CHAPTER 25

IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポートベースの認証を設定し、許可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ぐ方法について説明します。Release 12.1(13)E 以降のリリースで、802.1x ポート ベースの認証がサポートされます。

（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、『*Cisco 7600 Series Router Cisco IOS Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

802.1x ポートベースの認証

IEEE 802.1x 規格では、クライアント サーバ ベースのアクセス コントロールおよび認証プロトコルが定義されており、許可されていないクライアントが、公的にアクセス可能なポートを通じて LAN に接続するのを制限しています。認証サーバは、ルータポートに接続された各クライアントを認証し、VLAN にポートを割り当ててから、ルータまたは LAN が提供するサービスを利用できるようにします。

クライアントが認証されるまでは、802.1x アクセス コントロールによって、クライアントが接続しているポートを経由する Extensible Authentication Protocol Over LAN（EAPOL）トラフィックだけを許可します。認証が成功すれば、通常のトラフィックがポートを通過できます。

ここでは、IEEE 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

802.1x ポートベースの認証を使用すると、ネットワークのデバイスに図 25-1 で示されるような特定の役割が割り当てられます。

図 25-1　802.1x デバイスの役割

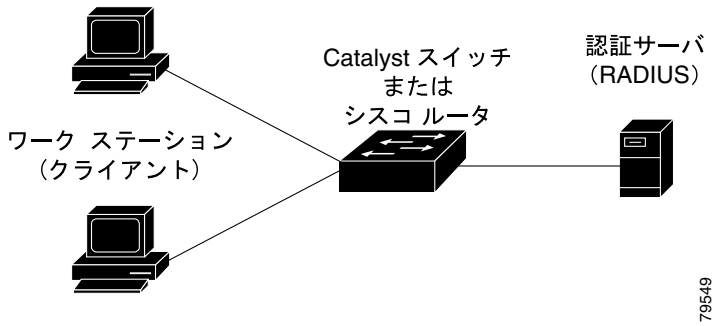


図 25-1 での特定の役割は、次のとおりです。

- *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している必要があります（クライアントは、IEEE 802.1x 規格で *supplicant* になります）。

（注）　Windows XP ネットワーク接続および 802.1x ポートベースの認証の問題を解決するには、次の URL の「Microsoft Knowledge Base」の項を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *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ルータに通知します。ルータはプロキシとして機能するので、認証サービスはクライアントに透過的です。サポート対象の認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を持つ Remote Authentication Dial-In User Service（RADIUS）のセキュリティ システムだけです。Cisco Secure Access Control Server のバージョン 3.0 で利用できます。RADIUS は、クライアント サーバ モデルを使用して、RADIUS と 1 つまたは複数の RADIUS クライアント間で安全な認証情報を交換します。
- *Cisco 7600 シリーズ 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間で媒介（プロキシ）として機能し、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て、クライアントに応答をリレーします。ルータには、RADIUS クライアントが組み込まれていて、EAP フレームのカプセル化およびカプセル化解除、さらには認証サーバとの相互作用の役割を果たしています。

  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と、イーサネット ヘッダーが取り除かれ、残りの EAP フレームは RADIUS 形式で再度カプセル化されます。カプセル化の間は、EAP フレームの変更または検査が行われず、認証サーバはネイティブのフレーム形式内で EAP をサポートする必要があります。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 EAP フレームが残ります。その後、これはイーサネット用にカプセル化されて、クライアントに送信されます。

認証の開始とメッセージ交換

ルータまたはクライアントは、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、ポートの認証をイネーブルにする場合、ルータはポート リンク ステートがダウンからアップに移行したと判別したときに、認証を開始する必要があります。次に、ルータはクライアントに EAP 要求 / アイデンティティ フレームを送信して、識別情報を要求します（一般にルータは、最初のアイデンティティ / 要求フレームを送信して、そのあとで認証情報の要求を 1 つまたは複数送信します）。クライアントが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。

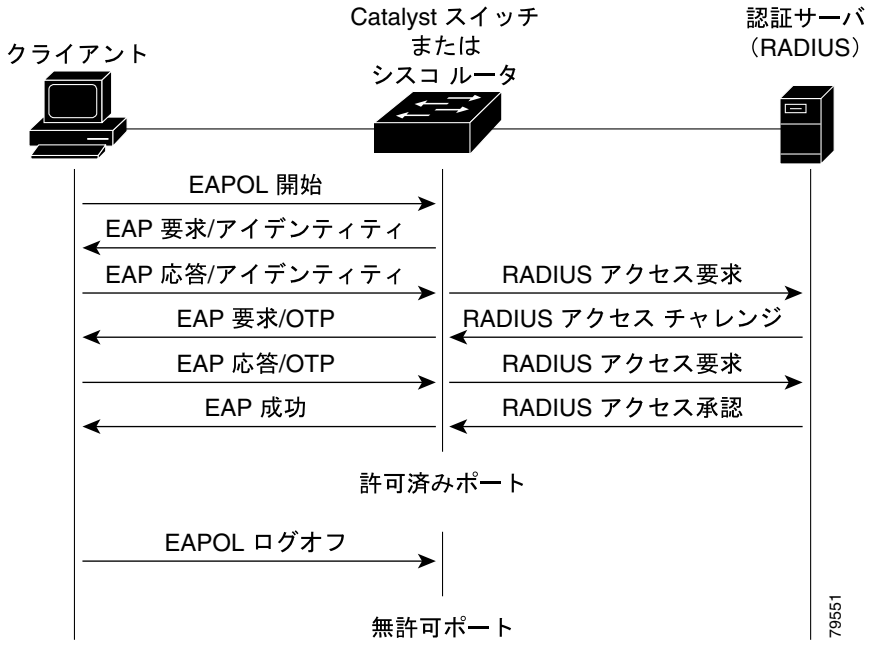
起動中にクライアントがルータから EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは EAPOL 開始フレームを送信して、認証を開始できます。これにより、ルータはクライアントの識別情報を要求するようになります。

（注）　ネットワーク アクセス デバイスで 802.1x がイネーブルになってない場合、またはサポートされていない場合は、クライアントからの EAPOL フレームはドロップされます。認証開始を 3 回試行しても、クライアントが EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは、ポートが許可済みステートにあると見なし、フレームを送信します。許可済みステートにあるポートは、実質的にクライアントが認証に成功したということを意味します。詳細については、「許可済みおよび無許可のステートのポート」（p.25-4）を参照してください。

クライアントが自身のアイデンティティを供給すると、ルータは媒介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間で EAP フレームを渡します。認証が成功すると、ルータ ポートは許可された状態になります。詳細については、「許可済みおよび無許可のステートのポート」（p.25-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に依存します。図 25-2 に、クライアントが RADIUS サーバで One-Time-Password（OTP; ワンタイム パスワード）認証方式を使用して開始するメッセージ交換を示します。

図 25-2　メッセージ交換



許可済みおよび無許可のステートのポート

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、*無許可の*ステートで開始します。このステートでは、ポートは 802.1x プロトコル パケット以外のすべての入トラフィックおよび出トラフィックを許可しません。クライアントが認証に成功すると、ポートは*許可済み*のステートに移行して、そのクライアントのすべてのトラフィックに通常のフローが許可されます。

802.1x をサポートしないクライアントが、無許可の 802.1x ポートに接続している場合、ルータがクライアントの識別情報を要求します。この場合、クライアントは要求に応答しないので、ポートは無許可のステートのままになり、クライアントはネットワークへのアクセスが許可されません。

対照的に、802.1x 対応のクライアントが、802.1x プロトコルを実行していないポートに接続している場合、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できます。応答を受信しない場合、クライアントは要求を一定回数だけ送信します。応答が受信されないため、クライアントは、ポートが許可済みステートにあると見なし、フレームの送信を開始します。

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

- **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 ベースの認証なしで通常のトラフィックを送受信します。これが、デフォルトの設定です。
- **force-unauthorized —** ポートを無許可ステートのままにして、クライアントが認証を試みてもすべて無視します。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 開始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て、クライアントと認証サーバ間での認証メッセージのリレーを開始します。ネットワークにアクセスを試みる各クライアントは、ルータによりクライアントの MAC アドレスを使用して一意に識別されます。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信する）、ポート ステートは、許可済みに切り替わり、認証されたクライアントからのフレームはすべて、そのポートを通じて許可されます。認証に失敗した場合は、ポートは無許可のままですが、認証を再試行できます。認証サーバにアクセスできない場合、ルータは要求を再送信できます。再試行を所定の回数行ってもサーバから応答が得られない場合には認証は失敗で、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、EAPOL ログオフメッセージを送信して、ルータポートを無許可ステートに移行させます。

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、ポートは無許可ステートに戻ります。

サポート対象のトポロジ

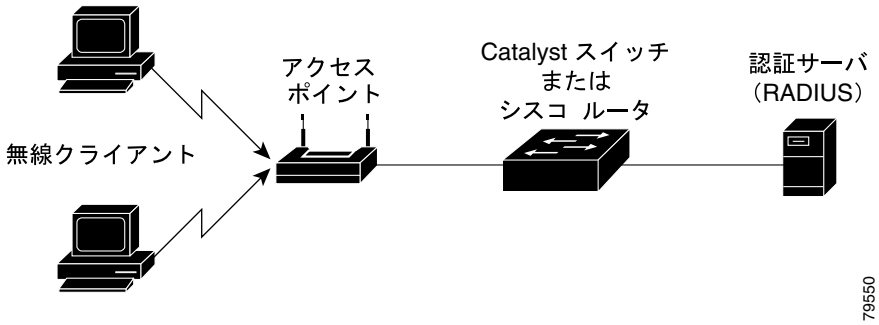
802.1x ポートベースの認証は、次の 2 つのトポロジでサポートされます。

- ポイントツーポイント
- 無線 LAN

ポイントツーポイントの構成（図 25-1 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 ステートに変わると、クライアントを検出します。クライアントがログオフするか、別のクライアントに交換されると、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 25-3 に、無線 LAN での 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いて、1 台のクライアントが認証されるとすぐに許可済みになります。ポートが許可されると、ポートに間接的に接続する残りのホストはすべて、ネットワーク アクセスが許可されます。ポートが（再認証に失敗したり EAPOL ログオフ メッセージを受信するなどして）無許可になると、ルータは接続するすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジでは、無線アクセス ポイントは、そのポイントに接続しているクライアントを認証する役割を持ち、ルータに対してクライアントとして動作します。

図 25-3　無線 LAN の例



802.1x ポートベースの認証のデフォルト設定

表 25-1 に、802.1x のデフォルト設定を示します。

表 25-1　802.1x のデフォルト設定

機能	デフォルト設定
Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）	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 UDP 認証ポート	1812
RADIUS サーバ キー	指定なし
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル（強制的に許可） **（注）** ポートは、クライアントの 802.1x ベースの認証なしで通常のトラフィックを送受信します。
定期的再認証	ディセーブル
再認証試行間隔の秒数	3600 秒
待機時間	60 秒（クライアントとの認証交換に失敗したあと、ルータが待機ステートにある秒数）
再送信時間	30 秒（ルータが、要求を再送信するまでに、クライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待機する時間）
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
クライアントのタイムアウト時間	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）
認証サーバのタイムアウト時間	30 秒（クライアントの応答を認証サーバにリレーするとき、サーバに応答を再送信するまでにルータが応答を待機する時間）

802.1x ポートベースの認証時の注意事項および制約事項

802.1x ポートベースの認証を設定する際、次の注意事項および制約事項に注意してください。

- 802.1x がイネーブルのときは、ポートが認証されてから他のレイヤ 2 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 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 ポートの両方でサポートされていますが、次のポート タイプではサポートされていません。
  - 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 インターフェイスまたは EtherChannel 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。EtherChannel のまだアクティブになっていない個々のポートで 802.1x をイネーブルにしようとすると、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 ポートとして設定できません。セキュア ポート上で 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すると、エラー メッセージが表示され、セキュリティ設定が変更されません。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポート — SPAN 宛先ポートであるポート上で 802.1x をイネーブルにできますが、SPAN 宛先ポートとしてポートを削除するまでは 802.1x はディセーブルに設定されます。SPAN 送信元ポートでは、802.1x をイネーブルにできます。

802.1x ポートベースの認証の設定

ここでは、802.1x ポートベースの認証の設定について説明します。

802.1x ポートベースの認証のイネーブル化

802.1x ポートベースの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のリストを指定する必要があります。方式リストでは、ユーザ認証のためクエリーされる順序と認証方式が記述されています。

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、ソフトウェアは方式リストから次の方式を選択します。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、定義された方式すべてを使い果たすまで続きます。このサイクルの任意のポイントで認証が失敗すると、認証プロセスは停止し、他の認証方式も試行されません。

802.1x ポートベースの認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA をイネーブルにします。
	`Router(config)# no aaa new-model`	AAA をディセーブルにします。
ステップ 2	`Router(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1x ポートベースの認証方式リストを作成します。
	`Router(config)# no aaa authentication dot1x {default | list_name}`	設定された方式リストを削除します。
ステップ 3	`Router(config)# dot1x system-auth-control`	グローバルに 802.1x ポートベースの認証をイネーブルにします。
	`Router(config)# no dot1x system-auth-control`	グローバルに 802.1x ポートベースの認証をディセーブルにします。
ステップ 4	`Router(config)# interface type[1] slot/port`	インターフェイス コンフィギュレーション モードを開始して、802.1x ポートベースの認証でイネーブルにするインターフェイスを指定します。
ステップ 5	`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。
	`Router(config-if)# no 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ディセーブルにします。
ステップ 6	`Router(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	`Router# show dot1x all`	設定を確認します。 出力の 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** に設定されたことを意味します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

802.1x ポートベースの認証をイネーブルにする際は、構文について次の点に注意してください。

- 名前付きリストが **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の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に従って、**default** キーワードを使用します。デフォルトの方式リストは、すべてのインターフェイスに自動的に適用されます。
- 次のキーワードを少なくとも 1 つ入力します。
  - **group radius —** 認証にすべての RADIUS サーバのリストを使用します。
  - **none —** 認証を使用しません。クライアントは、ルータによって自動的に認証され、クライアントが提供する情報を使用しません。

次に、ポート FastEthernet 5/1 上の AAA および 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
```

Cisco 7600 シリーズ ルータと RADIUS サーバ間の通信の設定

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
- ホスト名および特定の UDP ポート番号
- IP アドレスおよび特定の 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り、一意の識別情報が作成され、これにより同じ IP アドレスのサーバ上の複数の UDP ポートに RADIUS 要求を送信できます。同じ RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば認証）に対して設定されている場合、設定された 2 番目のホスト 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。RADIUS のホスト エントリは、設定された順序で試行されます。

RADIUS サーバのパラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットに、指定されたインターフェイスの IP アドレスが含まれることを指定します。
	`Router(config)# no ip radius source-interface`	RADIUS パケットが、先に指定されたインターフェイスの IP アドレスを含まないようにします。
ステップ 2	`Router(config)# radius-server host {hostname | ip_address}`	ルータ上で RADIUS サーバのホスト名または 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、次のコマンドを再入力します。
	`Router(config)# no radius-server host {hostname | ip_address}`	指定された RADIUS サーバを削除します。
ステップ 3	`Router(config)# radius-server key string`	ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証キーおよび暗号化キーを設定します。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。

RADIUS サーバのパラメータを設定する際、構文について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。
- 個々のコマンド ラインで **key** *string* を指定します。
- **key** *string* には、ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証キーおよび暗号化キーを指定します。キーは、RADIUS サーバ上で使用する暗号化キーと一致する必要がある文字列です。
- **key** *string* を指定する場合は、キーの一部および末尾にスペースを使用します。スペースをキーの一部として使用する場合は、キーの一部として引用符を使用する場合を除いて、キーを引用符で囲まないでください。このキーは、RADIUS デーモンで使用され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、暗号化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場合は、**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 の『*Cisco IOS Security Configuration Guide*』Release 12.1 および『*Cisco IOS Security Command Reference*』Release 12.1 を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm

（注）　さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定には、ルータの IP アドレス、およびサーバとルータで共有するキー ストリングが含まれます。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、ルータに RADIUS サーバの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
```

定期的再認証のイネーブル化

定期的な 802.1x クライアント再認証をイネーブル化して、その発生間隔を指定できます。再認証をイネーブルにする前に時間の間隔を指定しなかった場合は、再認証試行間隔は 3600 秒になります。

自動 802.1x クライアント再認証はグローバル設定で、個々のポートに接続しているクライアントには設定できません。特定のポートに接続しているクライアントを手動で再認証するには、「手動によるポート接続クライアントの再認証」（p.25-11）を参照してください。

クライアントの定期的な再認証をイネーブルにして、再認証試行間隔を秒単位で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
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。
	`Router(config-if)# no dot1x reauthentication`	クライアントの定期的な再認証をディセーブルにします。
ステップ 3	`Router(config-if)# dot1x timeout re-authperiod seconds`	再認証試行間隔を秒単位で設定します。 設定できる範囲は 1 ～ 4294967295 です。デフォルトでは、3600 秒に設定されています。 このコマンドがルータの動作に作用するのは、定期的再認証がイネーブルの場合だけです。
	`Router(config-if)# no dot1x timeout re-authperiod`	デフォルトの再認証間隔に戻します。
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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、定期的再認証をイネーブルにして、再認証試行間隔の秒数を 4000 に設定する例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout re-authperiod 4000
```

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、すでに許可済みのポートのステータスには影響しません。

ポート接続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[1] slot/port`	手動でポート接続クライアントを再認証します。
ステップ 2	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/1 に接続しているクライアントを手動で再認証する例を示します。

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

ポート接続クライアント認証の初期化

（注）　認証の初期化によって、既存の認証をディセーブルにしてから、ポート接続クライアントを認証します。

ポート接続クライアントの認証を初期化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dot1x initialize interface type[1] slot/port`	ポート接続クライアントの認証を初期化します。
ステップ 2	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/1 に接続しているクライアントの認証を初期化する例を示します。

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

待機時間の変更

ルータがクライアントを認証できないときは、ルータは一定時間アイドル状態のままで、その後再試行します。アイドル時間は、待機時間の値によって決まります。クライアントが無効なパスワードを指定したため、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力することで、ユーザに対する応答時間をより速くできます

待機時間を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout quiet-period seconds`	クライアントとの認証交換に失敗したあと、ルータが待機ステートになる時間を秒単位で設定します。 設定できる範囲は 0 ～ 65535 秒です。デフォルトでは、60 に設定されています。
	`Router(config-if)# no dot1x timeout quiet-period`	デフォルトの待機時間に戻ります。

	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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ルータの待機時間を 30 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout quiet-period 30
```

Cisco 7600 シリーズ 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、EAP 応答 / アイデンティティ フレームで応答します。ルータはこの応答を受信しなかった場合、一定時間（再送信時間という）待機してから、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の変更は、信頼性のないリンクや特定のクライアントや認証サーバの特殊な動作問題などの異状を調整する場合だけ行うようにしてください。

ルータがクライアントの通知を待機する時間を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout tx-period` *seconds*	ルータが、要求を再送信するまでに、クライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待機する時間を秒単位で設定します。 設定できる範囲は 1 ～ 65535 秒です。デフォルトでは、30 に設定されています。
	`Router(config-if)# dot1x timeout tx-period`	デフォルトの再送信時間に戻します。
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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ルータが、要求を再送信するまでに、クライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待機する時間を 60 秒に設定する例を示します。

```
Router(config)# dot1x timeout tx-period 60
```

Cisco 7600 シリーズ 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、ルータに EAP 要求フレームを受信したことを通知します。ルータがこの通知を受信していない場合は、ルータは一定時間待機してから、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 秒に設定できます。デフォルトでは、30 秒に設定されています。

ルータとクライアント間の EAP 要求フレーム再送信時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout supp-timeout seconds`	ルータとクライアント間の EAP 要求フレーム再送信時間を設定します。
	`Router(config-if)# no dot1x timeout supp-timeout`	デフォルトの再送信時間に戻します。
ステップ 3	`Router# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ルータとクライアント間の EAP 要求フレームの再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout supp-timeout 25
```

Cisco 7600 シリーズ 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。ルータがパケットを送信しているにもかかわらず通知を受信していない場合は、ルータは一定時間待機してから、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 秒に設定できます。デフォルトでは、30 秒に設定されています。

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値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout server-timeout seconds`	ルータと認証サーバ間のレイヤ 4 パケット再送信時間を設定します。
	`Router(config-if)# no dot1x timeout server-timeout`	デフォルトの再送信時間に戻します。
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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ルータと認証サーバ間のレイヤ 4 パケットの再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout server-timeout 25
```

Cisco 7600 シリーズ 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の変更以外に、認証プロセスを再開するまでに、ルータが（応答を受信していないという前提で）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できます。

（注） このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントや認証サーバの特殊な動作問題などの異状を調整する場合だけ行うようにしてください。

ルータとクライアント間のフレーム再送信回数を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
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 フレームを送信する回数を設定します。設定できる範囲は 1 ～ 10 です。デフォルトでは、2 に設定されています。
	`Router(config-if)# no dot1x max-req`	デフォルトの再送信回数に戻します。
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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ルータが認証プロセスを再開するまでに、EAP 要求 / アイデンティティ要求を送信する回数を 5 と設定する例を示します。

```
Router(config-if)# dot1x max-req 5
```

複数ホストのイネーブル化

図 25-3 に示すように、複数のホストを 1 つの 802.1x 対応ポートに接続できます。このモードでは、すべてのホストがネットワーク アクセスを許可されるため、接続ホストのいずれか 1 つだけが正常に許可される必要があります。ポートが（再認証が失敗したり EAPOL ログオフ メッセージを受信するなどして）無許可になると、接続されたすべてのクライアントのネットワーク アクセスが拒否されます。

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 許可済みポート上で、複数のホスト（クライアント）を許可するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x multi-hosts`	802.1x 許可済みポート上で、複数のホスト（クライアント）を許可します。 指定したインターフェイスについて **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ます。
	`Router(config-if)# no dot1x multi-hosts`	ポート上の複数のホストをディセーブルにします。
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 interface type[1] slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス FastEthernet 5/1 上で 802.1x をイネーブルにして、複数のホストを許可する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multi-hosts
```

802.1x 設定のデフォルト値へのリセット

802.1x 設定をデフォルト値にリセットするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
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`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

802.1x ステータスの表示

ルータのグローバルな 802.1x 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の 802.1x 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。

これらの出力におけるフィールドの詳細については、『*Cisco 7600 Series Router Cisco IOS Command Reference*』を参照してください。