CHAPTER 49

IEEE 802.1x ポートベースの認証の設定

この章では、認証されていないデバイス（クライアント）がネットワークにアクセスするのを防止するために、IEEE 802.1x ポートベースの認証を設定する手順を説明します。

（注） この章で使用し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、次の URL にある『Cisco 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

IEEE 802.1x ポートベースの認証の概要

IEEE 802.1x 標準は、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、ルータ ポートに接続する各クライアントを認証したうえで、ルータや LAN によって提供されるサービスを利用できるようにします。

802.1x アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックをポート経由で送受信することができます。

ここでは、802.1x ポートベースの認証について説明します。

デバイスの役割

IEEE 802.1x ポート ベースの認証では、図 49-1 に示すように、ネットワーク上のデバイスにはそれぞれ特定の役割があります。

図 49-1　802.1X デバイスのロール

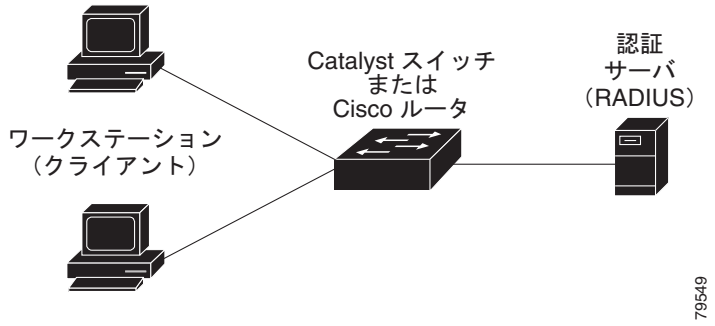


図 49-1 に示す特定の役割は、次のとおりです。

- *クライアント*：LAN およびルータ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションは、Microsoft Windows XP オペレーティング システムで提供されているような 802.1x 準拠のクライアント ソフトウェアを実行する必要があります（クライアントは、802.1x 規格では *supplicant* といいます）。

  （注） Windows XP のネットワーク接続および 802.1X ポートベース認証の問題に関しては、次の URL にある Microsoft Knowledge Base を参照してください。
  http://support.microsoft.com/kb/q303597/

- *認証サーバ*：実際にクライアントの認証を行います。認証サーバは、クライアントのアイデンティティを確認し、そのクライアントの LAN およびルータ サービスへのアクセスが許可されるかどうかをルータに通知します。ルータはプロキシとして動作するので、認証サービスはクライアントに対してはトランスペアレントに行われます。認証サーバとして、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。RADIUS はクライアント サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

- *ルータ（オーセンティケータおよびバックエンドのオーセンティケータともいう）*：クライアントの認証ステータスに基づいて、ネットワークへの物理的アクセスを制御します。ルータはクライアントと認証サーバとの仲介装置（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。ルータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

  ルータが EAPOL フレームを受信して認証サーバにリレーする際、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更または検証は行われず、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。ルータが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

認証の開始およびメッセージ交換

ルータまたはクライアントのどちらからも、認証を開始できます。**dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにした場合、ルータはポートのリンク ステートがダウンからアップに移行したと判断した時点で、認証を開始しなければなりません。その場合、ルータは EAP 要求/アイデンティティ フレームをクライアントに送信して識別情報を要求します（ルータは通常、最初のアイデンティティ/要求フレームに続いて、認証情報に関する 1 つまたは複数の要求を送信します）。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

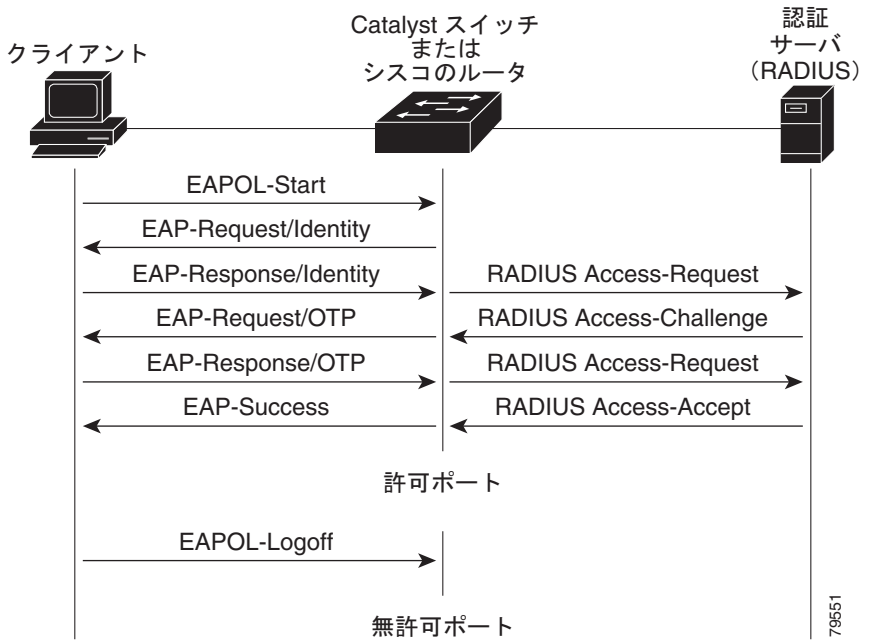
ただし、クライアントが起動時にルータから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはルータに対し、クライアントのアイデンティティを要求するように指示します。

（注）　ネットワーク アクセス デバイスで IEEE 802.1x がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートにあるかのようにフレームの送信を開始します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.49-4）を参照してください。

クライアントが自らの識別情報を提示すると、ルータは仲介装置としての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、ルータ ポートは許可ステートになります。詳細については、「許可ステートおよび無許可ステートのポート」（P.49-4）を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 49-2 に、クライアントが RADIUS サーバとの間でワンタイム パスワード（OTP）認証方式を使用する場合に行われるメッセージ交換を示します。

図 49-2　メッセージ交換



許可ステートおよび無許可ステートのポート

ルータ ポート ステートによって、クライアントがネットワーク アクセスを許可されているかどうか判別できます。ポートは最初、*無許可*ステートです。このステートでは、ポートは IEEE 802.1x プロトコル パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ステートに移行し、クライアントのトラフィック送受信を通常どおりに許可します。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、ルータはそのクライアントのアイデンティティを要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートのままであり、クライアントはネットワーク アクセスを許可されません。

これに対し、802.1x 対応のクライアントが、802.1x プロトコルプロトコルを実行していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答が得られないため、クライアントはポートが許可ステートにあるかのようにフレームの送信を開始します。

dot1x port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1x ポートベースの認証をディセーブルにして、必要な認証交換をせずにポートを許可ステートに移行させます。ポートはクライアントの 802.1x ベース認証なしで通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。ルータは、インターフェイスを介してクライアントに認証サービスを提供することができません。

- **auto**：802.1x ポートベースの認証をイネーブルにして、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。ルータは、クライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。ルータはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが正常に認証されると（認証サーバから Accept フレームを受信する）、ポートが許可ステートに変わり、認証されたクライアントのフレームはすべてそのポートを通じて許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、ルータは要求を再送信できます。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、ルータ ポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合に、ポートは無許可ステートに戻ります。

DHCP スヌーピングでの IEEE 802.1X 認証の使用

データ挿入機能を備えたダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングの Option 82 がイネーブルになると、ルータがクライアントの IEEE 802.1X 認証されたユーザ ID 情報を DHCP ディスカバリ プロセスに挿入でき、DHCP サーバが IP アドレスを別の IP アドレス プールから別のエンド ユーザのクラスに割り当てられます。この機能によって、アカウンティングのためにエンド ユーザに与えられた IP アドレスをセキュリティ保護し、レイヤ 3 基準に基づいてサービスを許可できます。

802.1X の認証に成功した後、ポートはフォワーディング ステートとなり、RADIUS サーバから受信した属性を保存します。DHCP スヌーピングを実行している場合、ルータは DHCP リレー エージェントとして機能し、DHCP メッセージを受信し、別のインターフェイスで送信のためにこれらのメッセージを再度生成します。

802.1X 認証後、クライアントが DHCP ディスカバリ メッセージを送信すると、ルータはパケットを受信し、RADIUS 属性サブオプション セクションを、クライアントの保存されている RADIUS 属性を含むパケットに追加します。ルータは、その後、ディスカバリ ブロードキャストを再度送信します。DHCP サーバは変更された DHCP ディスカバリ パケットを受信し、IP アドレスの割り当ての作成時に認証されたユーザ ID 情報を使用できます（設定されている場合）。

ユーザの IP アドレスへのマッピングは、1 対 1、1 対多、多対多で実行できます。1 対多のマッピングでは、同じユーザが複数のポートで 802.1X ホストによって認証を行えます。

801.X 認証とデータ挿入機能を備えた DHCP スヌーピングの Option 82 がイネーブルの場合は、ルータが認証されたユーザ ID 情報を自動的に挿入します。データ挿入機能を備えた DHCP スヌーピングの Option 82 を設定するには、37-3 ページの「DHCP スヌーピングの Option 82 データ挿入」の項を参照してください。

RADIUS 属性サブオプションで挿入されるデータについては、RFC 4014『Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option』を参照してください。

サポートされるトポロジ

IEEE 802.1x ポート ベース認証は、次の 2 つのトポロジーでサポートされます。

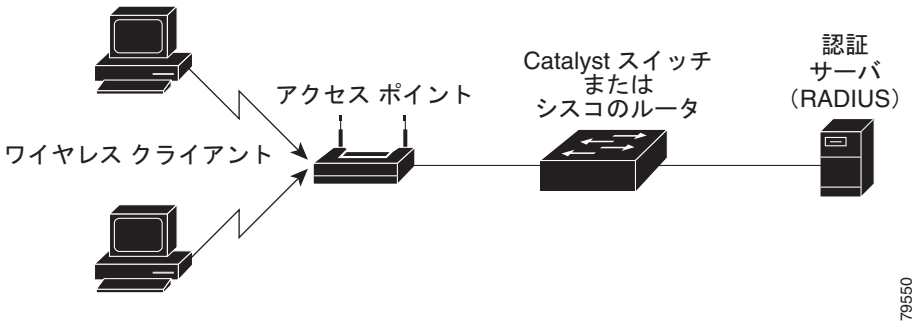
- ポイントツーポイント

- ワイヤレス LAN

ポイントツーポイントの構成（図 49-1（P.49-2）を参照）では、802.1x 対応のルータ ポートに接続できるクライアントは、1 台だけです。ルータは、ポートのリンク ステートがアップに変化したときに、クライアントを検出します。クライアントがログオフしたとき、または別のクライアントに替わったときには、ルータはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

図 49-3 に、ワイヤレス LAN における 802.1x ポート ベースの認証を示します。802.1x ポートは複数ホスト ポートとして設定されており、いずれか 1 つのクライアントが認証された時点で許可ステートになります。ポートが許可ステートになると、そのポートに間接的に接続している他のすべてのホストが、ネットワーク アクセスを許可されます。ポートが無許可ステートになると（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、ルータはすべての接続先クライアントのネットワーク アクセスを禁止します。このトポロジーでは、ワイヤレス アクセス ポイントが接続先クライアントの認証を処理し、ルータに対するクライアントとしての役割を果たします。

図 49-3　　ワイヤレス LAN の例



IEEE 802.1x ポートベースの認証のデフォルト設定

表 49-1 に、IEEE 802.1x のデフォルト設定を示します。

表 49-1　　802.1X のデフォルト設定

機能	デフォルト設定
認証、許可、アカウンティング（AAA）	ディセーブル
RADIUS サーバの IP アドレス	指定なし
RADIUS サーバの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）認証ポート	1812
RADIUS サーバ キー	指定なし
インターフェイスごとの 802.1x プロトコル イネーブル ステート	ディセーブル（force-authorized） **（注）**　ポートはクライアントの 802.1x ベース認証なしで通常のトラフィックを送受信します。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
待機時間	60 秒（ルータがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数）

表 49-1　802.1X のデフォルト設定 （続き）

機能	デフォルト設定
再送信時間	30 秒（ルータが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（ルータが認証プロセスを再開するまでに、EAP 要求/アイデンティティ フレームを送信する回数）
複数ホストのサポート	ディセーブル
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、クライアントに要求を再送信するまでにルータが応答を待機する時間）
認証サーバ タイムアウト時間	30 秒（認証サーバからの応答をクライアントにリレーするとき、ルータが応答を待ち、クライアントに要求を再送信するまでの時間）

IEEE 802.1x ポートベースの認証時の注意事項および制約事項

IEEE 802.1x ポートベースの認証を設定する場合、次の注意事項および制約事項に従ってください。

- 802.1x をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1x プロトコルは、レイヤ 2 のスタティック アクセス ポートおよびレイヤ 3 ルーテッド ポートではサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
  - EtherChannel ポート：ポート上で 802.1x をイネーブルにする前に、EtherChannel のポート チャネル インターフェイスから 802.1x を削除する必要があります。EtherChannel のポート チャネル インターフェイス上または EtherChannel 上の個々のアクティブ ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。まだアクティブになっていない EtherChannel 上の個々のポートで 802.1x をイネーブルにしても、そのポートは EtherChannel に加入しません。
  - セキュア ポート：セキュア ポートは 802.1x ポートにできません。セキュア ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートをセキュア ポートに変更しようとしても、エラー メッセージが表示され、セキュリティ設定は変更されません。
  - スイッチド ポート アナライザ（SPAN）宛先ポート：SPAN 宛先ポートであるポートで 802.1x をイネーブルにすることができます。ただし、ポートが SPAN 宛先として削除されるまで、802.1x はディセーブルになります。SPAN 送信元ポートでは 802.1x をイネーブルにすることができます。

IEEE 802.1x ポートベースの認証の設定

ここでは、IEEE 802.1x ポートベースの認証の設定方法を説明します。

IEEE 802.1x ポートベースの認証のイネーブル化

IEEE 802.1x ポート ベース認証をイネーブルにするには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

802.1x ポート ベースの認証を設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	`Router(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1x ポート ベース認証方式リストを作成します。
ステップ 4	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 5	`Router(config)# interface type slot/port`	インターフェイス コンフィギュレーション モードを開始し、802.1x ポートベースの認証をイネーブルにするインターフェイスを指定します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 6	`Router(config-if)# dot1x port-control auto`	インターフェイス上で 802.1x ポートベースの認証をイネーブルにします。

	コマンド	目的
ステップ 7	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Router# show dot1x all`	入力を確認します。 表示の 802.1x Port Summary セクションの Status カラムを確認してください。*enabled* というステータスは、ポート制御値が、**auto** または **force-unauthorized** に設定されていることを意味します。

802.1x ポートベースの認証をイネーブルにする場合、次の点に注意してください。

- **authentication** コマンドにリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストが、自動的にすべてのインターフェイスに適用されます。
- 次のキーワードのうち、少なくとも 1 つを入力します。
  - **group radius** : すべての RADIUS サーバのリストを認証に使用します。
  - **none** : 認証を使用しません。クライアントから提供される情報を使用することなく、クライアントはルータにより自動的に認証されます。

次に、ファスト イーサネット ポート 5/1 で AAA と 802.1x をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show dot1x all

Dot1x Info for interface FastEthernet5/1
----------------------------------------------------
AuthSM State      = FORCE UNAUTHORIZED
BendSM State      = IDLE
PortStatus        = UNAUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
Port Control      = Force UnAuthorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

ルータと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号

- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

RADIUS サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 3	`Router(config)# radius-server host {hostname | ip_address}`	ルータに RADIUS サーバ ホスト名や IP アドレスを設定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 4	`Router(config)# radius-server key string`	ルータと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証キーおよび暗号化キーを設定します。
ステップ 5	`Router(config)# end`	特権 EXEC モードに戻ります。

RADIUS サーバ パラメータを設定する場合、次の点に注意してください。

- *hostname* または *ip_address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。
- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、ルータと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号化キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。このキーは RADIUS デーモンで使用する暗号と一致する必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、すべての RADIUS サーバに対してタイムアウト、再送信回数、暗号キーの値をグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** 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。詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*, Release 12.2』と『*Cisco IOS Security Command Reference*, Release 12.2』を参照してください。

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

（注）　RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、ルータの IP アドレス、およびサーバとルータの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、ルータで RADIUS サーバ パラメータを設定する例を示します。

```
Router# configure terminal
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46
Router(config)# radius-server key rad123
Router(config)# end
```

定期的な再認証のイネーブル化

IEEE 802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定することができます。再認証をイネーブルにする前にその間隔を指定しない場合、3600 秒おきに再認証が試みられます。

802.1x クライアントの自動的な再認証はグローバルな設定であり、個々のポートに接続するクライアント別に設定はできません。特定のポートに接続するクライアントを手動で再認証する方法については、「手動によるポート接続クライアントの再認証」（P.49-12）を参照してください。

インターフェイス コンフィギュレーション モードでクライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x reauthentication`	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。
ステップ 3	`Router(config-if)# dot1x timeout reauth-period seconds`	再認証の間隔（秒）を設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 3600 秒です。 このコマンドがルータに影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show dot1x all`	入力を確認します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定して、入力を確認する例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 4000
Router(config-if)# end
Router# show dot1x all
```

手動によるポート接続クライアントの再認証

（注）　再認証は、すでに認証されているポートのステータスには影響しません。

特定のポートに接続するクライアントを手動で再認証するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dot1x re-authenticate interface` *type slot/port*	ポートに接続するクライアントを手動で再認証します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router# show dot1x all`	入力を確認します。

次に、ファスト イーサネット ポート 5/1 に接続されているクライアントを手動で再認証し、入力を確認する例を示します。

```
Router# dot1x re-authenticate interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
Router# show dot1x all
```

ポート接続クライアント認証の初期化

（注）　認証の初期化により、既存の認証をディセーブルにしてから、ポートに接続されているクライアントを認証します。

ポートに接続されているクライアントの認証を初期化するには、特権 EXEC モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dot1x initialize interface` *type slot/port*	ポートに接続されているクライアントの認証を初期化します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router# show dot1x all`	入力を確認します。

次に、ファスト イーサネット ポート 5/1 に接続されているクライアントに対する認証を初期化し、入力を確認する例を示します。

```
Router# dot1x initialize interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
Router# show dot1x all
```

待機時間の変更

ルータがクライアントを認証できなかった場合は、ルータは所定の時間だけアイドル状態を続け、そのあと再び認証を試みます。このアイドル時間は、待機時間の値によって決定されます。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout quiet-period seconds`	ルータがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数を設定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータの待機時間を 30 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout quiet-period 30
Router(config-if)# end
Router# show dot1x all
```

ルータとクライアント間の再送信時間の変更

クライアントはルータからの EAP 要求/アイデンティティ フレームに対し、EAP 応答/アイデンティティ フレームで応答します。ルータがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、そのあとフレームを再送信します。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

ルータがクライアントからの通知を待機する時間を変更するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout tx-period seconds`	ルータが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 30 秒です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定して、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x timeout tx-period 60
Router(config-if)# end
Router# show don1x all
```

ルータとクライアント間の EAP 要求フレーム再送信時間の設定

クライアントは EAP 要求フレームを受信したことをルータに通知します。ルータがこの通知を受信できなかった場合、ルータは所定の時間だけ待機し、そのあとフレームを再送信します。ルータが通知を待機する時間は、1 ～ 65535 秒の範囲に指定できます （デフォルトは 30 秒です）。

ルータからクライアントへの EAP 要求フレーム再送信時間を設定するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout supp-timeout seconds`	ルータからクライアントへの EAP 要求フレームの再送信時間を設定します。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータからクライアントへの EAP 要求フレームの再送信時間を 25 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x timeout supp-timeout 25
Router(config-if)# end
Router# show dot1x all
```

ルータと認証サーバ間のレイヤ 4 パケット再送信時間の設定

認証サーバは、レイヤ 4 パケットを受信するたびにルータに通知します。ルータがパケット送信後、通知を受信できない場合、ルータは所定の時間だけ待機し、そのあとパケットを再送信します。ルータが通知を待機する時間は、1 ～ 65535 秒の範囲に指定できます （デフォルトは 30 秒です）。

ルータから認証サーバへレイヤ 4 パケットを再送信する時間を設定するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout server-timeout seconds`	ルータから認証サーバへのレイヤ 4 パケットの再送信時間を設定します。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータから認証サーバへのレイヤ 4 パケットの再送信時間を 25 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# dot1x timeout server-timeout 25
Router(config-if)# end
Router# show dot1x all
```

ルータとクライアント間のフレーム再送信回数の設定

ルータとクライアント間の再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）ルータが認証プロセスを再起動する前に、クライアントに EAP 要求/アイデンティティ フレームを送信する回数を変更することができます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

ルータからクライアントへのフレーム再送信回数を設定するには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x max-req count`	ルータが認証プロセスを再開するまでに、EAP 要求/アイデンティティ フレームをクライアントに送信する回数を設定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。

	コマンド	目的
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータが認証プロセスを再起動する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x max-req 5
Router(config-if)# end
Router# show dot1x all
```

複数ホストのイネーブル化

図 49-3（P.49-6）に示すように、1 つの IEEE 802.1x 対応ポートに複数のホストを接続することができます。このモードでは、接続されたホストのうち 1 つが認証に成功すれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、および EAPOL ログオフ メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている 802.1x 許可ポートに、複数のホスト（クライアント）が接続できるようにするには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x host-mode multi-host`	802.1x 許可ポートで複数ホスト（クライアント）を許可します。 **（注）** 指定するインターフェイスでは、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ファスト イーサネット インターフェイス 5/1 で 802.1x をイネーブルにし、複数のホストを許可して入力を確認する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x host-mode multi-host
Router(config-if)# end
Router# show dot1x all
```

IEEE 802.1x 設定をデフォルト値にリセットする方法

IEEE 802.1x 設定をデフォルト値に戻すには、インターフェイス コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x default`	設定可能な 802.1x パラメータをデフォルト値にリセットします。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

IEEE 802.1x ステータスの表示

ルータのグローバルな IEEE 802.1x の管理ステータスおよび動作ステータスを表示するには、**show dot1x** 特権 EXEC コマンドを使用します。特定のインターフェイスに関する 802.1x の管理ステータスおよび動作ステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

これらのコマンドのキーワードと引数の詳細については『*Cisco IOS Security Command Reference, Release 12.2 SR*』を参照してください。