IEEE 802.1x ポートベースの認証の設定

この章では、Catalyst 3750 Metro スイッチで IEEE 802.1x ポートベースの認証を設定する方法について説明します。ホテル、空港、企業のロビーなどに LAN が拡張されると、安全とは言えない環境になりますが、IEEE 802.1x を使用すれば、無許可のデバイス（クライアント）がネットワークへアクセスするのを防ぐことができます。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス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。

IEEE 802.1x ポートベースの認証の概要

IEEE 802.1x 規格は、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について定義し、不正なクライアントが公的にアクセス可能なポートを介して LAN に接続するのを制限します。認証サーバは、スイッチ ポートに接続された各クライアントを認証してから、スイッチまたは LAN が提供するサービスを利用できるようにします。

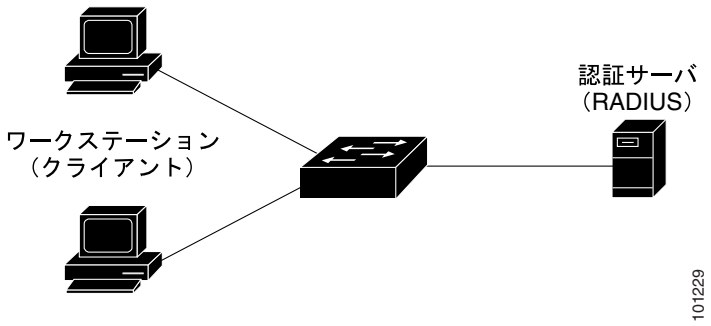
クライアントが認証されるまでは、IEEE 802.1x アクセス制御によって、クライアントに接続したポートを経由する Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、および Spanning-Tree Protocol（STP; スパニングツリー プロトコル）トラフィックのみを許可します。認証に成功すると、通常のトラフィックがポートを通過できます。

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 ポートベース認証を使用すると、ネットワーク内のデバイスには図 9-1 のような特定の役割が割り当てられます。

図 9-1　IEEE 802.1x デバイスの役割



- *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て、スイッチ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では、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります（クライアントは、IEEE 802.1x 規格の *supplicant* になります）。

（注）　Windows XP ネットワーク接続および IEEE 802.1x 認証の問題を解決するには、次の URL にアクセスして Microsoft Knowledge Base Article 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 ID を確認し、クライアントの LAN およびスイッチ サービスへのアクセスを許可する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機能するので、認証サービスはクライアントにトランスペアレントです。このリリースでサポートされている認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を装備した RADIUS セキュリティ システムのみです。これは、Cisco Secure Access Control Server バージョン 3.0 以降で対応しています。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。
- *スイッチ*（エッジ スイッチまたは無線アクセス ポイント）— 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な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間の媒介（プロキシ）として機能し、クライアントに ID 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 RADIUS クライアントが組み込まれています。RADIUS クライアントは、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相互作用の役割を果たします。

  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 フレームが RADIUS 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更や検査が行われず、認証サーバはネイティブのフレーム形式で EAP をサポートする必要があります。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、EAP フレームが残ります。これが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。

  媒介として機能できるデバイスには、Catalyst 3750、Catalyst 3550、Catalyst 2970、Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ、または無線アクセス ポイントがあります。これらのデバイスは、RADIUS クライアントおよび IEEE 802.1x をサポートするソフトウェアを実行している必要があります。

認証の開始とメッセージ交換

スイッチ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上で認証をイネーブルにする場合、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きに、認証を開始する必要があります。次に 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してアイデンティティを要求します（一般に、スイッチ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 1 つまたは複数の認証情報の要求を送信します）。フレームの受信後、クライアントは EAP 応答 / アイデンティティ フレームで応答します。

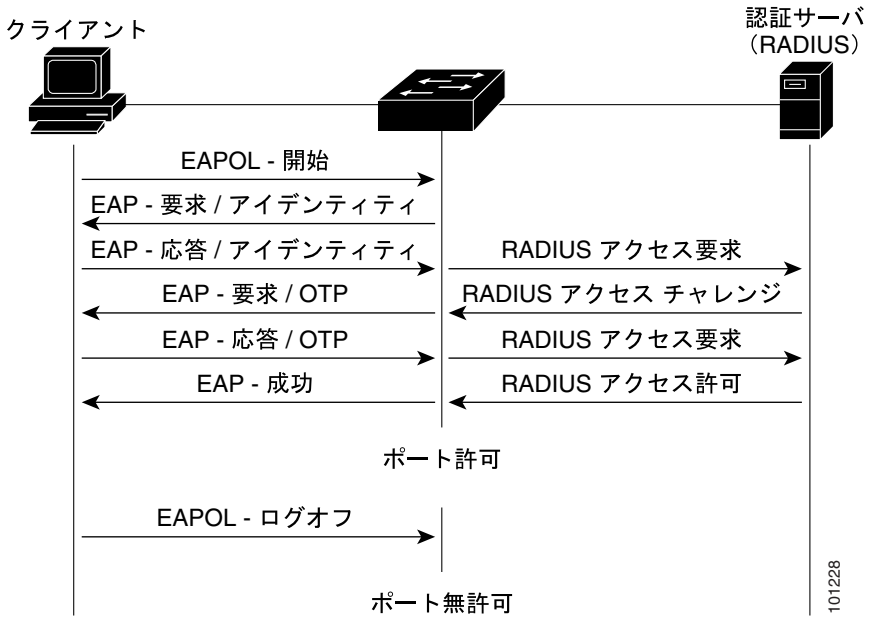
ただし、起動中にクライアントがスイッチから EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは、EAPOL 開始フレームを送信して認証を開始できます。これにより、スイッチはクライアントのアイデンティティを要求するようになります。

（注）　ネットワーク アクセス デバイスで IEEE 802.1x がイネーブルになっていない、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 フレームは廃棄されます。認証の開始を 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、ポートが許可ステートであるものとしてフレームを送信します。許可ステートにあるポートは、事実上クライアントが正常に認証されたということを意味します。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.9-4）を参照してください。

クライアントがそのアイデンティティを供給すると、スイッチ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との間で EAP フレームを受け渡します。認証が成功すると、スイッチのポートは許可された状態になります。詳細については、「許可ステートおよび無許可ステートのポート」（p.9-4）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 9-2 に、RADIUS サーバでクライアントが One Time Password（OTP）認証方式を使用するときに、クライアントによって開始されるメッセージ交換を示します。

図 9-2　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 ポートのステートによって、スイッチはネットワークへのクライアント アクセスを許可できます。ポートは、*無許可*ステートで開始します。このステートにある間は、ポートは、IEEE 802.1x、CDP、STP のプロトコル パケットを除くすべての入力トラフィックおよび出力トラフィックを許可しません。クライアントが正常に認証されると、ポートは*許可*ステートに移行し、そのクライアントへのすべてのトラフィックは通常のフローが許可されます。

IEEE 802.1x をサポートしないクライアントが無許可の IEEE 802.1x ポートに接続している場合は、スイッチがクライアントにアイデンティティを要求します。この場合、クライアントは要求に応答できないため、ポートは無許可ステートのままで、クライアントはネットワーク アクセスが許可されません。

対照的に、IEEE 802.1x 対応クライアントが IEEE 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します。応答が得られなかった場合、クライアントは要求を一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ものとして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 コマンドと以下のキーワードを使用します。

- **force-authorized** — IEEE 802.1x 認証をディセーブルにして、認証情報の交換を要求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 IEEE 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。これがデフォルト設定です。
- **force-unauthorized** — ポートを無許可ステートのままにし、クライアントが認証を試行してもすべて無視します。スイッチは、ポート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** — IEEE 802.1x 認証をイネーブルにして、ポートに無許可ステートで開始させ、EAPOL フレームだけがポート経由で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、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。スイッチは、クライアントのアイデンティティを要求し、クライアントと認証サーバ間で認証メッセージのリレーを開始します。スイッチはネットワークにアクセスしようとする各クライアントを、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（認証サーバから許可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のフレームはすべてそのポート経由で送受信を許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、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、スイッチは要求を再送信できます。指定された試行回数以降もサーバから応答が得られない場合は、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 EAPOL ログオフ メッセージを送信します。これにより、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は、ポートは無許可ステートに戻ります。

IEEE 802.1x アカウンティング

IEEE 802.1x 標準は、ネットワーク アクセスに対するユーザの許可および認証方法を定義しますが、ネットワークの使用状況の追跡は行いません。IEEE 802.1x アカウンティングは、デフォルトではディセーブルに設定されています。IEEE 802.1x アカウンティングをイネーブルにすると、IEEE 802.1x 対応ポートで次のアクティビティをモニタできます。

- ユーザー認証の成功
- ユーザのログオフ
- リンクダウンの発生
- 再認証の成功
- 再認証の失敗

スイッチは 802.1x アカウンティング情報をロギングしません。代わりに、この情報を RADIUS サーバに送信します。RADIUS サーバはアカウンティング メッセージをロギングするよう設定する必要があります。

サポート対象トポロジー

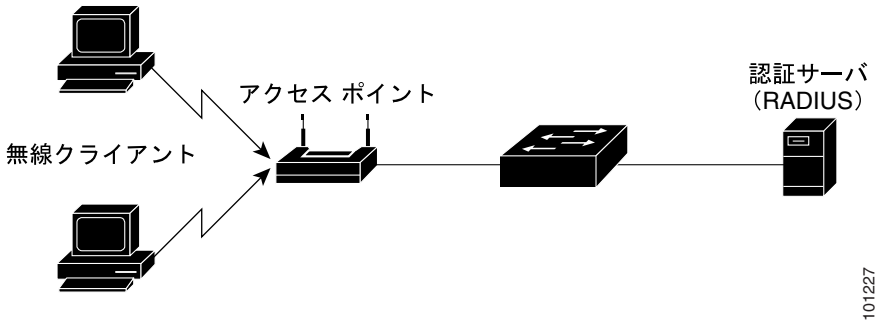
IEEE 802.1x ポートベースの認証は、次の 2 つのトポロジーでサポートされています。

- ポイントツーポイント
- 無線 LAN

ポイントツーポイントによる構成（図 9-1 を参照）では、IEEE 802.1x 対応のスイッチ ポートに接続できるクライアントは 1 台だけです。スイッチは、ポートのリンク ステートがアップに変化すると、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、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 9-3 に、無線 LAN での IEEE 802.1x ポートベースの認証を示します。IEEE 802.1x ポートは複数ホスト ポートとして設定されており、このポートは 1 つのクライアントが認証されるとすぐに許可ステートになります。ポートが許可されると、そのポートに間接的に接続されている残りのホストはすべて、ネットワーク アクセスを許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL ログオフ メッセージを受信する）、スイッチは、接続してい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。このトポロジーでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

図 9-3　無線 LAN の例



IEEE 802.1x とポート セキュリティの使用方法

単一ホスト モードまたは複数ホスト モードのどちらかで、IEEE 802.1x ポートおよびポート セキュリティを設定できます（**switchport port-security** 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にポート セキュリティを設定する必要があります）。ポート上のポート セキュリティと IEEE 802.1x をイネーブルにすると、IEEE 802.1x がポートを認証し、ポート セキュリティがクライアントの MAC アドレスを含むすべての MAC アドレスについてネットワーク アクセスを管理します。この場合、IEEE 802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

たとえば、スイッチにおいて、IEEE 802.1x とポート セキュリティの間には次のような相互作用があります。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

  クライアントが認証されてポート セキュリティが手動で設定された場合、クライアントはセキュア ホスト テーブル内にエントリが保証されます（ポート セキュリティのスタティック エージングがイネーブルになっていない場合）。

  クライアントが認証されてもセキュリティ テーブルがいっぱいの場合は、セキュリティ違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブルの位置は他のホストに取って代わられます。

  最初の認証ホストによってセキュリティ違反が発生した場合、ポートは errdisable となり、すぐにシャットダウンされます。

  ポート セキュリティ違反モードは、セキュリティ違反の動作を判別します。詳細については、「セキュリティ違反」（p.24-10）を参照してください。

- **no switchport port-security mac-address** *mac-address* 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、IEEE 802.1x クライアントのアドレスをポート セキュリティ テーブルから手動で削除した場合は、**dot1x re-authenticate interface** *interface-id* イネーブル EXEC コマンドを使用して IEEE 802.1x クライアントを再認証する必要があります。
- IEEE 802.1x クライアントがログオフすると、ポートが無許可ステートに移行し、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリがクリアされます。この場合、通常の認証が実行されます。
- ポートが管理上の理由からシャットダウンされる場合、ポートは無許可ステートになりすべてのダイナミック エントリはセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN（仮想 LAN）は、単一ホストまたは複数ホスト モードのどちらかで、IEEE 802.1x ポートに同時に設定できます。ポート セキュリティは、voice VLAN identifier（VVID）と port VLAN identifier（PVID; ポート VLAN ID）の両方に適用されます。

スイッチのポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（p.24-9）を参照してください。

IEEE 802.1x と音声 VLAN ポートの使用方法

音声 VLAN ポートは、2 つの VLAN ID に関連付けられた特殊なアクセス ポートです。

- IP Phone の入出力音声トラフィックを搬送するための VVID。VVID は、ポートに接続されている IP Phone を設定するために使用されます。
- IP Phone を通じてスイッチと接続しているワークステーションの入出力データ トラフィックを搬送するための PVID。PVID は、ポートのネイティブ VLAN です。

音声 VLAN に設定された各ポートに、PVID と VVID が関連付けられます。この設定によって、音声トラフィックとデータ トラフィックを異なる VLAN に分離できます。IP Phone はポートの許可または無許可ステートに関わらず、音声トラフィック用として VVID を使用します。これによって、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

単一ホスト モードをイネーブルにすると、その VVID によって複数の IP Phone が許可されます。ただし、PVID で許可されるのは、1 つの IEEE 802.1x クライアントのみです。複数ホスト モードをイネーブルにする場合に IEEE 802.1x ユーザがプライマリ VLAN で認証されている場合、IEEE 802.1x 認証がプライマリ VLAN で成功すれば、音声 VLAN へ無制限にクライアントを追加できます。

リンクが存在していれば、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取ると、デバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスからの CDP メッセージをリレーしません。そのため、複数の IP Phone が直列で接続されても、スイッチは自身に直接接続された IP Phone しか認識しません。音声 VLAN ポートで IEEE 802.1x をイネーブルにすると、2 ホップ以上離れた認識されていない IP Phone からのパケットはスイッチにより廃棄されます。

IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同等であるポート VLAN を設定できません。

音声 VLAN の詳細については、第 15 章「音声 VLAN の設定」を参照してください。

IEEE 802.1x と VLAN 割り当ての使用方法

スイッチは IEEE 802.1x と VLAN 割り当てをサポートしています。ポートの IEEE 802.1x 認証が成功すると、RADIUS サーバは、スイッチ ポートを設定するために VLAN 割り当てを送信します。RADIUS サーバのデータベースは、ユーザ名 /VLAN マッピングを維持します。このマッピングでは、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てています。この機能を使用して、特定ユーザのネットワーク アクセスを制限できます。

スイッチと RADIUS サーバを設定する場合、IEEE 802.1x と VLAN 割り当てには次の特性があります。

- RADIUS サーバが VLAN を割り当てていないか、または IEEE 802.1x 許可がディセーブルの場合、認証が成功してからポートがアクセス VLAN に設定されます。
- 802.1x 認証がイネーブルだが、RADIUS サーバからの VLAN 情報が有効でない場合には、ポートは無許可ステートに戻り、設定済みのアクセス VLAN 内に留まります。これにより、設定エラーによって不適切な VLAN 上にポートが突然現れることを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN の指定、誤った VLAN ID、存在しないまたは内部（ルーテッド ポートの）の VLAN ID、あるいは音声 VLAN ID への割り当て試行、などがあります。
- IEEE 802.1x 許可がイネーブルで RADIUS サーバからのすべての情報が有効の場合、ポートは認証のあとで指定した VLAN に配置されます。
- IEEE 802.1x ポートで複数ホスト モードがイネーブルの場合は、すべてのホストが最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定された）に配置されます。
- IEEE 802.1x とポート セキュリティがポート上でイネーブルの場合は、そのポートは RADIUS サーバによって割り当てられた VLAN に配置されます。
- IEEE 802.1x がポートでディセーブルの場合は、設定済みのアクセス VLAN に戻ります。

ポートが強制許可（force authorized）、強制無許可（force unauthorized）、無許可、シャットダウンのいずれかのステートの場合、そのポートは設定済みのアクセス VLAN に配置されます。

IEEE 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置された場合、ポートのアクセス VLAN 設定への変更は反映されません。

VLAN 割り当て機能付きの IEEE 802.1x は、トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）を使用したダイナミック アクセス ポート割り当てではサポートされていません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）許可をイネーブルにし、RADIUS サーバからのポート設定を可能にします。
- IEEE 802.1x をイネーブルにします。（VLAN 割り当て機能は、アクセス ポートに IEEE 802.1x が設定されると、自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに戻さなければなりません。
  - [64] tunnel-type = VLAN
  - [65] tunnel-medium-type = 802
  - [81] tunnel-private-group-ID = VLAN 名または VLAN ID

  アトリビュート [64] の値は、*VLAN*（type 13）である必要があります。アトリビュート [65] の値は、*802*（type 6）である必要があります。アトリビュート [81] には、IEEE 802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」（p.8-30）を参照してください。

IEEE 802.1x とゲスト VLAN の使用方法

スイッチ上の各 IEEE 802.1x ポートにゲスト VLAN を設定し、クライアントへのサービスを限定できます（たとえば、IEEE 802.1x クライアントのダウンロード方法）。これらのクライアントは IEEE 802.1x 認証対応のシステムにアップグレードされている場合があり、Windows 98 システムなどの一部のホストは IEEE 802.1x に対応していない場合があります。

認証サーバが EAP 要求 / アイデンティティ フレームへの応答を受信しなかった場合は、IEEE 802.1x 非対応のクライアントはポートのゲスト VLAN（設定されている場合）に配置されます。ただし、サーバは、ネットワークへの認証アクセスに失敗した IEEE 802.1x 対応のクライアントは許可しません。

スイッチは EAPOL パケット履歴を保持しています。EAPOL パケットがリンクのライフタイム中にインターフェイス上で検出されると、スイッチはそのインターフェイスに接続されたデバイスが IEEE 802.1x 対応のサプリカントであると判断し、インターフェイスがゲスト VLAN ステートには移行しません。EAPOL 履歴は、インターフェイス リンク ステータスがダウンになると、クリアされます。EAPOL パケットがインターフェイス上で検出されない場合は、インターフェイスがゲスト VLAN ステートに移行します。

（注）　インターフェイスがゲスト VLAN ステートに移行したあとに EAPOL パケットが回線上で検出された場合は、インターフェイスは無許可ステートに戻り、IEEE 802.1x 認証が再開されます。

スイッチ ポートがゲスト VLAN に移動された場合は、無制限にホストにアクセスが許可されます。IEEE 802.1x 対応のホストが、ゲスト VLAN が設定されているポートと同じポートに結合すると、そのポートはユーザ設定済みのアクセス VLAN 内 で無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、単一ホストまたは複数ホスト モードの IEEE 802.1x ポートでサポートされています。

RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定することができます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

詳細については、「ゲスト VLAN の設定」（p.9-21）を参照してください。

IEEE 802.1x と制限 VLAN の使用方法

スイッチ上の各 IEEE 802.1x ポートに制限 VLAN（*認証不可 VLAN* と呼ばれることもあります）を設定し、制限されたサービスをゲスト VLAN にアクセスできないクライアントに提供できます。これらのクライアントは IEEE 802.1x 準拠であり、認証プロセスに失敗しているため、別の VLAN にアクセスできません。制限 VLAN により、認証サーバで有効な証明書を持たないユーザ（一般的には企業への訪問者）が、制限されたサービス セットにアクセスできます。管理者は、制限 VLAN で使用可能なサービスを管理できます。

（注）　同じサービスを両方のタイプのユーザに提供する場合は、同じ VLAN をゲスト VLAN と制限 VLAN の両方として設定できます。

この機能を使用しないと、クライアントが無限に認証失敗を繰り返してしまい、スイッチ ポートがスパニングツリー ブロッキング ステートのままになります。この機能を使用すると、指定した回数（デフォルト値は 3 回）の認証試行のあとは制限 VLAN となるよう、スイッチ ポートを設定することができます。

クライアントの認証失敗回数は、認証者によりカウントされます。この回数が設定された最高失敗回数を超えると、ポートは制限 VLAN に移動します。認証失敗回数は、RADIUS サーバが *EAP 障害*、または EAP パケットのない空の応答を返したときにカウントされます。ポートが制限 VLAN に移動したときに、認証試行カウンタはリセットされます。

認証に失敗したユーザは、次回の再認証試行まで制限 VLAN のままとなります。制限 VLAN のポートは設定された間隔（デフォルトは 60 秒）で再認証を試行します。再認証に失敗すると、ポートは制限 VLAN のままです。再認証に成功した場合は、ポートが、設定された VLAN または RADIUS サーバにより送信された VLAN のいずれかに移動します。再認証はディセーブルにすることができます。ディセーブルにすると、認証プロセスを再開するためには、ポートが *リンク ダウン*または *EAP ログオフ* イベントを受信する必要があります。クライアントがハブ経由で接続している場合は、再認証をイネーブルのままにしておくことを推奨します。クライアントがハブから接続を切断すると、ポートが *リンク ダウン*と *EAP ログオフ*のいずれのイベントも受信しない可能性があります。

ポートは制限 VLAN に移動したあとに、EAP 失敗メッセージではなく、模擬 EAP 成功メッセージをクライアントに送信します。これにより、クライアントが無限に認証を試行することを防止します。一部のクライアント（Windows XP を実行するデバイスなど）では、EAP の成功を伴わない DHCP を実装できません。

制限 VLAN は、単一ホスト モードの IEEE 802.1x ポートおよびレイヤ 2 ポートでのみサポートされています。

RSPAN VLAN、プライマリ プライベート VLAN、および音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x 制限 VLAN として設定できます。制限 VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

この機能はポート セキュリティで機能します。ポートが認証されると同時に、MAC アドレスがポート セキュリティに提供されます。ポート セキュリティが MAC アドレスを許可しない場合、またはセキュア アドレスの数が最大値に達した場合は、ポートが無許可および errdisable となります。

ダイナミック ARP 検査、DHCP スヌーピング、および IP ソース ガードなどの他のポート セキュリティ機能は、制限 VLAN 上で独立して設定できます。

IEEE 802.1x とユーザ単位 ACL の使用方法

ユーザ単位の Access Control List（ACL; アクセス制御リスト）をイネーブルにして、IEEE 802.1x 認証ユーザが異なるレベルのネットワーク アクセスやサービスを使用可能にすることができます。RADIUS サーバは、IEEE 802.1x ポートに接続されているユーザを認証すると、ユーザ ID に基づいて ACL アトリビュートを検索し、それらをスイッチへ送信します。スイッチは、ユーザ セッションの間、それらのアトリビュートを IEEE 802.1x ポートに適用します。スイッチは、セッションの終了後、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位の ACL 設定を削除します。スイッチは、RADIUS 固有の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ルータ ACL および入力ポート ACL を設定できます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するポートに適用する場合は、VLAN インターフェイスに適用する入力済みのルータ ACL よりもポート ACL が優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信されるルーテッド パケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、Vendor Specific Attribute（VSA）などのユーザ単位アトリビュートをサポートします。これらの VSA は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向でのみサポートされます。スイッチは、入力方向でのみ VSA をサポートします。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文形式のみを使用して、RADIUS サーバに保存するユーザ単位の設定を定義します。RADIUS サーバから定義が渡される場合は、拡張命名規則を使用して作成されます。ただし、フィルタ ID アトリビュートを使用する場合、標準 ACL を示すことができます。

フィルタ ID アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、その後に入力フィルタリングか出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合は、アクセス リストがデフォルトで発信 ACL に適用されます。スイッチ上では Cisco IOS アクセス リストのサポートが限定されているため、フィルタ ID アトリビュートは番号が 1 ～ 199 および 1300 ～ 2699 までの IP ACL（IP 標準 ACL と IP 拡張 ACL）でのみサポートされています。

1 つのポートがサポートする IEEE 802.1x 認証ユーザは 1 ユーザのみです。複数ホスト モードがポートでイネーブルの場合、ユーザ単位 ACL アトリビュートは関連ポートでディセーブルです。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字です。

ベンダー固有のアトリビュートの例については、「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」（p.8-30）を参照してください。ACL の設定の詳細については、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのポート設定を可能にします。
- IEEE 802.1x をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートを単一ホスト モードに設定します。

IEEE 802.1x 認証の設定

ここでは、スイッチに 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。

IEEE 802.1x のデフォルト設定

表 9-1 に、IEEE 802.1x のデフォルト設定を示します。

表 9-1　IEEE 802.1x のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし • 1812 • 指定なし
スイッチの IEEE 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized） ポートは、クライアントの IEEE 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	3600 秒
再認証数	2 回（ポートが無許可ステートに変わるまでスイッチが認証プロセスを再起動する回数）
待機時間	60 秒（クライアントとの認証交換が失敗したあと、スイッチが待機ステートにとどまる秒数）
再送信時間	30 秒（スイッチが、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ち、要求を再送信するまでの秒数）

表 9-1　IEEE 802.1x のデフォルト設定（続き）

機能	デフォルト設定
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）
ホスト モード	単一ホスト モード
ゲスト VLAN	指定なし
制限 VLAN	指定なし
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、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、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。この値は設定不可能）

IEEE 802.1x 設定時の注意事項

IEEE 802.1x 認証の設定時の注意事項は次のとおりです。

- IEEE 802.1x がイネーブルに設定されていると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- IEEE 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、音声 VLAN ポート、レイヤ 3 ルーテッド ポート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 IEEE 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、IEEE 802.1x はイネーブルになりません。IEEE 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、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック ポート — ダイナミック モードのポートは、近接ポートとネゴシエーションしてトランク ポートになる可能性があります。ダイナミック ポートで IEEE 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、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート — ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで IEEE 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、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミック VLAN 割り当てに変更しようとすると、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel ポート — EtherChannel のアクティブ メンバーであるポートは IEEE 802.1x ポートとして設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。

    （注）　Cisco IOS Release 12.2(25)EY より前のソフトウェア リリースでは、まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。

  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）宛先ポート — SPAN または RSPAN 宛先ポートであるポートで IEEE 802.1x をイネーブルにすることができます。ただし、SPAN または RSPAN 宛先ポートとして削除するまでは、IEEE 802.1x はディセーブルになります。SPAN または RSPAN 送信元ポートでは、IEEE 802.1x をイネーブルにすることができます。

- RSPAN VLAN または音声 VLAN を除き、任意の VLAN を IEEE 802.1x ゲスト VLAN として設定することができます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。
- IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同等であるポート VLAN を設定できません。
- VLAN 割り当て機能付きの IEEE 802.1x は、トランク ポート、ダイナミック ポート、または VMPS を使用したダイナミック アクセス ポート割り当てではサポートされていません。
- RSPAN VLAN、プライマリ プライベート VLAN、および音声 VLAN を除き、任意の VLAN を IEEE 802.1x 制限 VLAN として設定できます。制限 VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。
- プライベート VLAN ポートでは IEEE 802.1x の設定ができますが、IEEE 802.1x とポート セキュリティ、音声 VLAN、ゲスト VLAN、制限 VLAN、またはユーザ単位 ACL をともに設定することはできません。

IEEE 802.1x 認証の設定

IEEE 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順番と認証方式を記述したものです。

ソフトウェアは、1 番めにリストされた方式を使用して、ユーザを認証します。その方式が応答に失敗すると、ソフトウェアは方式リストの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行するまで続きます。このサイクルのいずれかの地点で認証が失敗すると、認証プロセスは停止し、他の認証方式が試行されることはありません。

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

IEEE 802.1x ポートベースの認証を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	説明
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	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1* [*method2...*]	IEEE 802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定されていない場合に使用され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の状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 次のキーワードを最低 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。スイッチは、クライアントから提供される情報を使用せずに、クライアントを自動的に認証します。
ステップ 4	**dot1x system-auth-control**	スイッチ上で IEEE 802.1x 認証をグローバルにイネーブルにします。

	コマンド	説明
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 （注）　ユーザ単位 ACL の場合は、単一ホスト モードを設定する必要があります。これはデフォルト設定です。
ステップ 6	**interface** *interface-id*	クライアントに接続されたポートの中で IEEE 802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。 機能の相互作用の詳細については、「IEEE 802.1x 設定時の注意事項」（p.9-13）を参照してください。
ステップ 8	**end**	イネーブル EXEC モードに戻ります。
ステップ 9	**show dot1x**	設定を確認します。
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。

AAA をディセーブルにするには、**no aaa new-model** 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。IEEE 802.1x AAA 認証をディセーブルにするには、**no aaa authentication dot1x** {**default** | *list-name*} 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。IEEE 802.1x AAA 許可をディセーブルにするには、**no aaa authorization** 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。スイッチ上で IEEE 802.1x 認証をディセーブルにするには、**no dot1x system-auth-control** 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。

次に、ポート上で AAA および IEEE 802.1x をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet1/0/1
Switch(config)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

スイッチと RADIUS サーバ間通信を設定する方法

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、あるいは IP アドレスと特定の UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合わせにより、一意の識別子が作成され、これにより、サーバ上の同一の IP アドレスの複数の UDP ポートに RADIUS 要求を送信できます。同一の 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）を設定している場合、あとから設定されたホスト エントリは、最初のエントリの代替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されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	説明
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	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* | *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。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 で、指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。 （注）　先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されるため、鍵は必ず **radius-server host** コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。この鍵は、RADIUS デーモン上で使用する暗号と一致する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し入力してください。
ステップ 3	**end**	イネーブル EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
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。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} 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。

次に、IP アドレスが 172.20.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号化鍵を RADIUS サーバ上の鍵と *rad123* に設定する例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化鍵の値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**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、「すべての RADIUS サーバに対する設定」（p.8-30）を参照してください。

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。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー ストリングです。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。

定期的な再認証の設定

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て、その発生間隔を指定できます。再認証の間隔を指定しなかった場合は、再認証は 3600 秒ごとに行われます。

クライアントの定期的な再認証をイネーブルにして、再認証を試行する間隔（秒数）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。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x reauthentication**	デフォルトではディセーブルに設定されている定期的な再認証をイネーブルにします。
ステップ 4	**dot1x timeout reauth-period** *seconds*	再認証を試行する間隔（秒数）設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 3600 秒です。 このコマンドがスイッチの動作に影響するのは、定期的な再認証がイネーブルに設定されている場合だけです。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
ステップ 6	**show dot1x interface** *interface-id*	設定を確認します。
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。

定期的な再認証をディセーブルにするには、**no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの再認証試行間隔に戻すには、**no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、定期的再認証をイネーブルにし、再認証を試行する間隔を 4000 秒に設定します。

```
Switch(config-if)# dot1x reauthentication
Switch(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

dot1x re-authenticate interface *interface-id* イネーブル EXEC コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする場合は、「定期的な再認証の設定」（p.9-17）を参照してください。

次に、ポートに接続したクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface fastethernet1/0/1
```

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、スイッチは一定時間アイドル状態を続け、その後再試行します。このアイドル時間は、**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドによって制御します。クライアントが無効なパスワードを提供したため、クライアントの認証に失敗す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短縮できます。

待機時間を変更するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout quiet-period** *seconds*	クライアントとの認証交換が失敗したあと、スイッチが待機ステートになる秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 60 秒です。
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	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**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。

デフォルトの待機時間に戻すには、**no dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチ上の待機時間を 30 秒に設定する例を示します。

```
Switch(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、EAP 応答 / アイデンティティ フレームで応答します。スイッチはこの応答を受信しなかった場合、一定時間（再送信時間）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および認証サーバの動作に問題があるなど、異常な状況を調整する場合以外は行わないようにしてください。

スイッチがクライアントの通知を待機する時間を変更するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチが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 15 ～ 65535 秒で、デフォルトは 30 秒です。
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	**show dot1xinterface** *interface-id*	設定を確認します。
ステップ 6	**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。

デフォルトの再送信時間に戻すには、**no dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが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ち、要求を再送信するまでの秒数を 60 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

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の変更だけでなく、（応答を受信しなかった場合）認証プロセスを再開するまでに、スイッチがクライアントに 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および認証サーバの動作に問題があるなど、異常な状況を調整する場合以外は行わないようにしてください。

スイッチ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、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-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、デフォルトは 2 です。
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	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**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。

デフォルトの再送信回数に戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、認証プロセスを再開するまでに、スイッチが EAP 要求 / アイデンティティ フレームを送信する回数を 5 に設定する例を示します。

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

再認証回数の設定

2 回（ポートが無許可ステートに変わるまでスイッチが認証プロセスを再起動する回数）

（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および認証サーバの動作に問題があるなど、異常な状況を調整する場合以外は行わないようにしてください。

再認証回数を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	ポートが無許可ステートに変わるまでスイッチが認証プロセスを再起動する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
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	**show dot1x interface** ***interface-id***	設定を確認します。
ステップ 6	**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。

デフォルトの再認証回数に戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが無許可ステートに変わるまで、スイッチが認証プロセスを再起動する回数を 4 に設定する例を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

ホスト モードの設定

IEEE 802.1x ポートは、単一ホスト モードまたは複数ホスト モードに設定できます。単一ホスト モードでは、IEEE 802.1x ポートで 1 台のホストのみが許可されます。ホストが認証されると、ポートは許可ステートになります。ホストがポートから切断されると、ポートは無許可ステートになります。認証済みのホスト以外のホストからのパケットは廃棄されます。

図 9-3 のように、複数のホストを 1 つの IEEE 802.1x 対応ポートに接続できます。このモードでは、接続ホストのいずれか 1 つだけが許可されれば、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（再認証が失敗するか EAPOL ログオフ メッセージを受信した場合）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。

複数ホスト モードがイネーブルの場合、IEEE 802.1x をポートの認証に使用し、クライアントを含むすべての MAC アドレスへのネットワーク アクセスをポート セキュリティが管理します。

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	複数のホストを間接的に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x host-mode multi-host**	IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可します。 指定されたポートについて、**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。

	コマンド	説明
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	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**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。

ポート上の複数ホストをディセーブルにするには、**no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で IEEE 802.1x をイネーブルにして、複数ホストを許可する例を示します。

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAP 要求 / アイデンティティ フレームへの応答を受信しなかった場合に、IEEE 802.1x 非対応のクライアントがゲスト VLAN に配置されます。IEEE 802.1x 対応であっても、認証に失敗したクライアントにはネットワークへのアクセスが許可されません。スイッチは、単一ホスト モードまたは複数ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.9-13）を参照してください。
ステップ 3	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定できます。
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	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**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。

ゲスト VLAN をディセーブル化し削除するには、**no dot1x guest-vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートが現在、ゲスト VLAN で許可されている場合は、ボートは無許可ステートに戻ります。

次に、ポート上で VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# dot1x guest-vlan 2
```

制限 VLAN の設定

スイッチで制限 VLAN を設定した場合は、認証サーバが有効なユーザ名とパスワードを受信しないと、IEEE 802.1x 準拠のクライアントが制限 VLAN に移動します。スイッチは、単一ホスト モードでのみ制限 VLAN をサポートします。

制限 VLAN を設定するには、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポート タイプについては、10 ～ 18 ページの「IEEE 802.1x 設定時の注意事項」を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブ VLAN を IEEE 802.1x 制限 VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、および音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x 制限 VLAN として設定することができます。
ステップ 6	**end**	イネーブル EXEC モードに戻ります。
ステップ 7	**show dot1x interface** *interface-id*	（任意）設定を確認します。
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。

制限 VLAN をディセーブル化し削除するには、**no dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは、無許可ステートに戻ります。

次に、*VLAN 2* を IEEE 802.1x 制限 VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x auth-fail vlan 2
```

dot1x auth-fail max-attempts 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、ユーザが制限 VLAN に割り当てられるまでの認証失敗回数の最大値を設定します。指定できる認証失敗回数の範囲は 1 ～ 3 で、デフォルト値は 3 回です。

許可される認証失敗回数を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポート タイプについては、10 ～ 18 ページの「IEEE 802.1x 設定時の注意事項」を参照してください。

	コマンド	説明
ステップ 3	**switchport mode access**	ポートをアクセス モードに設定します。
	または	または
	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブ VLAN を IEEE 802.1x 制限 VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、および音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x 制限 VLAN として設定することができます。
ステップ 6	**dot1x auth-fail max-attempts** *max attempts*	ポートが制限 VLAN に移動する前に許可される認証失敗回数を指定します。指定できる範囲は 1 ～ 3 で、デフォルト値は 3 です。
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	**show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 9	**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。

デフォルトの回数に戻すには、**no dot1x auth-fail max attempts** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが制限 VLAN に移動するまでに許可される認証失敗回数として、*2* を設定する例を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts
```

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リセットするには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x default**	設定変更可能な IEEE 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 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**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。

IEEE 802.1x アカウンティングの設定

AAA システム アカウンティングと IEEE 802.1x アカウンティングをイネーブルにすることにより、ロギング用にシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用しているため、悪いネットワーク状態によりアカウンティング メッセージが失われる場合があります。設定したアカウンティング要求の再送信回数を超えても、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合は、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

停止メッセージが正常に送信されない場合は、次のメッセージが表示されます。

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

（注） 開始、停止、暫定的な更新メッセージ、タイム スタンプのロギングなどのアカウンティング タスクを実行するように RADIUS サーバを設定する必要があります。この機能をオンにするには、RADIUS サーバの Network Configuration タブで「Update/Watchdog packets from this AAA client」のロギングをイネーブルにします。次に、RADIUS サーバの System Configuration タブで「CVS RADIUS Accounting」をイネーブルにします。

AAA をスイッチでイネーブルにしたあとで IEEE 802.1x アカウンティングを設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
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	**aaa accounting dot1x default start-stop group radius**	すべての RADIUS サーバのリストを使用して、IEEE 802.1x アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting system default start-stop group radius**	（任意）（すべての RADIUS サーバのリストを使用して）システム アカウンティングをイネーブルにし、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
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	**show running-config**	設定を確認します。
ステップ 6	**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。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** イネーブル EXEC コマンドを使用します。

次に、IEEE 802.1x アカウンティングを設定する例を示します。最初のコマンドは RADIUS サーバを設定し、1813 をアカウンティング用の UDP ポートに指定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key
rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

IEEE 802.1x 統計情報およびステータスの表示

すべてのポートの IEEE 802.1x 統計情報を表示するには、**show dot1x all statistics** イネーブル EXEC コマンドを使用します。特定のポートの IEEE 802.1x 統計情報を表示するには、**show dot1x statistics interface** *interface-id* イネーブル EXEC コマンドを使用します。

スイッチについて IEEE 802.1x 管理および動作のステータスを表示するには、**show dot1x all** イネーブル EXEC コマンドを使用します。特定のポートの IEEE 802.1x 管理および動作の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。

表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。