CHAPTER 47

IEEE 802.1X ポートベースの認証の設定

この章では、認証されていない装置（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 の『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm

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 ベースのアクセス制御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、スイッチポートに接続する各クライアントを認証したうえで、スイッチや 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 アクセス制御では、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、IEEE 802.1X ポートベースの認証について説明します。

装置の役割

802.1X ポート ベースの認証では、図 47-1 に示すように、ネットワーク上の装置にはそれぞれ特定の役割があります。

図 47-1　802.1X 装置の役割

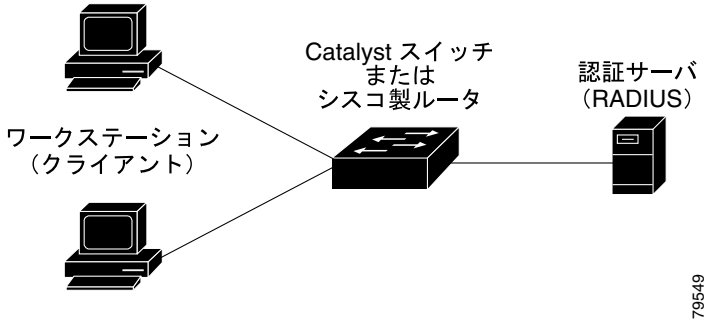


図 47-1 に示す特定の役割は、次のとおりです。

- *クライアント* — LAN およびスイッチ サービスへのアクセスを要求し、スイッチの要求に応答する装置（ワークステーション）。ワークステーション上では、802.1X に準拠するクライアント ソフトウェア（Microsoft Windows XP OS［オペレーティング システム］で提供されるクライアント ソフトウェアなど）が稼働している必要があります（クライアントは、IEEE 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 ポートベースの認証に関しては、次の URL にある「Microsoft Knowledge Base」を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ* — クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチ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。
- *スイッチ*（*認証者*または*バックエンド認証者*とも呼ばれます）— 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アクセスを制御します。スイッチ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。スイッチには、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。

  スイッチが 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。スイッチ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

スイッチ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、スイッチはポートのリンク 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、スイッチは 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（スイッチは通常、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。

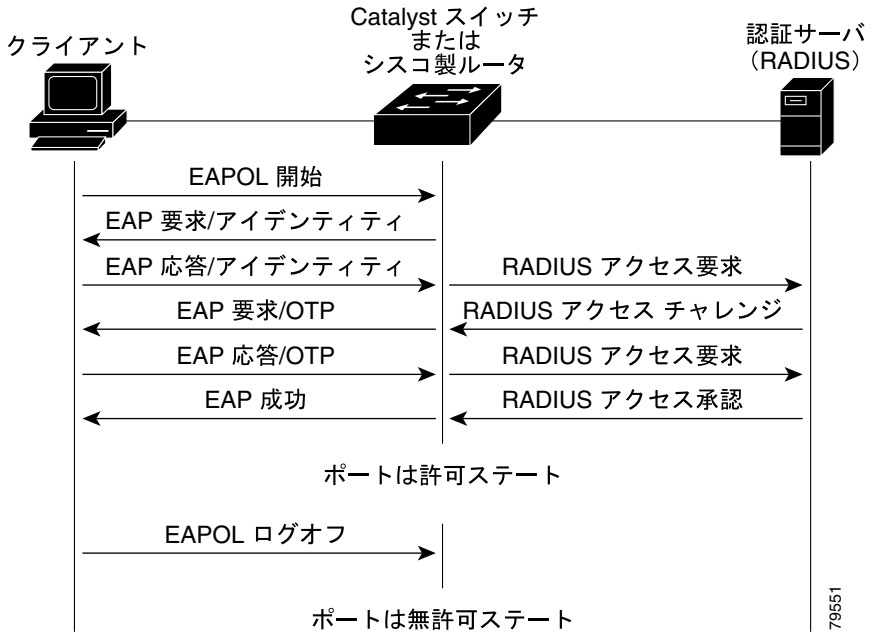
ただし、クライアントがブートアップ時にスイッチから EAP 要求 / アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス装置で 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 要求 / アイデンティティ フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。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.47-4）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、スイッチ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、スイッチ 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.47-4）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 47-2 に、クライアントが RADIUS サーバとの間で One-Time-Password（OTP; ワンタイム パスワード）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 47-2　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

スイッチ ポートのステートは、クライアントがネットワーク アクセスを許可されたかどうかを表します。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 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、スイッチはそのクライアントの識別情報を要求します。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となり、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。

反対に、802.1X 対応のクライアントが、802.1X プロトコルの稼働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。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

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、認証情報の交換を必要とせずに、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との 802.1X ベース認証を行わずに、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 —** クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、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ます。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。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き、または EAPOL 開始フレームを受信したときに、認証プロセスが開始されます。スイッチは、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。スイッチはクライアントの MAC（メディア アクセス制御）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と）、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からの全フレームがポート経由での送受信を許可されます。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、スイッチ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、スイッチ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。

サポートされるトポロジー

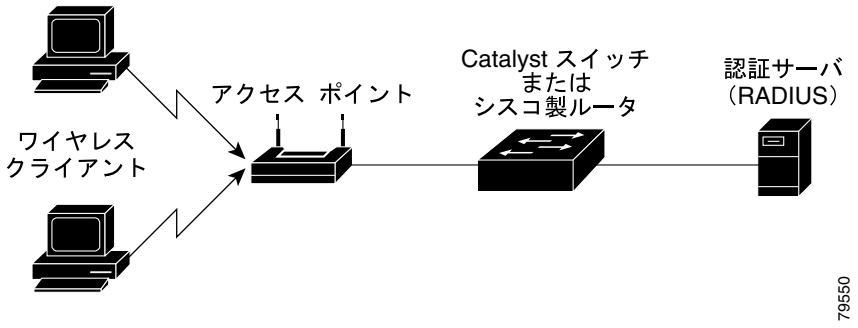
802.1X ポート ベース認証は、次の 2 つのトポロジーでサポートされます。

- 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構成（図 47-1 を参照）では、802.1X 対応のスイッチ ポートには、クライアントが 1 つしか接続できません。スイッチは、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代わったときには、スイッチはポートのリンク 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 47-3 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）、スイッチ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、スイッチに対するクライアントとしての役割を果たします。

図 47-3　ワイヤレス LAN の例



802.1X ポートベースの認証のデフォルト設定

表 47-1 に、802.1X のデフォルト設定を示します。

表 47-1　802.1X のデフォルト設定

機能	デフォルト設定
AAA（Authentication, Authorization, Accounting; 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（force-authorized） （注）　ポートはクライアントとの 802.1X ベース認証を行わずに、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（スイッチ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）
再送信時間	30 秒（スイッチが 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（スイッチ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、スイッチが応答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、サーバに応答を再送信するまでの時間）

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の注意事項および制約事項は、次のとおりです。

- 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。
  - 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方法を説明します。

802.1X ポートベース認証のイネーブル化

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、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}`	設定されている方式リストを消去します。
ステップ 3	`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。
	`Router(config)# no dot1x system-auth-control`	802.1X ポートベースの認証をグローバルに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、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。
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。

	コマンド	目的
ステップ 6	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 7	`Router# show dot1x all`	設定を確認します。 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。

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は、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 つを指定します。
  - **group radius —** すべての RADIUS サーバのリストを使用して認証します。
  - **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、クライアントはスイッチにより自動的に認証されます。

次に、ポート FastEthernet 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
```

スイッチと 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、同一 IP アドレスのサーバ上にある複数の 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（例えば認証など）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、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。
	`Router(config)# no ip radius source-interface`	RADIUS パケットが、以前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}`	スイッチに RADIUS サーバ 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、このコマンドを再度入力します。
	`Router(config)# no radius-server host {hostname | ip_address}`	指定した RADIUS サーバを削除します。
ステップ 3	`Router(config)# radius-server key string`	スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証鍵および暗号鍵を設定します。
ステップ 4	`Router(config)# end`	イネーブル 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、スイッチと 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鍵および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、鍵の途中および末尾のスペースが利用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号に一致している必要があります。
- **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、タイムアウト、再送信回数、暗号鍵の値を、すべての RADIUS サーバに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 の『*Cisco IOS Security Configuration Guide*』Release 12.2、『*Cisco IOS Security Command Reference*』Release 12.2 を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

（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、スイッチの IP アドレス、およびサーバとスイッチ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、スイッチで 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

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、3,600 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することはできません。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.47-12）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、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[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 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 3,600 秒です。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
	`Router(config-if)# no dot1x timeout reauth-period`	デフォルトの再認証の間隔に戻します。
ステップ 4	`Router(config-if)# end`	イネーブル 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、定期的な再認証をイネーブルにし、再認証の間隔を 4,000 秒に設定する例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 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されてい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[1] slot/port`	ポートに接続されているクライアントを手動で再認証します。
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 に接続され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）　認証の初期化により、既存の認証は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、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`	ポートに接続されている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 に接続されているクライアントに対する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

スイッチがクライアントを認証できなかった場合は、スイッチ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、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`	スイッチ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 です。デフォルトは 60 秒です。
	`Router(config-if)# no dot1x timeout quiet-period`	デフォルトの待機時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル 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、スイッチの待機時間を 30 秒に設定する例を示します。

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

スイッチとクライアント間の再送信時間の変更

クライアントはスイッチからの 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。スイッチ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。

スイッチ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、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`	スイッチが 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 です。デフォルトは 30 秒です。
	`Router(config-if)# dot1x timeout tx-period`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル 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、スイッチが 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 秒に設定する例を示します。

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

スイッチ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スイッチに通知します。スイッチがこの通知を受信できなかった場合、スイッチ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。スイッチが通知を待機する時間は、1 ～ 65,535 秒の範囲に指定できます（デフォルトは 30 秒です）。

スイッチ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、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*	スイッチ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。
	`Router(config-if)# no dot1x timeout supp-timeout`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router# end`	イネーブル 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、スイッチ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 秒に設定する例を示します。

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

スイッチ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スイッチに通知します。スイッチがパケット送信後、通知を受信できない場合、スイッチ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。スイッチが通知を待機する時間は、1 ～ 65,535 秒の範囲に指定できます（デフォルトは 30 秒です）。

スイッチから認証サーバへのレイヤ 4 パケットの再送信値を設定するには、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*	スイッチ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。
	`Router(config-if)# no dot1x timeout server-timeout`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル 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、スイッチ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 秒に設定する例を示します。

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

スイッチとクライアント間のフレーム再送信回数の設定

スイッチ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）スイッチが認証プロセスを再開する前に、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。

スイッチ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、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*	スイッチ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。
	`Router(config-if)# no dot1x max-req`	デフォルトの再送信回数に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル 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、スイッチが認証プロセスを再開する前に、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 47-3 に示すように、1 つの 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、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 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。
	`Router(config-if)# dot1x host-mode single-host`	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`	イネーブル 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 で 802.1X をイネーブルにし、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戻すには、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`	イネーブル 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

スイッチのグローバルな 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** イネーブル 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* イネーブル EXEC コマンドを使用します。

この出力に表示されるフィールドの詳細については、『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。