



IEEE 802.1X ポートベースの認証の設定

この章では、Catalyst 3550 スイッチで IEEE 802.1X ポートベースの認証を設定して、不正なデバイス（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方法について説明します。



(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、このリリースに対応するスイッチのコマンドリファレンス、および『Cisco IOS Security Command Reference』 Release 12.2 の「RADIUS Commands」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 \(p.8-2\)](#)
- [IEEE 802.1X 認証の設定 \(p.8-13\)](#)
- [IEEE 802.1X 統計情報およびステータスの表示 \(p.8-28\)](#)

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、適切に認証されていないかぎり、許可のない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 に接続するのを防ぎます。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) トラフィックだけが許可されます。認証が成功すると、通常のトラフィックがポートを通過できます。

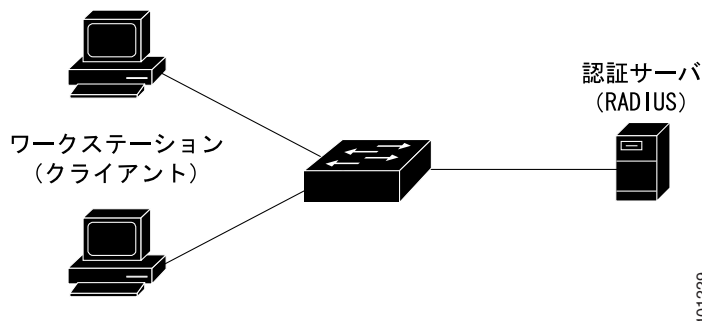
ここでは、IEEE 802.1X ポートベース認証について説明します。

- [デバイスの役割 \(p.8-2\)](#)
- [認証の開始とメッセージ交換 \(p.8-3\)](#)
- [許可状態および無許可状態のポート \(p.8-4\)](#)
- [IEEE 802.1X アカウンティング \(p.8-5\)](#)
- [IEEE 802.1X アカウンティング AV のペア \(p.8-6\)](#)
- [IEEE 802.1X ホスト モード \(p.8-7\)](#)
- [IEEE 802.1X とポート セキュリティの使用法 \(p.8-7\)](#)
- [IEEE 802.1X と音声 VLAN ポートの使用法 \(p.8-8\)](#)
- [IEEE 802.1X と VLAN 割り当ての使用法 \(p.8-9\)](#)
- [IEEE 802.1X とゲスト VLAN の使用法 \(p.8-10\)](#)
- [IEEE 802.1X と Wake-on-LAN の使用法 \(p.8-10\)](#)
- [IEEE 802.1X とユーザ単位の ACL の使用法 \(p.8-12\)](#)

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は図 8-1 のような特定の役割が割り当てられます。

図 8-1 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、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は、Microsoft Windows XP オペレーティングシステムに付属しているような IEEE 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 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、クライアントから 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。このリリースでは、認証サーバとして Extensible Authentication Protocol (EAP) 拡張機能を備えた RADIUS セキュリティ システムのみ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 以降で使用可能です。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されず、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。

媒介として機能するデバイスには、Catalyst 3750、Catalyst 3650、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か、または定期的にポートがアップで未認証状態の間に、認証を開始します。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アイデンティティを要求します。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。

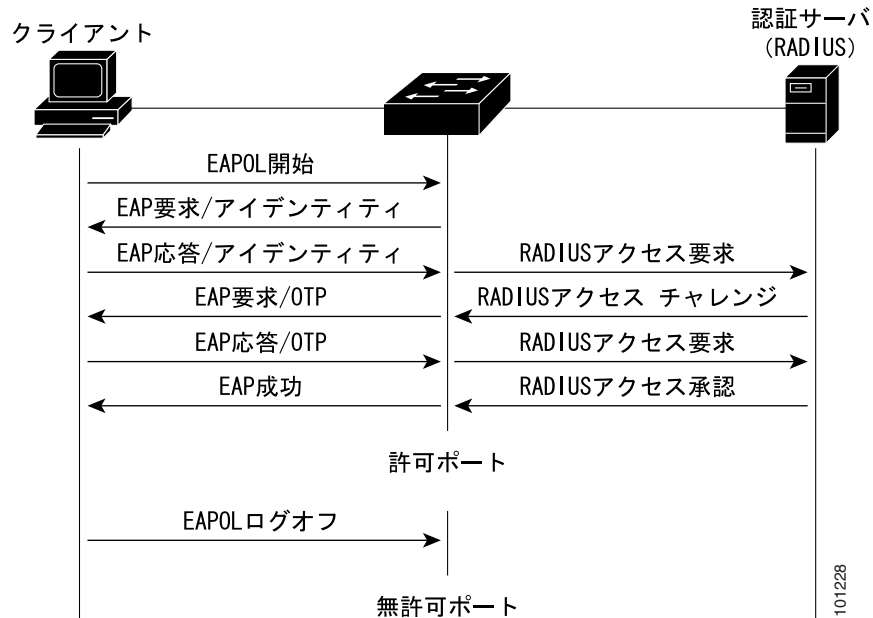


(注) ネットワーク アクセス デバイスで IEEE 802.1X がイネーブルになっていないかサポートされていない場合は、クライアントからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもクライアントが EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは、ポートが許可状態であるものとしてフレームを送信します。許可状態にあるポートは、事実上クライアントが正常に認証されたということです。詳細については、「許可状態および無許可状態のポート」(p.8-4) を参照してください。

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.8-4) 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 8-2 に、RADIUS サーバで One-Time-Password (OTP; ワンタイム パスワード) 認証方式を使用する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 8-2 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、スイッチがクライアントにネットワークのアクセスを許可します。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、音声 VLAN ポートに設定されていないポートは、IEEE 802.1X、CDP、および STP パケットを除いてすべての入力トラフィックおよび出力トラフィックが許可されていません。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。ポートが音声 VLAN ポートに設定されている場合、クライアントが正常に認証される前にポートは Voice over IP (VoIP) トラフィックおよび IEEE 802.1X プロトコル パケットを許可します。

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、スイッチは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ので、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 標準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。応答が得られないので、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** ポートは無許可ステートのままにし、クライアントが認証を試みてもすべて無視します。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できません。
- **auto** IEEE 802.1X 認証をイネーブルにして、ポートを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 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のある後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 規格には、ネットワーク アクセスに対するユーザの許可と認証方法は定義されていますが、ネットワーク使用率を監視するものではありません。IEEE 802.1X アカウンティングは、デフォルトで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して、IEEE 802.1X 対応ポートで次の内容をモニタできます。

- 正常なユーザ認証
- ユーザのログ オフ
- リンク ダウンの発生
- 正常な再認証の発生
- 再認証の失敗

スイッチは IEEE 802.1X アカウンティング情報を記録しません。その代わりに、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 メッセージを記録するように設定する必要があります。

IEEE 802.1X アカウンティング AV のペア

RADIUS サーバに送信される情報は、Attribute-Value (AV) のペア形式で表示されます。AV ペアは異なるアプリケーションにデータを提供します (たとえば、課金アプリケーションは RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性にある情報を必要とする場合があります)。

AV ペアは IEEE 802.1X アカウンティング用に設定されたスイッチによって自動的に送信されます。次の 3 タイプの RADIUS アカウンティング パケットがスイッチによって送信されます。

- START 新規ユーザ セッションの開始時に送信されます。
- INTERIM アップデートのため、既存のセッション中に送信されます。
- STOP セッション終了時に送信されます。

表 8-1 に、スイッチによって送信されたときの AV ペアを示します。

表 8-1 アカウンティング AV ペア

アトリビュート番号	AV ペア名	START	INTERIM	STOP
アトリビュート [1]	User-Name	有効	有効	有効
アトリビュート [4]	NAS-IP-Address	有効	有効	有効
アトリビュート [5]	NAS-Port	有効	有効	有効
アトリビュート [8]	Framed-IP-Address	無効	以下の条件でのみ有効 ¹	以下の条件でのみ有効 ¹
アトリビュート [25]	Class	有効	有効	有効
アトリビュート [30]	Called-Station-ID	有効	有効	有効
アトリビュート [31]	Calling-Station-ID	有効	有効	有効
アトリビュート [40]	Acct-Status-Type	有効	有効	有効
アトリビュート [41]	Acct-Delay-Time	有効	有効	有効
アトリビュート [42]	Acct-Input-Octets	無効	無効	有効
アトリビュート [43]	Acct-Output-Octets	無効	無効	有効
アトリビュート [44]	Acct-Session-ID	有効	有効	有効
アトリビュート [45]	Acct-Authentic	有効	有効	有効
アトリビュート [46]	Acct-Session-Time	無効	無効	有効
アトリビュート [49]	Acct-Terminate-Cause	無効	無効	有効
アトリビュート [61]	NAS-Port-Type	有効	有効	有効

1. Framed-IP-Address の AV ペアは、有効な動的ホスト制御プロトコル (DHCP) バインディングが DHCP スヌーピング バインディング テーブルのホストに存在する場合にのみ、送信されます。

`debug radius accounting` イネーブル EXEC コマンドを入力すると、スイッチによって送信される AV ペアを表示できます。このコマンドの詳細については、次の URL の『Cisco IOS Debug Command Reference』Release 12.2 を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122debug>

AV ペアの詳細については、RFC 3580「IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines」を参照してください。

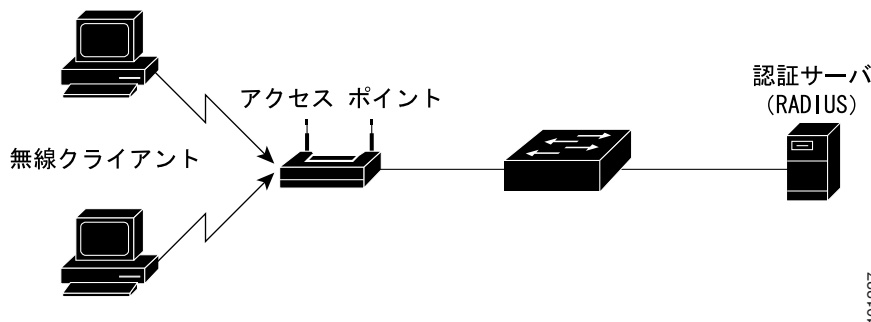
IEEE 802.1X ホスト モード

IEEE 802.1X ポートを 1 つのホスト モードまたは複数のホスト モードに設定できます。1 つのホスト モード (図 8-1[p.8-2] 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、EAPOL フレームを送信して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。

複数のホスト モードでは、複数のホストを単一 IEEE 802.1X 対応ポートに接続できます。図 8-3 (p.8-7) に、無線 LAN での IEEE 802.1X ポートベースの認証を示します。このモードでは、接続クライアントのいずれか 1 つだけが許可されれば、すべてのクライアントがネットワーク 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も機能します。

複数のホスト 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。

図 8-3 複数のホスト モードの例



IEEE 802.1X とポート セキュリティの使用法

1 つのホスト モードでも複数のホスト モードでも、IEEE 802.1X ポートでポート 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しなければなりません)。ポート上でポート セキュリティおよび IEEE 802.1X がイネーブルの場合、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 アドレスへのネットワーク 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、セキュア ホスト テーブル内の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、セキュア違反が発生します。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。

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.21-11)を参照してください。

- IEEE 802.1X クライアントがログオフすると、ポートが無許可状態に移行し、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。ここで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、ポートは無許可状態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。
- IEEE 802.1X ポートでは、1つのホストモードでも複数のホストモードでも、ポートセキュリティおよび音声 VLAN (仮想 LAN) を同時に設定できます。ポートセキュリティは、Voice VLAN Identifier (VVID) および Port VLAN Identifier (PVID; ポート VLAN ID) の両方に適用されます。
- ポートセキュリティテーブルから IEEE 802.1X クライアントアドレスを手動で削除するときは、`dot1x re-authenticate` イネーブル EXEC コマンドを入力して、クライアントを再認証することを推奨します。

スイッチのポートセキュリティのイネーブル化については、「[ポートセキュリティの設定](#)」(p.21-10)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 識別子に関連付けられた特別なアクセスポートです。

- IP Phone 間の音声トラフィックを搬送する VVID。VVID は、ポートに接続している IP phone の設定に使用されます。
- 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間のデータトラフィックを搬送する PVID。PVID は、ポートのネイティブ VLAN です。

1つのホストモードでは、IP Phone のみが音声 VLAN で許可されます。複数のホストモードでは、要求元が PVID で認証されたあとに追加のクライアントが音声 VLAN にトラフィックを送信できません。複数のホストモードがイネーブルの場合、要求元認証は、PVID および VVID の両方に影響します。

リンクがあると音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージのあとにデバイス MAC アドレスが表示されます。Cisco IP Phone は、ほかのデバイスからの CDP メッセージを転送しません。その結果、複数の Cisco IP Phone が連続して接続されている場合は、スイッチは直接接続されている Cisco IP Phone のみを認識します。IEEE 802.1X が音声 VLAN ポート上でイネーブルの場合、スイッチは 2 ホップ以上離れた認証されない Cisco IP Phone からのパケットを廃棄します。

IEEE 802.1X をポートでイネーブルにすると、音声 VLAN と同じようにポート VLAN を設定できません。

音声 VLAN の詳細については、[第 13 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

VLAN 割り当てを使用して、特定のユーザのネットワーク アクセスを制限できます。ポートの IEEE 802.1X 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信して、スイッチ ポートを設定します。RADIUS サーバ データベースは、スイッチ ポートに接続されたクライアントのユーザ名に基づく VLAN を割り当て、ユーザ名と VLAN のマッピングを維持します。

スイッチと RADIUS サーバを設定する際、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、ポートは認証が成功したあとにアクセス VLAN に設定されます。
- IEEE 802.1X 許可がイネーブルの場合でも、RADIUS サーバからの VLAN 情報が無効の場合、ポートは無許可ステートに戻り、設定済みのアクセス VLAN に保持されます。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止します。
設定エラーには、ルーテッド ポートへの VLAN の指定、間違った VLAN ID、存在しないかまたは内部(ルーテッド ポート)の VLAN ID、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、ポートは認証後指定した VLAN に配置されます。
- IEEE 802.1X ポート上で複数のホスト モードがイネーブルの場合、すべてのホストは、最初に認証されたホストとして同じ VLAN (RADIUS サーバで指定された) 内に配置されます。
- IEEE 802.1X およびポート セキュリティがポートでイネーブルの場合、ポートは RADIUS サーバで割り当てられた 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、設定済みのアクセス VLAN に戻ります。

ポートが強制許可、強制無許可、無許可、またはシャットダウン ステートの場合は、設定済みのアクセス VLAN に配置されます。

IEEE 802.1X ポートが許可されて、RADIUS サーバで割り当てられた VLAN に配置される場合、ポート アクセス VLAN の設定変更は無効になります。

VLAN 割り当て機能を備えた 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) を介したダイナミック アクセス ポートの割り当てではサポートされません。

VLAN 割り当てを設定するには、以下を実行する必要があります。

- Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントリング) 許可をイネーブルにします。
- IEEE 802.1X をイネーブルにします (アクセス ポートに IEEE 802.1X を設定すると、VLAN 割り当て機能は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] トンネル タイプ = VLAN
 - [65] トンネル メディア タイプ = IEEE 802
 - [81] トンネル プライベート グループ ID = VLAN 名または VLAN ID

アトリビュート [64] は、値 *VLAN* (type 13) でなければなりません。アトリビュート [65] は、値 *IEEE 802* (type 6) でなければなりません。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.7-31) を参照してください。

IEEE 802.1X とゲスト VLAN の使用方法

スイッチの各 IEEE 802.1X ポートにゲスト VLAN を設定することにより、クライアントに制限付きのサービスを提供できます (IEEE 802.1X クライアントのダウンロード方法など)。このようなクライアントは、IEEE 802.1X 認証用にシステムをアップグレードする場合もあります。また、Windows 98 システムなどのホストには、IEEE 802.1X に対応していないものもあります。

IEEE 802.1X ポートでゲスト VLAN がイネーブルの場合、認証サーバが EAPOL 要求 / アイデンティティフレームへの応答を受信しない場合または EAPOL パケットがクライアントに送信されない場合に、スイッチはクライアントにゲスト VLAN を割り当てます。

Cisco IOS Release 12.2(25)SE より前では、スイッチは EAPOL パケット履歴を保持せず、EAPOL パケットがインターフェイスで検出されていたかどうかにかかわらず、ゲスト VLAN への認証アクセスに失敗したクライアントを許可していました。dot1x guest-vlan supplicant 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、このオプションの動作をイネーブルにできます。

Cisco IOS Release 12.2(25)SE 以降、スイッチは EAPOL パケット履歴を保持するようになりました。リンクのライフタイム中に別の EAPOL パケットがインターフェイスで検出された場合、ネットワークアクセスは拒否されます。EAPOL 履歴はリンク消失でリセットされます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1X 非対応クライアントのアクセス数に制限がなくなります。IEEE 802.1X 対応のクライアントが、ゲスト VLAN が設定されているのと同じポートに追加された場合、ポートはユーザ設定のアクセス VLAN で無許可ステートになり、認証が再開されます。

ゲスト VLAN は、IEEE 802.1X ポートで 1 つのホストおよび複数のホスト モードでサポートされます。

RSPAN VLAN または音声 VLAN 以外であればいずれのアクティブな VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。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ません。アクセス ポートでのみサポートされます。

設定手順の詳細については、「[ゲスト VLAN の設定](#)」(p.8-23) を参照してください。

IEEE 802.1X と Wake-on-LAN の使用方法

IEEE 802.1X の Wake-on-LAN (WoL) 機能を使用すると、*Magic Packet* と呼ばれる特定のイーサネットフレームを受信すると、休止状態の PC を起動できます。この機能は、管理者が電源が切られたシステムに接続する必要がある環境で使用できます。

IEEE 802.1X ポートに接続されたホストで WoL を使用すると、ホストの電源が切断された場合に IEEE 802.1X ポートが無許可になるという特有の問題が発生します。このステートでは、ポートは EAPOL パケットの送受信のみが可能です。したがって、WoL Magic Packet はホストにまで到達できません。起動しないと PC は認証されず、ポートは開きません。

WoL 機能を搭載した IEEE 802.1X は、無許可の IEEE 802.1X ポートにパケットを送信することでこの問題を解決します。この機能は IEEE 802.1X 仕様の単一方向制御ポートとも呼ばれます。

PortFast がポート上でイネーブルでない場合、ポートは強制的に双方向ステートになります。

単一方向ステート

dot1x control-direction in 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を単一方向ポートとして設定する場合、ポートはスパニングツリー フォワーディング ステートに変更されます。

WoL がイネーブルの場合、接続されたホストはスリーピング モードまたはパワーダウン ステートになり、ホストはネットワークの他のデバイスとトラフィックを交換しません。ホストがネットワークにトラフィックを送信できない単一方向ポートに接続された場合、ホストはネットワークの他のデバイスからのトラフィックのみを受信できます。単一方向ポートが着信トラフィックを受信した場合、ポートは双方向 (デフォルト) ステートに戻り、スパニングツリー ステートはブロッキング ステートに変更されます。ポートが初期化ステートに変更された場合、EAPOL パケット以外のトラフィックは許可されません。ポートが双方向ステートに戻った場合、スイッチは 5 分タイマーを開始します。タイマーが満了する前にポートが認証されない場合、ポートは単一方向ポートになります。

双方向ステート

dot1x control-direction both 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を双方向ポートとして設定する場合、ポートは両方向でアクセス制御されます。このステートでは、スイッチ ポートはパケットを送受信しません。

IEEE 802.1X とユーザ単位の 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えるようにできます。RADIUS サーバが IEEE 802.1X ポートに接続しているユーザを認証する場合、ユーザ ID に基づく ACL アトリビュートを取得し、スイッチに送信します。スイッチは、ユーザセッションの間このアトリビュートを IEEE 802.1X ポートに適用します。認証失敗、またはリンクダウン状態が発生した場合は、スイッチがセッション終了時にユーザ単位の ACL 設定を削除します。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションに保存しません。ポートが許可されない場合、スイッチはポートから ACL を削除します。

スイッチ ポートには、ユーザ単位の ACL を 1 タイプだけ設定できます。ルータ ACL またはポート ACL です。ルータ ACL はレイヤ 3 インターフェイスに適用され、ポート ACL はレイヤ 2 インターフェイスに適用されます。あるポートがポートベース ACL に設定されている場合、同じポートのルータベース ACL を設定しようとするとスイッチがこれを拒否します。ただし、あるポートがルータベース ACL に設定されていて、そのあとでポートベース ACL に設定される場合、ルータ ACL はポートベース ACL によって上書きされます。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) などのユーザ単位の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tring 形式で、認証プロセス中にスイッチに渡されます。ユーザ単位の 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、入力方向のみサポートされます。

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、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、そのあと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、アクセス リストはデフォルトで発信 ACL に適用されます。サポートされるスイッチの Cisco IOS アクセス リストは制限されているため、フィルタ ID アトリビュートは、IP ACL 番号 1 ~ 199 および 1300 ~ 2699 でしかサポートされません (IP 標準および IP 拡張 ACL)。

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、ユーザ単位の ACL アトリビュートは関連ポートでディセーブルです。

ユーザ単位の ACL の最大サイズは、4000 ACSII 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.7-31) を参照してください。ACL 設定の詳細については、[第 28 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。

ユーザ単位の ACL を設定するには、以下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 サーバからのインターフェイス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。
- IEEE 802.1X ポートを 1 つのホスト 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 \(p.8-13\)](#)
- [IEEE 802.1X 設定時の注意事項 \(p.8-14\)](#)
- [旧ソフトウェアリリースからのアップグレード \(p.8-15\)](#)
- [IEEE 802.1X 認証のイネーブル化 \(p.8-15\)\(必須\)](#)
- [スイッチと RADIUS サーバ間通信を設定する方法 \(p.8-17\)\(必須\)](#)
- [定期的な再認証のイネーブル化 \(p.8-19\)\(任意\)](#)
- [手動によるポート接続クライアントの再認証 \(p.8-19\)\(任意\)](#)
- [待機時間の変更 \(p.8-20\)\(任意\)](#)
- [スイッチとクライアント間の再送信時間の変更 \(p.8-20\)\(任意\)](#)
- [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 \(p.8-21\)\(任意\)](#)
- [再認証回数の設定 \(p.8-22\)\(任意\)](#)
- [ホスト モードの設定 \(p.8-22\)\(任意\)](#)
- [ゲスト VLAN の設定 \(p.8-23\)\(任意\)](#)
- [IEEE 802.1X 設定をデフォルト値にリセットする方法 \(p.8-25\)\(任意\)](#)
- [IEEE 802.1X 認証の設定 \(p.8-25\)\(任意\)](#)
- [IEEE 802.1X アカウンティングの設定 \(p.8-27\)\(任意\)](#)

IEEE 802.1X のデフォルト設定

表 8-2 に、IEEE 802.1X のデフォルト設定を示します。

表 8-2 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	
<ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • 鍵 	<ul style="list-style-type: none"> • 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
インターフェイス単位の IEEE 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 (秒)	3600 秒
再認証回数	2 回 (ポートが無許可ステートに変わる前に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)

表 8-2 IEEE 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 (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)
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	1 つのホスト モード
ゲスト 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、サーバに応答を送信するまでの時間。この値は設定変更不可能)

IEEE 802.1X 設定時の注意事項

IEEE 802.1X 認証設定の注意事項は、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、ポートは認証されます。
- 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、およびレイヤ 3 ルーテッド ポートでは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、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、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、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、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、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、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 アクティブまたはアクティブにする予定の EtherChannel メンバーのポートを、IEEE 802.1X ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1X をイネーブルにしようとする、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。



(注) Cisco IOS Release 12.2(25)SE より前のソフトウェア リリースでは、IEEE 802.1X が EtherChannel の未アクティブ ポートでイネーブルになっている場合、ポートは EtherChannel に追加されません。

- 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 宛先ポート、RSPAN 宛先ポート、または RSPAN リフレクタ ポートで IEEE 802.1X をイネーブルにできます。ただし、ポートが SPAN 宛先ポート、RSPAN 宛

先ポート、または RSPAN リフレクタ ポートとして削除されるまでは、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 をイネーブルにできません。

- RSPAN VLAN または音声 VLAN 以外であればいずれの VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。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ません。アクセス ポート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 と同じようにポート VLAN を設定できません。
- トランク ポート、ダイナミック ポート、または VMPS を介したダイナミック アクセス ポート 割り当てでは、VLAN 割り当て機能を備えた IEEE 802.1X をサポートしません。
- `dot1x system-auth-control` グローバル コンフィギュレーション コマンドを入力して、スイッチで IEEE 802.1X をグローバルにイネーブルにする前に、IEEE 802.1X および EtherChannel が設定されているインターフェイスから EtherChannel 設定を削除してください。
- EAP-Transparent LAN Services (TLS; 透過型 LAN サービス) および EAP-MD5 を使用した IEEE 802.1X 認証用の Cisco Access Control Server (ACS) アプリケーションを実行しているデバイスを使用していて、さらにスイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、デバイスで実行している ACS のバージョンが 3.2.1 以降であることを確認してください。
- DHCP クライアントが接続されている IEEE 802.1X ポートに対してゲスト VLAN を設定したあと、ホスト IP アドレスを DHCP サーバから取得する必要があります。また、クライアントの DHCP プロセスがタイムアウトし、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチの IEEE 802.1X 認証プロセスを再起動するための設定を変更できます。IEEE 802.1X 認証プロセスの設定(IEEE 802.1X 待機期間およびスイッチからクライアントへの転送時間)を減らします。

旧ソフトウェア リリースからのアップグレード

Cisco IOS Release 12.1(14)EA1 では、IEEE 802.1X に関する実装が旧リリースから変更されました。グローバル コンフィギュレーション コマンドの一部は、インターフェイス コンフィギュレーション コマンドになり、新しいコマンドも追加されました。


スイッチで IEEE 802.1X が設定済みであり、Cisco IOS Release 12.1(14)EA1 以降にアップグレードする場合は、コンフィギュレーション ファイルに新しいコマンドが含まれないので、IEEE 802.1X は動作しません。アップグレードの終了後、`dot1x system-auth-control` グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1X をグローバルにイネーブルにする必要があります。IEEE 802.1X が、旧リリースでインターフェイス上の複数のホスト モードで稼働していた場合、`dot1x host-mode multi-host` インターフェイス コンフィギュレーション コマンドを使用して再設定する必要があります。

IEEE 802.1X 認証のイネーブル化

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送信を行う手順と認証方式を記述したものです。

ユーザ単位の ACL および 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	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication dot1x {default} method1</code>	<p>IEEE 802.1X 認証方式リストを作成します。</p> <p>authentication コマンドに名前付きリストが指定され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法を指定します。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せん。</p> <p><i>method1</i> の場合、group radius キーワードを入力して認証用のすべての RADIUS サーバのリストを使用します。</p> <p> (注) 他のキーワードがコマンドラインのヘルプ スtring に表示されていても、default および group radius キーワードのみがサポートされています。</p>
ステップ 4	<code>dot1x system-auth-control</code>	スイッチで IEEE 802.1X 認証をグローバルにイネーブルにします。
ステップ 5	<code>aaa authorization network {default} group radius</code>	<p>(任意) ユーザ単位の 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。</p> <p>ユーザ単位の ACL を設定するには、1 つのホスト モードをイネーブルにする必要があります。これがデフォルト設定です。</p>
ステップ 6	<code>radius-server host ip-address</code>	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7	<code>radius-server key string</code>	(任意) スイッチと RADIUS サーバ上で稼働する RADIUS デモンの間で使用する認証および暗号化鍵を指定します。
ステップ 8	<code>interface interface-id</code>	IEEE 802.1X 認証をイネーブルにするクライアントに接続されたポートを指定して、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 9	<code>switchport mode access</code>	(任意) ステップ 6 および 7 で RADIUS サーバを設定する場合にのみ、ポートをアクセスモードに設定します。
ステップ 10	<code>dot1x port-control auto</code>	<p>インターフェイスで IEEE 802.1X 認証をイネーブルにします。</p> <p>設定の詳細については、「IEEE 802.1X 設定時の注意事項」(p.8-14) を参照してください。</p>
ステップ 11	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 12	<code>show dot1x</code>	<p>設定を確認します。</p> <p>出力された IEEE 802.1X Port Summary セクションの Status カラムを調べてください。<i>enabled</i> 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。</p>
ステップ 13	<code>copy running-config startup-config</code>	(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 fastethernet0/1
Switch(config-if)# 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、または 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されます。

スイッチに 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	<code>configure terminal</code>	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	<code>radius-server host {hostname ip-address} auth-port port-number key string</code>	<p>スイッチに RADIUS サーバ パラメータを設定します。</p> <p><code>hostname ip-address</code> 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。</p> <p><code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。デフォルト値は 1812 です。</p> <p><code>key string</code> 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がある文字列です。</p> <p> (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 <code>radius-server host</code> 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。</p> <p>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。</p>
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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。

指定された 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。

次の例は、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 サーバ上の鍵と一致する `rad123` に設定します。

```
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.7-31) 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用するキー テキスト スtring 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。

RADIUS サーバを使用した IEEE 802.1X 認証の設定

Cisco IOS Release 12.2(25)SEC では、RADIUS サーバを使用して IEEE 802.1X 認証を設定することもできます。

RADIUS サーバを使用して IEEE 802.1X 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。この手順は任意です。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x guest-vlan vlan-id</code>	IEEE 802.1X ゲスト VLAN として、アクティブな VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 RSPAN VLAN または音声 VLAN 以外であればいずれのアクティブな VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。
ステップ 4	<code>dot1x reauthentication</code>	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 5	<code>dot1x timeout reauth-period {seconds server}</code>	再認証を試行する間隔 (秒数) 設定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <code>seconds</code> 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 3600 秒です。 <code>server</code> Session-Timeout RADIUS アトリビュート (アトリビュート [27]) の値として秒数を指定します。 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 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show dot1x interface interface-id</code>	IEEE 802.1X 認証設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、RADIUS サーバの使用中に IEEE 802.1X を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

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)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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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	<code>dot1x reauthentication</code>	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	<code>dot1x timeout reauth-period {seconds server}</code>	<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <code>seconds</code> 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 3600 秒です。 <code>server</code> Session-Timeout RADIUS アトリビュート (アトリビュート [27]) の値として秒数を指定します。スイッチが NAC レイヤ 2 の IEEE 802.1X を使用する場合に、このキーワードを使用できます。 <p>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。</p>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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を試行する間隔に戻すには、`no dot1x timeout reauth-period` 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。

次の例では、定期的な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 コマンドを入力すると、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、「[定期的な再認証のイネーブル化](#)」(p.8-19)を参照してください。

次の例では、ポートに接続したクライアントを手動で再認証します。

```
Switch# dot1x re-authenticate interface fastethernet0/1
```

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。アイドル時間は、quiet-period 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提供したため、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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	<code>dot1x timeout quiet-period seconds</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次の例では、スイッチの待機時間を 30 秒に設定します。

```
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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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。

	コマンド	説明
ステップ 3	<code>dot1x timeout tx-period seconds</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次の例では、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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	<code>dot1x max-req count</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次の例では、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 回に設定します。

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

再認証回数の設定

ポートが無許可状態になる前にスイッチが認証プロセスを再起動する回数も変更できます。



(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。

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	ポートが無許可状態に変更する前に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、ポートが無許可状態になる前に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

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	間接的に接続されている複数のホストに対してインターフェイスを指定し、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。

	コマンド	説明
ステップ 3	<code>dot1x host-mode multi-host</code>	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。 指定されたインターフェイスについて、 <code>dot1x port-control</code> インターフェイス コンフィギュレーション コマンドが <code>auto</code> に設定されていることを確認します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	（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。

```
Switch(config)# interface fastethernet0/1
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 を設定する場合、サーバが EAPOL 要求 / アイデンティティ フレームへの応答を受信しなければ、IEEE 802.1X 未対応のクライアントはゲスト VLAN になります。IEEE 802.1X 対応のクライアントでも認証に失敗すれば、ネットワーク アクセスは許可されません。スイッチは、1 つのホスト モードでも複数のホスト モードでもゲスト 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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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。サポートされるインターフェイスのタイプについては、「 IEEE 802.1X 設定時の注意事項 」(p.8-14) を参照してください。
ステップ 3	<code>switchport mode access</code>	ポートをアクセス モードに設定します。
ステップ 4	<code>dot1x port-control auto</code>	ポートで IEEE 802.1X 認証をイネーブルにします。
ステップ 5	<code>dot1x guest-vlan vlan-id</code>	IEEE 802.1X ゲスト VLAN として、アクティブな VLAN を指定します。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 以外であれば、いずれのアクティブな VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	（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 をディセーブルにして削除する場合は、`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。ポートは無許可ステートに戻ります。

次に、ポートで IEEE 802.1X ゲスト VLAN をイネーブルにする例を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x guest-vlan 9
```

次に、スイッチの待機時間を 3 に設定して、スイッチが要求を再送信するまでクライアントからの EAP 要求 / アイデンティティ フレームの応答を待機する秒数を 15 に設定し、IEEE 802.1X ポートが DHCP クライアントに接続されるときに VLAN2 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-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

`dot1x guest-vlan supplicant` 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、オプションのゲスト VLAN 動作をイネーブルにできます。イネーブルにするときに、スイッチは EAPOL パケット履歴を保持せず、EAPOL パケットがインターフェイスで検出されていたかどうかにかかわらず、ゲスト VLAN への認証アクセスに失敗したクライアントを許可します。

オプションのゲスト VLAN 動作をイネーブルにしてゲスト 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	<code>configure terminal</code>	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	<code>dot1x guest-vlan supplicant</code>	オプションのゲスト VLAN 動作をスイッチでグローバルにイネーブルにします。
ステップ 3	<code>interface interface-id</code>	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のタイプについては、「IEEE 802.1X 設定時の注意事項」(p.8-14) を参照してください。
ステップ 4	<code>switchport mode access</code>	ポートをアクセス モードに設定します。
ステップ 5	<code>dot1x port-control auto</code>	ポートで IEEE 802.1X 認証をイネーブルにします。
ステップ 6	<code>dot1x guest-vlan vlan-id</code>	IEEE 802.1X ゲスト VLAN として、アクティブな VLAN を指定します。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 以外であれば、いずれのアクティブな VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。
ステップ 7	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 8	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(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。

オプションのゲスト VLAN 動作をディセーブルにするには、`no dot1x guest-vlan supplicant` 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。ゲスト VLAN を削除するには、`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。ポートは無許可ステートに戻ります。

次に、オプションのゲスト VLAN 動作をイネーブルにして VLAN 5 を IEEE 802.1X ゲスト VLAN として指定する例を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x guest-vlan 5
```

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。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するインターフェイスを指定し、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	<code>dot1x default</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 認証の設定

IEEE 802.1X ポートベースの認証を設定するには、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。

ソフトウェアは方式リストの最初の方式を使用してユーザを認証します。この方式で応答に失敗した場合、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すまで続きます。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。

ユーザ単位の 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 AAA の手順は、次のとおりです。

- ステップ 1 ユーザがスイッチのポートに接続します。
- ステップ 2 認証が実行されます。
- ステップ 3 VLAN 割り当てが (場合によっては RADIUS サーバ設定に基づいて) イネーブルになります。
- ステップ 4 スイッチが開始メッセージをアカウントिंगサーバに送信します。
- ステップ 5 必要であれば、再認証が実行されます。

- ステップ 6 スイッチは、再認証の結果に基づいて仮のアカウントिंग アップデートをアカウントिंग サーバに送信します。
- ステップ 7 ユーザがポートの接続を解除します。
- ステップ 8 スイッチが停止メッセージをアカウントング サーバに送信します。

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。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication dot1x {default} method1 [method2...]</code>	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法を指定します。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せん。 次のキーワードを 1 つ以上入力します。 <ul style="list-style-type: none"> 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	<code>dot1x system-auth-control</code>	スイッチで IEEE 802.1X 認証をグローバルにイネーブルにします。
ステップ 5	<code>aaa authorization network {default} group radius</code>	(任意) ユーザ単位の 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) ユーザ単位の ACL は、1 つのホスト モードを設定する必要があります。これがデフォルト設定です。
ステップ 6	<code>interface interface-id</code>	IEEE 802.1X 認証をイネーブルにするクライアントに接続されたポートを指定して、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	<code>dot1x port-control auto</code>	ポートで IEEE 802.1X 認証をイネーブルにします。 設定の詳細については、「 IEEE 802.1X 設定時の注意事項 」(p.8-14) を参照してください。
ステップ 8	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 9	<code>show dot1x</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(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

IEEE 802.1X アカウンティングによる AAA システムのアカウンティングをイネーブルにすると、システムがイベントをリロードしてアカウンティング RADIUS サーバに記録するために送信できるようになります。これにより、サーバはすべてのアクティブ IEEE 802.1X セッションがクローズされたと判断します。

RADIUS は信頼性のない UDP 転送プロトコルを使用しているため、ネットワークの状態が悪いとアカウンティングメッセージが紛失する場合があります。アカウンティング要求の再送信を設定した回数行ったあとも、アカウンティングの応答メッセージをスイッチが RADIUS サーバから受信していない場合、次のシステム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と、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) RADIUS サーバがアカウンティング タスク (ロギングの開始、停止、中間アップデートメッセージ、タイムスタンプなど) を実行するように設定する必要があります。これらの機能を有効にするには、RADIUS サーバの Network Configuration タブにある [Update/Watchdog packets from this AAA client] のロギングをイネーブルにしてください。次に、RADIUS サーバの System Configuration タブにある [CVS RADIUS Accounting] をイネーブルにしてください。

AAA がスイッチでイネーブルになったあと、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>aaa accounting dot1x default start-stop group radius</code>	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 4	<code>aaa accounting system default start-stop group radius</code>	(任意) システムのアカウンティングをイネーブルにして (すべての RADIUS サーバのリストを使用)、スイッチのリロードのときに、システム アカウンティングのリロード イベント メッセージを生成します。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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。

`show radius statistics` イネーブル EXEC コマンドを使用して、アカウンティング応答メッセージを受信していない RADIUS メッセージ数を表示します。

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、アカウンティング用の UDP ポートとして 1813 を指定し、RADIUS サーバを設定します。

```
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

すべてのインターフェイスの 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。特定のインターフェイスの 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。特定のインターフェイスの 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。