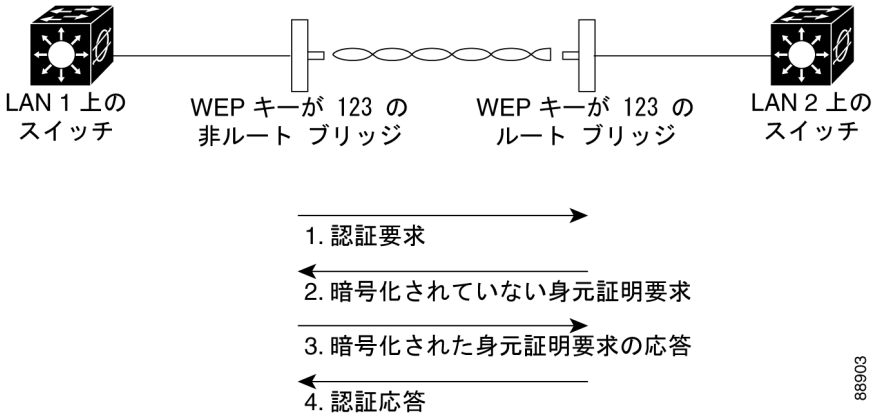
シスコでは、IEEE 802.11b 規格に準拠するために、Shared key 認証も採用しています。ただし、Shared key 認証にはセキュリティ上の弱点があるため、なるべく使用しないようにしてください。

Shared Key 認証では、ルート ブリッジが、ルート ブリッジとの通信を試みるその他のブリッジに対して、暗号化されていない身元証明要求テキスト文字列を送信します。認証を求めるブリッジは身元証明要求テキストを暗号化して、ルート ブリッジに返送します。身元証明要求テキストが正しく暗号化されていれば、ルート ブリッジはそのデバイスに認証を許可します。暗号化されていない身元証明要求も暗号化された身元証明要求も、どちらも監視することができます。ただしそのために、ルート ブリッジは、暗号化前のテキストと暗号化後のテキストを比較して WEP キーを計算す

る不正侵入者の攻撃に対し、無防備な状態になります。このような弱点により、Shared Key 認証は Open 認証よりも安全性が劣る場合があります。Open 認証と同様に、Shared Key 認証ではネットワーク上の RADIUS サーバは使用されません。

図 10-2 は、認証を試みるデバイスと、Shared Key 認証を使用しているブリッジとの認証シーケンスを示しています。この例では、デバイスの WEP キーがブリッジのキーと一致しているため、認証が成立し、通信が許可されます。

図 10-2　Shared Key 認証のシーケンス



ネットワークに対する EAP 認証

この認証タイプは、無線ネットワークに最高レベルのセキュリティを提供します。EAP を使用して EAP 互換の RADIUS サーバと対話することにより、ルート ブリッジは、別のブリッジと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを引き出す補助をします。RADIUS サーバはルート ブリッジに WEP キーを送ります。ブリッジはこのキーを、非ルート ブリッジとの間で送受信するすべてのユニキャスト データ信号に使用します。さらに、ルート ブリッジはブロードキャスト WEP キー（ブリッジの WEP キー スロット 1 に入力されたキー）を非ルート ブリッジのユニキャスト キーと共に暗号化して、非ルート ブリッジに送信します。

ブリッジで EAP を有効にすると、ネットワークに対する認証は、図 10-3 に示すシーケンスで実行されます。

図 10-3　EAP 認証のシーケンス

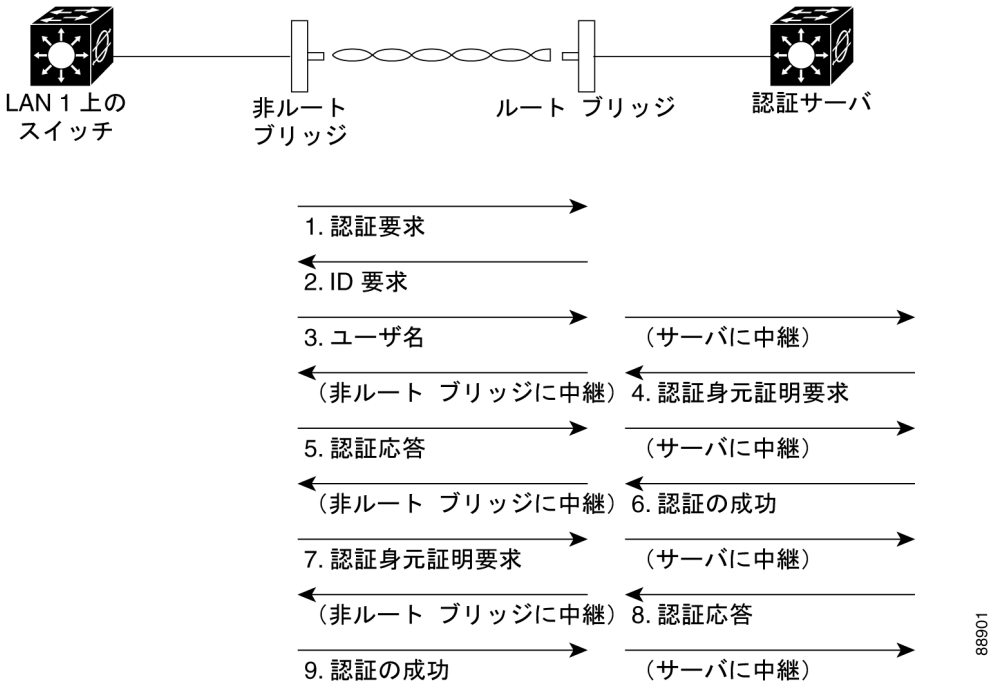


図 10-3 の 1 ～ 9 では、有線 LAN 上の非ルート ブリッジと RADIUS サーバが 802.1x および EAP を使用して、ルート ブリッジ経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求を非ルート ブリッジに送信します。非ルート ブリッジはユーザが入力したパスワードを一方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、それを非ルート ブリッジからの応答と比較します。RADIUS サーバが非ルート ブリッジを認証すると、同じ処理が逆方向から繰り返され、今度は非ルート ブリッジが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバと非ルート ブリッジは、非ルート ブリッジ固有の WEP キーを特定して、適切なレベルのネットワーク アクセスを提供します。これにより、有線のスイッチド セグメントのセキュリティ レベルは、個々のデスクトップのレベルまで近付きます。非ルート ブリッジはこのキーをロードして、ログオン セッションでの使用に備えます。

ログオン セッションでは、RADIUS サーバが *セッション キー*と呼ばれる WEP キーを暗号化し、有線 LAN 経由でルート ブリッジに送信します。ルート ブリッジは、セッション キーを使用してブロードキャスト キーを暗号化し、非ルート ブリッジに送信します。非ルート ブリッジは、送信されてきたキーを、セッション キーを使用して復号化します。非ルート ブリッジとルート ブリッジが WEP を有効にして、セッションおよびブロードキャスト WEP キーを残りのセッションのすべての通信に使用します。

EAP 認証には複数のタイプがありますが、ブリッジはどのタイプについても同じように機能します。ブリッジは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。ブリッジで EAP を設定する方法については、「SSID への認証タイプの割り当て」の項（P.10-6）を参照してください。

（注）　EAP 認証を使用する場合は、Open または Shared Key 認証を選択できますが、これは必須ではありません。EAP 認証は、ブリッジとネットワークの両方に対する認証を制御します。

認証されたブリッジの CCKM の利用

Cisco Centralized Key Management（CCKM）を使って、認証された非ルート ブリッジは、1 つのルート ブリッジから別のルート ブリッジへ、再アソシエーションの際にほとんど遅延することなくローミングできます。ネットワーク上のアクセス ポイントまたはスイッチは、Wireless Domain Services（WDS）を提供し、サブネット上の CCKM 対応ブリッジに対してセキュリティ認証のキャッシュを生成します。WDS デバイスの認証キャッシュは、CCKM 対応非ルート ブリッジが新しいルート ブリッジにローミングする場合の再アソシエーションに必要な時間を大幅に短縮します。非ルート ブリッジがローミングする場合、WDS デバイスはブリッジのセキュリティ認証を新しいルート ブリッジに転送し、再アソシエーション プロセスは、ローミングするブリッジと新しいルート ブリッジ間での 2 つのパケット交換だけになります。ローミングするブリッジは非常にすばやく再アソシエートするので、音声やその他の時間に敏感なアプリケーションにおける遅延はほぼなくなります。ブリッジで CCKM を有効にする方法の詳細は、「SSID への認証タイプの割り当て」の項（P.10-6）を参照してください。無線 LAN 上の WDS アクセス ポイント設定の詳細は、『Cisco IOS Software Configuration Guide for Cisco Aironet Access Points』の第 10 章を参照してください。

WPA キー管理の使用

Wi-Fi Protected Access（WPA）は、既存および将来の無線 LAN システムのデータ保護と、アクセス制御のレベルを大幅に向上する、標準の、相互運用性の優れたセキュリティ強化法です。WPA は、現在策定中の IEEE 802.11i 規格のサブセットで、この規格と互換性があります。WPA では、データ保護に Temporal Key Integrity Protocol（TKIP）を使用し、認証済みキー管理に 802.1X を使用しています。

WPA キー管理は、2 つの相互排他的な管理タイプである WPA および WPA-Pre-shared key（WPA-PSK）をサポートしています。非ルート ブリッジと認証サーバは、WPA キー管理を使用して、EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してルート ブリッジに渡します。ただし、そのためには、WPA-PSK を使用して非ルート ブリッジとルート ブリッジの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

（注）　WPA 情報エレメントでアドバタイズされる（さらに 802.11 でのアソシエーション中に決定される）ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、ルート ブリッジと非ルート ブリッジは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は認められていません。このような場合、非ルート ブリッジと無線 LAN とのアソシエーションが解除されてしまいます。

WPA キー管理をブリッジで設定する方法の詳細は、「SSID への認証タイプの割り当て」の項（P.10-6）を参照してください。

認証タイプの設定

この項では、認証タイプを設定する方法について説明します。認証タイプはブリッジの SSID に割り当てます。ブリッジの SSID 設定の詳細は、第 7 章「SSID の設定」を参照してください。この項では、次の項目を取り上げます。

デフォルトの認証設定

ブリッジのデフォルトの SSID は *autoinstall* です。表 10-1 にデフォルトの SSID のデフォルト認証設定を示します。

表 10-1　デフォルトの認証設定

機能	デフォルト設定
SSID	autoinstall
ゲスト モード SSID	autoinstall（ブリッジはビーコンでこの SSID をブロードキャストし、SSID を指定されていないブリッジのアソシエーションを許可します。）
tsunami に割り当てられる認証タイプ	Open

SSID への認証タイプの割り当て

イネーブル EXEC モードから、次の手順に従って SSID に認証タイプを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 3	**ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID 設定モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 （注）　SSID に空白は使用できません。
ステップ 4	**authentication open** [**eap** *list-name*]	（オプション）この SSID の認証タイプを Open に設定します。Open 認証では、すべてのブリッジに認証およびブリッジとの通信の試みを許可します。 • （オプション）SSID の認証タイプを EAP 認証を使用する Open に設定します。ブリッジは、他のすべてのブリッジに対して、ネットワーク接続を許可される前に EAP 認証の実行を強制します。*list-name* には、認証方式リストを指定します。 （注）　EAP 認証が設定されたブリッジは、アソシエートするすべてのブリッジに対して EAP 認証の実行を強制します。EAP を使用しないブリッジは EAP 認証が設定されたブリッジと通信できません。

	コマンド	目的
ステップ 5	**authentication shared** [**eap** *list-name*]	（オプション）SSID の認証タイプを Shared key に設定します。 （注）　ただし、Shared key 認証にはセキュリティ上の弱点があるため、なるべく使用しないようにしてください。 • （オプション）SSID の認証タイプを EAP 認証を使用する Shared Key に設定します。*list-name* には、認証方式リストを指定します。
ステップ 6	**authentication network-eap** *list-name*	（オプション）認証およびキー配布については、LEAP を使用するように SSID の認証タイプを設定します。シスコのブリッジでサポートされるのは LEAP のみですが、他の無線クライアントでは、EAP、PEAP、TLS など他の EAP 方式がサポートされる場合があります。
ステップ 7	**authentication key-management** {[**wpa**] [**cckm**]} [**optional**]	（オプション）SSID の認証タイプを CCKM または WPA、あるいはその両方に設定します。**optional** キーワードを使用すると、WPA または CCKM 用に設定されていない非ルート ブリッジもこの SSID を使用できます。**optional** キーワードを指定しないと、WPA または CCKM ブリッジのみがこの SSID を使用できます。 この SSID の CCKM 機能を有効にするには、Network-EAP 認証も有効にしなければなりません。また、この SSID の WPA 機能を有効にするには、Open 認証または Network-EAP 認証、あるいはその両方を有効にする必要があります。 （注）　WPA と CCKM を同時にサポートしているのは、802.11b と 802.11g 無線だけです。 （注）　CCKM または WPA を有効にするには、まず、SSID の VLAN に対する暗号化モードを、暗号スイート オプションの 1 つに設定しなければなりません。CCKM と WPA の両方を有効にするには、暗号化モードを、TKIP を含む暗号スイートに設定する必要があります。VLAN 暗号化モードの設定方法については、「暗号スイートと WEP の有効化」の項（P.9-5）を参照してください。 （注）　事前共有キーなしで SSID の WPA を有効にすると、キー管理タイプは WPA になります。事前共有キーを設定して SSID の WPA を有効にすると、キー管理タイプは WPA-PSK になります。事前共有キーの設定方法については、「追加の WPA の設定」の項（P.10-9）を参照してください。 （注）　CCKM をサポートするには、ルート ブリッジがネットワーク上の WDS デバイスと対話する必要があります。WDS デバイスと対話するようにルート ブリッジを設定する方法の詳細は、「WDS デバイスと対話するようルート ブリッジを設定する」の項（P.10-8）を参照してください。

	コマンド	目的
ステップ 8	**end**	イネーブル EXEC モードに戻ります。
ステップ 9	**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。

SSID を無効にする場合、または SSID 機能を無効にする場合は、SSID コマンドの **no** フォームを使用します。

次の例では、SSID bridgeman の認証タイプを、EAP 認証を使用する Open に設定します。bridgeman SSID を使用するブリッジは、*adam* というサーバを使用して EAP 認証を試行します。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication open eap adam
bridge(config-ssid)# end
```

このブリッジにアソシエートされる非ルート ブリッジの設定には、次のコマンドも含まれます。

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bridge7 password catch22
bridge(config-ssid)# authentication open eap adam
```

次の例では、SSID bridget の認証タイプを、静的 WEP キーを使用する Network-EAP に設定します。bridget SSID を使用する EAP 対応のブリッジは、*eve* というサーバを使用して EAP 認証を試行します。静的 WEP を使用するブリッジは、静的 WEP キーを使用します。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption key 2 size 128 12345678901234567890123456
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication network-eap eve
bridge(config-ssid)# end
```

このブリッジにアソシエートされる非ルート ブリッジの設定には、次のコマンドも含まれます。

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication client username bridge11 password 99bottles
```

WDS デバイスと対話するようルート ブリッジを設定する

CCKM を使用する非ルート ブリッジをサポートするには、ルート ブリッジがネットワーク上の WDS デバイスと対話することが必要であり、認証サーバにルート ブリッジのユーザ名とパスワードを設定する必要があります。無線 LAN 上での WDS と CCKM の設定方法の詳細は、『Cisco IOS Software Configuration Guide for Cisco Aironet Access Points』の第 11 章を参照してください。

ルート ブリッジで、次のコマンドをグローバル設定モードで入力します。

```
bridge(config)# wlccp ap username username password password
```

認証サーバ上でクライアントとしてルート ブリッジを設定する場合は、同じユーザ名とパスワードの組み合わせで設定する必要があります。

追加の WPA の設定

2 つのオプションの設定を使ってブリッジに事前共有キーを設定し、グループ キーの更新頻度を調整します。

事前共有キーの設定

802.1x ベースの認証が使用できない無線 LAN で WPA をサポートするには、ブリッジに事前共有キーを設定する必要があります。事前共有キーを ASCII 文字または 16 進文字として入力できます。キーを ASCII 文字として入力する場合は、8 ～ 63 文字を入力します。ブリッジはこのキーを、*Password-based Cryptography Standard*（RFC2898）に記載されているプロセスを使用して展開します。キーを 16 進文字として入力する場合は、64 桁 の 16 進文字を入力する必要があります。

グループ キー更新の設定

WPA プロセスの最後の段階で、ルート ブリッジは、認証された非ルート ブリッジにグループ キーを配布します。次のオプションの設定を使って、非ルート ブリッジのアソシエーションとアソシエーション解除をベースにして、グループ キーを変更、配布するようにルート ブリッジを設定できます。

- Membership termination : ルート ブリッジは、任意の認証済み非ルート ブリッジがルート ブリッジからアソシエーションを解除するときに、新しいグループ キーを生成、配布します。この機能は、アソシエートされているブリッジに対してグループ キーを秘匿します。
- Capability change : ルート ブリッジは、最後の非キー管理（静的 WEP）非ルート ブリッジがアソシエーションを解除するときに、動的グループ キーを生成、配布します。また、最初の非キー管理（静的 WEP）非ルート ブリッジが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、ルート ブリッジにアソシエートしている静的 WEP ブリッジが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。

イネーブル EXEC モードから、次の手順に従って、WPA 事前共有キーとグループ キー更新オプションを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 3	**ssid** *ssid-string*	SSID の SSID 設定モードを開始します。
ステップ 4	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	ブリッジ用の事前共有キーを、静的 WEP キーも利用する WPA を使って入力します。 16 進数または ASCII 文字を使用して、キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合は、8 桁以上の文字、数字、記号を入力する必要があります。入力したキーをブリッジが展開します。ASCII 文字は 63 文字まで入力できます。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
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。

次の例は、WPA および静的 WEP を使用する非ルート ブリッジ用の事前共有キーを、グループ キー更新オプションと共に設定する方法を示しています。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(config-ssid)# end
```

認証のホールドオフ、タイムアウト、間隔の設定

イネーブル EXEC モードから、次の手順に従って、ルート ブリッジを介して認証を行う非ルート ブリッジにホールドオフ時間、再認証間隔、認証タイムアウトを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**dot11 holdoff-time** *seconds*	クライアントがルート ブリッジからアソシエーションを解除されアイドル状態になるまで、ルート ブリッジが待機する時間を秒数で入力します。値を 1 ～ 65555 秒の範囲で入力します。
ステップ 3	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 4	**dot1x client-timeout** *seconds*	認証を試みる非ルート ブリッジが認証に失敗するまでに、ブリッジがその非ルート ブリッジからの返答を待つ時間を秒数で入力します。値を 1 ～ 65555 秒の範囲で入力します。
ステップ 5	**dot1x reauth-period** *seconds* [**server**]	認証された非ルート ブリッジに対して再認証するように強制する前に、ブリッジが待つ間隔を秒数で入力します。 • （オプション）認証サーバが指定した再認証間隔を使用するようにブリッジを設定する場合は、**server** キーワードを入力します。このオプションを使用する場合は、認証サーバを RADIUS 属性 27、Session-Timeout に設定します。この属性により、セッションまたはプロンプトが終了するまでに非ルート ブリッジに提供されるサービスの最大秒数が設定されます。サーバは、非ルート ブリッジが EAP 認証を実行するときにこの属性をルート ブリッジに送信します。
ステップ 6	**end**	イネーブル EXEC モードに戻ります。
ステップ 7	**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。

値をデフォルトに戻すには、各コマンドの no フォームを使用します。

LEAP クライアントとしての非ルート ブリッジの設定

非ルート ブリッジを、他の無線クライアント デバイスと同様に、ネットワークに対する認証を実行するよう設定できます。非ルート ブリッジのネットワーク ユーザ名とパスワードを入力すると、非ルート ブリッジはシスコの無線認証方式である LEAP を使用してネットワークに対する認証を実行し、動的な WEP キーを受け取って使用します。

非ルート ブリッジを LEAP クライアントとして設定する場合、次の 3 つの手順が必要です。

1. 認証サーバで非ルート ブリッジの認証ユーザ名とパスワードを作成します。
2. 非ルート ブリッジがアソシエートするルート ブリッジに、LEAP 認証を設定します。

3. LEAP クライアントとして機能するように非ルート ブリッジを設定します。

イネーブル EXEC モードから、次の手順に従って非ルート ブリッジを LEAP クライアントとして設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 3	**ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID 設定モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では大文字と小文字が区別されます。
ステップ 4	**authentication client username** *username* **password** *password*	非ルート ブリッジが LEAP 認証を実行するときに使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバで非ルート ブリッジに設定したユーザ名とパスワードに一致しなければなりません。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
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。

次の例では、SSID bridgeman の LEAP ユーザ名とパスワードを設定します。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bugsy password run4yerlife
bridge(config-ssid)# end
```

ルート ブリッジと非ルート ブリッジの認証タイプのマッチング

この項で説明する認証タイプを使用する場合は、ルート ブリッジの認証設定が、ルート ブリッジにアソシエートする非ルート ブリッジの設定に一致している必要があります。

表 10-2 は、ルート ブリッジと非ルート ブリッジの各認証タイプに必要な設定のリストです。

表 10-2　クライアントとブリッジのセキュリティ設定

セキュリティ機能	非ルート ブリッジ設定	ルート ブリッジ設定
静的 WEP キー（Open 認証）	WEP の設定および有効化	WEP の設定および有効化、Open 認証の有効化
静的 WEP キー（Shared Key 認証）	WEP の設定および有効化、Shared Key 認証の有効化	WEP の設定および有効化、Shared Key 認証の有効化
LEAP 認証	LEAP ユーザ名とパスワードの設定	WEP の設定および有効化、Network-EAP 認証の有効化
CCKM キー管理	WEP の設定および有効化、CCKM 認証の有効化	WEP の設定および有効化、CCKM 認証の有効化、ルート ブリッジの WDS デバイスとの対話の設定、クライアント デバイスとしてのルート ブリッジの認証サーバへの追加
WPA キー管理	WEP の設定および有効化、WPA 認証の有効化	WEP の設定および有効化、WPA 認証の有効化