CHAPTER 14

認証タイプ

このマニュアルでは、認証タイプの設定方法について説明します。説明する内容は、次のとおりです。

認証タイプの概要

ここでは、WMIC 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 WMIC に設定された Service Set Identifier（SSID; サービス セット ID）に関連付けられます。

ワイヤレス デバイスが相互に通信するには、オープン認証、802.1x/Extensible Authentication Protocol（EAP; 拡張認証プロトコル）に基づく認証、または共有鍵認証を使用して、相互に認証しておく必要があります。これらの認証タイプの他に、セキュリティを最大にするには、EAP 認証（ネットワークの認証サーバを利用）も使用する必要があります。サプリカントとバックエンド RADIUS は、同一の CA サーバから取得されたお互いの証明書を使用して、相互に認証します。

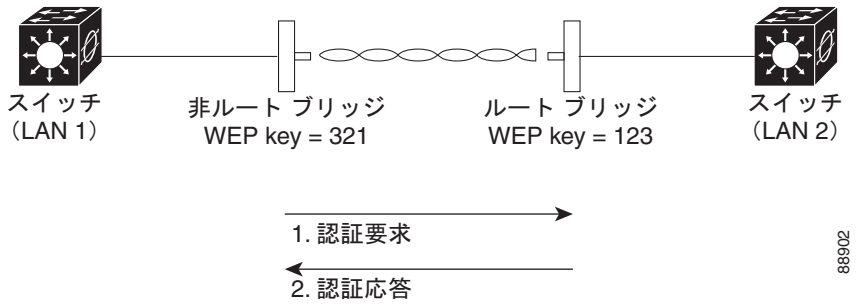
WMIC は 4 つの認証メカニズム（認証タイプ）を使用します。複数の認証タイプを同時に使用できます。

WMIC に対するオープン認証

オープン認証を使用すると、すべてのワイヤレス デバイスは認証を行い、それから別のワイヤレス デバイスと通信できます。オープン認証はネットワーク上の RADIUS サーバを利用しません。

図 14-1 に、非ルート ブリッジとオープン認証を使用するルート デバイス間の認証シーケンスを示します。この例では、非ルート ブリッジの WEP キーはブリッジの鍵と一致しません。したがって、デバイスは認証できますが、データを送信できません。

図 14-1　オープン認証のシーケンス



WMIC に対する共有鍵認証

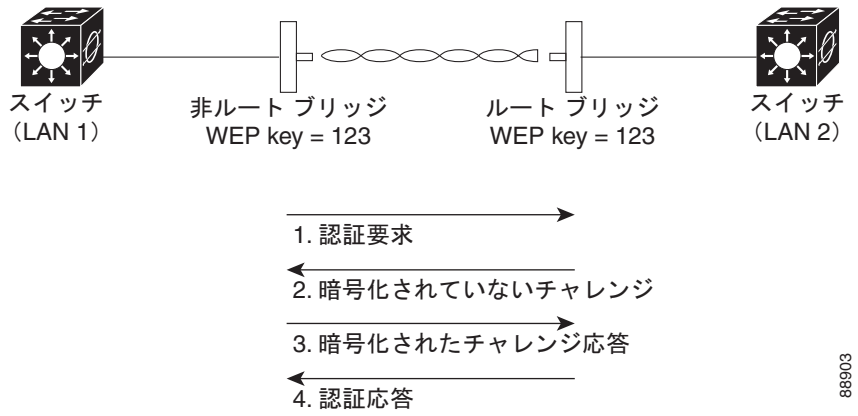
シスコは、IEEE 802.11b および IEEE 802.11g 標準に準拠する共有鍵認証を提供しています。ただし、共有鍵にはセキュリティ上の欠陥があるため、セキュリティが必要な環境では、EAP などの別の認証方式を使用することを推奨します。

共有鍵認証中に、ルート デバイスは暗号化されていないチャレンジ テキスト ストリングを、ルート デバイスとの通信を試行しているクライアント デバイスに送信します。認証の要求元クライアント デバイスはチャレンジ テキストを暗号化して、ルート デバイスに返信します。

暗号化されていないチャレンジと暗号化されたチャレンジを両方ともモニタできますが、ルート デバイスは無防備になり、侵入者は暗号化されていないテキスト ストリングと暗号化されたテキスト ストリングを比較して WEP キーを計算できます。

図 14-2 に、認証を試行するデバイスと、共有鍵認証を使用するブリッジ間の認証シーケンスを示します。この例では、デバイスの WEP キーはブリッジの鍵と一致します。したがって、デバイスは認証と通信の両方ができます。

図 14-2　共有鍵認証のシーケンス



ネットワークに対する EAP 認証

ネットワークに対する EAP 認証は、無線ネットワークに最高レベルのセキュリティをもたらします。ルート デバイスは EAP を使用して EAP 互換 RADIUS サーバと相互作用することにより、認証元デバイスおよび RADIUS サーバが相互認証し、ダイナミック セッション キーを取得できるように支援します。さらにルート デバイスおよび認証元デバイスはこのダイナミック セッション キーを使用して、ユニキャスト キーを取得します。ルートはブロードキャスト キーを生成し、ユニキャスト キーで暗号化したら、認証元デバイスに送信します。ユニキャスト キーは、ルート デバイスと認証されるデバイスとの間でユニキャスト データを交換するために使用されます。ブロードキャスト キーは、マルチキャスト データおよびブロードキャスト データを交換するために使用されます。

ブリッジ上で EAP をイネーブルにすると、ネットワーク認証が図 14-3 の順に発生します。

図 14-3　　EAP 認証のシーケンス

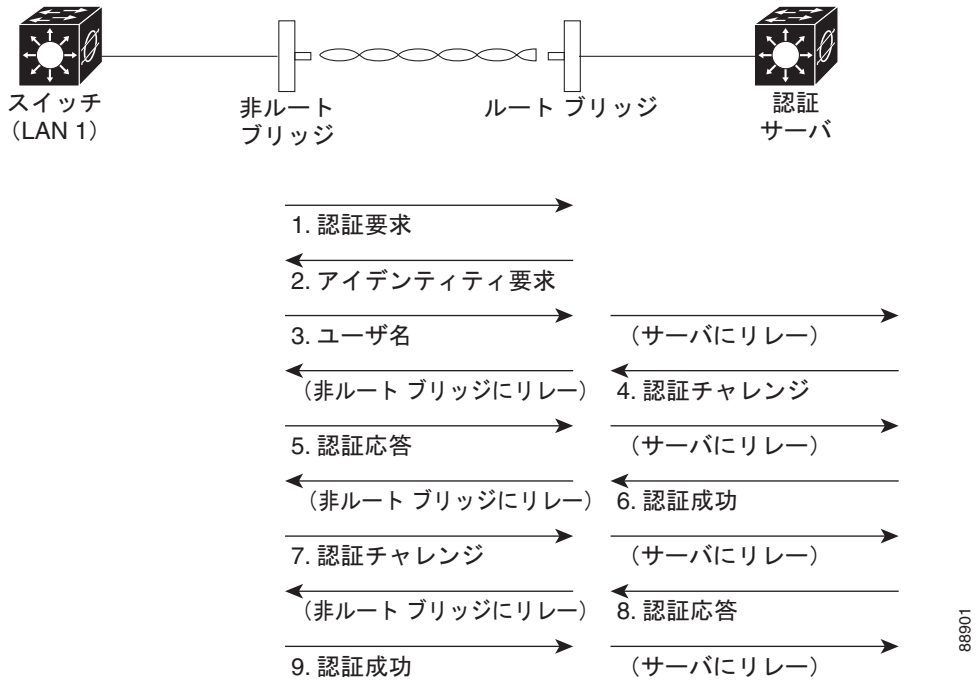


図 14-3 では、有線 LAN の非ルート ブリッジおよび RADIUS サーバは 802.1x および EAP を使用して、ルート デバイスによる相互認証を実行します。RADIUS サーバは非ルート ブリッジに認証チャレンジを送信します。非ルート ブリッジはユーザが指定したパスワードを一方向に暗号化して、チャレンジへの応答を生成し、RADIUS サーバに送信します。RADIUS サーバは、ユーザ データベースの情報を使用して独自の応答を作成し、非ルート ブリッジからの応答と比較します。RADIUS サーバが非ルート ブリッジを認証すると、プロセスが逆方向で繰り返され、非ルート ブリッジは RADIUS サーバを認証します。

相互認証が完了すると、RADIUS サーバおよび非ルート ブリッジは RADIUS サーバと非ルート ブリッジ間のこのセッションに対して一意のセッション キーを判別し、非ルート ブリッジに適切なネットワーク アクセス レベルを設定します。RADIUS サーバはセッション キーを暗号化し、有線 LAN を介してルート デバイスに送信します。ルート デバイスと非ルート ブリッジは、このセッション キーからユニキャスト キーを取得します。ルートはブロードキャスト キーを生成し、ユニキャスト キーで暗号化したら、非ルート ブリッジに送信します。非ルート ブリッジは、ユニキャスト キーを使用してブロードキャスト キーを復号化します。非ルート ブリッジおよびルート デバイスは WEP をアクティブにし、セッションの残りの期間中のすべての通信に対して、ユニキャストおよびブロードキャスト WEP キーを使用します。

複数の EAP 認証タイプがありますが、どのタイプでもブリッジは同じように動作します。ブリッジは無線クライアント デバイスから RADIUS サーバに、および RADIUS サーバから無線クライアント デバイスに認証メッセージをリレーします。WMIC での EAP の設定手順については、「SSID への認証タイプの割り当て」（P.14-15）を参照してください。

（注）　EAP 認証を使用する場合は、オープン認証または共有鍵認証を選択できますが、この選択は必須ではありません。EAP 認証はブリッジおよびネットワークに対する認証を制御します。

EAP-TLS

EAP-Transport Layer Security（TLS）では、デジタル証明書の取得と検証に Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）を使用します。デジタル証明書は、暗号化して署名された構造であり、1 つ以上の ID と公開鍵 1 つの間でアソシエーションを保証します。有効な期間と用途には制限があり、証明書のポリシー条件に従うものとします。Certificate Authority（CA; 認証局）は、クライアントとサーバに証明書を発行します。

サプリカントとバックエンド RADIUS サーバの双方で EAP-TLS 認証がサポートされている必要があります。ルート デバイスは、AAA クライアントとして動作し、Network Access Server（NAS; ネットワーク アクセス サーバ）とも呼ばれます。ルート デバイスでは 802.1x/EAP 認証プロセスをサポートする必要がありますが、EAP 認証プロトコルのタイプは留意されません。NAS は、ピア（認証を試行するユーザ マシン）と AAA サーバ（Cisco ACS など）の間の認証メッセージをトンネルします。NAS が EAP 認証プロセスを認識するのは、認証プロセスの開始時と終了時のみです。

EAP-TLS 認証には、次の注意事項が適用されます。

- 2.4 GHz WMIC（C3201-WMIC）では、VRAM メモリ内にデジタル証明書を 1 つ保存できます。
- EAP-TLS 認証メカニズムでは、PKI インフラストラクチャが Certificate Authority（CA; 認証局）サーバと同じ場所にある必要があります。トラストポイントの提供には、Microsoft と OpenSSL の両方の CA サーバを使用できます。
- EAP-TLS 認証は、クライアント デバイス（ワークグループ ブリッジまたは非ルート ブリッジ）と AAA サーバとの間で行われます。EAP に基づく認証をサポートしているのは、ルート デバイスのみです。
- Cisco C3201 WMIC と AAA サーバは、それぞれが独自のキー ペアに対して CA 証明書を取得します。CA 証明書の設定手順については、「crypto pki CLI による証明書の設定」（P.14-6）を参照してください。

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、TLS トンネル内の EAP トランザクションを暗号化します。TLS トンネルの暗号化によって、Light Extensible Authentication Protocol（LEAP）を使用して可能になる辞書攻撃から守ることができます。EAP-FAST トンネルは、ユーザに対して一意である共有秘密鍵を使用して確立されます。共有秘密鍵に基づくハンドシェイクは、PKI インフラストラクチャに基づくハンドシェイクよりも本質的に高速なため、EAP-FAST は Protected Extensible Authentication Protocol（PEAP）および EAP-TLS よりも非常に高速です。

EAP-FAST の動作は 3 つのフェーズにわかれています。

- キーをクライアントに配信する
- キーを使用して保護されたトンネルを確立する
- 保護されたトンネルでクライアントを認証する

EAP-FAST サーバに対するクライアント認証に成功すると、RADIUS アクセス許可メッセージが（マスター セッション キーとともに）ルート デバイスに渡され、EAP 成功メッセージがルート デバイスで生成されます（他の EAP 認証プロトコルの場合と同様）。クライアントは EAP 成功パケットを受信すると、セッション キーを取得します。そのアルゴリズムは、ルート デバイスに渡すセッション キーを生成するためにサーバで使用されるアルゴリズムを補完するものです。

EAP-TTLS

EAP-Tunneled TLS（TTLS）は、Funk Software でサポートされている 802.1X 認証タイプです。TLS（サーバ証明書）を使用し、レガシー メカニズムを含む各種のクライアント認証メカニズムをサポートしています。EAP-TTLS は、ユーザ名 / パスワード認証と相互認証の両方をサポートします。

ネットワークに対する MAC アドレス認証

アクセス ポイントは、無線クライアント デバイスの MAC アドレスをネットワーク上の RADIUS サーバにリレーし、RADIUS サーバは、許可される MAC アドレスのリストでアドレスを確認します。侵入者は偽造 MAC アドレスを作成できるため、MAC に基づく認証は、EAP 認証よりも安全性が低下します。ただし MAC に基づく認証では、EAP に対応していないクライアント デバイス用に代替の認証方式を提供します。

ヒント　ネットワークに RADIUS サーバがない場合は、許可される MAC アドレスのリストをアクセス ポイントの [Advanced Security: MAC Address Authentication] ページで作成できます。MAC アドレスがリストに載っていないデバイスは、認証できません。

ヒント　無線 LAN で MAC 認証されたクライアントが頻繁にローミングされる場合は、アクセス ポイントで MAC 認証キャッシュをイネーブルにできます。MAC 認証キャッシュを使用すると、アクセス ポイントでは認証サーバに要求を送信しなくても MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが削減されます。この機能をイネーブルにする方法については、11 ～ 15 ページの「Configuring MAC Authentication Caching」を参照してください。

CCKM 鍵管理の使用方法

Cisco Centralized Key Management（CCKM）を使用すると、EAP 認証されたクライアント デバイスは、再アソシエーション中に認識可能な遅延を発生させることなく、ルート デバイス間でローミングできます。ネットワーク上のルート デバイスまたはスイッチは Wireless Domain Services（WDS）を提供して、サブネットの CCKM 対応デバイスにセキュリティ クレデンシャルのキャッシュを作成します。WDS デバイスのクレデンシャルのキャッシュによって、CCKM 対応クライアント装置を新しいルート デバイスにローミングしたときに、再アソシエーションの所要時間が大幅に短縮されます。

クライアント デバイスがローミングするときに、前のルート デバイスを提供していたのと同じ WDS デバイスが提供するルート デバイスに対して再アソシエーションを試行する場合、WDS デバイスは RADIUS サーバにクライアントの認証を要求するのではなく、クライアントのクレデンシャルのキャッシュを使用してクライアントを認証します。再アソシエーション プロセスは、ローミングするクライアント デバイスと新しいルート デバイスとの間で 2 パケットを交換するだけに短縮されます。クライアントのローミングによる再アソシエーションは短時間で終了するため、音声または時間に依存するアプリケーションには、認識される遅延が発生しません。

ブリッジ上で CCKM をイネーブルにする手順については、「SSID への認証タイプの割り当て」（P.14-15）を参照してください。

WPA 鍵管理の使用方法

Wi-Fi Protected Access（WPA）は相互運用可能な標準ベースのセキュリティ強化機能です。これにより、既存の、および将来の無線 LAN システムのデータ保護レベルおよびアクセス制御レベルが大幅に向上します。WPA は IEEE 802.11i 標準をベースとしています。WPA はデータの保護に Temporal Key Integrity Protocol（TKIP）や Advanced Encryption Standard（AES; 高度暗号化規格）を利用します。

WPA 鍵管理は、WPA および WPA-Pre-Shared Key（WPA-PSK）の相互に排他的な 2 つの管理タイプをサポートしています。WPA 鍵管理を使用した場合、クライアント デバイスおよび認証サーバは EAP 認証方式を使用して相互に認証し、Pairwise Master Key（PMK）を生成します。また、認証サーバは WPA を使用して PMK を動的に生成し、ルート デバイスに送信します。WPA-PSK を使用する場合は、ユーザがクライアント デバイスおよびルート デバイスに事前共有鍵を設定し、この鍵を PMK として使用します。

（注）　WPA 情報要素内でアドバタイズされた（および 802.11 アソシエーション中にネゴシエートされた）ユニキャストおよびマルチキャスト暗号スイートは、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ことがあります。RADIUS サーバによって割り当てられた新しい VLAN ID が、以前にネゴシエートされた暗号スイートと異なる暗号スイートを使用している場合、ルート デバイスおよびクライアント デバイスが新しい暗号スイートに切り替わることはありません。現在、WPA および CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ後に暗号スイートを変更できません。この場合は、非ルート ブリッジと無線 LAN の対応付けが解除されます。

ブリッジに WPA 鍵管理を設定する手順については、「SSID への認証タイプの割り当て」（P.14-15）を参照してください。

crypto pki CLI による証明書の設定

ここでは、crypto PKI CLI を使用して CA およびルータの証明書をインポートする方法、およびトラストポイントを dot1x クレデンシャルに追加する方法について説明します。PKI 操作を開始する前に、CA は独自の公開鍵ペアを生成し、自己署名された CA 証明書を作成します。その後、CA は証明書要求に署名して PKI のピア登録を開始できるようになります。

（注）　証明書の登録に先立って、ドメイン名とクロックを設定する必要があります。

次のいずれかの方法で CA およびルータの証明書をインポートできます。

- カット アンド ペーストを使用した設定：ルータと CA の間に接続がない場合、またはスクリプトが必要な場合に便利です。この方法では、ルータで生成される証明書要求が CA サーバにコピーされ、ルータのキー ペアの証明書を受け取るようにします。CA およびルータの両方の証明書が CLI を使用してインポートされます。
- TFTP を使用した設定：この方法では、ルータで生成される証明書要求が TFTP サーバに自動でコピーされます。CA およびルータの証明書は、CA サーバから TFTP サーバにコピーされた後、TFTP サーバから自動でインポートされます。
- SCEP を使用した設定：この方法では、CA およびルータの証明書が CA サーバから自動でインポートされます。

カット アンド ペースト方法を使用した設定

トラストポイントの設定と CA およびルータの証明書のインポートを手動で行うには、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	**crypto pki trustpoint** *name*	トラストポイントの名前を指定します。
ステップ 3	**enrollment terminal**	端末が証明書の登録に使用されるように指定します。
ステップ 4	**rsakeypair** *name* **1024**	指定された名前の手動鍵が長さ 1024 で生成されるように指定します。
ステップ 5	**subject-name CN=***name*	証明書に件名を追加します。**dot1x credentials** *name* コマンドで定義したユーザ名と同じ名前にする必要があります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto pki authenticate** *name*	証明書のインポート プロセスを開始します。CA 証明書を入力（コピー アンド ペースト）するプロンプトが表示されます。
ステップ 8	**quit**	CA 証明書のインポート プロセスを終了します。
ステップ 9	**crypto pki enroll** ***name***	CA にルータ証明書を要求します。ルータ証明書を受け取れるように CA サーバにコピーされる証明書要求が生成されます。
ステップ 10	**crypto pki import** *name* **certificate**	ルータ証明書をインポートします。
ステップ 11	**quit**	ルータ証明書のインポート プロセスを完了します。
ステップ 12	**end**	EXEC モードを終了します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、手動で設定する方法の例を示します。

```
maldives-ap#
maldives-ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
maldives-ap(config)#crypto pki trustpoint TFTP-CUT-PASTE
maldives-ap(ca-trustpoint)#enrollment terminal
maldives-ap(ca-trustpoint)#rsakeypair manual-keys 1024
maldives-ap(ca-trustpoint)#exit

!
maldives-ap#show run
...
crypto pki trustpoint TEST-TFTP
 enrollment terminal
 rsakeypair manual-keys 1024
!

After the trustpoint was defined for enrollment via the terminal, the CA certificate must
be imported:

maldives-ap(config)#crypto pki authenticate TFTP-CUT-PASTE

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIC5zCCApGgAwIBAgIQdngf6fp6ZqdEX1QPnzgqiDANBgkqhkiG9w0BAQUFADB9
MQswCQYDVQQGEwJBVTEMMAoGA1UECBMDTlNXMQ8wDQYDVQQHEwZTeWRuZXkxFjAU
BgNVBAoTDUNpc2NvIFN5c3RlbXMxFDASBgNVBAsTC1dOQlUgU3lkbmV5MSEwHwYD
VQQDExh3bmJ1LXN5ZC1hY3MtYS5jaXNjby5jb20wHhcNMDUwNjE1MDQ1MzQ5WhcN
MDgwNjE1MDUwMzM0WjB9MQswCQYDVQQGEwJBVTEMMAoGA1UECBMDTlNXMQ8wDQYD
VQQHEwZTeWRuZXkxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxFDASBgNVBAsTC1dO
QlUgU3lkbmV5MSEwHwYDVQQDExh3bmJ1LXN5ZC1hY3MtYS5jaXNjby5jb20wXDAN
BgkqhkiG9w0BAQEFAANLADBIAkEAnDZq1u+RhYyC8uNdsuXDwOve1yEZvKJerrb6
XFVyJZV4jfSKSnZ2ZRNf3VX3NcRyQxKSszgCHMGcUyBnH350ZwIDAQABo4HsMIHp
MAsGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSB9hMkazhs
ebKHX3b9qw8VPilQRzCBlwYDVR0fBIGPMIGMMEOgQaA/hj1odHRwOi8vd25idS1z
eWQtYWNzLWEvQ2VydEVucm9sbC93bmJ1LXN5ZC1hY3MtYS5jaXNjby5jb20uY3Js
MEWgQ6BBhj9maWxlOi8vXFx3bmJ1LXN5ZC1hY3MtYVxDZXJ0RW5yb2xsXHduYnUt
c3lkLWFjcy1hLmNpc2NvLmNvbS5jcmwwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZI
hvcNAQEFBQADQQA7G8rL3ZHFfc3EdeklxMz72qdSnXg05uZZ51USuAMJKc1rGJUT
C0Bkre8+ov2xmZGVHC8xOpDk7bZzs/iinLnq
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint: 45EC6866 A66B4D8F 2E05960F BC5C1B76
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

The next step is to generate the keys and an enrollment request (see below). Note that
although it is possible to explicitly generate the keys, it is not necessary as the
enrollment process will automatically generate (or re-generate if previously configured)
the required keys. This request must then be submitted to the Certificate Authority to
have it signed and a certificate issued.

maldives-ap(config)#crypto pki enroll TEST-CUT-PASTE
% Start certificate enrollment..

% The fully-qualified domain name in the certificate will be: maldives-ap.cisco.com
% The subject name in the certificate will be: maldives-ap.cisco.com
% Include the router serial number in the subject name? [yes/no]:yes
Jun 29 12:17:08.232: %CRYPTO-6-AUTOGEN: Generated new 1024 bit key pair
% The serial number in the certificate will be: 80AD5AD4
% Include an IP address in the subject name? [no]:
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIBmDCCAQECAQAwNzE1MA8GA1UEBRMIODBBRDVBRDQwIgYJKoZIhvcNAQkCFhVt
YWxkaXZlcy1hcC5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AOexwH9eW7n+3MEivmSHpBO3kqSdvZnf5dvOKyVoy8ZJpM2O6j0jfzOTD3IxHeQE
MUiEzWKybt2k/HQTuND+zVhbgWQd9J3JnCrvUMij48fV7MydyZYQ2eHDgQEN64d4
RBPFi51C+2xX1SzELJfGU2oxeQ6AsW/A/2S7GCycFW7rAgMBAAGgITAfBgkqhkiG
9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDANBgkqhkiG9w0BAQQFAAOBgQBoph/j
DHMh7U4yN0lYUS3OfpCtDl8e5QBp1MFYqMDP4aWeL/AdKVTNWBBElQh+M96uMyY2
/AEwFfsJsU1q6u3Kg4kJWht8F7a60OhQRfQ1CSiy18Z9vqA4KY15hbWhwj3JtuTA
kpqCzR30u+auN7WuS/PnVr+vnSCMt69P6wLHHw==

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
maldives-ap(config)#

After the certificate (or multiple certificates if separate signature and encryption certs
are required) is issued by the CA, it must be imported into the device via:

maldives-ap(config)#crypto pki import ?
  WORD  Trustpoint label to associate certificate or pkcs-12 file with
```

```
maldives-ap(config)#crypto pki import TEST-CUT-PASTE ?
  certificate  Import a certificate from a TFTP server or the terminal
  pem          Import from PEM files
  pkcs12       Import from PKCS12 file

maldives-ap(config)#crypto pki import TEST-CUT-PASTE certificate
% The fully-qualified domain name in the certificate will be: maldives-ap.cisco.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIERjCCA/CgAwIBAgIKHVHsoQAAAAAAJzANBgkqhkiG9w0BAQUFADB9MQswCQYD
VQQGEwJBVTEMMAoGA1UECBMDTlNXMQ8wDQYDVQQHEwZTeWRuZXkxFjAUBgNVBAoT
DUNpc2NvIFN5c3RlbXMxFDASBgNVBAsTC1dOQlUgU3lkbmV5MSEwHwYDVQQDExh3
bmJ1LXN5ZC1hY3MtYS5jaXNjby5jb20wHhcNMDUwNjI5MDExMzQyWhcNMDYwNjI5
MDEyMzQyWjA5MREwDwYDVQQFEwg4MEFENUFENDEkMCIGCSqGSIb3DQEJAhMVbWFs
ZGl2ZXMtYXAuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDn
scB/Xlu5/tzBIr5kh6QTt5Knb2Z3+XbzislaMvGSaTNjuo9I38zkw9yMR3kBDFI
hM1ism7dpPx0E7jQ/s1YW4FkHfSdyZwq71DIo+PH1ezMncmWENnhw4EBDeuHeEQT
xYudQvtsV9UsxCyXxlNqMXkOgLFvwP9kuxgsnBVu6wIDAQABo4ICUDCCAkwwDgYD
VR0PAQH/BAQDAgWgMB0GA1UdDgQWBBRdEW6dE+j3/3/CCJrjDCzA9r47oDCBtwYD
VR0jBIGvMIGsgBSB9hMkazhsebKHX3b9qw8VPilQR6GBgaR/MH0xCzAJBgNVBAYT
AkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEWMBQGA1UEChMNQ2lz
Y28gU3lzdGVtczEUMBIGA1UECxMLV05CVSBTeWRuZXkxITAfBgNVBAMTGHduYnUt
c3lkLWFjcy1hLmNpc2NvLmNvbYIQdngf6fp6ZqdEX1QPnzgqiDCBlwYDVR0fBIGP
MIGMMEOgQaA/hjlodHRwOi8vd25idS1zeWQtYWNzLWEvQ2VydEVucm9sbC93bmJ1
LXN5ZC1hY3MtYS5jaXNjby5jb20uY3JsMEWgQ6BBhj9maWxlOi8vXFx3bmJ1LXN5
ZC1hY3MtYVxDZXJ0RW5yb2xsXHduYnUtc3lkLWFjcy1hLmNpc2NvLmNvbS5jcmww
gcYGCCsGAQUFBwEBBIG5MIG2MFgGCCsGAQUFBzAChkxodHRwOi8vd25idS1zeWQt
YWNzLWEvQ2VydEVucm9sbC93bmJ1LXN5ZC1hY3MtYV93bmJ1LXN5ZC1hY3MtYS5j
aXNjby5jb20uY3J0MFoGCCsGAQUFBzAChk5maWxlOi8vXFx3bmJ1LXN5ZC1hY3Mt
YVxDZXJ0RW5yb2xsXHduYnUtc3lkLWFjcy1hX3duYnUtc3lkLWFjcy1hLmNpc2Nv
LmNvbS5jcnQwDQYJKoZIhvcNAQEFBQADQQCEqZgEAMExlMAiQ3aOiajY/NjuKeXX
A5yMsTxQIWxVmj+o1U4T2dvYk60/ab/9hV1n6h3msKVcoYUFj8otLtAs
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported

The following show commands can be used to view the trustpoint and certificates status:
maldives-ap#sh crypto pki trust TEST-CUT-PASTE
Trustpoint TEST-CUT-PASTE:
    Subject Name:
    cn=wnbu-syd-acs-a.cisco.com
    ou=WNBU Sydney
    o=Cisco Systems
    l=Sydney
    st=NSW
    c=AU
          Serial Number: 76781FE9FA7A66A7445F540F9F382A88
    Certificate configured.



maldives-ap#show crypto pki cert TEST-CUT-PASTE
Certificate
  Status: Available
  Certificate Serial Number: 1D51ECA1000000000027
  Certificate Usage: General Purpose
  Issuer:
    cn=wnbu-syd-acs-a.cisco.com
    ou=WNBU Sydney
    o=Cisco Systems
    l=Sydney
```

```
    st=NSW
    c=AU
  Subject:
    Name: maldives-ap.cisco.com
    Serial Number: 80AD5AD4
    hostname=maldives-ap.cisco.com
    serialNumber=80AD5AD4
  CRL Distribution Point:
    http://wnbu-syd-acs-a/CertEnroll/wnbu-syd-acs-a.cisco.com.crl
  Validity Date:
    start date: 12:13:42 AEST Jun 29 2005
    end   date: 12:23:42 AEST Jun 29 2006
    renew date: 11:00:00 AEST Jan 1 1970
  Associated Trustpoints: TEST-CUT-PASTE
```

TFTP の方法を使用した設定

TFTP 証明書での登録は、手動で登録する場合と似ていますが、TFTP サーバが CA およびルータの証明書を提供する点が異なります。TFTP を使用するには、イネーブル 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	**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	**crypto pki trustpoint** *name*	トラストポイントの名前を指定します。
ステップ 3	**enrollment url** *tftp://address*	証明書の登録に使用される URL を指定します。
ステップ 4	**rsakeypair** *name* **1024**	指定された名前の手動鍵が長さ 1024 で生成されるように指定します。
ステップ 5	**subject-name CN=***name*	証明書に件名を追加します。**dot1x credentials** *name* コマンドで定義したユーザ名と同じ名前にする必要があります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto pki authenticate** *name*	証明書のインポート プロセスを開始します。
ステップ 8	**quit**	CA 証明書のインポート プロセスを終了します。
ステップ 9	**crypto pki enroll *name***	CA にルータ証明書を要求します。証明書要求が生成されて TFTP サーバに保存されます。この要求は、ルータ証明書を受け取れるように CA サーバにコピーされなければなりません。
ステップ 10	**crypto pki import** *name* **certificate**	ルータ証明書をインポートします。
ステップ 11	**end**	EXEC モードを終了します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

TFTP の方法では、次の点に注意してください。

- URL にファイル名が含まれる場合、ルータがファイルに拡張子を付加します。**crypto pki authenticate** を入力すると、ルータは CA の証明書を指定された TFTP サーバから取得します。
- TFTP サーバで CA 証明書を探すため、ルータはファイル名（ファイル名が URL で指定されている場合）または Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）に拡張子 .ca を付加します。たとえば URL オプションが tftp://TFTP-server/TFTPfiles/router1 である場合、TFTP サーバ TFTP-server からファイル TFTPfiles/router1.ca が読み込まれます。ルータの FQDN が router1.cisco.com で URL オプションが tftp://tftp.cisco.com である場合、TFTP サーバ tftp.cisco.com からファイル router1.cisco.com.ca が読み込まれます。このファイルには、CA の証明書がバイナリ フォーマット（Distinguished Encoding Rules [DER]）であるか、または base 64 エンコード（Privacy Enhanced Mail（PEM））である必要があります。
- ユーザが **crypto pki enroll** コマンドを使用してルータを登録すると、登録に関する情報のプロンプトが表示されます。この時点でファイル名は判断済みであり、証明書要求であることを表す拡張子 .req が付加されます。用途の異なる鍵ごとに 2 つの要求が生成され、2 つの証明書が認可されることが想定されます。したがって、証明書要求の拡張子は -sign.req および -encr.req となります。
- ユーザが **crypto pki import** コマンドを入力すると、ルータは認可された証明書を取得しようとします。使用されるファイル名は、要求の送信に使用されたファイル名と同じですが、拡張子 .req が拡張子 .crt で置き換えられます。証明書は base 64 でエンコードされた Personal Information Exchange Syntax Standard（PCKS）#10 フォーマットにする必要があります。

次に、TFTP で設定する方法の例を示します。

```
maldives-ap#show run
...
crypto pki trustpoint TEST-TFTP
 enrollment url tftp://10.67.64.21/ndupreez/my-acs
 revocation-check crl
 rsakeypair 1024
```

SCEP を使用した設定

Certificate Enrollment Protocol（SCEP）を使用した設定は、CA サーバとして Windows 2003 サーバを使用している場合に利用でき、CA およびルータの証明書を簡単にインポートできます。SCEP を使用する手順は、次のとおりです。

	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	**crypto pki trustpoint** *name*	トラストポイントの名前を指定します。
ステップ 3	**enrollment url** *http://address*	証明書の登録に使用される URL を指定します。
ステップ 4	**rsakeypair** *name* **1024**	SCEP 鍵が長さ 1024 で生成されるように指定します。
ステップ 5	**subject-name CN=***name*	証明書に件名を追加します。**dot1x credentials** *name* コマンドで定義したユーザ名と同じ名前にする必要があります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto pki authenticate** *name*	CA 証明書のインポート プロセスを開始します。
ステップ 8	**crypto pki enroll** ***name***	CA にルータ証明書を要求します。証明書要求が生成されて TFTP サーバに保存されます。この要求は、ルータ証明書を受け取れるように CA サーバにコピーされなければなりません。
ステップ 9	**end**	EXEC モードを終了します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ヒント　Windows 2003 サーバ用の SCEP アドオンは、次のリンクからインストールできます。
http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=9f306763-d036-41d8-8860-1636411b2d01

Cisco ACS サーバと連携する Windows CA サーバが Enterprise Certificate Server（CA）モードにあるときに証明書を取得するために SCEP を選択する場合は、Windows Server 2003 Enterprise Edition を Windows オペレーティング システムとして使用することをお勧めします。Windows Server 2003 Enterprise Edition では、CA サーバ テンプレートを変更できます。Enterprise CA サーバで SCEP を使用するには、拡張鍵用途拡張がユーザ テンプレートのものと同じになるように IPSec テンプレート（オフライン要求）を変更する必要があります。テンプレートの変更には certtmpl.msc、変更されたテンプレートをインストールするには ertsrv.msc を使用してください。

次に、SCEP 証明書を登録する例を示します。

```
maldives-ap#
maldives-ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
maldives-ap(config)#crypto pki trustpoint TEST-SCEP
maldives-ap(ca-trustpoint)#enrollment url http://10.67.73.11/certsrv/mscep/mscep.dll
maldives-ap(ca-trustpoint)#rsakeypair scep-keys 1024
maldives-ap(ca-trustpoint)#exit
maldives-ap(config)#

!
maldives-ap#show run
...
crypto pki trustpoint TEST-SCEP
 enrollment mode ra
 enrollment url http://10.67.73.11:80/certsrv/mscep/mscep.dll
 serial-number
 ip-address BVI1
 revocation-check crl
 rsakeypair scep-keys 1024
!

And to retrieve the CA certificate:

maldives-ap(config)#crypto pki authenticate TEST-SCEP
Certificate has the following attributes:
Fingerprint: 45EC6866 A66B4D8F 2E05960F BC5C1B76
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
maldives-ap(config)#

Finally to enroll the router certificate(s):

maldives-ap(config)#
maldives-ap(config)#crypto pki enroll TEST-SCEP
%
% Start certificate enrollment..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
```

```
Password:
Jun 29 13:18:46.606: %CRYPTO-6-AUTOGEN: Generated new 1024 bit key pair
Re-enter password:

% The fully-qualified domain name in the certificate will be: maldives-ap.cisco.com
% The subject name in the certificate will be: maldives-ap.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 80AD5AD4
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: BVI1
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.


maldives-ap(config)#
Jun 29 13:19:12.776: CRYPTO_PKI:    Fingerprint:  6BF9EAC9 BE515B76 E7767395 8FA00FCC
Jun 29 13:19:12.776:
Jun 29 13:19:15.161: %PKI-6-CERTRET: Certificate received from Certificate Authority
maldives-ap(config)# end
```

The crypto show commands are used to view the certificates associated with the trustpoint, in this case both the CA and single router certificate:

```
maldives-ap#show crypto pki cert TEST-SCEP
Certificate
  Status: Available
  Certificate Serial Number: 1D89524F000000000028
  Certificate Usage: General Purpose
  Issuer:
    cn=wnbu-syd-acs-a.cisco.com
    ou=WNBU Sydney
    o=Cisco Systems
    l=Sydney
    st=NSW
    c=AU
  Subject:
    Name: maldives-ap.cisco.com
    IP Address: 10.67.73.49
    Serial Number: 80AD5AD4
    hostname=maldives-ap.cisco.com
    ipaddress=10.67.73.49
    serialNumber=80AD5AD4
  CRL Distribution Point:
    http://wnbu-syd-acs-a/CertEnroll/wnbu-syd-acs-a.cisco.com.crl
  Validity Date:
    start date: 13:14:13 AEST Jun 29 2005
    end   date: 13:24:13 AEST Jun 29 2006
  Associated Trustpoints: TEST-SCEP

CA Certificate
  Status: Available
  Certificate Serial Number: 76781FE9FA7A66A7445F540F9F382A88
  Certificate Usage: Signature
  Issuer:
    cn=wnbu-syd-acs-a.cisco.com
    ou=WNBU Sydney
    o=Cisco Systems
    l=Sydney
    st=NSW
    c=AU
  Subject:
    cn=wnbu-syd-acs-a.cisco.com
    ou=WNBU Sydney
```

```
    o=Cisco Systems
    l=Sydney
    st=NSW
    c=AU
  CRL Distribution Point:
    http://wnbu-syd-acs-a/CertEnroll/wnbu-syd-acs-a.cisco.com.crl
  Validity Date:
    start date: 15:53:49 AEST Jun 15 2005
    end   date: 16:03:34 AEST Jun 15 2008
  Associated Trustpoints: TEST-SCEP WEBCERT-01
```

dot1x クレデンシャルへのトラストポイントの追加

認証に使用されるトラストポイントを指定するには、次の手順を実行します。

（注）　トラストポイントを指定しない場合は、デフォルトのトラストポイントが EAP-TLS で使用されます。

	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	**dot1x credentials** *name*	トラストポイントの名前を指定します。
ステップ 3	**username** *name*	トラストポイントを設定するユーザ名を指定します。
ステップ 4	**password** *password*	トラストポイントを設定するユーザ パスワードを指定します。
ステップ 5	**pki-trustpoint** *name*	PKI トラストポイント名を指定します。
ステップ 6	**end**	イネーブル EXEC モードに戻ります。

次に、トラストポイントを指定する例を示します。

```
keeling-ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
keeling-ap(config)#dot1x credentials test
keeling-ap(config-dot1x-creden)#username myname
keeling-ap(config-dot1x-creden)#password mypass
keeling-ap(config-dot1x-creden)#pki-trustpoint TP_001
keeling-ap(config-dot1x-creden)#end


keeling-ap#sh run | beg test
dot1x credentials test
 username myname
 password 7 060B16314D5D1A
 pki-trustpoint TP_001
```

認証タイプの設定

ここでは、認証タイプの設定方法について説明します。WMIC の SSID に認証タイプを付加します。WMIC SSID の設定の詳細については、「Service Set Identifier」を参照してください。ここでは、次の内容について説明します。

認証のデフォルト設定

WMIC のデフォルト SSID は *autoinstall* です。表 14-1 に、デフォルト SSID の認証のデフォルト設定を示します。

表 14-1　認証のデフォルト設定

機能	デフォルトの設定
SSID	autoinstall
ゲスト モード SSID	autoinstall（WMIC はビーコン内でこの SSID をブロードキャストし、SSID が設定されていないクライアント デバイスの対応付けを可能にします）
autoinstall に割り当てられた認証タイプ	open

SSID への認証タイプの割り当て

ルート デバイスで SSID の認証タイプを設定するには、イネーブル 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	**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 ssid** *ssid-string*	SSID を作成します。SSID には最大 32 文字の英数字を指定できます。SSID では大文字と小文字が区別されます。 **（注）**　SSID にはスペースを含めないでください。

	コマンド	目的
ステップ 3	**authentication open [mac-address** *list-name* **[alternate]] [[optional] eap** *list-name*]	現在の SSID の認証タイプをオープンに設定します。オープン認証を使用すると、すべてのクライアント デバイスは認証を行い、それから WMIC と通信できます。 **（注）** ステップ 3、ステップ 4、またはステップ 5 に示したいずれかのコマンド リストを使用する必要があります。 • （任意）SSID の認証タイプをオープン（MAC アドレス認証を使用）に設定します。アクセス ポイントは、MAC アドレス認証の実行後にネットワークへの参加が許可されるように、すべてのクライアント デバイスを設定します。list-name には、認証方式リストを指定します。方式リストの詳細については、次のリンクを参照してください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 alternate キーワードを使用すると、クライアント デバイスは MAC 認証または EAP 認証を使用してネットワークに参加できます。どちらかの認証が完了したクライアントは、ネットワークへの参加が許可されます。 • （任意）SSID の認証タイプをオープン（EAP 認証を使用）に設定します。WMIC は、EAP 認証の実行後にネットワークへの参加が許可されるように、その他のすべてのクライアント デバイスを設定します。*list-name* には、認証方式リストを指定します。 optional キーワードを使用すると、オープン認証または EAP 認証を使用するクライアント デバイスは、対応付けが可能になり、認証を受けられるようになります。この設定は、主に特別なクライアント アクセシビリティを要求するサービス プロバイダーによって使用されます。 **（注）** EAP 認証が設定されたルート デバイスは、対応するすべてのクライアント デバイスに強制的に EAP 認証を実行させます。EAP を使用しないクライアント デバイスは、EAP 認証が設定されたルート デバイスと通信できません。

	コマンド	目的
ステップ 4	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	SSID の認証タイプを共有鍵に設定します。 **（注）** ステップ 3、ステップ 4、またはステップ 5 に示したいずれかのコマンド リストを使用する必要があります。 **（注）** 共有鍵のセキュリティには欠陥があるため、使用しないことを推奨します。 **（注）** 共有鍵認証を割り当てられる SSID は 1 つだけです。 • （任意）SSID の認証タイプを共有鍵（MAC アドレス認証を使用）に設定します。*list-name* には、認証方式リストを指定します。 • （任意）SSID の認証タイプを共有鍵（EAP 認証を使用）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 5	**authentication network-eap** ***list-name*** [**mac-address** *list-name*]	認証および鍵配布に EAP を使用するように、SSID の認証タイプを設定します。 **（注）** ステップ 3、ステップ 4、またはステップ 5 に示したいずれかのコマンド リストを使用する必要があります。 • （任意）SSID の認証タイプを Network-EAP （MAC アドレス認証を使用）に設定します。MAC アドレス認証を実行するには、アクセス ポイントに対応付けられたすべてのクライアント デバイスが必要です。list-name には、認証方式リストを指定します。

	コマンド	目的
ステップ 6	**authentication key-management** {[**wpa**] [**cckm**]} [**optional**]	（任意）SSID のキー管理タイプを WPA、CCKM、または両方に設定します。**optional** キーワードを使用した場合、WPA または CCKM が設定されていないクライアント デバイスは、現在の SSID を使用できます。**optional** キーワードを使用しない場合は、WPA または CCKM クライアント デバイスのみが現在の SSID を使用できます。 SSID に対して CCKM をイネーブルにするには、Network-EAP 認証もイネーブルにする必要があります。SSID に対して WPA をイネーブルにするには、オープン認証、Network-EAP 認証、または両方もイネーブルにする必要があります。 **（注）** WPA および CCKM を両方ともサポートするのは、802.11b および 802.11g 無線のみです。 **（注）** CCKM または WPA をイネーブルにする前に、暗号化モードを、TKIP/AES-CCMP を含む暗号スイートに設定する必要があります。CCKM と WPA を両方ともイネーブルにするには、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 暗号化モードを設定する手順については、「暗号スイートおよび WEP」を参照してください。 **（注）** SSID に対して WPA をイネーブルにし、事前共有鍵をイネーブルにしない場合、鍵管理タイプは WPA になります。WPA および事前共有鍵をともにイネーブルにした場合、鍵管理タイプは WPA-PSK になります。事前共有鍵を設定する手順については、「追加 WPA の設定」（P.14-24）を参照してください。 **（注）** CCKM をサポートするには、ルート デバイスをネットワークの WDS デバイスと相互作用させる必要があります。ルート デバイスと WDS デバイスとの相互作用を設定する手順については、「ルート デバイスと WDS デバイスとの相互作用の設定」（P.14-24）を参照してください。
ステップ 7	**end**	イネーブル EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EAP クライアントとしての 2.4 GHz WMIC 無線の設定

非ルート側で SSID の認証タイプを設定するには、イネーブル EXEC モードで次の手順を実行します。

2.4 GHz WMIC を EAP クライアントして設定するには、主に 3 つのステップを実行する必要があります。

- 認証サーバ上に、WMIC の認証用ユーザ名およびパスワードを作成します。
- WMIC を対応付けるルート デバイスに EAP 認証を設定します。
- EAP クライアントとして機能するように WMIC を設定します。

クライアント側で SSID に EAP 認証タイプを設定するには、イネーブル 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	**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	**dot1x credentials** *profile*	dot1x クレデンシャル プロファイルを作成し、dot1x クレデンシャル設定サブモードを開始します。
ステップ 3	**username** *name*	WMIC の認証ユーザ名を指定します。
ステップ 4	**password** *password*	WMIC の認証パスワードを指定します。
ステップ 5	**crypto pki trustpoint** *name*	トラストポイントの名前を指定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**eap profile** *profile-name-string*	EAP プロファイルを作成します。
ステップ 8	**method [fast | gtc | leap | md5 | mschapv2 | tls]**	認証に使用する EAP 認証方式を選択します。 **（注）** クライアント モードの WMIC では、FAST、LEAP、TLS の各方式のみをサポートします。 **（注）** EAP 認証が設定されたルート デバイスは、対応するすべてのクライアント デバイスに強制的に EAP 認証を実行させます。EAP を使用しないクライアント デバイスは、EAP 認証が設定されたルート デバイスと通信できません。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**dot11 ssid** *ssid-string*	グローバル SSID モードを開始します。
ステップ 11	**authentication network-eap** ***list-name***	（任意）認証および鍵配布に EAP を使用するように、SSID の認証タイプを設定します。
ステップ 12	**dot1x credentials** *profile*	ステップ 2 で作成した dot1x クレデンシャル プロファイルを指定し、dot1x クレデンシャル設定サブモードを開始します。
ステップ 13	**eap profile** *profile-name-string*	ステップ 7 で作成した EAP プロファイルを指定します。

	コマンド	目的
ステップ 14	**authentication key-management** {[**wpa**] [**cckm**]} [**optional**]	（任意）SSID のキー管理タイプを WPA、CCKM、または両方に設定します。**optional** キーワードを使用した場合、WPA または CCKM が設定されていないクライアント デバイスは、現在の SSID を使用できます。**optional** キーワードを使用しない場合は、WPA または CCKM クライアント デバイスのみが現在の SSID を使用できます。 SSID に対して CCKM をイネーブルにするには、Network-EAP 認証もイネーブルにする必要があります。SSID に対して WPA をイネーブルにするには、オープン認証、Network-EAP 認証、または両方もイネーブルにする必要があります。 **（注）** WPA および CCKM を両方ともサポートするのは、802.11b および 802.11g 無線のみです。 **（注）** CCKM または WPA をイネーブルにする前に、暗号化モードを、TKIP/AES-CCMP を含む暗号スイートに設定する必要があります。CCKM と WPA を両方ともイネーブルにするには、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 暗号化モードを設定する手順については、「暗号スイートおよび WEP」を参照してください。 **（注）** SSID に対して WPA をイネーブルにし、事前共有鍵をイネーブルにしない場合、鍵管理タイプは WPA になります。WPA および事前共有鍵をともにイネーブルにした場合、鍵管理タイプは WPA-PSK になります。事前共有鍵を設定する手順については、「追加 WPA の設定」（P.14-24）を参照してください。 **（注）** CCKM をサポートするには、ルート デバイスをネットワークの WDS デバイスと相互作用させる必要があります。ルート デバイスと WDS デバイスとの相互作用を設定する手順については、「ルート デバイスと WDS デバイスとの相互作用の設定」（P.14-24）を参照してください。
ステップ 15	**end**	イネーブル EXEC モードに戻ります。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSID または SSID 機能をディセーブルにするには、SSID コマンドの **no** 形式を使用します。

次に、ルート デバイスで AES 暗号化を使用して EAP 認証を実行するように SSID *bridgeman* の認証タイプを設定する例を示します。この SSID を使用するルート デバイスは、EAP 方式名 *eap_adam* を使用して認証を試みます。ルート側で関連する RADIUS/AAA 設定も示します。

```
bridge# configure terminal
bridge(config)# dot11 ssid bridgeman
bridge(config-ssid)# authentication network-eap eap_adam
bridge(config-ssid)# authentication key-management wpa
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# exit

bridge(config)# interface dot11radio 0
bridge(config-if)# encryption mode ciphers aes-ccm
```

```
bridge(config-if)# ssid bridgeman
bridge(config-if)# end

bridge# configure terminal
bridge(config)# aaa new-model
bridge(config)# aaa group server radius rad_eap
bridge(config-sg-radius)# server 13.1.1.99 auth-port 1645 acct-port 1646
bridge(config)# aaa authentication login eap_adam group rad_eap
bridge(config)# aaa session-id common
bridge(config)# radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7 141B1309
bridge(config)# radius-server authorization permit missing Service-Type
bridge(config)# ip radius source-interface BVI1
bridge(config)# end
```

次に、クライアント デバイス（ワークグループ ブリッジまたは非ルート ブリッジ）で AES 暗号化を使用して EAP-TLS 認証を実行するように SSID *bridgeman* の認証タイプを設定する例を示します。

```
bridge# configure terminal
bridge(config)# eap profile authProfile
bridge(config-eap-profile)# method tls
bridge(config-eap-profile)# exit

bridge(config)# dot1x credentials authCredentials
bridge(config-dot1x-creden)# username adam
bridge(config-dot1x-creden)# password adam
bridge(config-dot1x-creden)# exit

bridge(config)# dot11 ssid bridgeman
bridge(config-ssid)# authentication network-eap eap_adam
bridge(config-ssid)# authentication key-management wpa
bridge(config-ssid)# dot1x eap_profile authProfile
bridge(config-ssid)# dot1x credentials authCredentials
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# exit

bridge(config)# interface dot11radio 0
bridge(config-if)# encryption mode ciphers aes-ccm
bridge(config-if)# ssid bridgeman
bridge(config-if)# end

bridge# configure terminal
bridge(config)# aaa new-model
bridge(config)# aaa group server radius rad_eap
bridge(config-sg-radius)# server 13.1.1.99 auth-port 1645 acct-port 1646
bridge(config)# aaa authentication login eap_adam group rad_eap
bridge(config)# aaa session-id common
bridge(config)# radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7 141B1309
bridge(config)# radius-server authorization permit missing Service-Type
bridge(config)# ip radius source-interface BVI1
bridge(config)# end
```

非ルート ブリッジの 4.9 GHz WMIC 無線用 LEAP クライアントとしての設定

4.9 GHz 無線の場合、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行うように、非ルート ブリッジを設定できます。非ルート ブリッジにネットワークのユーザ名およびパスワードを設定すると、非ルート ブリッジは LEAP（シスコの無線認証プロトコル）を使用してネットワーク認証を行い、ダイナミック WEP キーを受信して使用します。

非ルート ブリッジを LEAP クライアントして設定するには、主に 3 つのステップを実行する必要があります。

1. 認証サーバ上に、非ルート ブリッジの認証用ユーザ名およびパスワードを作成します。
2. 非ルート ブリッジを対応付けるルート デバイスに 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。

非ルート側で SSID の認証タイプを設定するには、イネーブル 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	**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 ssid** *ssid-string*	グローバル SSID モードを開始します。
ステップ 3	**authentication network-eap** *list-name*	（任意）認証および鍵配布に LEAP を使用するように、SSID の認証タイプを設定します。シスコ製ブリッジがサポートするのは LEAP のみですが、無線クライアントの中には EAP、PEAP、TLS などその他の EAP 方式をサポートするものもあります。
ステップ 4	**authentication client username** ***username*** **password** ***password***	LEAP クライアントの認証ユーザ名およびパスワードを指定します。

	コマンド	目的
ステップ 5	**authentication key-management** {[**wpa**] [**cckm**]} [**optional**]	（任意）SSID のキー管理タイプを WPA、CCKM、または両方に設定します。**optional** キーワードを使用した場合、WPA または CCKM が設定されていない非ルート ブリッジは、現在の SSID を使用できます。**optional** キーワードを使用しない場合は、WPA または CCKM ブリッジのみが現在の SSID を使用できます。 SSID に対して CCKM をイネーブルにするには、Network-EAP 認証もイネーブルにする必要があります。SSID に対して WPA をイネーブルにするには、オープン認証、Network-EAP 認証、または両方もイネーブルにする必要があります。 **（注）** WPA および CCKM を両方ともサポートするのは、802.11b および 802.11g 無線のみです。 **（注）** CCKM または WPA をイネーブルにする前に、SSID の VLAN の暗号化モードを暗号スイート オプションの 1 つに設定する必要があります。CCKM と WPA を両方ともイネーブルにするには、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 暗号化モードを設定する手順については、「暗号スイートおよび WEP」を参照してください。 **（注）** SSID に対して WPA をイネーブルにし、事前共有鍵をイネーブルにしない場合、鍵管理タイプは WPA になります。WPA および事前共有鍵をともにイネーブルにした場合、鍵管理タイプは WPA-PSK になります。事前共有鍵を設定する手順については、「追加 WPA の設定」（P.14-24）を参照してください。 **（注）** CCKM をサポートするには、ルート デバイスをネットワークの WDS デバイスと相互作用させる必要があります。ルート デバイスと WDS デバイスとの相互作用を設定する手順については、「ルート デバイスと WDS デバイスとの相互作用の設定」（P.14-24）を参照してください。
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**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、クライアント デバイス（ワークグループ ブリッジまたは非ルート ブリッジ）で AES 暗号化を使用して LEAP 認証を実行するように SSID *bridgeman* の認証タイプを設定する例を示します。

```
bridge(config)# interface dot11radio 0
bridge(config-if)# encryption mode ciphers aes-ccm
bridge(config)# dot11 ssid bridgeman
bridge(config-ssid)# authentication network-eap eap_adam
bridge(config-ssid)# authentication key-management wpa
bridge(config-ssid)# authentication client username adam password adam
bridge(config-ssid)# infrastructure-ssid
bridge(config-if)# end
```

ルート デバイスと WDS デバイスとの相互作用の設定

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 デバイスとネットワーク上の WDS デバイスを相互作用させ、認証サーバにルート デバイス用のユーザ名およびパスワードを設定する必要があります。無線 LAN に WDS および CCKM を設定する手順については、『*Cisco IOS Software Configuration Guide for Cisco Access Points*』の第 11 章を参照してください。

グローバル コンフィギュレーション モードで、ルート デバイスに次のコマンドを入力します。

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

ルート デバイスを認証サーバのクライアントとして設定する場合は、同じユーザ名およびパスワードのペアを設定する必要があります。

追加 WPA の設定

ブリッジに事前共有鍵を設定し、グループ キーの更新頻度を調整するには、2 つのオプション設定を使用します。

事前共有鍵の設定

802.1x ベース認証を使用できない無線 LAN で WPA をサポートするには、ブリッジに事前共有鍵を設定する必要があります。事前共有鍵は ASCII 文字または 16 進文字で入力できます。鍵を ASCII 文字で入力する場合は、8 ～ 63 文字を入力します。ブリッジは『*Password-based Cryptography Standard*』（RFC 2898）に記載されたプロセスに従って、鍵を展開します。鍵を 16 進文字で入力する場合は、64 個の 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

2 番目のオプション WPA 設定で、ルート デバイスは認証された非ルート ブリッジにグループ キーを配信します。次に示すオプションの設定を使用すると、非ルート ブリッジのアソシエーションおよびアソシエーション解除に基づいてグループ キーを変更および配布するように、ルート デバイスを設定できます。

- メンバーシップの終了：認証されたすべての非ルート ブリッジとルート デバイスのアソシエーションが解除されると、ルート デバイスは新しいグループ キーを生成して、配布します。この機能により、対応付けられたブリッジのグループ キーはプライバシーが保護されます。
- 機能変更：最後の非鍵管理（スタティック WEP）非ルート ブリッジのアソシエーションが解除されると、ルート デバイスはダイナミック グループ キーを生成して、配布します。最初の非鍵管理（スタティック WEP）非ルート ブリッジが認証を行うと、ルート デバイスはスタティックに設定された WEP を配布します。ルート デバイスに対応付けられたスタティック WEP ブリッジが存在しない場合に、WPA マイグレーション モードでこの機能を使用すると、鍵管理対応クライアントのセキュリティが大幅に向上します。

WPA 事前共有鍵を設定するには、イネーブル 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	**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 ssid** *ssid-string*	SSID の SSID 設定モードを開始します。
ステップ 3	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	スタティック WEP キーと WPA を併用するブリッジに、事前共有鍵を入力します。 鍵を入力する場合は、16 進文字または ASCII 文字を使用します。16 進文字を使用する場合は、64 個の 16 進文字を入力して、256 ビット鍵を作成する必要があります。ASCII 文字を使用する場合は、文字、数字、または記号を 8 個以上入力する必要があります。入力した鍵はブリッジで展開されます。ASCII 文字は 63 文字まで入力できます。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、WPA を使用する非ルート ブリッジに事前共有鍵を設定する例を示します。

```
bridge# configure terminal
bridge(config)# dot11 ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(config-ssid)# end
```

認証の延期、タイムアウト、およびインターバルの設定

ルート デバイスを通して認証を行う非ルート ブリッジの延期時間、再認証期間、および認証タイムアウトを設定するには、イネーブル 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	**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 holdoff-time** *seconds*	ルート デバイスがクライアントとのアソシエーションを解除して、クライアントをアイドルにするまでに待機する秒数を入力します。1 ～ 65555 秒の値を入力します。
ステップ 3	**dot1x reauth-period** *seconds* [**server**]	認証された非ルート ブリッジを強制的に再認証させるまで WMIC が待機するインターバルを秒数で入力します。 • （任意）認証サーバで指定された再認証期間を使用するようにブリッジを設定するには、**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、認証サーバに RADIUS アトリビュート 27 の Session-Timeout を設定します。このアトリビュートは、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 ブリッジに提供するサービスの最大秒数を設定します。非ルート ブリッジが EAP 認証を実行すると、サーバはこのアトリビュートをルート デバイスに送信します。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

値をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ルート デバイスおよび非ルート ブリッジの認証タイプの一致

ここに記載された認証タイプを使用するには、ルート デバイスの認証設定が、ルート デバイスに対応付けられた非ルート ブリッジの設定と一致する必要があります。

（注）　ルート デバイスには、ルート ブリッジとアクセス ポイントが含まれます。非ルート ブリッジには、ワークグループ ブリッジと非ルート ブリッジが含まれます。

表 14-2 に、ルート ブリッジおよび非ルート ブリッジの認証タイプごとに必要な設定を示します。

表 14-2　クライアントおよび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 ブリッジの設定	ルート デバイスの設定
スタティック WEP（オープン認証を使用）	WEP を設定し、イネーブル化して、オープン認証をイネーブル化します。	WEP を設定し、イネーブル化して、オープン認証をイネーブル化します。
スタティック WEP（共有鍵認証を使用）	WEP を設定し、イネーブル化して、共有鍵認証をイネーブル化します。	WEP を設定し、イネーブル化して、共有鍵認証をイネーブル化します。
LEAP 認証	LEAP のユーザ名およびパスワードを設定し、Network-EAP 認証をイネーブルにします。	Network-EAP 認証をイネーブルにします。
CCKM 鍵管理	WEP を設定し、イネーブル化して、CCKM 認証をイネーブル化します。	WEP を設定し、イネーブル化して、CCKM 認証をイネーブル化します。さらに、WDS デバイスと相互作用するようにルート デバイスを設定し、ルート デバイスをクライアント デバイスとして認証サーバに追加します。
WPA 鍵管理	WEP を設定し、イネーブル化して、WPA 認証をイネーブル化します。	WEP を設定し、イネーブル化して、WPA 認証をイネーブル化します。