



# IEEE 802.1x ポート ベース認証の設定

この章では、Catalyst 2960 スイッチ上で IEEE 802.1x ポート ベース認証を設定する方法について説明します。IEEE 802.1x は、不正な装置 (クライアント) によるネットワーク アクセスを防止します。



(注)

この章で使用す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 ベース認証の概要 \(p.9-2\)](#)
- [IEEE 802.1x 認証の設定 \(p.9-13\)](#)
- [IEEE 802.1x の統計情報およびステータスの表示 \(p.9-29\)](#)

## IEEE 802.1x ポート ベース認証の概要

IEEE 802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント / サーバ型のアクセス制御および認証プロトコルを定めています。認証サーバが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。

IEEE 802.1x アクセス制御では、クライアントを認証するまでの間、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)、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。

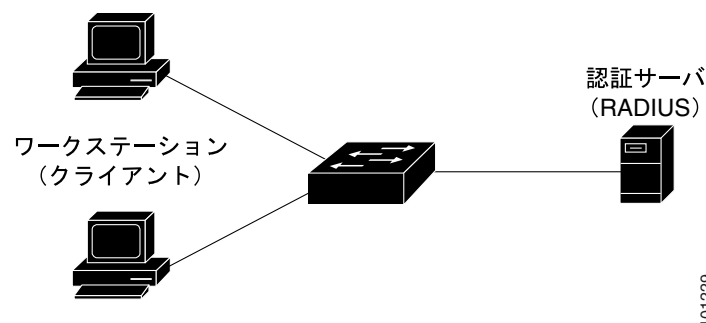
ここでは、IEEE 802.1x ポート ベース認証について説明します。

- 装置の役割 (p.9-2)
- 認証の開始およびメッセージ交換 (p.9-3)
- 許可ステートおよび無許可ステートのポート (p.9-4)
- IEEE 802.1x アカウンティング (p.9-5)
- IEEE 802.1x アカウンティング属性値 (AV) ペア (p.9-6)
- IEEE 802.1x のホストモード (p.9-7)
- ポートセキュリティを使用した IEEE 802.1x の利用 (p.9-7)
- 音声 VLAN ポートを使用した IEEE 802.1x の利用 (p.9-8)
- VLAN 割り当てを使用した IEEE 802.1x の利用 (p.9-9)
- ゲスト VLAN を使用した IEEE 802.1x の利用 (p.9-10)
- 制限 VLAN を使用した IEEE 802.1x の利用 (p.9-10)
- Wake on LAN を使用した IEEE 802.1x の利用 (p.9-11)

## 装置の役割

IEEE 802.1x ポート ベース認証では、ネットワーク上の装置にはそれぞれ、固有の役割があります (図 9-1 を参照)。

図 9-1 IEEE 802.1x における装置の役割



- 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装置 (ワークステーション)。ワークステーションでは、Microsoft Windows XP OS (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する必要があります (クライアントは、IEEE 802.1x 仕様ではサブリクランドといえます)。



(注) Windows XP のネットワーク接続および IEEE 802.1x 認証については、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。今回のリリースでサポートされる認証サーバは、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 システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。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(エッジスイッチまたはワイヤレスアクセス 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とカプセル化解除、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場合、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 フレームの変更は行われたいため、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。

仲介装置として動作できるものには、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ、またはワイヤレス アクセス ポイントがあります。これらの装置では、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が稼働している必要があります。

## 認証の開始およびメッセージ交換

スイッチとクライアントのどちらからでも、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 ステータスがダウンからアップに変化した時点で、またはポートが認証されていないままアップの状態であるかぎり定期的に、認証を開始しなければなりません。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。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。

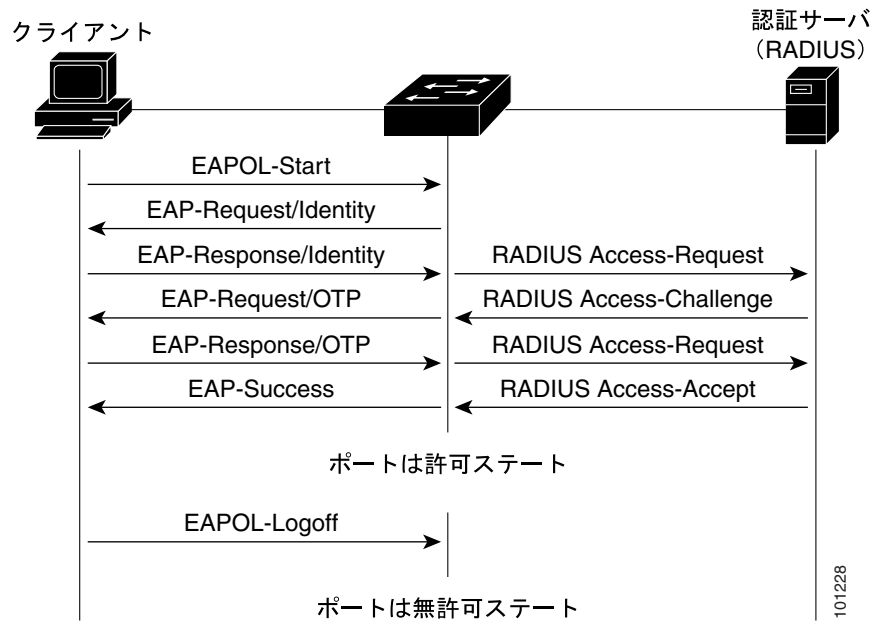


(注) ネットワーク アクセス装置で IEEE 802.1x がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステータスであるものとしてフレームを送信します。ポートが許可ステータスであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステータスおよび無許可ステータスのポート」(p.9-4) を参照してください。

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 ポートは許可状態になります。詳細については、「許可状態および無許可状態のポート」(p.9-4) 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 9-2 に、クライアントが RADIUS サーバとの間で 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 9-2 メッセージ交換



## 許可状態および無許可状態のポート

スイッチのポート 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 アクセスを許可します。ポートは最初、*無許可状態*です。このステートでは、音声 VLAN (仮想 LAN) ポートとして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*許可状態*になり、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。ポートが音声 VLAN として設定されている場合、VoIP トラフィックおよび IEEE 802.1x プロトコルパケットが許可されたあとクライアントが正常に認証されます。

IEEE 802.1x をサポートしていないクライアントが、無許可状態の IEEE 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状態となり、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、IEEE 802.1x 対応のクライアントが、IEEE 802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start 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。また、応答がない場合は、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** — IEEE 802.1x 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変更します。ポートはクライアントの IEEE 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、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変化したとき、または EAPOL-Start 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化し、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可されます。認証に失敗すると、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します。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-Logoff 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 ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変化した場合、または EAPOL-Logoff 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。

## IEEE 802.1x アカウンティング

IEEE 802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法については監視しません。IEEE 802.1x アカウンティングは、デフォルトでディセーブルです。IEEE 802.1x アカウンティングをイネーブルにすると、次のアクティビティを IEEE 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

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、スイッチはこの情報を 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 アカウンティング属性値 (AV) ペア

RADIUS サーバに送信された情報は、属性値 (AV) ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます (たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です)。

AV ペアは、IEEE 802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の3つのタイプの 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が始まると送信されます。
- INTERIM — 既存のセッションが更新されると送信されます。
- STOP — セッションが終了すると送信されます。

次の表 9-1 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 9-1 アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信 <sup>1</sup>	条件に応じて送信 <sup>1</sup>
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	非送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	非送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	非送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol (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に存在している場合にのみ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、`debug radius accounting` イネーブル EXEC コマンドを入力することで表示できます。このコマンドの詳細については、次の URL で『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/ios122/12sup/122debug>

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

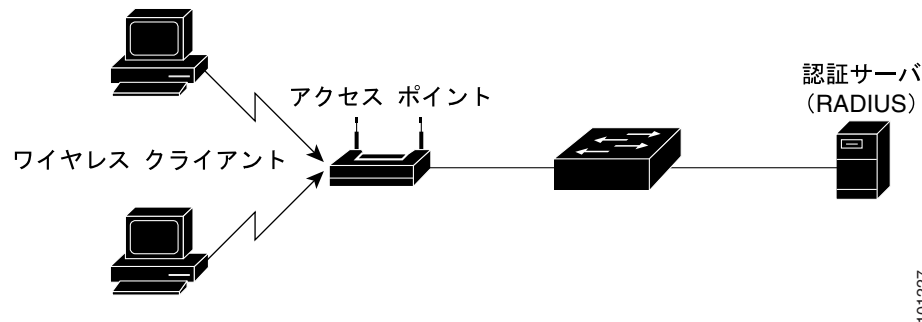
## IEEE 802.1x のホスト モード

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で設定できます。単一ホストモード（図 9-1 [p.9-2] を参照）では、IEEE 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、EAPOL フレームを送信することで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。

複数ホストモードでは、単一の IEEE 802.1x 対応ポートに複数のホストを接続できます。図 9-3 (p.9-7) に、ワイヤレス LAN における IEEE 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち1つが許可されれば、すべてのクライアントのネットワークアクセスが許可されます。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-Logoff 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。

複数ホストモードがイネーブルの場合、IEEE 802.1x をポートおよびポートセキュリティの認証に使用し、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管理します。

図 9-3 複数ホストモードの例



## ポートセキュリティを使用した IEEE 802.1x の利用

単一ホストモードと複数ホストモードのどちらでも IEEE 802.1x ポートの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)。ポートでポートセキュリティおよび IEEE 802.1x をイネーブルに設定すると、IEEE 802.1x はそのポートを認証し、ポートセキュリティはそのクライアントを含むすべての MAC アドレスに対する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関係があります。

- 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は保証されます（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ポートセキュリティテーブルがいっぱいの場合、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内でのエントリは他のホストに取って代わられます。

最初の認証ホストでセキュリティ違反が発生すると、ポートは `errdisable` になり、ただちにシャットダウンします。

セキュリティ違反発生時の動作は、ポートセキュリティ違反モードによって決まります。詳細については、「[セキュリティ違反](#)」(p.21-9)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、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場合、`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変化し、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。
- ポートが管理上のシャットダウン状態になった場合、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。
- 単一ホストモードと複数ホストモードのいずれの場合でも、IEEE 802.1x ポート上でポートセキュリティと音声 VLAN を同時に設定できます。ポートセキュリティは、Voice VLAN Identifier (VVID; 音声 VLAN ID) と Port VLAN Identifier (PVID; ポート VLAN ID) の両方に適用されます。

スイッチ上でポートセキュリティをイネーブルにする手順については、「[ポートセキュリティの設定](#)」(p.21-8)を参照してください。

## 音声 VLAN ポートを使用した IEEE 802.1x の利用

音声 VLAN ポートは特別なアクセスポートで、次の2つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された 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との間でデータトラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

IP Phone では、ポートの許可ステートに関係なく、音声トラフィックに VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作することが可能になります。

単一ホストモードでは、IP Phone のみが音声 VLAN で許可されます。複数ホストモードでは、サブリカントが PVID で認証されたあと、追加のクライアントのトラフィックが音声 VLAN 上で送信できます。複数ホストモードがイネーブルの場合、サブリカント認証は PVID と VVID の両方に影響します。

リンクがある場合、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装置の MAC アドレスが表示されます。Cisco IP Phone は、他の装置から受け取った CDP メッセージを中継しません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている1台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x がイネーブルの場合、スイッチは2ホップ以上離れた認識されない IP Phone からのパケットを廃棄します。

IEEE 802.1x をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。



(注)

音声 VLAN が設定され、Cisco IP Phone が接続されているアクセスポートで IEEE 802.1x をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、[第14章「音声 VLAN の設定」](#)を参照してください。



## VLAN 割り当てを使用した IEEE 802.1x の利用

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 サーバデータベースは、ユーザ名と VLAN のマッピングを維持し、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 を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した IEEE 802.1x には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または IEEE 802.1x 許可がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN は、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべてこの VLAN に属します。
- IEEE 802.1x 許可がイネーブルで、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タスに戻り、設定済みのアクセス VLAN にとどまります。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。  
設定エラーには、間違った VLAN ID、存在しない VLAN ID の指定、または音声 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、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 ポートで複数ホスト 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同じ VLAN (RADIUS サーバにより指定) に配置されます。
- ポート上で IEEE 802.1x およびポート セキュリティがイネーブルの場合、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、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) ステータス、強制無許可 (force-unauthorized) ステータス、無許可ステータス、またはシャットダウン ステータスの場合、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 に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。

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) によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した IEEE 802.1x はサポートされません。

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 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 (アクセス ポートで 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属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID

属性 [64] は、値 *VLAN* (タイプ 13) でなければなりません。属性 [65] は、値 *802* (タイプ 6) でなければなりません。属性 [81] 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。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(p.8-31) を参照してください。

## ゲスト VLAN を使用した IEEE 802.1x の利用

スイッチ上の各 IEEE 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的な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など)。これらのクライアントは IEEE 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は IEEE 802.1x 対応ではありません。

スイッチが EAP-Request/Identity フレームに対する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よって送信されない場合に、IEEE 802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは、EAPOL パケットの履歴を保存します。リンクの存続時間中にインターフェイスで EAPOL パケットが検出されると、スイッチではそのインターフェイスに接続された装置は IEEE 802.1x 対応のサブリカントとみなされ、インターフェイスはゲスト VLAN ステートに移行しません。インターフェイスのリンク ステータスがダウンになると、EAPOL 履歴はクリアされます。インターフェイスで EAPOL パケットが検出されないと、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で EAPOL パケットが検出された場合、インターフェイスが無許可ステートに戻り、IEEE 802.1x 認証が再開します。

スイッチ ポートがゲスト VLAN に移動すると、任意の数の IEEE 802.1x 非対応クライアントがアクセスを許可されます。ゲスト VLAN が設定されているポートに IEEE 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、IEEE 802.1x ポート上で単一ホスト モードまたは複数ホスト モードでサポートされています。

RSPAN VLAN または音声 VLAN を除く任意のアクティブな VLAN を IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能はトランク ポート上ではサポートされず、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.9-23) を参照してください。

## 制限 VLAN を使用した IEEE 802.1x の利用

スイッチの各 IEEE 802.1x ポートに対して 1 つの制限 VLAN (認証失敗 VLAN とも言う) を設定し、ゲスト VLAN にアクセスできないクライアントへ限られたサービスを提供できます。このようなクライアントは IEEE 802.1x に準拠していますが、認証プロセスに失敗したために別の VLAN にアクセスできません。制限 VLAN では、認証サーバ内に有効な証明書がないユーザ (企業への来訪者など) でも、限られたサービスにアクセスできます。管理者は、制限 VLAN で利用できるサービスを制御できます。



(注)

両方のタイプのユーザに同様のサービスを提供できるよう、VLAN にゲスト VLAN と制限 VLAN の両方の設定を行うことも可能です。

この機能がなければ、クライアントの認証が無制限に失敗しつづけば、スイッチ ポートはスパニング ツリーのブロッキング ステートのままとなってしまいます。この機能を利用すると、認証の試行が指定回数行われたあと (デフォルトは 3 回)、スイッチ ポートが制限 VLAN 内のポートになるよう設定できます。

認証機能は、失敗した認証試行をクライアントごとにカウントします。このカウントが認証試行回数の設定最大値を超えると、ポートは制限 VLAN に移動します。試行失敗のカウントが加算されるのは、RADIUS サーバが *EAP 失敗* の応答を返した場合、または *EAP* パケットなしで空の応答を返した場合です。ポートが制限 VLAN に移動すると、試行失敗のカウントはリセットされます。

認証に失敗したユーザは、次の認証試行まで、制限 VLAN に留まります。制限 VLAN 内のポートは、設定した間隔（デフォルトは 60 秒）で再認証を実行します。再認証に失敗すると、ポートは制限 VLAN に留まったままとなります。再認証に成功すると、ポートは設定した VLAN または RADIUS サーバから返された VLAN に移動します。再認証はディセーブルにできます。ディセーブルにしたポートで認証プロセスを再起動するには、ポートが *link down* または *EAP logoff* 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される場合、再認証をイネーブルにしておくことを推奨します。クライアントをハブから接続解除したとき、ポートが *link down* または *EAP logoff* イベントを受信しないことがあります。

ポートが制限 VLAN に移動したあと、シミュレーテッド EAP 成功メッセージがクライアントに送信されます。これにより、クライアントが無制限に認証試行を繰り返す状況が回避されます。EAP 成功を受信しないと DHCP を実行できないクライアントもあります（Windows XP の稼動する装置など）。

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 ポート上でのみサポートされています。

RSPAN VLAN または音声 VLAN を除く任意のアクティブな VLAN を IEEE 802.1x 制限 VLAN として設定できます。制限 VLAN 機能はトランク ポート上ではサポートされず、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と連動します。ポートが認証されると、すぐに MAC アドレスがポートセキュリティに通知されます。ポートセキュリティでその MAC アドレスが許可されない、またはセキュア アドレス カウントが最大値に達した場合、ポートが無許可の状態となり、*errdisable* になります。

制限 VLAN には、ダイナミック ARP 検査、DHCP スヌーピング、IP 送信元ガードなどのポートセキュリティ機能を、個別に設定できます。

詳細については、「[制限 VLAN の設定](#)」(p.9-25) を参照してください。

## Wake on LAN を使用した IEEE 802.1x の利用

IEEE 802.1x Wake on LAN (WoL) 機能は、スイッチが特別なイーサネットフレーム（マジック パケット）を受信した場合に休止状態の PC の電源をオンにします。この機能は、管理者が電源がオフのシステムに接続する必要のある環境で使用できます。

WoL を使用するホストが IEEE 802.1x ポート経由で接続されていて、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。この状態では、ポートは EAPOL パケットの送受信しかできないため、WoL マジック パケットはホストに到達しません。電源がオフの PC は認証されず、スイッチ ポートはオープンになりません。

スイッチで WoL 対応 IEEE 802.1x を使用している場合、スイッチは無許可 IEEE 802.1x ポートにパケットを送信します。この機能は、IEEE 802.1x 仕様では *単一方向制御* ポートといえます。



(注)

ポートで PortFast がイネーブル化されていない場合、ポートは双方向ステートとなります。

## 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 コマンドでポートを単一方向として設定すると、ポートはスパンニングツリー フォワーディング ステートに移行します。

WoL をイネーブル化すると、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 ステートになります。ホストは、ネットワーク内の他の装置とトラフィックを交換しません。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ホストは、ネットワーク内の他の装置から送信されるトラフィックの受信しかできません。単一方向ポートで着信トラフィックを受信すると、ポートはデフォルト双方向ステートに戻り、スパンニングツリー ブロッキング ステートに移行します。ホストが初期化ステートに移行すると、EAPOL パケット以外のトラフィックは処理できなくなります。ポートが双方向ステートに戻ると、スイッチは 5 分タイマーを起動します。タイマーが時間切れになる前にポートが認証されないと、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 コマンドでポートを双方向として設定すると、ポートは双方向でアクセス制御されます。この状態では、スイッチ ポートはパケットの送受信をしません。

## IEEE 802.1x 認証の設定

ここでは、次の設定情報について説明します。

- IEEE 802.1x のデフォルト設定 (p.9-13)
- IEEE 802.1x 設定時の注意事項 (p.9-14)
- IEEE 802.1x 認証の設定 (p.9-15) (必須)
- スイッチと RADIUS サーバの間の通信の設定 (p.9-16) (必須)
- 定期的な再認証の設定 (p.9-19) (任意)
- ポートに接続するクライアントの手動での再認証 (p.9-19) (任意)
- 待機時間の変更 (p.9-20) (任意)
- スイッチからクライアントへの再送信時間の変更 (p.9-20) (任意)
- スイッチからクライアントへのフレーム再送信回数の設定 (p.9-21) (任意)
- 再認証回数の設定 (p.9-22) (任意)
- ホストモードの設定 (p.9-23) (任意)
- ゲスト VLAN の設定 (p.9-23) (任意)
- 制限 VLAN の設定 (p.9-25) (任意)
- IEEE 802.1x 設定のデフォルト値へのリセット (p.9-27) (任意)
- IEEE 802.1x アカウンティングの設定 (p.9-27) (任意)

## IEEE 802.1x のデフォルト設定

表 9-2 に、IEEE 802.1x のデフォルト設定を示します。

表 9-2 IEEE 802.1x のデフォルト設定

機能	デフォルト設定
Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング)	ディセーブル
方向制御	双方向制御
RADIUS サーバ <ul style="list-style-type: none"> <li>• IP アドレス</li> <li>• UDP 認証ポート</li> <li>• 鍵</li> </ul>	<ul style="list-style-type: none"> <li>• 指定なし</li> <li>• 1812</li> <li>• 指定なし</li> </ul>
スイッチの IEEE 802.1x イネーブル ステータス	ディセーブル
ポート単位の IEEE 802.1x イネーブル ステータス	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
再認証回数	2 回 (ポートが未許可ステータスに移行する前に、スイッチが認証プロセスを再開する回数)
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)

表 9-2 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 EAP-Request/Identity 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起動する前に、EAP-Request/Identity 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
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、スイッチが返答を待ち、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、応答をサーバに再送信するまでの時間。この値は設定変更ができません。)

## IEEE 802.1x 設定時の注意事項

IEEE 802.1x 認証を設定する場合の注意事項は、次のとおりです。

- IEEE 802.1x をイネーブルにすると、他のレイヤ 2 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 のスタティック アクセス ポートおよび音声 VLAN ポート上ではサポートされますが、次のタイプのポートではサポートされません。
  - トランク ポート — トランク ポート上で 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、ネイバとトランク ポートへの変更をネゴシエートする場合があります。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]) ポート上で 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 対応ポートを変更してダイナミック VLAN を割り当てようとしても、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、またはこれからアクティブ メンバーにするポートを 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。
  - Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および RSPAN 宛先ポート — SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x をイネーブルにできます。ただし、ポートを 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 をイネーブルにできます。
- RSPAN VLAN または音声 VLAN を除く任意の VLAN を IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能はトランク ポート上ではサポートされず、アクセス ポート上でのみサポートされます。



- RSPAN VLAN または音声 VLAN を除く任意の VLAN を IEEE 802.1x 制限 VLAN として設定できます。制限 VLAN 機能はトランク ポート上ではサポートされず、アクセス ポート上でのみサポートされます。
- IEEE 802.1x をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した IEEE 802.1x はサポートされません。
- スイッチ上で、**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 IEEE 802.1x をグローバルにイネーブルにする前に、IEEE 802.1x と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Dynamic Host Configuration Protocol (DHCP) クライアントが接続する IEEE 802.1x ポートにゲスト VLAN を設定したあとは、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の IEEE 802.1x 認証プロセスを再開するための設定を変更することができます。IEEE 802.1x 認証プロセスの設定値を小さくします (**dot1x timeout quiet-period** および **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)。設定値を小さくする度合は、接続されている IEEE 802.1x クライアントのタイプによって異なります。

## IEEE 802.1x 認証の設定

IEEE 802.1x ポート ベース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、ユーザ認証のためにクエリ送信を行う手順と認証方式を記述したものです。

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。

次に、IEEE 802.1x の AAA プロセスを示します。

- 
- 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** RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜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** 必要に応じて、再認証が実行されます。
  - ステップ 6** スイッチが仮のアカウントिंग アップデートを、再認証結果に基づいたアカウントिंग サーバに送信します。
  - ステップ 7** ユーザがポートから切断します。
  - ステップ 8** スイッチが停止メッセージをアカウントिंग サーバに送信します。
- 


IEEE 802.1x ポート ベース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	目的
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>	IEEE 802.1x 認証方式リストを作成します。  <b>authentication</b> 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するデフォルトのリストを作成するには、 <b>default</b> キーワードの後ろにデフォルト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。  <i>method1</i> には、 <b>group radius</b> キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。   <b>(注)</b> <b>group radius</b> キーワード以外にもコマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 4	<code>dot1x system-auth-control</code>	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。
ステップ 5	<code>aaa authorization network {default} group radius</code>	(任意) 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。
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) RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
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しているポートを指定し、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 9	<code>switchport mode access</code>	(任意) ステップ 6 およびステップ 7 で RADIUS サーバを設定した場合のみ、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>	ポート上で IEEE 802.1x 認証をイネーブルにします。  機能の相互作用については、「 <a href="#">IEEE 802.1x 設定時の注意事項</a> 」(p.9-14) を参照してください。
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>	設定を確認します。
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 ファイルにエントリを保存します。

## スイッチと RADIUS サーバの間の通信の設定

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 ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス (たとえば認証) 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。

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	目的
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>RADIUS サーバパラメータを設定します。</p> <p><i>hostname   ip-address</i> 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><i>auth-port port-number</i> 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 です。指定できる範囲は 0 ~ 65536 です。</p> <p><i>key string</i> 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。</p> <p> (注) 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず <b>radius-server host</b> コマンド構文の最後のアイテム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、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないとください。鍵は RADIUS デーモンで使用する暗号鍵に一致する必要があります。</p> <p>複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。</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 ファイルにエントリを保存します。

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 172.120.39.46 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、暗号鍵を RADIUS サーバ上の鍵と同じ *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
```

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**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、「すべての RADIUS サーバの設定」(p.8-31) を参照してください。

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。

## 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 サーバを使用した IEEE 802.1x 認証を設定することもできます。

RADIUS サーバを使用した 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	目的
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>	アクティブな VLAN を、IEEE 802.1x ゲスト VLAN に指定します。指定できる範囲は 1 ~ 4094 です。  RSPAN VLAN または音声 VLAN を除く任意のアクティブな VLAN を IEEE 802.1x ゲスト VLAN として設定できません。
ステップ 4	<code>dot1x reauthentication</code>	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。
ステップ 5	<code>dot1x timeout reauth-period {seconds   server}</code>	再認証の間隔（秒）を指定します。  キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><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。</li> <li><code>server</code> — Session-Timeout RADIUS 属性（属性 [27]）の値として秒数を設定します。</li> </ul> このコマンドがスイッチに影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 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 ファイルにエントリを保存します。

次に、RADIUS サーバを使用した 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、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

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	目的
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 reauthentication</code>	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。
ステップ 4	<code>dot1x timeout reauth-period {seconds   server}</code>	再認証の間隔（秒）を指定します。  キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><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。</li> <li><code>server</code> — Session-Timeout RADIUS 属性（属性 [27]）の値として秒数を設定します。スイッチで NAC レイヤ 2 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。</li> </ul> このコマンドがスイッチに影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 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 ファイルにエントリを保存します。

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。再認証の間隔をデフォルトの秒数に戻すには、`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。

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

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

## ポートに接続するクライアントの手動での再認証

`dot1x re-authenticate interface interface-id` イネーブル EXEC コマンドを入力することにより、いつでも特定のポートに接続するクライアントを手動で再認証できます。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方法については、「[定期的な再認証の設定 \(p.9-19\)](#)」を参照してください。

次に、ポートに接続する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 gigabitethernet0/1
```

## 待機時間の変更

スイッチはクライアントを認証できなかった場合に、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。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、イネーブル 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	目的
ステップ 1	<b>configure terminal</b>	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	<b>interface interface-id</b>	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	<b>dot1x timeout quiet-period seconds</b>	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 1 ~ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show dot1x interface interface-id</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

待機時間をデフォルトに戻すには、**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
```

## スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity 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い場合や、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、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	目的
ステップ 1	<b>configure terminal</b>	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	<b>interface interface-id</b>	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。



	コマンド	目的
ステップ 3	<code>dot1x timeout tx-period seconds</code>	スイッチが EAP-Request/Identity 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 5 ~ 65535 秒です。デフォルトは 5 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 ファイルにエントリを保存します。

再送信時間をデフォルトに戻すには、`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 EAP-Request/Identity 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。

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

## スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへ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起動する前に、クライアントに EAP-Request/Identity 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は、リンクの信頼性が低い場合や、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、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	目的
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 max-reauth-req count</code>	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを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。
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 ファイルにエントリを保存します。

再送信回数をデフォルトに戻すには、`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、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 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

ポートが未許可状態に変化する前に、スイッチが認証プロセスを再開する回数を変更することもできます。



(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、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。

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	目的
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 max-reauth-req count</code>	ポートが未許可状態に変化する前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。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 ファイルにエントリを保存します。

再認証回数をデフォルトに戻すには、`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、ポートが未許可状態に変化する前に、スイッチが認証プロセスを再開する回数として 4 を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	目的
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>	複数ホストが間接的に接続されているポートを指定し、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 host-mode multi-host</code>	IEEE 802.1x 許可ポートで複数のホスト（クライアント）を接続できるようにします。  指定するインターフェイスでは、 <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 <b>auto</b> に設定されていることを確認してください。
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 ファイルにエントリを保存します。

ポート上で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、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 gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

## ゲスト VLAN の設定

サーバが EAP-Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、IEEE 802.1x 対応でないクライアントはゲスト 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実行します。この手順は任意です。

	コマンド	目的
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。サポートされるポートのタイプについては、「 <a href="#">IEEE 802.1x 設定時の注意事項</a> 」(p.9-14) 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 モードにします。
	または <code>switchport mode private-vlan host</code>	または 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。

	コマンド	目的
ステップ 4	<code>dot1x port-control auto</code>	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	<code>dot1x guest-vlan vlan-id</code>	アクティブな VLAN を、IEEE 802.1x ゲスト VLAN に指定します。指定できる範囲は 1 ~ 4094 です。  RSPAN VLAN または音声 VLAN を除く任意のアクティブな VLAN を 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 ファイルにエントリを保存します。

ゲスト VLAN をディセーブルにして削除するには、`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、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 gigabitethernet0/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間 (秒) を 15 に設定し、IEEE 802.1x ポートの DHCP クライアント接続時に、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-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 機能をイネーブルにできます。イネーブルにすると、スイッチは EAPOL パケットヒストリを維持せずに、インターフェイス上で EAPOL パケットが検出されている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するクライアントを許可します。

オプションのゲスト VLAN 機能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	目的
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>	スイッチ上でオプションのゲスト VLAN の機能を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、「 <a href="#">IEEE 802.1x 設定時の注意事項</a> 」(p.9-14) を参照してください。
ステップ 4	<code>switchport mode access</code>  または  <code>switchport mode private-vlan host</code>	ポートをアクセス モードにします。  または  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 5	<code>dot1x port-control auto</code>	ポート上で IEEE 802.1x 認証をイネーブルにします。

	コマンド	目的
ステップ 6	<code>dot1x guest-vlan vlan-id</code>	アクティブな VLAN を、IEEE 802.1x ゲスト VLAN に指定します。指定できる範囲は 1 ~ 4094 です。  RSPAN VLAN または音声 VLAN を除く任意のアクティブな VLAN を IEEE 802.1x ゲスト VLAN として設定できません。
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 ファイルにエントリを保存します。

`no dot1x guest-vlan supplicant` グローバル コンフィギュレーション コマンドを使用してオプションのゲスト VLAN 機能をディセーブルにできます。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。ポートがゲスト VLAN で許可されている場合、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 機能をイネーブルにし、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
```

## 制限 VLAN の設定

スイッチに制限 VLAN を設定した場合、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 対応のクライアントは制限 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実行します。この手順は任意です。

	コマンド	目的
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。サポートされるポートのタイプについては、「 <a href="#">IEEE 802.1x 設定時の注意事項</a> 」(p.9-14) 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 モードにします。
	または <code>switchport mode private-vlan host</code>	または 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	<code>dot1x port-control auto</code>	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	<code>dot1x auth-fail vlan vlan-id</code>	IEEE 802.1x 制限 VLAN にするアクティブな 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 を除く任意のアクティブな VLAN を IEEE 802.1x 制限 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。

	コマンド	目的
ステップ 7	<code>show dot1x interface interface-id</code>	(任意) 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 ファイルにエントリを保存します。

制限 VLAN をディセーブルにして削除するには、`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
```

認証の試行が可能な最大回数（この回数を超えるとユーザは制限 VLAN に割り当てられる）を設定するには、`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。認証試行に指定できる範囲は 1～3 です。デフォルトは 3 回です。

許可される認証試行の最大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	目的
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。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.9-14) を参照してください。
ステップ 3	<code>switchport mode access</code> または <code>switchport mode private-vlan host</code>	ポートをアクセス モードにします。 または 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	<code>dot1x port-control auto</code>	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	<code>dot1x auth-fail vlan vlan-id</code>	IEEE 802.1x 制限 VLAN にするアクティブな 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 を除く任意のアクティブな VLAN を IEEE 802.1x 制限 VLAN として設定できます。
ステップ 6	<code>dot1x auth-fail max-attempts max attempts</code>	認証の試行が可能な回数（この回数を超えるとポートは制限 VLAN に移動）を指定します。指定できる範囲は 1～3 です。デフォルトは 3 です。
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>	(任意) 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 ファイルにエントリを保存します。

デフォルト値に戻すには、`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、認証の試行が可能な回数（この回数を超えるとポートは制限 VLAN に移動）として 2 を設定する例を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```



## IEEE 802.1x 設定のデフォルト値へのリセット

IEEE 802.1x 設定をデフォルト値に戻すには、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	目的
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>	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、設定するポートを指定します。
ステップ 3	<code>dot1x default</code>	IEEE 802.1x パラメータをデフォルト値に戻します。
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 ファイルにエントリを保存します。

## IEEE 802.1x アカウンティングの設定

IEEE 802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、システムはログングのためアカウンティング RADIUS サーバに送信するイベントをリロードできます。サーバは、アクティブな IEEE 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、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。設定した回数のアカウンティング要求の再送信を行ったあと、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、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.
```

メッセージが正常に送信されない場合、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)

ログングの開始、停止、仮のアップデート メッセージ、タイム スタンプ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。これらの機能をオンにするには、RADIUS サーバの Network Configuration タブの [Update/Watchdog packets from this AAA client] のログングをイネーブルにします。次に、RADIUS サーバの System Configuration タブの [CVS RADIUS Accounting] をイネーブルにします。

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	目的
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。

	コマンド	目的
ステップ 4	<code>aaa accounting system default start-stop group radius</code>	(任意) システム アカウンティングをイネーブルにし (すべての RADIUS サーバのリストを使用して)、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 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 ファイルにエントリを保存します。

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、アカウンティングの UDP ポートとして 1813 を指定して、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 の統計情報およびステータスの表示

すべてのポートに関する 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。特定のポートに関する 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。

スイッチに関する IEEE 802.1x 管理および動作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。特定のポートに関する IEEE 802.1x 管理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。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

