CHAPTER 34

802.1X ポートベース認証の設定

この章では、IEEE 802.1X ポートベース認証を設定して、不正なクライアント デバイスによるネットワークへのアクセスを防止する方法について説明します。

この章の主な内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

802.1X ポートベース認証の概要

802.1X では、クライアント/サーバ ベースのアクセス コントロールと認証プロトコルとして 802.1X ポートベース認証を定義し、不正なクライアントが一般的にアクセス可能なポートを通じて LAN に接続するのを制限します。認証サーバは、オーセンティケータ（ネットワーク アクセス スイッチ）ポートに接続された各サプリカント（クライアント）を確認してから、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。

（注） 802.1X をサポートするには、Remote Authentication Dial-In User Service（RADIUS）用に設定された認証サーバが必要です。ネットワーク アクセス スイッチが設定済みの RADIUS サーバにパケットをルーティングできないと、802.1X 認証は機能しません。スイッチがパケットをルーティングできることを確認するには、スイッチからサーバに ping を送信します。

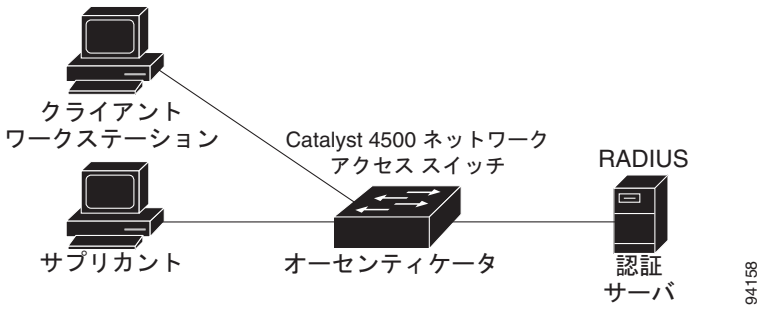
クライアントが認証されるまでは、クライアントが接続されたポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許容されます。認証が成功すると、通常のトラフィックがポートを通過できるようになります。

802.1X ポートベースの認証を設定するには、以下に説明する概念を理解する必要があります。

デバイスの役割

802.1X ポートベース認証では、ネットワーク装置は特定の役割を果たします。図 34-1 に、下記の各装置の役割を示します。

図 34-1　802.1x デバイスの役割



- クライアント：LAN へのアクセスを要求し、スイッチからの要求に応答するワークステーション。ワークステーションは、802.1X 準拠のクライアント ソフトウェアが動作するものでなければなりません。

（注）　802.1X 準拠のクライアント アプリケーション ソフトウェア（Microsoft の Windows 2000 Professional や Windows XP など）の詳細については、次の URL にある Microsoft Knowledge Base Article の資料を参照してください。http://support.microsoft.com

- オーセンティケータ：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。Catalyst 4500 シリーズ スイッチは、クライアントと認証サーバ間の仲介装置として機能し、クライアントに識別情報を要求して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。スイッチは Extensible Authentication Protocol（EAP）フレームのカプセル化およびカプセル化解除を行い、RADIUS 認証サーバと対話します。

  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。カプセル化では EAP フレームの変更または検証は行われず、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバからフレーム 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。

（注）　Catalyst 4500 シリーズ スイッチでは、RADIUS クライアントおよび 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、クライアントの識別情報を確認し、LAN およびスイッチ サービスへのクライアントのアクセスを許可することをスイッチに通知します （サポートされる認証サーバは、EAP 拡張機能を備えた RADIUS 認証サーバのみです。これは、Cisco Secure Access Control Server バージョン 3.2 以上で使用できます）。

802.1X とネットワーク アクセス コントロール

ネットワーク アクセス コントロールは、ポート アクセス ポリシーが認証装置のアンチウイルス ポスチャによって影響を受ける機能です。

アンチウイルス ポスチャの要素には、装置で実行するオペレーティング システム、オペレーティング システムのバージョン、アンチウイルス ソフトウェアのインストールの有無、使用可能なアンチウイルス シグニチャのバージョンなどがあります。認証装置に Network Admission Control（NAC）認識 802.1X サプリカントがあり、認証サーバが 802.1X 経由で NAC をサポートする設定の場合、アンチウイルス ポスチャ情報は自動的に 802.1X 認証交換の一部になります。

NAC の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6128/index.html

認証の開始およびメッセージ交換

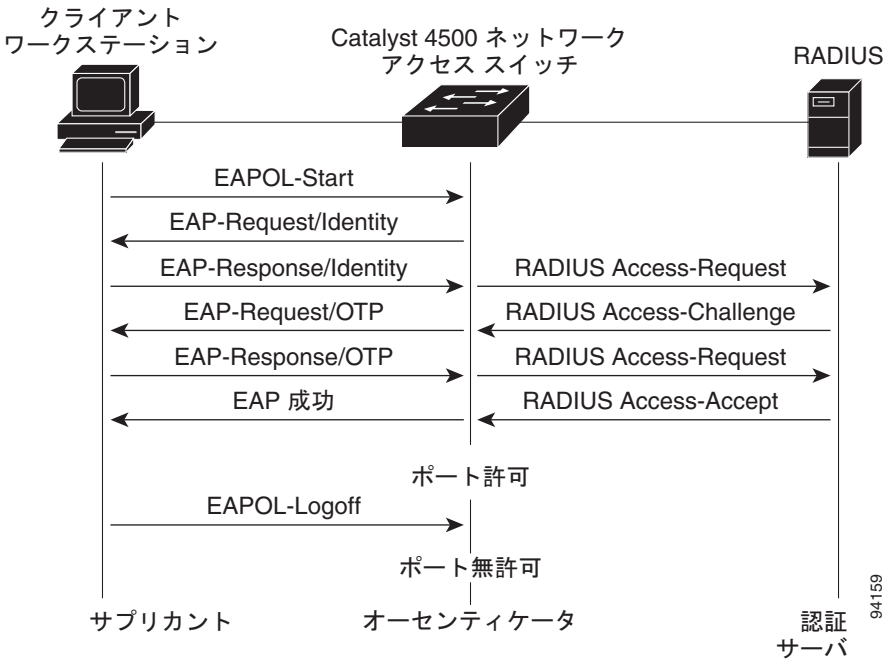
スイッチまたはクライアントのどちらからでも、認証を開始できます。**dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにする場合、スイッチは、ポートのリンク ステートが移行したことを確認したときに、認証を開始する必要があります。次に EAP-Request/Identity フレームをクライアントに送信して識別情報を要求します（一般に、スイッチは最初の Identity/Request フレームを送信して、そのあとで 1 つまたは複数の認証情報の要求を送信します）。クライアントはフレームを受信すると、EAP-Response/Identity 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。

ネットワーク アクセス スイッチで 802.1X がイネーブルになっていない場合、またはサポートされていない場合は、クライアントからの EAPOL フレームはドロップされます。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トであるものとしてフレームを送信します。ポートが認証ステートであるということは、クライアントが正しく認証されていることを意味します。クライアントが識別情報を送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間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。

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 34-2 に、認証サーバで One-Time-Password（OTP）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 34-2　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、クライアントがネットワーク アクセスを許可されているかどうかがわかります。ポートは、無許可ステートで開始します。ポートはこのステートにある間、802.1X プロトコル 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を許容しません。クライアントの認証が成功すると、ポートは許可ステートに移行し、クライアントのトラフィック送受信を通常どおりに許可します。

802.1X 非対応クライアントが無許可ステートの 802.1X ポートに接続している場合、スイッチはクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。802.1X 非対応クライアントに接続されたポート上にゲスト VLAN が設定されている場合、このポートは設定されたゲスト VLAN に追加され、許可ステートになります。詳細については、「ゲスト VLAN を使用した 802.1X 認証の使用」（P.34-8）を参照してください。

反対に、802.1x 対応のクライアントが、802.1x プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答を受信しなかった場合、クライアントは要求を固定回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

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 コマンドと次のキーワードを使用します。

- **force-authorized**：802.1X 認証をディセーブルにして、認証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との 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。この設定は、デフォルトです。
- **force-unauthorized**：ポートを無許可ステートのままにして、クライアントが認証を試みてもすべて無視します。スイッチはインターフェイス経由でクライアントに認証サービスを提供できません。
- **auto**：802.1X 認証をイネーブルにして、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start 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 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できます。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗した場合、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。指定された回数試行して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。

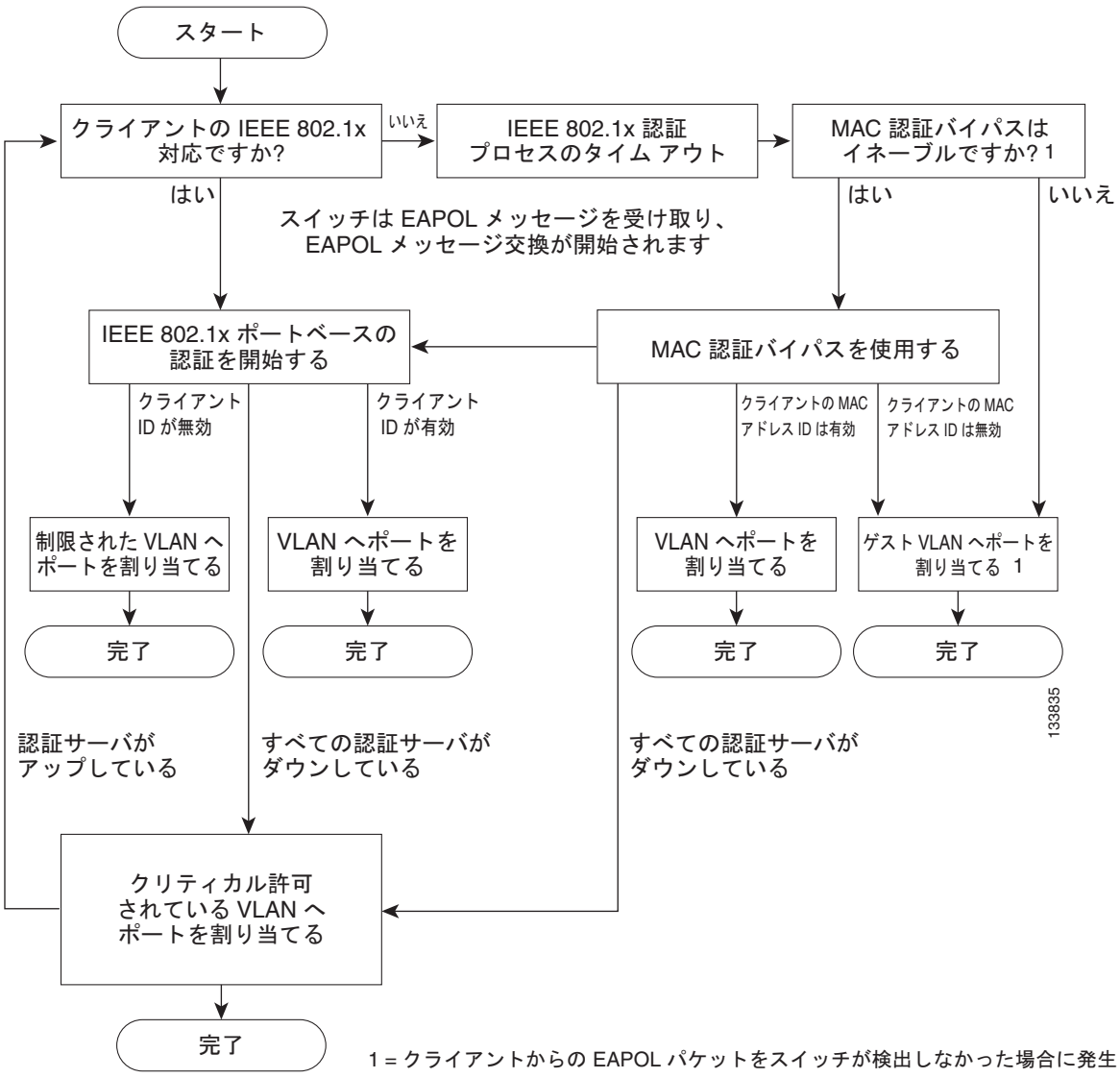
ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL-Logoff フレームを受信した場合、ポートは無許可ステートに戻ります。

図 34-3 に、認証プロセスを示します。

MDA がポートでイネーブルになっている場合、音声許可に適用可能な一部の例外付きでこのフローを使用できます。MDA の詳細については、「マルチドメイン認証の使用」（P.34-19）を参照してください。

（注）　Supervisor Engine 6-E は、MDA をサポートしていません。

図 34-3　認証フローチャート



1 = クライアントからの EAPOL パケットをスイッチが検出しなかった場合に発生

802.1X ホスト モード

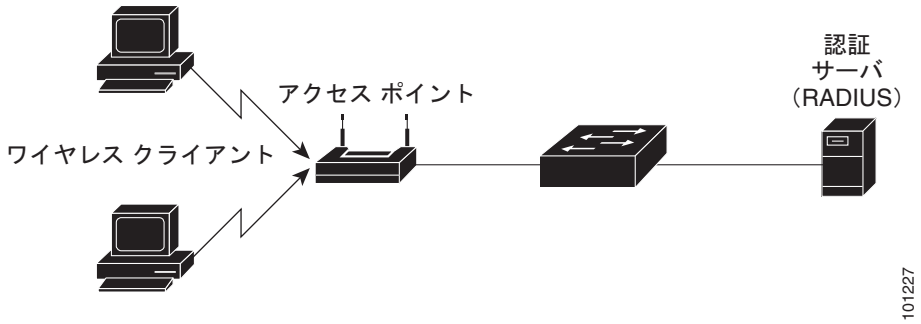
単一ホストまたは複数ホスト モードの 802.1X ポートを設定できます。単一ホスト モード（図 34-1 (P.34-2) を参照）では、802.1X 対応スイッチ ポートに接続できるのは 1 つのクライアントだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モードでは、複数のホストを 1 つの 802.1X 対応ポートに接続できます。図 34-4（P.34-7）に、ワイヤレス LAN における 802.1x ポート ベースの認証を示します。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、クライアントすべてのネットワーク 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（再認証が失敗するか、または EAPOL-Logoff メッセージを受

信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチ ホスト モードがイネーブルになっている場合、802.1X 認証を使用してポートおよびポート セキュリティを認証し、クライアントも含めて、すべての MAC アドレスへのネットワーク アクセスを管理できます。

図 34-4　　マルチ ホスト モードの例



Cisco IOS Release 12.2(37)SG およびそれ以降のリリースは、データ デバイスと IP Phone（Cisco または Cisco 以外）などの音声デバイスの両方が同じスイッチ ポートに接続することを許可する MDA をサポートします。MDA の設定方法については、「マルチドメイン認証の使用」（P.34-19）を参照してください。

VLAN 割り当てを使用した 802.1X 認証の利用

VLAN 割り当てを使用すると、ネットワーク アクセスを特定のユーザに限定できます。VLAN 割り当てでは、802.1X で認証されたポートはポートに接続したクライアントのユーザ名に基づいて VLAN に割り当てられます。RADIUS サーバ データベースは、ユーザ名 /VLAN マッピングを保持します。ポートの 802.1X 認証が成功すると、RADIUS サーバは VLAN 割り当てをスイッチに送信します。この場合の VLAN は、「標準」VLAN または PVLAN です。

PVLAN をサポートするプラットフォームでは、ポートを PVLAN に割り当てることによってホストを分離できます。

スイッチおよび RADIUS サーバ上で設定する場合、VLAN 割り当てを使用した 802.1X 認証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は、認証が成功したときにポートは自身のアクセス VLAN または独立 PVLAN に設定されます。
- 認証サーバが無効な VLAN 情報を提供した場合、ポートは無許可ステートのままになります。これは、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ぐためです。
- 認証サーバが有効な VLAN 情報を提供した場合、認証に成功すると、ポートは許可ステートになり、指定された VLAN に追加されます。
- 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ユーザと同じ VLAN 内にあります。
- ポート上で 802.1X がディセーブルになると、そのポートは設定されたアクセス VLAN に戻ります。

- ポートは、アクセス ポート（「通常の」VLAN にのみ割り当て可能）か、または PVLAN ホスト ポート（PVLAN にのみ割り当て可能）として設定する必要があります。ポートを PVLAN ホスト ポートとして設定すると、ポート上のすべてのホストはそのポスチャが適合か不適合かにかかわらず、PVLAN に割り当てられることになります。Access-Accept に示された VLAN タイプが、ポートに割り当てられると予測される VLAN タイプ（アクセス ポートには通常の VLAN、プライベート VLAN ホスト ポートにはセカンダリ プライベート VLAN）と一致しない場合、VLAN 割り当ては失敗します。
- ゲスト VLAN が応答しないホストを処理するよう設定されている場合、ゲスト VLAN として設定されている VLAN タイプがポート タイプと一致する必要があります（つまり、アクセス ポート上で設定されたゲスト VLAN の場合は標準 VLAN、PVLAN ホスト ポート上で設定されたゲスト VLAN の場合は PVLAN）。ゲスト VLAN のタイプが、ポート タイプと一致しない場合、応答しないホストはゲスト VLAN が設定されていない場合と同じように処理されます（つまり、ネットワーク アクセスを拒否されます）。
- ポートを PVLAN に割り当てるには、示された VLAN がセカンダリ PVLAN である必要があります。スイッチは、ローカルに設定されたセカンダリ/プライマリのアソシエーションから暗黙のプライマリ VLAN を判別します。

（注） RADIUS が割り当てた VLAN で認証されているポートのアクセス VLAN または PVLAN ホスト VLAN マッピングを変更すると、ポートは RADIUS が割り当てた VLAN に残ったままになります。

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。**aaa authorization network group radius** コマンドを適用する方法については、「802.1X 認証のイネーブル化」（P.23）を参照してください。
- 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 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属性を割り当てます。VLAN を適切に割り当てるには、RADIUS サーバが次の属性をスイッチに返す必要があります。
  - トンネル タイプ = VLAN
  - トンネル メディア タイプ = 802
  - トンネル プライベート グループ ID = VLAN NAME

ゲスト VLAN を使用した 802.1X 認証の使用

（注） Supervisor Engine 6-E は、この機能をサポートして*いません*。

ゲスト VLAN を使用すると、802.1X 非対応ホストが 802.1X 認証を使用するネットワークにアクセスできるようになります。たとえば、802.1X 認証をサポートするようにシステムをアップグレードしている間も、ゲスト VLAN を使用できます。

ゲスト VLAN はポート単位でサポートされ、その VLAN タイプがポート タイプと一致するかぎり、すべての VLAN をゲスト VLAN として使用できます。ポートがすでにゲスト VLAN 上で転送を行っている場合に、そのホストのネットワーク インターフェイス上で 802.1X サポートをイネーブルにすると、ポートはただちにゲスト VLAN から除外され、オーセンティケータは認証の開始を待機します。

ポート上での 802.1X 認証をイネーブルにすると、802.1X プロトコルが開始されます。ホストが一定期間内にオーセンティケータからのパケットに応答できなかった場合、オーセンティケータはそのポートを設定済みのゲスト VLAN に追加します。

ポートが PVLAN ホスト ポートとして設定されている場合、ゲスト VLAN はセカンダリ PVLAN である必要があります。ポートがアクセス ポートとして設定されている場合、ゲスト VLAN は通常の VLAN である必要があります。ポート上で設定されたゲスト VLAN が、ポート タイプに適さない場合、スイッチはゲスト VLAN が設定されていないように動作します（すなわち、応答しないホストはネットワーク アクセスを拒否されます）。

ゲスト VLAN の設定方法については、「ゲスト VLAN を使用した 802.1X 認証の設定」（P.34-31）を参照してください。

ゲスト VLAN を使用した 802.1X 認証の使用上の注意事項

ゲスト VLAN を使用した 802.1X 認証の使用上の注意事項は次のとおりです。

- ゲスト VLAN を別の VLAN に再設定すると、認証失敗ポートもすべて移動され、ポートは現在の許可ステートのままです。
- ゲスト VLAN をシャット ダウンするか、または VLAN データベースから削除すると、すべての認証失敗ポートはただちに無許可ステートに移行し、認証プロセスが再び開始されます。

（注）　ゲスト VLAN では定期的な再認証を行うことはできません。

Windows XP ホスト上でのゲスト VLAN 使用 802.1X 認証の使用上の注意事項

Windows XP ホスト上でのゲスト VLAN に対する 802.1X 認証の使用上の注意事項は次のとおりです。

- ホストがオーセンティケータに応答しない場合、ポートは接続を 3 回試行します（試行間隔は 30 秒です）。このあとは、ログイン/パスワード ウィンドウはホストに表示されなくなります。ネットワーク インターフェイス ケーブルを取り外し、再接続する必要があります。
- 不正なログイン/パスワードで応答するホストは、認証に失敗します。認証に失敗したホストは、ゲスト VLAN に追加されません。ホストが初めて認証に失敗すると、待機時間タイマーが始動し、タイマーが満了するまでアクティビティが一切発生しません。待機時間タイマーが満了すると、ホストにログイン/パスワード ウィンドウが表示されます。ホストが 2 度めも認証に失敗すると、待機時間タイマーが再度始動し、タイマーが満了するまでアクティビティは一切発生しません。ホストにはこのあとさらに、3 度めのログイン/パスワード ウィンドウが表示されます。ホストが 3 度めの認証に失敗すると、ポートは無許可ステートになり、ネットワーク インターフェイス ケーブルを取り外して再接続することが必要になります。

MAC 認証バイパスを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートして*いません*。

802.1X プロトコルには、クライアント（サプリカント）、オーセンティケータ、認証サーバの 3 つのエンティティがあります。通常、ホスト PC はサプリカント ソフトウェアを実行し、自分自身を認証するために資格情報をオーセンティケータに送信します。オーセンティケータはその情報を認証サーバに送信して認証を求めます。

しかし、すべてのホストにサプリカント機能があるわけではありません。802.1X を使用して自分自身を認証できないがネットワークにアクセスする必要がある装置は、MAC 認証バイパス（MAB）が使用できます。MAB は、接続先装置の MAC アドレスを使用してネットワーク アクセスを認可または拒否します。

通常、この機能はプリンタなどの装置が接続されているポートで使用します。これらの装置には 802.1X サプリカント機能がありません。

通常の構成では、RADIUS サーバはアクセスが必要な MAC アドレスのデータベースを保持します。この機能によって新しい MAC アドレスがポートで検出されると、装置の MAC アドレスとしてユーザ名とパスワードが使用された RADIUS 要求が生成されます。許可に成功したら、802.1X サプリカントを処理するときに 802.1X 認証で行われるのと同じコード パスを通じて、ポートからその装置にアクセスできるようになります。認証に失敗すると、ポートはゲスト VLAN に移動するか（ゲスト VLAN が設定されている場合）、未認証のままになります。

Catalyst 4500 シリーズ スイッチは、ポート レベルごとの MAC の再認証もサポートします。再認証機能は 802.1X から提供され、MAB 固有ではありません。再認証モードでは、ポートは RADIUS から送信された VLAN にとどまり、自分自身を再認証しようとします。再認証に成功すると、ポートは RADIUS から送信された VLAN にとどまります。失敗した場合は、ポートは未認証になり、ゲスト VLAN が設定されている場合はゲスト VLAN に移動します。

MAB の設定方法については、「MAC 認証バイパスを使用した 802.1X 認証の設定」（P.34-34）を参照してください。

機能の相互作用

ここでは、MAB がイネーブルの場合の機能の相互作用と制約事項を示します。MAB とシームレスに相互作用する機能については説明していません（単方向制御ポートなど）。

- MAB は、ポートに 802.1X が設定されている場合にだけイネーブルにできます。MAB は MAC を認証するフォール バック メカニズムとしてのみ機能します。ポートに MAB と 802.1X を同時に設定すると、ポートは 802.1X を使用して認証しようとします。ホストが EAPOL 要求への応答に失敗した場合に MAB が設定されていると、802.1X ポートが開かれパケットを受信して MAC アドレスを取得します。無限に認証が続くことはありません。

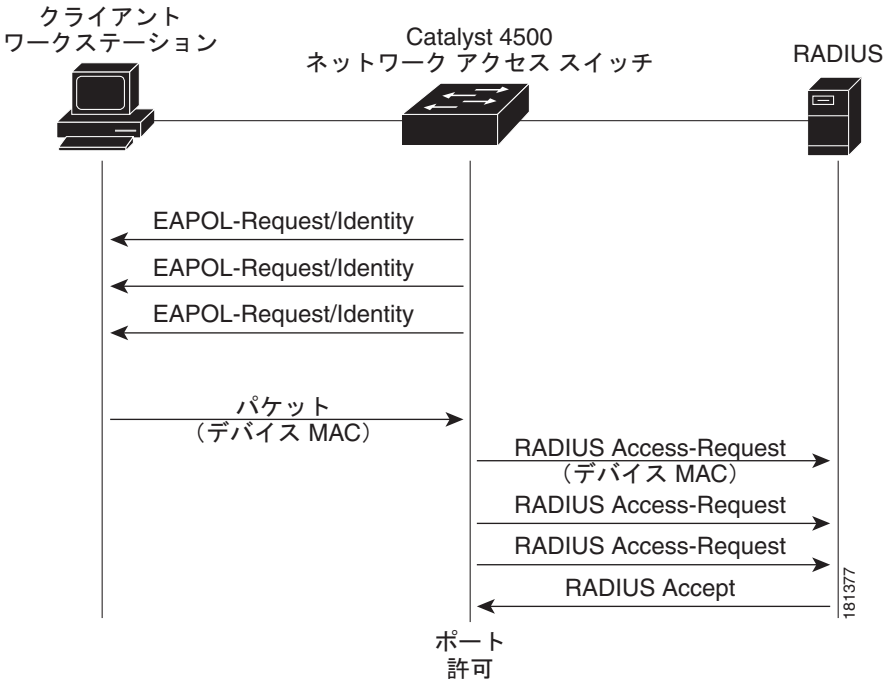
  デフォルトの 802.1X タイマー値に基づき、メカニズム間の移行にはおよそ 90 秒かかります。転送時間の値を小さくすれば時間を短くできますが、EAPOL 転送頻度に影響を与えます。値が小さくなると EAPOL の送信間隔が短くなります。MAB がイネーブルな状態で 802.1X が EAPOL のフルセットを 1 回実行すると、学習された MAC アドレスが認証サーバに送信されて処理されます。

  MAB モジュールは、ライン上で検出された最初の MAC アドレスの許可を実行します。RADIUS が承認する有効な MAC アドレスが受信されると、ポートは許可されたと見なされます。

  MAB の結果として最初に許可されたポートで EAPOL パケットが受信されると、802.1X 認証は再起動できます。

  図 34-5 に、MAB 時のメッセージ交換を示します。

図 34-5　MAC 認証バイパス時のメッセージ交換



- 認証に失敗した VLAN は、802.1X 認証に失敗したユーザだけが使用します。MAB は 802.1X 認証に失敗したユーザに対しては試みられません。802.1X 認証に失敗すると、MAB の設定の有無にかかわらずポートは認証失敗 VLAN（設定されている場合）に移動します。
- MAB とゲスト VLAN の両方が設定されており EAPOL パケットがポートで受信されなかった場合、802.1X ステート マシンは MAB ステートに移行し、ここでポートが開いてトラフィックを受信し MAC アドレスを取得します。ポートは、MAC を認識するまではこのステートのままです。アドレスが許可に失敗すると、ポートはゲスト VLAN（設定されている場合）に移動します。

  ゲスト VLAN 内のポートは、指定されたゲスト VLAN のすべてのトラフィックに対してオープンです。このため、通常は許可されるが、許可に失敗した装置が早い段階で検出されたためにゲスト VLAN になった非 802.1X サプリカントは、いつまでもゲスト VLAN に残ります。ただし、リンクが消失したりライン上で EAPOL が検出されるとゲスト VLAN 外に移動し、デフォルトの 802.1X モードに戻ります。
- MAB によって新しい MAC が認証されると、802.1X オーセンティケータ（またはポート セキュリティ）によってアクセスが制限されるようになり、ポートのセキュリティが保護されます。802.1X デフォルト ホスト パラメータは、単一ホストだけに定義されます。ポートがマルチユーザ ポストに変更されると、ポート セキュリティが採用され、このポートで許容される MAC アドレスの数が適用されます。

- Catalyst 4500 シリーズ スイッチは VVID を持つ MAB をサポートしますが、MAC アドレスはポート データ VLAN だけに表示されます。CDP を通じて学習したすべての IP フォンの MAC は、音声 VLAN で許容されます。
- MAB と VMPS の機能は重複しており、相互に排他的です。

アクセス不能認証バイパスを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートして*いません*。

スイッチが設定された RADIUS サーバに到達できないためにクライアント（サプリカント）が認証されない場合、アクセス不能認証バイパスがイネーブルの*クリティカル* ポートに接続するホストにネットワーク アクセスできるようにスイッチを設定できます。

この機能がイネーブルの場合、スイッチは設定された RADIUS サーバのステータスをモニタリングします。使用できる RADIUS サーバがない場合、アクセス不能認証バイパスがイネーブルのポートは許可されます。アクセス不能認証バイパス VLAN はポート ベースごとに設定できます。

RADIUS が使用できなくなった時点で許可されているポートは、アクセス不能認証バイパスの影響を受けません。ただし、再認証時に次のポーリング サイクルで RADIUS が復旧しない場合、すでに許可されているポートはクリティカル認証 VLAN に戻ります。

RADIUS が使用できるようになると、クリティカル許可されたポートは、自動的に自分自身を再認証するように設定されます。

アクセス不能認証バイパスの設定方法については、「アクセス不能認証バイパスを使用した 802.1X 認証の設定」（P.34-35）を参照してください。

単方向制御ポートを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートして*いません*。

単方向制御ポートはハードウェアおよびソフトウェア機能が組み合わせられており、*マジック パケット*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 の「電源を投入」します。通常、単方向制御ポートは、システムの電源が切断されていると考えられるような時間帯に管理者がリモート システムを管理する環境で使用されます。

802.1X ポート経由で接続されているホストで単方向制御ポートを使用した場合、ホストの電源が切断されると 802.1X ポートが未認証になるという独特の問題が発生します。この場合、ポートでは EAPOL パケットだけしか送受信できません。このため単方向制御ポートのマジック パケットはホストに到達できず、電源を投入しない限り PC で認証することもポートを開くこともできません。

単方向制御ポートは、未許可 802.1X ポートでパケットの送信を許容することにより、この問題を解決します。

（注）　単方向制御ポートは、ポートのスパニングツリー PortFast がイネーブルである場合のみ機能。

802.1X 単方向制御ポートの設定方法については、「単方向制御ポートを使用した 802.1X 認証の設定」（P.34-38）を参照してください。

単方向ステート

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に設定すると、そのポートはスパニングツリー フォワーディング ステートに移行します。

単方向制御ポートをイネーブルにすると、接続ホストはスリープ モードまたは電源切断状態になります。ホストはそのネットワークの他の装置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方向ポートに接続されている場合、ホストはネットワークの他の装置からのトラフィックだけを受信します。

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に設定すると、ポートは両方向のアクセスを制御します。この場合、スイッチ ポートは EAPOL パケット以外のパケットを送受信しません。

認証失敗 VLAN 割り当てを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

ポート単位で認証失敗 VLAN 割り当てを使用すると、認証失敗ユーザがアクセスできるようにします。認証失敗ユーザは、802.1X には対応できるが認証サーバ内に有効な資格情報を持たないエンド ホストか、またはユーザ側の認証ポップアップ ウィンドウでユーザ名とパスワードの組み合わせが入力されていないエンド ホストです。

ユーザが認証プロセスに失敗した場合、このポートは認証失敗 VLAN に置かれます。このポートは再認証タイマーが切れるまで、認証失敗 VLAN に残ります。再認証タイマーが切れると、スイッチはポート再認証要求の送信を開始します。ポートが再認証に失敗した場合は、認証失敗 VLAN に残ります。ポートが再認証に成功した場合は、RADIUS サーバにより送信された VLAN、または新たに認証されたポートに設定された VLAN に移動されます。移動先は、RADIUS サーバが VLAN 情報を送信するように設定されているかどうかによって異なります。

（注）　定期的な再認証をイネーブルにする場合（「定期的な再認証のイネーブル化」（P.34-41）を参照）、ローカル再認証タイマー値だけが使用できます。RADIUS サーバを利用して再認証タイマー値を割り当てることはできません。

ポートが認証失敗 VLAN に移動される前に、オーセンティケータが送信する最大認証試行回数を設定できます。オーセンティケータは、各ポートの失敗した認証試行回数をカウントします。失敗した認証試行とは、空の応答または EAP 失敗のいずれかを指します。オーセンティケータは、認証試行回数に対して失敗した認証のすべての試行をまとめてカウントします。最大試行回数を超えると、ポートは再認証タイマーが次に切れるまで認証失敗 VLAN に置かれます。

（注）　EAP をサポートしない RADIUS は、EAP パケットを含まない応答を送信する場合があります。また、サードパーティ製の RADIUS サーバも空の応答を送信する場合があります。このような場合、認証試行カウンタは増加します。

認証失敗 VLAN 割り当てを設定する方法については、「認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定」（P.34-39）を参照してください。

認証失敗 VLAN 割り当ての使用上の注意事項

- 再認証をイネーブルにする必要があります。再認証がディセーブルの場合、認証失敗 VLAN 内のポートは再認証試行を受け入れません。再認証プロセスを開始するには、認証失敗 VLAN がポートからのリンク ダウン イベントまたは EAP ログオフ イベントを受信する必要があります。ホストがハブの背後にある場合は、次の再認証が試行されるまでリンク ダウン イベントを受信しなかったり、新しいホストを検出しなかったりする可能性があります。したがって、このような場合は再認証をイネーブルにすることを推奨します。
- EAP 失敗メッセージは、ユーザに送信されません。ユーザが認証に失敗した場合、ポートは認証失敗 VLAN に移され、EAP 成功メッセージがユーザに送信されます。ユーザには認証失敗が通知されないため、ネットワークへのアクセスが制限される理由がわからない場合があります。EAP 成功メッセージが送信される理由は、次のとおりです。
  - EAP 成功メッセージが送信されなければ、ユーザは EAP 開始メッセージを送信して 60 秒ごとに（デフォルト）認証を試行します。
  - 場合によっては、ユーザが EAP 成功に DHCP を設定していて、成功を確認しない限り、ポート上で DHCP が動作しないこともあります。
- ユーザはオーセンティケータから EAP 成功メッセージを受信したあと、不正なユーザ名とパスワードの組み合わせをキャッシュして、再認証ごとにこの情報を再利用する場合があります。ユーザが正確なユーザ名とパスワードの組み合わせを渡すまで、ポートは認証失敗 VLAN に残されます。
- 認証失敗ポートが無許可ステートに移行すると、認証プロセスが再開されます。再度認証プロセスに失敗する場合には、オーセンティケータは保留ステートで待機します。正しく再認証されると、すべての 802.1X ポートは再度初期化され、通常の 802.1X ポートとして扱われます。
- 認証失敗 VLAN を別の VLAN に再設定すると、認証失敗ポートもすべて移動され、ポートは現在の許可ステートのままになります。
- 認証失敗 VLAN をシャット ダウンするか、または VLAN データベースから削除すると、すべての認証失敗ポートはただちに無許可ステートに移行され、認証プロセスが再開されます。認証失敗 VLAN 設定がまだ存在するため、オーセンティケータは保留ステートで待機しません。認証失敗 VLAN が非アクティブである間は、すべての認証試行がカウントされ、VLAN がアクティブになるとすぐにポートは認証失敗 VLAN に置かれます。
- VLAN で許容される最大認証失敗数を再設定した場合、この変更は再認証タイマーが切れたあとで有効になります。
- レイヤ 3 ポートで使用されるすべての内部 VLAN は、認証失敗 VLAN として設定できません。
- 認証失敗 VLAN は、単一ホスト モード（デフォルトのポート モード）でのみサポートされます。
- ポートが認証失敗 VLAN に置かれると、ユーザの MAC アドレスが MAC アドレス テーブルに追加されます。ポートで新しい MAC アドレスが検出されると、セキュリティ違反として扱われます。
- 認証失敗ポートが認証失敗 VLAN に移動されると、Catalyst 4500 シリーズ スイッチは通常の 802.1X 認証の場合とは異なり、RADIUS-Account Start メッセージを送信しません。

ポート セキュリティを使用した 802.1X 認証の利用

単一ホスト モードまたは複数ホスト モードのどちらかの 802.1X ポートでポート セキュリティをイネーブルにできます （そのためには、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 セキュリティを設定する必要があります。このガイドの第 nb 章を参照）。ポート上のポート セキュリティと 802.1X をイネーブルにすると、802.1X がポートを認証し、

ポート セキュリティがポート上で許容される MAC アドレス数（クライアントの MAC アドレスを含む）を管理します。したがって、ポート セキュリティがイネーブルの状態で 802.1X ポートを使用すると、ネットワークに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。

複数ホスト モードの指定については、「802.1X 設定をデフォルト値にリセットする方法」（P.34-47）を参照してください。

次に、スイッチ上の 802.1X とポート セキュリティ間の対話の例を示します。

- 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でない場合、そのクライアントの 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）。

  ポート上で別のホストが学習されると、セキュリティ違反が発生します。その場合に取られる処置は、セキュリティ違反を検出した機能（802.1X またはポート セキュリティ）によって異なります。

  - 802.1X が違反を検出した場合は、ポートが errdisable になります。
  - ポート セキュリティが違反を検出した場合は、ポートがシャットダウンするか、または制限されます（対処法は設定可能です）。

  ポート セキュリティおよび 802.1X セキュリティ違反が発生した場合の説明を、次に示します。

  - 単一ホスト モードの場合にポートが許可されると、クライアント MAC アドレス以外の受信されたすべての MAC アドレスによって、802.1X セキュリティ違反が引き起こされます。
  - 単一ホスト モードの場合に、（設定済みのセキュア MAC アドレスによって）ポート セキュリティが限度に達していることが原因で、802.1X クライアントの MAC アドレスの導入に失敗すると、ポート セキュリティ違反が引き起こされます。
  - 複数ホスト モードの場合にポートが許可されると、ポート セキュリティが限度に達していることが原因で導入できない追加 MAC アドレスにより、ポート セキュリティ違反が引き起こされます。

- 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 エントリが削除されます。そのあと、通常の認証が行われます。
- ポートが管理上のシャットダウン状態になると、ポートは無許可ステートになり、すべてのダイナミック エントリがセキュア ホスト テーブルから削除されます。
- ポート セキュリティ テーブルからクライアントの MAC アドレスを削除できるのは、802.1X のみです。複数ホスト モードでは、クライアントの MAC アドレスを除き、ポート セキュリティによって学習されたすべての MAC アドレスを、ポート セキュリティ CLI を使用して削除できます。
- ポート セキュリティによって 802.1X クライアントの MAC アドレスが期限切れになると、802.1X はクライアントの再認証を試行します。ポート セキュリティ テーブル内でクライアントの MAC アドレスを保持できるのは、再認証に成功した場合のみです。
- CLI を使用してポート セキュリティ テーブルを表示すると、802.1X クライアントのすべての MAC アドレスに dot1x というタグが付けられます。

RADIUS によるセッション タイムアウトを使用した 802.1X 認証の利用

スイッチで使用する再認証タイムアウトを、ローカルに設定されたものと RADIUS によるもののどちらにするかを指定できます。スイッチがローカル設定のタイムアウトを使用するように設定されている場合、タイマーが切れるとホストを再認証します。

スイッチが RADIUS によるセッション タイムアウトを使用するように設定されている場合、スイッチは RADIUS Access-Accept メッセージの Session-Timeout および任意の Termination-Action 属性を確認します。スイッチは、セッションの期間を判断するためには Session-Timeout 属性の値を使用し、セッションのタイマーが切れた際のスイッチのアクションを判断するためには Termination-Action 属性の値を使用します。

Termination-Action 属性が存在し、その値が RADIUS-Request である場合、スイッチはホストを再認証します。Termination-Action 属性が存在しないか、またはその値が Default である場合、スイッチはセッションを終了します。

（注）　ポート上のサプリカントは、そのセッションが終了され、新しいセッションを開始しようとすることを認識します。認証サーバがこの新しいセッションを別に処理しない限り、スイッチが新しいセッションを確立しても、クライアントはネットワーク接続に少しの割り込みしか確認しない可能性があります。

スイッチが RADIUS によるタイムアウトを使用するように設定されているが、Access-Accept メッセージに Session-Timeout 属性が含まれない場合、スイッチはサプリカントを再認証しません。これは、シスコのワイヤレス アクセス ポイントに一貫した動作です。

RADIUS によるセッション タイムアウトを設定する方法については、「RADIUS によるセッション タイムアウトの設定」（P.34-30）を参照してください。

RADIUS アカウンティングを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

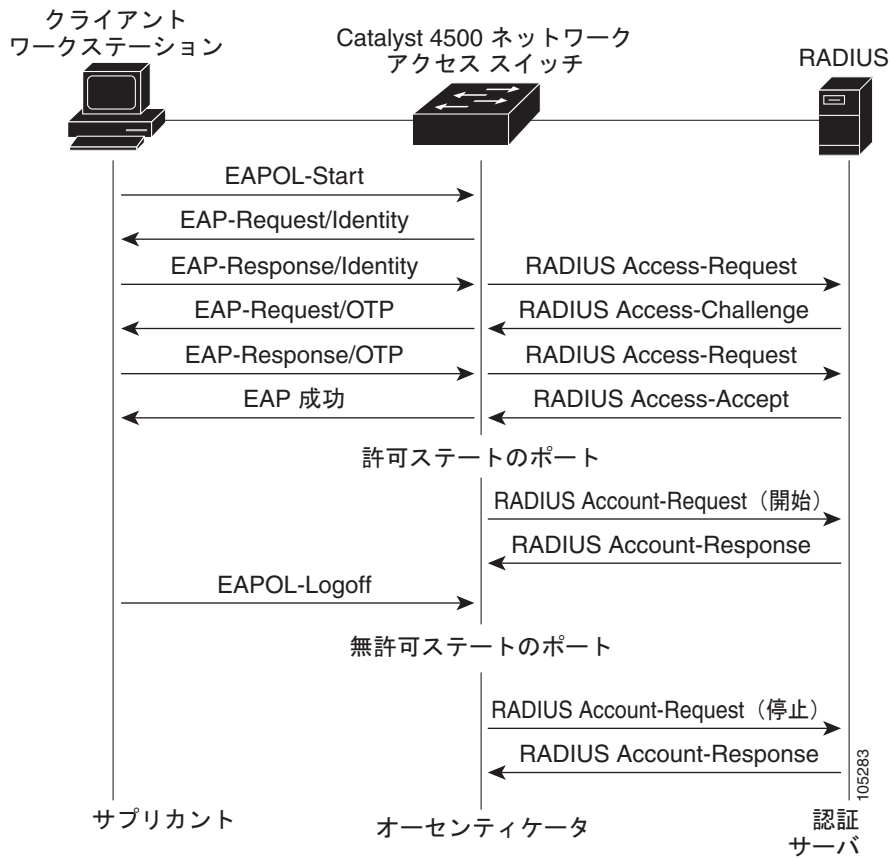
（注）　システム全体にアカウンティングを実装する場合は、802.1X アカウンティングも設定する必要があります。さらに、システムのリロード時にシステム リロード イベントをアカウンティング サーバに通知する必要もあります。これにより、アカウンティング サーバは、このシステム上のすべての未処理 802.1X セッションが終了していることを確認できます。

（注）　802.1X アカウンティングをイネーブルにするには、最初に 802.1X 認証を設定し、スイッチから RADIUS サーバへの通信を設定する必要があります。

802.1X RADIUS アカウンティングは重要なイベント（クライアントの接続セッションなど）を RADIUS サーバにリレーします。このセッションは、クライアントがポートの使用を許可された時点から、クライアントがポートの使用を停止した時点までの間隔として定義されます。

図 34-6 に RADIUS アカウンティング プロセスを示します。

図 34-6　RADIUS アカウンティング



クライアントが認証されると、スイッチはアカウンティング要求パケットを RADIUS サーバに送信します。RADIUS サーバはアカウンティング応答パケットで応答して、要求受領に確認応答を行います。

RADIUS アカウンティング要求パケットには、各種イベントおよび関連情報を RADIUS サーバにレポートするための Attribute/Value ペアが 1 つ以上格納されます。追跡されるイベントは、次のとおりです。

- ユーザの正常な認証
- ユーザのログオフ
- 802.1X ポートで発生したリンクダウン
- 再認証の成功
- 再認証の失敗

ポートが許可ステートから無許可ステートに移行すると、RADIUS メッセージが RADIUS サーバに送信されます。

スイッチはアカウンティング情報を記録しないで、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。

802.1X の認証、許可、およびアカウンティング プロセスは、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　ユーザ名 / パスワード方式などを使用して、認証が実行されます。

ステップ 3　必要に応じて、RADIUS サーバ設定ごとに、VLAN 割り当てが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ティング 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、再認証の結果に基づく内部アカウンティング アップデートをアカウンティング 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ティング サーバに送信します。

802.1X アカウンティングを設定するには、次の作業を実行する必要があります。

- 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。
- RADIUS サーバの [System Configuration] タブで、[Logging>CVS RADIUS Accounting] をイネーブルにします。
- スイッチ上で 802.1X アカウンティングをイネーブルにします。
- **aaa system accounting** コマンドを使用して、AAA アカウンティングをイネーブルにします。「802.1X RADIUS アカウンティングのイネーブル化」（P.34-31）を参照してください。

802.1X アカウンティングとともに 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 リロード イベントをアカウンティング RADIUS サーバに送信して、記録できます。これにより、アカウンティング RADIUS サーバは、すべてのアクティブな 802.1X セッションが適切に終了すると推測します。

RADIUS は信頼性のないトランスポート プロトコルである UDP を使用するため、ネットワーク状態が悪い場合は、アカウンティング メッセージが失われることがあります。設定可能な回数だけアカウンティング要求を再送信しても、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.
```

Stop 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.
```

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** コマンドを使用します。

音声 VLAN ポートを使用した 802.1X 認証の利用

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

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

- IP Phone へ、または IP Phone から音声トラフィックを伝送するための Voice VLAN ID（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 経由でスイッチに接続されたワークステーションへ、またはワークステーションからデータ トラフィックを伝送する Port VLAN ID（PVID）。PVID は、ポートのネイティブ VLAN です。

音声 VLAN に設定する各ポートは、VVID および PVID に関連付けられています。この設定により、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。

ポートが AUTHORIZED か UNAUTHORIZED かにかかわらずリンクがある場合、音声 VLAN ポートはアクティブになります。音声 VLAN を介するすべてのトラフィックは正常に認識され、MAC アドレス テーブルに表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、いくつかの Cisco IP Phone が連続して接続されている場合、スイッチは直接接続している IP Phone だけを認識します。802.1X が音声 VLAN ポートでイネーブルの場合、スイッチは複数のホップの認識されていない Cisco IP Phone からのパケットをドロップします。

802.1X がポートでイネーブルの場合、VVID と同じ PVID を設定できません。音声 VLAN の詳細については、第 33 章「音声インターフェイスの設定」を参照してください。

次の機能の相互作用に注意してください。

- 802.1X VLAN 割り当ては、音声 VLAN と同じ VLAN のポートに割り当てることができません。割り当てると 802.1X 認証が失敗します。
- 802.1X ゲスト VLAN は、802.1X 音声 VLAN ポート機能と連動します。ただし、同一 VLAN をゲスト VLAN と音声 VLAN には設定できません。
- 802.1X ポート セキュリティは 802.1X 音声 VLAN ポート機能と連動し、ポート単位で設定されます。VVID の Cisco IP Phone MAC アドレスと PVID の PC MAC アドレスの、2 つの MAC アドレスを設定する必要があります。

  ただし、802.1 X ポート セキュリティのスティッキ MAC アドレス設定および静的に設定された MAC アドレス設定とともに、802.1X 音声 VLAN ポート機能を使用することはできません。
- 802.1X アカウンティングは、802.1X 音声 VLAN ポート機能による影響を受けません。
- 802.1X がポート上で設定されている場合、ハブを介して複数の IP Phone を Catalyst 4500 シリーズ スイッチに接続することはできません。
- 音声 VLAN はプライベート VLAN のホスト ポートとして設定できず、プライベート VLAN のホスト ポートに割り当てられるのはプライベート VLAN だけであるため、VLAN 割り当てでは音声 VLAN が設定されたポートにプライベート VLAN を割り当てることができません。

音声 VLAN に 802.1X を設定する方法については、「音声 VLAN に対する 802.1X 認証の設定」（P.34-40）を参照してください。

マルチドメイン認証の使用

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

Multiple Domain Authentication（MDA; マルチドメイン認証）は、データ デバイスと IP Phone（Cisco または Cisco 以外）などの音声デバイスの両方が、データ ドメインと音声ドメインに分割される同一スイッチ ポートで認証できるようにします。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応ポートで、データ デバイスを認証する前に音声デバイスを認証する必要があります。

MDA の設定には、次の注意事項を参考にしてください。

- MDA のスイッチ ポートを設定するには、「マルチドメイン認証の設定」（P.34-27）を参照してください。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 33 章「音声インターフェイスの設定」を参照してください。

（注）　MDA 対応スイッチ ポートでの音声 VLAN の割り当てにダイナミック VLAN を使用すると、音声デバイスは許可されません。

- 音声デバイスを許可するには、値を device-traffic-class=voice に設定した Cisco 属性値（AV）ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応ポートでのデータ デバイスにだけ適用されます。スイッチは、許可されなかった音声デバイスをデータ デバイスと 見なします。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errordisable になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ デバイスにだけ RADIUS サーバからダイナミック VLAN 割り当てを使用できます。

（注）　Supervisor Engine 6-E は、*ダイナミック VLAN をサポートしていません。*

- MDA はフォールバック メカニズムとして MAC 認証バイパスを使用して、スイッチ ポートが 802.1X 認証をサポートしないデバイスに接続できるようにします。これは特に 802.1X サプリカントのないサードパーティ電話で役立ちます。詳細については、「MAC 認証バイパスを使用した 802.1X 認証の利用」（P.34-9）を参照してください。
- *データ*または*音声*デバイスがポートで検出されると、許可に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスが*データ* VLAN で検出された場合や、複数の音声デバイスが*音声* VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、音声 VLAN のポートで許可されている Cisco IP Phone は自動的に削除されるため、そのポート上で再認証される必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- データ ドメインが最初に許可され、ゲスト VLAN に設定された場合、非 802.1X 対応音声デバイスは音声 VLAN のパケットにタグを付け、認証をトリガーする必要があります。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

サポートされるトポロジー

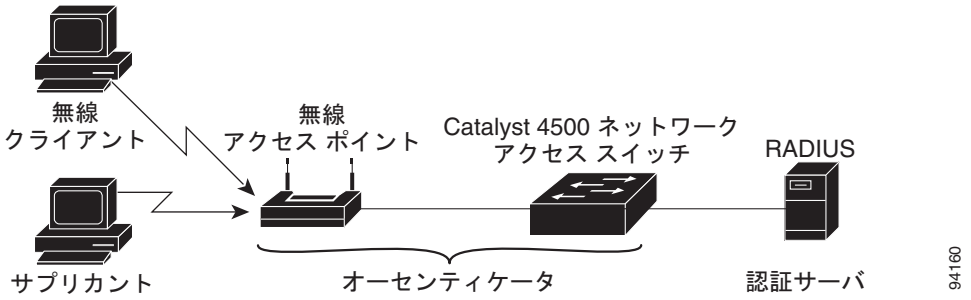
802.1X ポートベースの認証は、次の 2 つのトポロジをサポートします。

- ポイントツーポイント
- ワイヤレス LAN

ポイントツーポイント構成（図 34-1（P.34-2）を参照）では、複数ホスト モードがイネーブルでない場合（デフォルト）、802.1X 対応スイッチ 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 ステートに変化すると、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。

ワイヤレス LAN の 802.1X ポートベース認証（図 34-7）では、クライアントが認証されるとすぐにワイヤレス アクセス ポイントとして認証される 802.1X ポートを複数ホスト ポートとして設定します（「802.1X 設定をデフォルト値にリセットする方法」（P.34-47）を参照）ポートが許可されると、ポートに間接的に接続されたホストを除くすべてのホストに対して、ネットワーク アクセスが許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL-Logoff メッセージを受信すると）、スイッチは、ワイヤレス アクセス ポイントに接続されたすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジでは、ワイヤレス 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 34-7　　ワイヤレス LAN の例



802.1X の設定

802.1X を設定する手順は次のとおりです。

ステップ 1　802.1X 認証をイネーブルにします。「802.1X 認証のイネーブル化」（P.34-23）を参照してください。

ステップ 2　スイッチ/RADIUS サーバ通信を設定します。「スイッチ/RADIUS サーバ通信の設定」（P.34-25）を参照してください。

ステップ 3　802.1X タイマー値を調整します。「待機時間の変更」（P.34-43）を参照してください。

ステップ 4　任意の機能を設定します。「RADIUS によるセッション タイムアウトの設定」（P.34-30）を参照してください。

ここでは、802.1X を設定する方法について説明します。

802.1X のデフォルト設定

表 34-1 に、802.1X のデフォルト設定を示します。

表 34-1　802.1x のデフォルト設定

機能	デフォルト設定
認証、許可、アカウンティング（AAA）	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • Key	 • 指定なし • 1812 • 指定なし
インターフェイス単位の 802.1x プロトコル イネーブル ステート	強制認証 ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
定期的な再認証	ディセーブル

表 34-1　802.1x のデフォルト設定 （続き）

機能	デフォルト設定
再認証の試行間隔	3600 秒
待機時間	60 秒 スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数。
再送信時間	30 秒 要求を再送信するまでに、スイッチがクライアントからの EAP-Request/Identity フレームに対する応答を待機する秒数です。
最大再送信回数	2 認証プロセスを再開するまでにスイッチが EAP-Request/Identity フレームを送信する回数です。
複数ホストのサポート	ディセーブル
クライアント タイムアウト時間	30 秒 認証サーバからの要求をクライアントにリレーするとき、クライアントに要求を再送信するまでにスイッチが応答を待機する時間です。
認証サーバ タイムアウト時間	30 秒 クライアントの応答を認証サーバにリレーするとき、サーバに応答を再送信するまでにスイッチが応答を待機する時間です。この値は設定不可能です。

802.1X 設定時の注意事項

802.1X 認証を設定する場合の注意事項は次のとおりです。

- 802.1X プロトコルがサポートされるのは、レイヤ 2 スタティック アクセス、プライベート VLAN ホスト ポート、およびレイヤ 3 ルーテッド ポートにかぎられます。その他のポート モードには 802.1X を設定できません。
- 802.1X アカウンティングまたは VLAN 割り当てのどちらかを使用する場合は、両方の機能で一般的な AAA コマンドが利用されることに留意してください。AAA の設定については、「802.1X 認証のイネーブル化」（P.34-23）を参照してください。または、Cisco IOS セキュリティに関する次のマニュアルを参照してください。
  - http://www.cisco.com/en/US/products/ps6586/products_ios_technology_home.html

802.1X 認証のイネーブル化

802.1X ポート ベース認証をイネーブルにするには、まずスイッチ上で 802.1X をグローバルにイネーブルにしてから、AAA をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

ソフトウェアは、方式リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリスト内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し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

（注）　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。

802.1X ポートベース認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# dot1x system-auth-control`	スイッチ上で 802.1X をイネーブルにします。 スイッチ上で 802.1X をグローバルにディセーブルにするには、**no dot1x system-auth-control** コマンドを使用します。
ステップ 3	`Switch(config)# aaa new-model`	AAA をイネーブルにします。 AAA をディセーブルにするには、**no aaa new-model** コマンドを使用します。
ステップ 4	`Switch(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1X AAA 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式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 次のキーワードのうち、少なくとも 1 つを指定します。 • **group radius**：すべての RADIUS サーバのリストを認証に使用します。 • **none**：認証を使用しません。クライアントは、クライアントが提供する情報を使用しないで、スイッチによって自動的に認証されます。 802.1X AAA 認証をディセーブルにするには、**no aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2...*] 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。
ステップ 5	`Switch(config)# aaa authorization network {default} group radius`	（任意）ネットワーク関連のすべてのサービス要求（VLAN 割り当てなど）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	`Switch(config)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 7	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 8	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 9	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 10	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	`Switch # show dot1x interface interface-id details`	入力を確認します。 この出力の 802.1X ポート サマリー セクションの PortControl 行を調べます。PortControl 値は **auto** に設定されています。
ステップ 12	`Switch# show running-config`	入力を確認します。
ステップ 13	`Switch# 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。

（注）　スパニングツリー PortFast をイネーブルにすると、許可直後にポートが必ずアップになります。

（注）　ポートに任意の 802.1X パラメータを設定すると、ポート上に 802.1X 認証が自動的に作成されます。結果的に、設定に **dot1x pae authenticator** が表示されます。手動での操作を行わずに、802.1X 認証をレガシー コンフィギュレーション上でそのまま実行することができます。これは、今後のリリースで変更される可能性があります。

次に、ファスト イーサネット ポート 2/1 で 802.1X と AAA をイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch# show dot1x interface f7/1 details

Dot1x Info for FastEthernet7/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 1000.0000.2e00
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED

Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = N/A
```

スイッチ/RADIUS サーバ通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と各 UDP ポート番号、あるいは IP アドレスと各 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って、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービ

ス（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 のホストエントリは、設定された順序で試行されます。

スイッチ上で RADIUS サーバ パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# radius-server host {hostname | ip-address} auth-port port-number [acct-port port-number] [test username name] [ignore-auth-port] [ignore-acct-port] [idle-time min] key string`	スイッチ上に 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。 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。 **auth-port** *port-number* には、認証要求のための UDP 宛先ポートを指定します。デフォルトは 1812 です。 **acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。デフォルト値は 1813 です。 RADIUS サーバの自動テストをイネーブルにし、RADIUS サーバのアップとダウンを検出するには、**test username** *name* を使用します。**name** パラメータはテスト アクセス要求で使用するユーザ名で、RADIUS サーバに送信されます。サーバに設定されている有効なユーザである必要はありません。**ignore-auth-port** オプションと **ignore-acct-port** オプションを使用すると、認証ポートとアカウンティング ポートのテストをそれぞれディセーブルにします。 **idle-time** *min* パラメータには、アイドル状態の RADIUS サーバがまだアップであることを確認するまでの時間を分単位で指定します。デフォルトは 60 分です。 **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 **（注）** キーの先行スペースは無視されますが、キーの内部および終わりのスペースは有効であるため、キーは必ず **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。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し使用してください。
ステップ 3	`Switch(config-if)# radius deadtime min`	（任意）ダウンしていた RADIUS サーバがアップしたかどうかをテストするまでの時間を分単位で指定します。デフォルトは 1 分です。

	コマンド	目的
ステップ 4	`Switch(config-if)# radius dead-criteria time seconds tries num`	（任意）RADIUS サーバがダウンしているかどうかを判断する基準を設定します。**time** パラメータには、サーバへの要求に応答がなくなってからサーバがダウンと判断されるまでの時間を秒単位で指定します。**tries** パラメータには、サーバがダウンと判断されるまでにサーバへの要求に応答がない回数を指定します。 これらのパラメータの推奨値は、**radius-server retransmit** に等しい **tries** および **radius-server retransmit** x **radius-server timeout** に等しい **time** です。
ステップ 5	`Switch(config-if)# ip radius source-interface m/p`	すべての発信 RADIUS パケットの送信元アドレスとして使用する IP アドレスを確立します。
ステップ 6	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show running-config`	入力を確認します。
ステップ 8	`Switch# 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。

次に、IP アドレスが 172.120.39.46 であるサーバを RADIUS サーバとして指定する例を示します。最初のコマンドはポート 1612 を許可ポートとして指定し、暗号キーを rad123 に設定します。

2 番めのコマンドは、RADIUS サーバ上でキーを照合するように指定します。

```
Switch# configure terminal
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
Switch(config)# ip radius source-interface m/p
Switch(config)# end
Switch#
```

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号化キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。

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。

マルチドメイン認証の設定

MDA を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# radius-server vsa send authentication`	ネットワーク アクセス サーバが、ベンダー固有属性（VSA）を認識して使用するように設定します。
ステップ 3	`Switch(config)# interface` *interface-id*	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。

	コマンド	目的
ステップ 4	`Switch(config-if)# [no] dot1x host-mode {single-host | multi-host | multi-domain}`	キーワードの意味は次のとおりです。 • **single-host**：IEEE 802.1X 許可ポートのシングル ホスト（クライアント）を許可します。 • **multi-host**：シングル ホストの認証後に 802.1X 許可ポートのマルチ ホストを許可します。 • **multi-domain**：ホストおよび IP Phone（Cisco または Cisco 以外）などの音声デバイスの両方が、IEEE 802.1X 許可ポートで認証されるようにします。 **（注）** ホスト モードが **multi-domain** に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 33 章「音声インターフェイスの設定」を参照してください。 指定されたインターフェイスについて、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。 ポート上の複数の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。
ステップ 5	`Switch(config-if)# switchport voice vlan` *vlan-id*	（任意）音声 VLAN を設定します。
ステップ 6	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show dot1x interface` *interface-id* `[detail]`	入力を確認します。
ステップ 8	`Switch# 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。

次に、802.1X 認証をイネーブルにし、複数ホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにし、ポート上でホストと 802.1X 音声デバイス（802.1X サプリカントを持つ Cisco またはサードパーティ電話など）の両方を許可する例を示します。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shut
Switch(config-if)# end
```

次に、MDA をイネーブルにし、ポート上でホストと 802.1X 以外の音声デバイスを許可する例を示します。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# no shut
Switch(config-if)# end
```

次に、インターフェイス FastEthernet6/1 での dot1x MDA 設定を確認する例を示します。

```
Switch# show dot1x interface FastEthernet3/1 detail

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_DOMAIN
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List
-------------------------------
Domain                    = DATA
Supplicant                = 0000.0000.ab01
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = 12

Domain                    = VOICE
Supplicant                = 0060.b057.4687
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server

Switch#
```

RADIUS によるセッション タイムアウトの設定

Catalyst 4500 シリーズ スイッチでは、RADIUS による再認証タイムアウトを使用するように設定できます。

RADIUS によるタイムアウトを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface` *interface-id*	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	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 5	`Switch(config-if)# dot1x timeout reauth-period` {*interface* | `server`}	再認証時間（秒）を設定します。
ステップ 6	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show dot1x interface` *interface-id* `details`	入力を確認します。
ステップ 8	`Switch # 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。

次に、スイッチがサーバから再認証時間を取得するように設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch# show dot1x interface f7/1 det

Dot1x Info for FastEthernet7/11
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = (From Authentication Server)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List Empty

Port Status               = AUTHORIZED

Switch#
```

802.1X RADIUS アカウンティングのイネーブル化

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

802.1X アカウンティングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# aaa accounting dot1x default start-stop group radius`	全 RADIUS サーバのリストを使用して、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	`Switch(config)# clock timezone PST -8`	アカウンティングのイベントタイム スタンプ フィールドで使用する時間帯を設定します。
ステップ 4	`Switch(config)# clock calendar-valid`	アカウンティングのイベントタイム スタンプ フィールドの日付をイネーブルにします。
ステップ 5	`Switch(config)# aaa accounting system default start-stop group radius`	（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）、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 6	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show running-config`	入力を確認します。
ステップ 8	`Switch# 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。

次に、IP アドレスが 172.120.39.46 であるサーバを RADIUS サーバとして指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、ポート 1612 を許可ポートに、1813 をアカウンティング用の UDP ポートに、rad123 を暗号キーに指定します。

```
Switch# configure terminal
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
Switch(config)# end
Switch#
```

（注）　ロギングの開始、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] のロギ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。

ゲスト VLAN を使用した 802.1X 認証の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

Catalyst 4500 シリーズ スイッチの各 802.1X ポートにゲスト VLAN を設定して、クライアントに限定されたサービス（802.1X クライアントのダウンロードなど）を提供できます。これらのクライアントは 802.1X 認証用にシステムをアップグレードできる場合もありますが、一部のホストには（Windows 98 システムなど）802.1X 対応でないものもあります。

802.1X ポート上でゲスト VLAN をイネーブルにすると、(1) 認証サーバが EAPOL request/identity フレームに対する応答を受信しない場合、または（2）EAPOL パケットがクライアントにより送信されない場合、Catalyst 4500 シリーズ スイッチはクライアントをゲスト VLAN に割り当てます。

Cisco IOS Release 12.2(25)EWA 以降では、Catalyst 4500 シリーズ スイッチでは EAPOL パケット履歴が保持されます。リンクの存続期間中に他の EAPOL パケットがインターフェイス上で検出された場合、ネットワーク アクセスは拒否されます。EAPOL 履歴は、リンクの消失時にリセットされます。

スイッチ ポートがゲスト VLAN に移されると、許可される 802.1X 非対応クライアントの許容数に制限がなくなります。802.1X 対応クライアントが、ゲスト VLAN が設定されたのと同じポートに参加する場合、ポートはユーザ設定のアクセス VLAN 内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、単一ホスト モードまたは複数ホスト モードの 802.1X ポートでサポートされます。

（注） ポートがゲスト VLAN に追加されると、自動的に複数ホスト モードになり、このポートを介してポートを無制限に接続できるようになります。複数ホスト設定を変更しても、ゲスト VLAN 内のポートには影響しません。

（注） RSPAN VLAN または音声 VLAN 以外の任意のアクティブな VLAN を、802.1X ゲスト VLAN として設定できます。

ポート上のゲスト VLAN に 802.1X を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。

ステップ 3	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		PVLAN トランクとのアソシエーションが有効であるポートが、アクティブ ホストのプライベート VLAN トランク ポートになるように指定します。

ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 5	`Switch(config-if)# dot1x guest-vlan` *vlan-id*	特定のインターフェイス上でゲスト VLAN をイネーブルにします。 特定のポート上でゲスト VLAN 機能をディセーブルにするには、**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。
ステップ 6	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 7	`Switch(config-if)# end`	コンフィギュレーション モードに戻ります。
ステップ 8	`Switch(config)# end`	特権 EXEC モードに戻ります。

次に、FastEthernet 4/3 上の通常の VLAN 50 をスタティックなアクセス ポート上のゲスト VLAN としてイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 50
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

次に、セカンダリ プライベート VLAN 100 をプライベート VLAN ホスト ポート上のゲスト VLAN としてイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 100
Switch(config-if)# end
Switch#
```

サプリカントがスイッチ上のゲスト VLAN で許容されるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch# dot1x guest-vlan supplicant`	（任意）サプリカントがスイッチ上のゲスト VLAN にグローバルに許容されるようにします。 **（注）** Cisco IOS リリース 12.3(31)SG の CLI では表示されませんが、**dot1x guest-vlan supplicant** コマンドを含むレガシー コンフィギュレーションは現在も動作します。ただし、認証失敗 VLAN オプションによってこのコマンドの必要性がなくなったため、推奨しません。 スイッチ上でサプリカントのゲスト VLAN 機能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。
ステップ 3	`Switch(config)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。

ステップ 4	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		PVLAN トランクとのアソシエーションが有効であるポートが、アクティブ ホストのプライベート VLAN トランク ポートになるように指定します。

ステップ 5	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 6	`Switch(config-if)# dot1x guest-vlan` *vlan-id*	アクティブ VLAN を 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。
ステップ 7	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 8	`Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	`Switch# show dot1x interface interface-id`	入力を確認します。
ステップ 10	`Switch# 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。

次に、ゲスト VLAN 機能をイネーブルにし、ゲスト VLAN として VLAN 5 を指定する例を示します。

```
Switch# configure terminal
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

MAC 認証バイパスを使用した 802.1X 認証の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

MAB をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# 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	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		PVLAN トランクとのアソシエーションが有効であるポートが、アクティブ ホストのプライベート VLAN トランク ポートになるように指定します。

ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 5	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 6	`Switch(config-if)# dot1x mac-auth-bypass [eap]`	スイッチの MAB をイネーブルにします。
ステップ 7	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show dot1x interface interface-id details`	（任意）入力を確認します。
ステップ 9	`Switch# 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。

（注）　ポートの 802.1X MAB 設定を削除しても、ポートの許可ステートおよび認証ステートには影響がありません。ポートが無認証ステートであれば、そのステートのまま残ります。MAB のためにポートが認証ステートであれば、スイッチは 802.1X オーセンティケータに戻ります。MAC アドレスによりポートがすでに許可されている場合に、MAB 設定が削除されると、再認証されるまでポートは許可ステートのままになります。そのとき 802.1X サプリカントがライン上で検出されれば、MAC アドレスは削除されます。

次に、ギガビット イーサネット インターフェイス 3/3 で MAB をイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# end
Switch# show dot1x int g3/3 details
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 1
RateLimitPeriod           = 0
Mac-Auth-Bypass           = Enabled

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0000.0000.0001
 Auth SM State     = AUTHENTICATED
 Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
Authentication Method     = MAB
Authorized By             = Authentication Server
Vlan Policy               = N/A

Switch#
```

アクセス不能認証バイパスを使用した 802.1X 認証の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

注意　アクセス不能認証バイパスを正しく機能させるには、「スイッチ /RADIUS サーバ通信の設定」（P.34-25）で説明されているようにスイッチを設定して RADIUS サーバのステートをモニタリングする必要があります。特に、RADIUS テスト ユーザ名、アイドル時間、ダウン時間、およびダウン

基準を設定する必要があります。設定しない場合、スイッチは RADIUS サーバがダウンしても検出できなかったり、動作しない RADIUS サーバを動作していると早まってマーキングしてしまったりします。

ポートをクリティカル ポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# dot1x critical eapol`	（任意）EAP 交換を通じてポートが部分的にクリティカル許可されているとき EAPOL-Success パケットを送信するかどうかを設定します。 **（注）**　一部のサプリカントでは必須です。 デフォルトでは、ポートがクリティカル許可されている場合は EAPOL-Success パケットは送信しません。
ステップ 3	`Switch(config)# dot1x critical recovery delay` *msec*	（任意）RADIUS サーバが使用可能になったとき、クリティカル許可されたポートの再初期化スロットル レートを指定します。デフォルトのスロットル レートは 100 ミリ秒です。これは、1 秒に 10 ポートが再初期化されることを表します。
ステップ 4	`Switch(config)# 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 5	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		PVLAN トランクとのアソシエーションが有効であるポートが、アクティブ ホストのプライベート VLAN トランク ポートになるように指定します。

ステップ 6	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 7	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 8	`Switch(config-if)# dot1x critical`	ポートのアクセス不能認証バイパス機能をイネーブルにします。 この機能をディセーブルにするには、**no dot1x critical** コンフィギュレーション コマンドを使用します。
ステップ 9	`Switch(config-if)# dot1x critical vlan` *vlan*	（任意）ポートがクリティカル許可されている場合に割り当てられる VLAN を指定します。 **（注）**　Supervisor Engine 6-E は、この機能をサポートしていません。 デフォルトでは、ポートで設定された VLAN を使用します。
ステップ 10	`Switch(config-if)# dot1x critical recovery action reinitialize`	（任意）ポートがクリティカル許可されており RADIUS が使用可能であれば、ポートを再初期化することを指定します。 デフォルトでは、ポートを再初期化しません。
ステップ 11	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 12	`Switch# show dot1x interface` *interface-id* `details`	（任意）入力内容を確認します。
ステップ 13	`Switch# 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。

次に、アクセス不能認証バイパスを使用した 802.1X 認証の完全な設定例を示します。これには、「802.1X 認証のイネーブル化」（P.34-23）および「スイッチ/RADIUS サーバ通信の設定」（P.34-25）で指定した必須の AAA および RADIUS 設定が含まれます。

設定された RADIUS サーバの IP アドレスは 10.1.2.3 で、認証にはポート 1812 を、アカウンティングには 1813 を使用します。RADIUS 秘密キーは *mykey* です。テスト サーバ プローブに使用するユーザ名は *randomuser* です。アップとダウンの両方のサーバに対するテスト プローブは 1 分間に 1 回生成されます。ファスト イーサネット インターフェイス 3/1 は、AAA の応答がなくなると VLAN 17 でクリティカル認証され、AAA が再び使用可能になると自動的に再初期化するように設定されます。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# radius-server host 10.1.2.3 auth-port 1812 acct-port 1813 test username
randomuser idle-time 1 key mykey
Switch(config)# radius deadtime 1
Switch(config)# radius dead-criteria time 15 tries 3
Switch(config)# interface f3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical vlan 17
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# end
Switch# show dot1x int fastethernet 3/1 det

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Critical-Auth             = Enabled
Critical Recovery Action  = Reinitialize
Critical-Auth VLAN        = 17

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0000.0000.0001

Auth SM State     = AUTHENTICATING
Auth BEND SM Stat = RESPONSE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Critical-Auth
Operational HostMode      = SINGLE_HOST
Vlan Policy               = 17

Switch#
```

単方向制御ポートを使用した 802.1X 認証の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

単方向制御ポートを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# 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	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
		PVLAN トランクとのアソシエーションが有効であるポートが、アクティブ ホストのプライベート VLAN トランク ポートになるように指定します。

ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 5	`Switch(config-if)# dot1x control-direction {in | both}`	ポート ベースごとに単方向ポート制御をイネーブルにします。
ステップ 6	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show dot1x interface` *interface-id* `details`	（任意）入力を確認します。
ステップ 8	`Switch# 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。

（注）　単方向制御ポートは、ポートのスパニングツリー PortFast がイネーブルである場合のみ機能。

デバイスが単方向制御ポート（Wake On LAN とも呼ばれる）に対してイネーブルになっている場合、インターフェイスは、デバイスがスリープ状態の場合にアップのままになります。そのため、デバイスに接続されたポートがリンク アップ（接続）として表示されます。ポートに特殊なパケットを転送すると、デバイスが起動します。

次に、単方向ポート制御をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x control-direction in
Switch(config-if)# end
Switch# show dot1x int g3/3
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In (Inactive)
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
```

```
SuppTimeout                 = 30
ReAuthPeriod                = 3600 (Locally configured)
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30
RateLimitPeriod             = 0

Switch#
```

認証失敗 VLAN 割り当てを使用した 802.1X 認証の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

Catalyst 4500 シリーズ スイッチのレイヤ 2 ポートに認証失敗 VLAN アライメントを設定すると、認証プロセスに失敗するクライアントに限定的なネットワーク サービスを提供できます。

（注）　認証失敗 VLAN 割り当ては、他のセキュリティ機能（ダイナミック ARP インスペクション（DAI）、Dynamic Host Configuration Protocol（DHCP）スヌーピング、および IP ソース ガードなど）と併用できます。認証失敗 VLAN 上では、これらの機能を個別にイネーブルおよびディセーブルにできます。

認証失敗 VLAN 割り当てを使用した 802.1X を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 5	`Switch(config-if)# dot1x auth-fail vlan` *vlan-id*	特定のインターフェイス上で認証失敗 VLAN をイネーブルにします。 特定のポートで認証失敗 VLAN 機能をディセーブルにするには、**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。
ステップ 6	`Switch(config-if)# dot1x auth-fail max-attempts` *max-attemtps*	ポートが認証失敗 VLAN に移される前の、最大試行回数を設定します。 デフォルトの試行回数は 3 です。
ステップ 7	`Switch(config-if)# end`	コンフィギュレーション モードに戻ります。
ステップ 8	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	`Switch# show dot1x interface` *interface-id* `details`	（任意）入力を確認します。
ステップ 10	`Switch# 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。

次に、スタティック アクセス ポート上の認証失敗 VLAN としてファスト イーサネット インターフェイス 4/3 上の通常の VLAN 40 をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch(config)# end
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet3/1
----------------------------------------------------
PortStatus         = AUTHORIZED(AUTH-FAIL-VLAN)
MaxReq             = 2
MaxAuthReq         = 2
HostMode           = Single(AUTH-FAIL-VLAN)
PortControl        = Auto
QuietPeriod        = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod       = 3600 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 30 Seconds
Guest-Vlan         = 6
Switch
```

音声 VLAN に対する 802.1X 認証の設定

（注） Supervisor Engine 6-E は、この機能をサポートしていません。

（注） 802.1X と音声 VLAN を同時に設定する必要があります。

音声 VLAN で 802.1X をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface` *interface-id*	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	`Switch(config-if)# switchport access vlan` *vlan-id*	VLAN をアクセス モードのスイッチド インターフェイスに設定します。
ステップ 4	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 5	`Switch(config-if)# switchport voice vlan` *vlan-id*	音声 VLAN をインターフェイスに設定します。
ステップ 6	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 7	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 8	`Switch(config-if)# end`	コンフィギュレーション モードに戻ります。
ステップ 9	`Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 10	`Switch# show dot1x interface interface-id details`	（任意）入力を確認します。
ステップ 11	`Switch# 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。

次に、ファスト イーサネット インターフェイス 5/9 上の音声 VLAN 機能で 802.1X をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch(config# end
Switch#
```

定期的な再認証のイネーブル化

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

自動 802.1X クライアント再認証はインターフェイス単位の設定で、個々のポートに接続しているクライアントに対して設定できます。特定のポートに接続するクライアントを手動で再認証する方法については、「待機時間の変更」（P.34-43）を参照してください。

クライアントの定期的再認証をイネーブルにして、再認証を試行する間隔を秒数で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface interface-id`	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、定期的再認証をイネーブルにするインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。
ステップ 5	`Switch(config-if)# dot1x re-authentication`	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。 定期的再認証をディセーブルにするには、**no dot1x re-authentication** 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。

	コマンド	目的
ステップ 6	`Switch(config-if)# dot1x timeout reauth-period {seconds | server}`	再認証を試行する間隔（秒）を指定するか、またはスイッチが RADIUS によるセッション タイムアウトを使用するようにします。 指定できる範囲は 1 ～ 65,535 秒です。デフォルトは 3600 秒です。 再認証を試行する間隔をデフォルトの秒数に戻すには、**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。 このコマンドがスイッチの動作に影響を与えるのは、定期的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 7	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 8	`Switch(config-if)# end`	特権 EXEC モードに戻ります。

次に、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 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

複数ホストのイネーブル化

図 34-7（P.34-21）のように、複数のホスト（クライアント）を 1 つの 802.1X 対応ポートに接続できます。このモードでは、ポートが許可されると、ポートに間接的に接続された他のすべてのホストに対して、ネットワーク アクセスが許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL-Logoff メッセージを受信すると）、スイッチは、ワイヤレス アクセス ポイントに接続された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。

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている 802.1X 許可ポート上で、複数のホスト（クライアント）を許容するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface interface-id`	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、複数のホストを間接的に接続するインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。

	コマンド	目的
ステップ 5	`Switch(config-if)# dot1x host-mode multiple-hosts`	802.1x 許可ポートで複数ホスト（クライアント）を許可します。 （注）　指定されたインターフェイスについて、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。 ポート上で複数のホストをディセーブルにするには、**no dot1x host-mode multiple-hosts** インターフェイス コンフィギュレーション コマンド使用します。
ステップ 6	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 7	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show dot1x all interface` *interface-id*	入力を確認します。
ステップ 9	`Switch# 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。

次に、インターフェイス FastEthernet 0/1 上で 802.1X をイネーブルにし、マルチ ホストを許容する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x host-mode multiple-hosts
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

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、その後再び認証を試みます。アイドル時間は、**quiet-period** の値によって決まります。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始して、タイムアウトの待機時間（**quiet-period**）をイネーブルにするインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。

	コマンド	目的
ステップ 5	`Switch(config-if)# dot1x timeout quiet-period seconds`	クライアントとの認証交換が失敗したあと、スイッチが待機する秒数（**quiet-period**）を設定します。 デフォルトの待機時間に戻すには、**no dot1x timeout quiet-period** コンフィギュレーション コマンドを使用します。 指定できる範囲は 0 ～ 65,535 秒です。デフォルトは 60 秒です。
ステップ 6	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 7	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show dot1x all`	入力を確認します。
ステップ 9	`Switch# 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。

次に、スイッチ上の待機時間（**quiet-period**）を 30 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

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。この応答を受信しなかった場合、スイッチは一定時間（再送信時間といいます）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特殊な動作問題など、異常な状況を調整する場合だけ行う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、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始して、タイムアウトの再送信時間をイネーブルにするインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。

	コマンド	目的
ステップ 5	`Switch(config-if)# dot1x timeout tx-period seconds`	要求を再送信するまでに、スイッチがクライアントからの EAP-Request/Identity フレームに対する応答を待機する秒数を設定します。 指定できる範囲は 1 ～ 65,535 秒です。デフォルトは 30 秒です。 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。
ステップ 6	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 7	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show dot1x all`	入力を確認します。
ステップ 9	`Switch# 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。

次に、再送信時間を 60 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

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/クライアント間の再送信回数の変更以外に、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-Request/Identity フレームおよびその他の EAP-Request フレームを送信する回数を変更できます。EAP-Request/Identity 再送信の回数は、**dot1x max-reauth-req** コマンドによって制御され、その他の EAP-Request フレームの再送信回数は **dot1x max-req** コマンドによって制御されます。

（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特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

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

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# interface interface-id`	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、**max-reauth-req** および **max-req** またはいずれか一方に対してイネーブルにするインターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode access`	非トランキング、タグなし単一 VLAN レイヤ 2 インターフェイスを指定します。
ステップ 4	`Switch(config-if)# dot1x pae authenticator`	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。 「802.1X のデフォルト設定」（P.34-22）を参照してください。

	コマンド	目的

ステップ 5	`Switch(config-if)# dot1x max-req count`
	
	または
	
	`Switch(config-if)# dot1x max-reauth-req count`
		（消失したり応答がない場合に）EAPOL DATA パケットが再送信される回数を指定します。たとえば、認証の途中にサプリカントがあってそこで問題が発生した場合、オーセンティケータは認証要求を中止する前にデータ要求を 3 回再送信します。*count* の範囲は 1 ～ 10 回です。デフォルトは 2 回です。
		
		EAPOL-Identity-Request フレーム（のみ）のタイマーを指定します。802.1X に対応していないデバイスを接続した場合、ステート マシンがリセットされる前に 3 つの EAPOL-Id-Req フレームが送信されます。代わりに、ゲスト VLAN を設定している場合、このポートがイネーブルになる前に 3 フレームが送信されます。このパラメータのデフォルト値は 2 です。*count* の範囲は 1 ～ 10 です。デフォルトは 2 です。
		
		再送信回数をデフォルトに戻すには、**no dot1x max-req** および **no dot1x max-reauth-req** 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。

ステップ 6	`Switch(config-if)# dot1x port-control auto`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 7	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show dot1x all`	入力を確認します。
ステップ 9	`Switch# 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。

次に、認証プロセスを再開するまでに、スイッチが EAP-Request/Identity フレームを再送信する回数を 5 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

手動によるポート接続クライアントの再認証

次のコマンドを入力すると、任意のときに、特定のポートに接続されたクライアントを手動で再認証できます。

dot1x re-authenticate interface 特権 EXEC コマンド。定期的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.34-41）を参照してください。

次に、FastEthernet 1/1 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 fastethernet1/1
Starting reauthentication on FastEthernet1/1
```

802.1X 認証ステートの初期化

dot1x initialize コマンドを実行すると、現在のステートにかかわらず認証プロセスが再開されます。

次に、ファスト イーサネット ポート 1/1 で認証プロセスを再開する例を示します。

```
Switch# dot1x initialize interface fastethernet1/1
```

次に、スイッチの全ポートで認証プロセスを再開する例を示します。

```
Switch# dot1x initialize
```

802.1X クライアント情報の削除

clear dot1x コマンドを実行すると、既存の全サプリカントを 1 つのインターフェイスまたはスイッチの全インターフェイスから完全に削除します。

次に、ファスト イーサネット ポート 1/1 の 802.1X クライアント情報を削除する例を示します。

```
Switch# clear dot1x interface fastethernet1/1
```

次に、スイッチの全ポートの 802.1X クライアント情報を削除する例を示します。

```
Switch# clear dot1x all
```

802.1X 設定をデフォルト値にリセットする方法

802.1X 設定をデフォルト値にリセットするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# dot1x default`	設定可能な 802.1x パラメータをデフォルト値にリセットします。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show dot1x all`	入力を確認します。
ステップ 5	`Switch# 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。

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 802.1X 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。

スイッチの 802.1X の管理および動作ステータスを表示するには、**show dot1x all details** 特権 EXEC コマンドを使用します。特定のインターフェイスの 802.1X 管理および動作ステータスを表示するには、**show dot1x interface details** 特権 EXEC コマンドを使用します。