CHAPTER 34

802.1X ポートベース認証の設定

この章では、Catalyst 4500 シリーズ スイッチで IEEE（米国電気電子学会）802.1X ポートベース認証を設定して、不正なデバイス（クライアント）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） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

Catalyst 4500 のコマンド リファレンスに掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』と関連資料を参照してください。

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

802.1X ポートベース認証について

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。

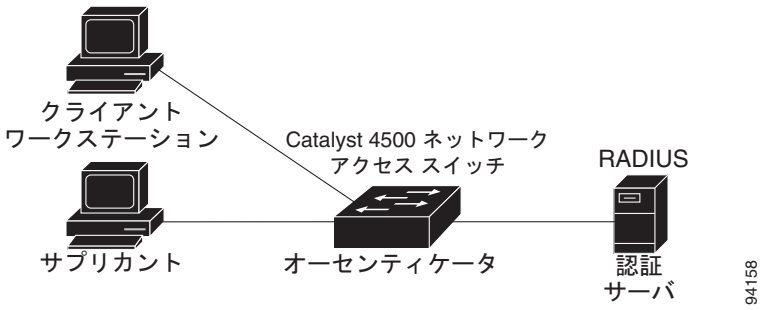
クライアントが認証されるまでは、クライアントが接続されたポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許容されます。認証が成功すると、通常のトラフィックがポートを通過できるようになります。

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。

装置の役割

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 装置の役割



- 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。カプセル化の間は EAP フレームの変更や検査が行われないので、認証サーバはネイティブのフレーム形式内で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバからフレーム 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：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、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/netsol/ns617/networking_solutions_sub_solution_home.html

認証の開始とメッセージ交換

スイッチまたはクライアントのどちらからでも、認証を開始できます。**authentication 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（Cisco IOS Release 12.2(46)SG 以前のリリースでは **dot1x port-control auto** コマンド）を使用してポート上の認証をイネーブルにする場合は、スイッチでポートのリンク状態の変化が検出された時点で認証が開始される必要があります。次に、ス

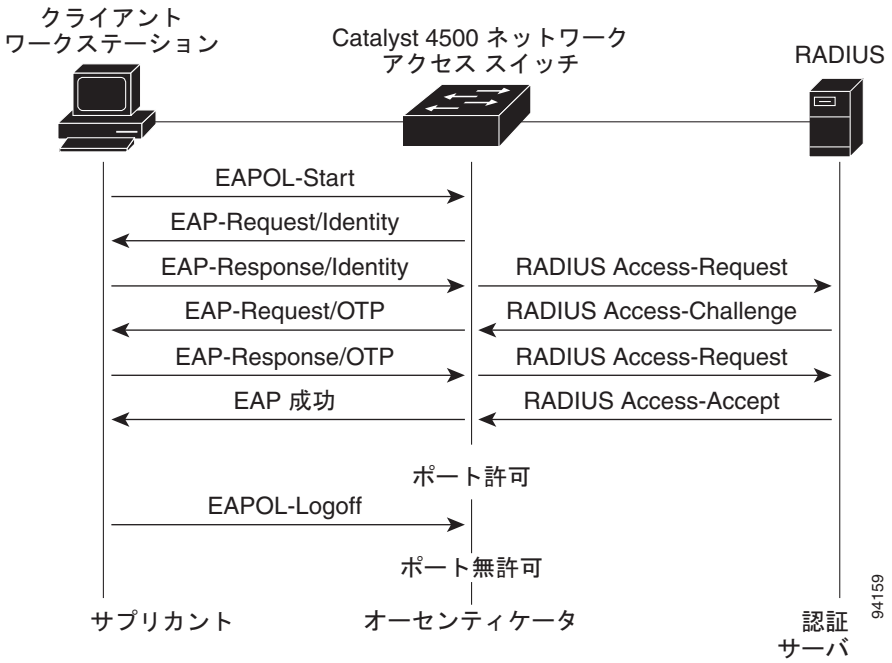
イッチは EAP-Request/Identity フレームをクライアントに送信して識別情報を要求します（一般に、スイッチは最初の Request/Identity フレームを送信して、そのあとで 1 つまたは複数の認証情報要求を送信します）。フレームの受信後、クライアントは EAP-Responce/Identity フレームで応答します。

ただし、起動中にクライアントがスイッチから EAP-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 フレームを送信することによって認証を開始できます。これにより、スイッチはクライアントの識別情報を要求します。

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。認証の開始を 3 回試行してもクライアントが EAP-Request/Identity フレームを受信できなかった場合、クライアントは、ポートが許可ステートにある場合と同じように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 ポートは許可された状態になります。

特定の EAP フレーム交換は、使用され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。クライアントが正常に認証されると、ポートは許可ステートに移行し、そのクライアントへのすべてのトラフィックが許容されます。

802.1X 非対応クライアントが無許可の 802.1X ポートに接続する場合、スイッチはクライアントに識別情報を要求します。この場合、クライアントは要求に応答しないので、ポートは無許可ステートにとどまり、クライアントにはネットワーク アクセスが許可されません。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.34-10）を参照してください。

それに対して、802.1X 対応クライアントが 802.1X プロトコルを実行していないポートに接続する場合、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。応答が得られないので、クライアントはポートが許可ステートにある場合と同じようにフレームの送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：802.1X 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、クライアントの 802.1X ベース認証なしで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**：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、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します。

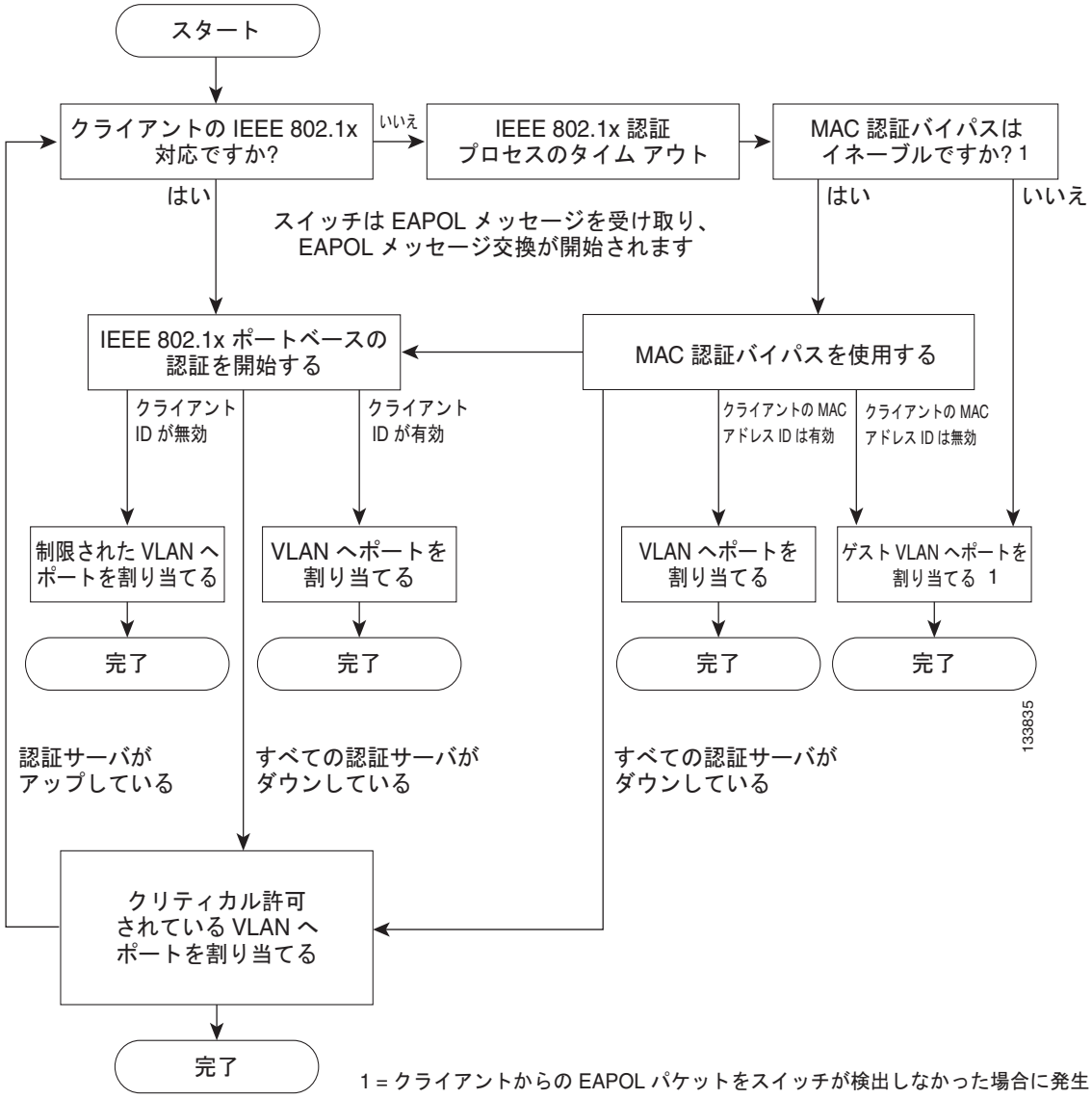
クライアントが正常に認証されると（認証サーバから Accept フレームを受信すると）、ポート ステートが許可に切り替わり、認証されたクライアントのフレームはすべてそのポートを通じて許容されます。認証が失敗した場合、ポートは無許可ステートのままですが、認証を再試行できます。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。指定された回数試行してもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

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、音声認証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、
「複数ドメイン認証と複数認証の使用」（P.34-20）を参照してください。

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

802.1X ポートのホスト モードでは、ポート上で複数のクライアントが認証可能かどうかや、認証方法が、決定されます。次のセクションの説明のとおり、802.1X ポートを設定すると、5 つのホスト モードのうち任意のものを使用できます。さらに、各モードは、認証前オープン アクセスを行えるよう変更できます。

- 「単一ホスト モード」（P.34-7）
- 「複数ホスト モード」（P.34-7）
- 「マルチドメイン認証モード」（P.34-7）
- 「マルチ認証モード」（P.34-8）
- 「認証前オープン アクセス」（P.34-8）

単一ホスト モード

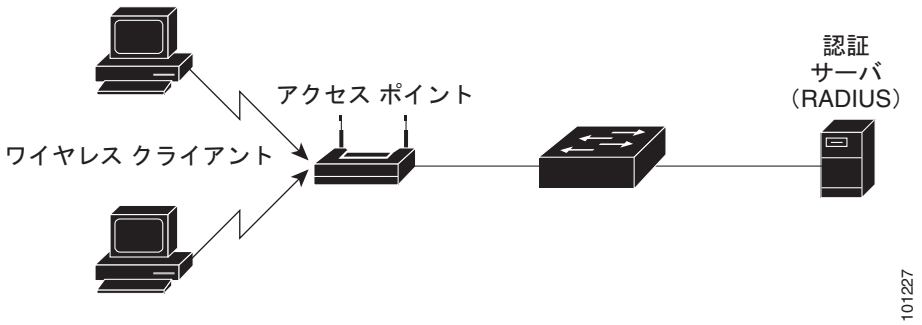
単一ホストまたは複数ホスト モードの 802.1X ポートを設定できます。単一ホスト モード（図 34-1（P.34-2）を参照）では、802.1X 対応スイッチ ポートに接続できるのは 1 つのクライアントだけです。スイッチは、ポートのリンク ステートがアップ ステートに変化すると、EAPOL フレームを送信してクライアントを検出します。クライアントが脱退するか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モード

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 での 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 つだけを、ネットワーク アクセスが付与されるすべてのクライアントに対して許可する必要があります。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、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、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

複数ホスト モードがイネーブルになっている場合は、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 34-4　　複数ホスト モードの例



マルチドメイン認証モード

802.1X を使用して、IP 電話機（シスコ製またはサードパーティ製）とその背後にある単一ホストで個別の認証を可能にする Multidomain Authentication（MDA; マルチドメイン認証）、MAC Authentication Bypass（MAB; MAC 認証バイパス）、または（ホストのみの場合）Web ベース認証。このアプリケーションでは、*マルチドメイン*は、データと音声の 2 つのドメインを指し、1 ポートごとに 2 つの MAC アドレスのみ使用できます。1 つのスイッチでは、これらが同じスイッチ ポートにある場合でも、データ VLAN にホストを、音声 VLAN に IP Phone をそれぞれ置くことができます。データ VLAN および音声 VLAN は、CLI 設定で指定できます。デバイスは、認証、許可、アカウンティング（AAA）サーバから受信した Vendor-Specific-Atribute（VSA; ベンダー固有属性）によって、データまたは音声のいずれかとして認識されます。データ VLAN と音声 VLAN は、認証中に（AAA）サーバから受信した VSA からも取得されます。

図 34-5　マルチドメイン認証モードの例

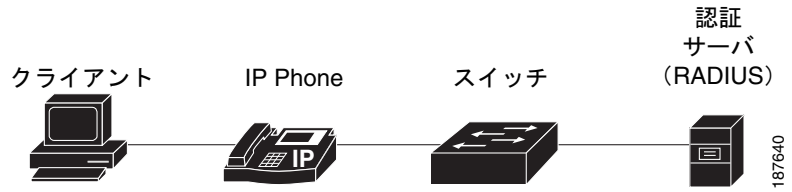


図 34-5 に、802.1X がイネーブルのポートに接続されている IP Phone に接続された単一ホストがある、典型的な MDA アプリケーションを示します。クライアントはスイッチに直接接続されないため、クライアントが接続されていない場合、スイッチでは、ポート リンクの切断を検出できません。別のデバイスで、接続されていないクライアントで確立された認証が後で使用されることを防ぐため、Cisco IP Phone は、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）のホスト表示 Type-Length-Value（TLV）に対して、接続されているクライアントのポート リンク状態に変更があったスイッチを通知します。

MDA の設定方法については、「複数ドメイン認証と複数認証の使用」（P.34-20）を参照してください。

マルチ認証モード

Cisco IOS Release 12.2(50)SG から、マルチ認証モードでは、音声 VLAN 上の 1 つのクライアントと、データ VLAN 上の複数の認証済みクライアントを使用できます。ハブまたはアクセス ポイントが 802.1X ポートに接続されているときに、接続されている各クライアントの認証を要求することにより、マルチ認証モードによって、複数ホスト モードを介して拡張セキュリティが用意されます。非 802.1X デバイスの場合は、個々のホスト認証のフォールバック方式として MAB または Web ベース認証を使用します。これにより、1 つのポート上で複数の方式を介して複数のホストを認証できます。

マルチ認証では、認証サーバから受信した VSA により、データ VLAN または音声 VLAN のいずれかに対して認証済みデバイスを割り当てることによって、音声 VLAN 上で MDA 機能もサポートされます。

（注）　ポートがマルチ認証モードの場合は、RADIUS サーバによる VLAN 割り当て、ゲスト VLAN、アクセス不能認証バイパス、認証失敗 VLAN を含む、すべての VLAN 割り当て機能が、データ デバイスに対してアクティブになりません。ただし、RADIUS サーバによる VLAN の割り当ては、音声デバイスでは使用可能です。

認証前オープン アクセス

Cisco IOS Release 12.2(50)SG から、認証前にデバイスからネットワークにアクセスできるよう、4 つのホスト モードのうち任意のモードを追加設定することができます。この認証前オープン アクセスは、Pre-boot eXecution Environment（PXE）などのアプリケーションで役に立ちます。PXE では、デバイスがネットワークにアクセスし、認証クライアントを含むブート可能イメージをダウンロードする必要があります。

ホスト モード設定後に、**authentication open** コマンドを入力することにより、認証前オープン アクセスをイネーブルにします。設定済みホスト モードに対する拡張機能として動作します。たとえば、単一ホスト モードで認証前オープン アクセスがイネーブルにされている場合、ポートでは、1 つの MAC アドレスのみ使用できます。認証前オープン アクセスがイネーブルの場合、ポート上に設定されている 802.1X とは別の他のアクセス制限によってのみ、ポート上の初期トラフィックは、制限されます。ポート上で 802.1X 以外のアクセス制限が設定されていない場合は、設定された VLAN 上でクライアント デバイスがフル アクセスできます。

VLAN 割り当てを使用した 802.1X 認証の利用

VLAN 割り当てを使用すれば、特定のユーザのネットワーク アクセスを制限することができます。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 またはプライベート VLAN（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。
- 802.1X ポート上でマルチ認証モードがイネーブルの場合、データ デバイスに対する VLAN 割り当ては無視されます。マルチ認証モードでポートが設定されている場合、音声デバイスに対する VLAN 割り当ては使用できます。
- 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）として設定される必要があります。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 PVLAN タイプが、ポートに割り当てられると予測される PVLAN タイプ（アクセス ポートには通常の VLAN、PVLAN ホスト ポートにはセカンダリ PVLAN）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 Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）許可をイネーブルにし、RADIUS サーバからの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.24）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 アトリビュートを割り当てます。VLAN を適切に割り当てるには、RADIUS サーバが次のアトリビュート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

ゲスト VLAN を使用すると、802.1X 非対応ホストから 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する場合にゲスト VLAN を使用します。

ゲスト VLAN はポート単位でサポートされます。タイプがポート タイプと一致する任意の VLAN がゲスト VLAN として機能します。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.34-46）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

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 Authentication Bypass（MAB; MAC 認証バイパス）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。認証に成功したら、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 固有でないことに注意してください。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.34-48）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。

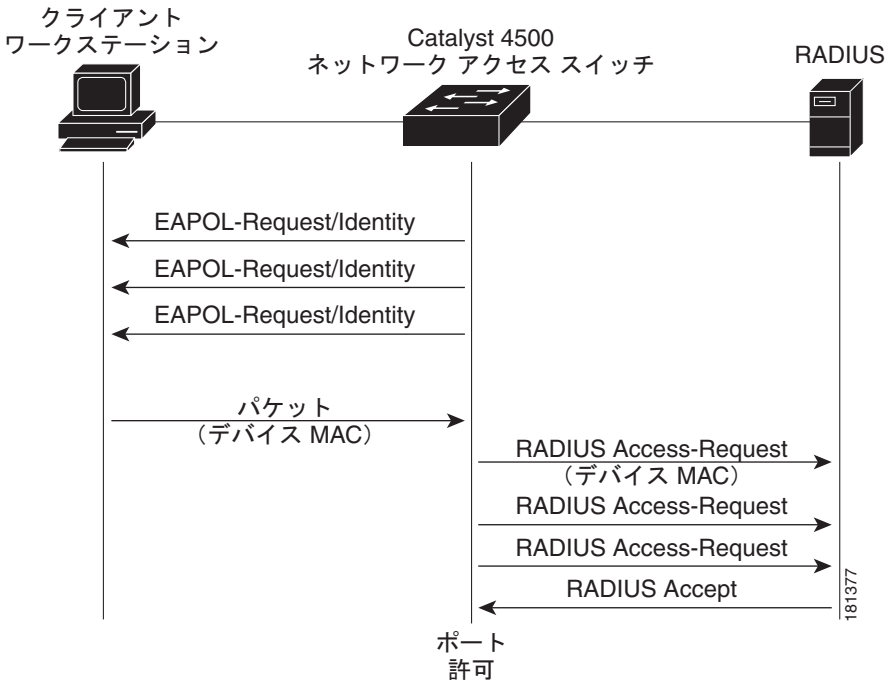
  デフォルトの 802.1X タイマー値に基づき、メカニズム間の移行にはおよそ 90 秒かかります。転送時間の値を小さくすれば時間を短くできますが、EAPOL 転送頻度に影響を与えます。値が小さくなると EAPOL の送信間隔が短くなります。MAB がイネーブルな状態で 802.1X が EAPOL のフルセットを 1 回実行すると、学習された MAC アドレスが認証サーバに送信されて処理されます。

  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 34-6 に、MAB 時のメッセージ交換を示します。

図 34-6　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。アドレスが認証に失敗すると、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、通常は認証されるが、認証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 電話の 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。

Web ベース認証を使用した 802.1X 認証の利用

Web ベース認証機能（別名 Web 認証プロキシ）を使用して、IEEE 802.1X サプリカントを実行していないホスト システムでエンド ユーザを認証できます。

Web ベース認証を設定する場合、次の点に注意してください。

- Web ベース認証に対するフォールバックは、スイッチ ポート上のアクセス モードで設定されます。トランク モードのポートはサポートされません。
- Web ベース認証に対するフォールバックは、EtherChannels または EtherChannel メンバではサポートされません。
- Web ベース認証に対するフォールバックは、インターフェイス固有の設定ですが、Web ベース認証の動作は、グローバル フォールバック プロファイルで定義されます。グローバル フォールバック設定を変更する場合、認証フォールバックの次のインスタンスまで、新しいプロファイルは使用されません。

Web ベース認証の設定方法の詳細については、第 35 章「Web ベース認証の設定」を参照してください。

アクセス不能認証バイパスを使用した 802.1X 認証の利用

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。

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.34-50）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

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別なイーサネット フレームを受信すると、休止 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.34-52）を参照してください。

単方向ステート

authentication 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（Cisco IOS Release 12.2(46) またはそれ以前では **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

authentication 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（Cisco IOS Release 12.2(46) またはそれ以前では **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をしません。

認証失敗 VLAN 割り当てを使用した 802.1X 認証の利用

認証失敗 VLAN 割り当てを使用すれば、ポート単位で認証失敗ユーザにアクセスを提供することができます。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（「定期的再認証のイネーブル化」（P.34-60）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 サーバを使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、「認証失敗の場合の 802.1X 認証の設定」（P.34-53）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（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定します）。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 セキュリティ付きの 802.1X ポートを使用すると、ネットワークにアクセス可能な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.34-66）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ていて、ポート セキュリティ テーブルがフルでなければ、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。そのあと、ポートが正常に起動します。

  クライアントが認証されていて、手動でポート セキュリティが設定されている場合、ポート セキュリティはセキュア ホスト テーブルへのエントリが保証されます（ポート セキュリティのスタティック エージングがイネーブルになっている場合は除く）。

  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 Command-Line Interface（CLI; コマンドライン インターフェイス）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 アドレスを維持できるのは、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] というタグが付加されます。

ACL 割り当てとリダイレクト URL を使用した 802.1X 認証の使用

ホストの 802.1X または MAB 認証中に、ACL などのホスト単位ポリシーをダウンロードして、RADIUS サーバからスイッチに URL をリダイレクトできます。ACL ダウンロードは、802.1X または MAB からのフォールバック後、Web 認証でもサポートされます。

ポートの 802.1X ホスト モードが、単一ホスト、MDA またはマルチ認証のいずれかの場合、ダウンロードされる ACL（DACL）は、認証ホストの IP アドレスをソース アドレスとして使用して変更されます。ホスト モードが複数ホストの場合、ソース アドレスは ANY として設定され、ダウンロードされる ACL またはリダイレクトは、ポート上のすべてのデバイスに適用されます。

ホストの認証中に ACL が指定されない場合、ポート上に設定されるスタティック デフォルト ACL は、ホストに適用されます。音声 VLAN ポートでは、ポートのスタティック デフォルト ACL だけが電話に適用されます。

次の内容について説明します。

- 「URL リダイレクトでの Cisco Secure ACS と AV のペア」（P.34-18）
- 「ACL」（P.34-18）

ダウンロード可能な ACL と URL リダイレクトの設定方法については、「ACL 割り当てとリダイレクト URL を使用した 802.1X 認証の設定」（P.34-32）を参照してください。

URL リダイレクトでの Cisco Secure ACS と AV のペア

ダウンロード可能な ACL がイネーブルの場合、Cisco Secure ACS では、RADIUS を介して AAA サービスが用意されます。

これらの Attribute-Value（AV）のペアは、RADIUS *cisco-av-pair* ベンダー固有属性（VSA）で Cisco Secure ACS に設定できます。

CiscoSecure-Defined-ACL では、Cisco Secure ACS に DACL の名前を指定します。スイッチでは、ACL の名前を CiscoSecure-Defined-ACL AV ペアを介して #ACL#-IP-*name-number* の形式で受信します。

name は ACL 名です。*number* は（3f783768 などの）バージョン番号です。

Auth-Manager コードにより、指定されたダウンロード可能な ACL のアクセス コントロール エントリ（ACE）が、前にダウンロードされたかどうかが確認されます。前にダウンロードされていない場合、ACE がダウンロードされるよう、Auth-Manager コードにより、ダウンロード可能な ACL 名をユーザ名として AAA 要求が送信されます。次に、ダウンロード可能な ACL は、名前付き ACL としてスイッチ上に作成されます。この ACL には、任意のソース アドレスで ACE が存在し、エンドポイントに暗黙拒否ステートメントは存在しません。認証の完了後にダウンロード可能な ACL がインターフェイスに適用される場合、インターフェイスのホスト モードにより、ソース アドレスが任意のものからソース IP アドレスに変更されます。ACE は、エンドポイント デバイスが接続されているスイッチ インターフェイスに適用されているダウンロード可能な ACL に、プリペンドされます。トラフィックが CiscoSecure-Defined-ACL ACE に一致する場合、適切なアクションが実行されます。

url-redirect および url-redirect-acl により、スイッチ上にローカル URL が指定されます。スイッチは、これらの cisco-av-pair VSA を次のように使用します。

- url-redirect = <HTTP または HTTPS URL>
- url-redirect-acl = スイッチの ACL 名または番号

これらの AV ペアは、エンドポイント デバイスから HTTP または HTTPS の要求を代行受信するようスイッチをイネーブルにし、ダウンロード可能な最新のアンチウイルス ファイルから指定されたリダイレクト アドレスへ、クライアント Web ブラウザを転送します。Cisco Secure ACS の url-redirect AV ペアには、Web ブラウザのリダイレクト先の URL が含まれています。url-redirect-acl AV ペアには、リダイレクトされる HTTP トラフィックまたは HTTPS トラフィックが指定されている ACL の名前または番号が含まれています。リダイレクト ACL の許可エントリに一致するトラフィックは、リダイレクトされます。

（注）　リダイレクトまたはデフォルト ACL は、スイッチ上に定義する必要があります。

ACL

ダウンロード可能な ACL が認証サーバ上の特定のクライアントに設定されている場合、クライアント側のスイッチ ポートにデフォルト ポート ACL を設定する必要があります。

デフォルト ACL がスイッチ上に設定されている場合で、Cisco Secure ACS からスイッチにホスト アクセス ポリシーが送信される場合、スイッチ ポートに接続されているホストからトラフィックに、ポリシーが適用されます。ポリシーが存在しない場合、スイッチにより、デフォルト ACL が適用されます。Cisco Secure ACS からスイッチにダウンロード可能な ACL が送信される場合、この ACL は、スイッチ ポート上にすでに設定されているデフォルト ACL より優先されます。ただし、スイッチで、Cisco Secure ACS からホスト アクセス ポリシーを受信する場合で、デフォルト ACL が設定されていない場合、認可の失敗が宣言されます。

ダウンロード可能なポリシーの設定方法については、「ダウンロード可能なポリシーの設定」（P.34-37）を参照してください。

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 アトリビュートをスキャンします。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 アトリビュートの値を使用します。

Termination-Action アトリビュートが存在し、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 アトリビュートが存在しないか、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 アトリビュートが含まれない場合、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.34-45）を参照してください。

音声 VLAN ポートを使用した 802.1X 認証の利用

音声 VLAN ポートは、次の 2 つの VLAN 識別子で関連付けられる特殊なアクセス ポートです。

- 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 を設定するのに使用します。
- 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 にあ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 Cisco Discovery Protocol（CDP; シスコ検出プロトコル）メッセージをリレーしません。このため、いくつかの Cisco IP Phone がシリーズで接続されている場合、スイッチは直接接続している IP Phone のみを認識します。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 については、第 32 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。これは、ダイナミック VLAN 割り当てでも同様です。

- 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。2 つの MAC アドレスを設定する必要があります。1 つは VVID の Cisco IP Phone MAC アドレスで、もう 1 つは PVID の PC MAC アドレスです。

  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 802.1X ポート セキュリティの静的に設定された MAC アドレス設定と一緒に、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。
- ポート上で 802.1X が設定されている場合は、ハブ経由で複数の IP 電話機を Catalyst 4500 シリーズ スイッチに接続することができません。
- 音声 PVLAN は PVLAN のホスト ポートとして設定できず、PVLAN のホスト ポートに割り当てられるのは PVLAN だけであるため、PVLAN 割り当てでは音声 VLAN が設定されたポートに PVLAN 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.34-54）を参照してください。

複数ドメイン認証と複数認証の使用

MDA は、データ デバイスと IP Phone（Cisco または Cisco 以外のサードパーティ）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。

複数認証は、複数のデータ デバイスと音声デバイスを許可します。複数認証ポート上で音声 VLAN が設定されている場合は、MDA ポートと同様に、音声ドメイン内で認証を実行することができます。

MDA は、デバイス認証の順番を強制しません。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。

（注）　音声 VLAN の設定時にも同じ注意事項が複数認証に適用されます。

- DoS 攻撃（サービス拒絶攻撃）を防ぐために MDA 対応ポートで CoPP をイネーブルにすることを強く推奨します。第 37 章「コントロール プレーン ポリシングの設定」を参照してください。
- スイッチ ポートを MDA または複数認証用に設定するには、「複数ドメイン認証および複数認可の設定」（P.34-29）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ときは、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 32 章「音声インターフェイスの設定」を参照してください。
- 音声デバイスを許可するには、AAA サーバが Cisco Attribute-Value（AV）ペアアトリビュートを `device-traffic-class=voice` にして送信するように設定する必要があります。この値がないと、スイッチは音声デバイスをデータ デバイスとして扱います。
- ゲスト VLAN および制限された VLAN 機能は、MDA 対応ポートのデータ デバイスにのみ適用されます。スイッチは、認証に失敗した音声デバイスをデータ デバイスとして 扱います。
- 複数のデバイスが、ポートの音声ドメインまたはデータ ドメインのいずれかで認証を試行する場合、errdisable です。

- デバイスが認証されるまで、ポートはそのトラフィックをドロップします。Cisco 以外の IP 電話または音声デバイスは、データ VLAN と音声 VLAN の両方で許可されます。データ VLAN により、音声デバイスは DHCP サーバに接続し、IP アドレスを取得して音声 VLAN 情報を入手できます。音声デバイスが音声 VLAN での送信を開始したあと、データ VLAN へのアクセスはブロックされます。音声デバイスがデータ VLAN 上にトラフィックを送信し続けていると、MDA 内でセキュリティ違反が発生する可能性があります。
- 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.34-11）を参照してください。
- *データ*デバイスまたは*音声*デバイスがポート上で検出されると、その MAC アドレスは認証が正常に完了するまでブロックされます。認証が失敗した場合、MAC アドレスは 5 分間ブロックされたままになります。
- *データ* VLAN で複数のデバイスが検出された場合、またはポートが許可されていないときに*音声* VLAN で複数の音声デバイスが検出された場合、そのポートは errdisable になります。
- ポートのホスト モードがシングル モードからマルチドメイン モードに変更されると、許可されたデータ デバイスはポート上で許可されたままとなります。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 および制限 VLAN などのアクティブ フォールバック メカニズムは、ポートが単一または複数ホスト モードからマルチドメイン モードに変更されたあとも設定済みのままになります。
- ポートのホスト モードをマルチドメイン モードから単一または複数ホスト モードに切り替えると、許可された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 対応ポートを使用したユーザ単位の ACL は推奨しません。ユーザ単位 ACL ポリシーを持つ許可されたデバイスは、ポートの音声 VLAN およびデータ 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。使用する場合、ポート上の 1 つのデバイスだけが、ユーザ単位 ACL を強制する必要があります。

サポート対象トポロジ

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。

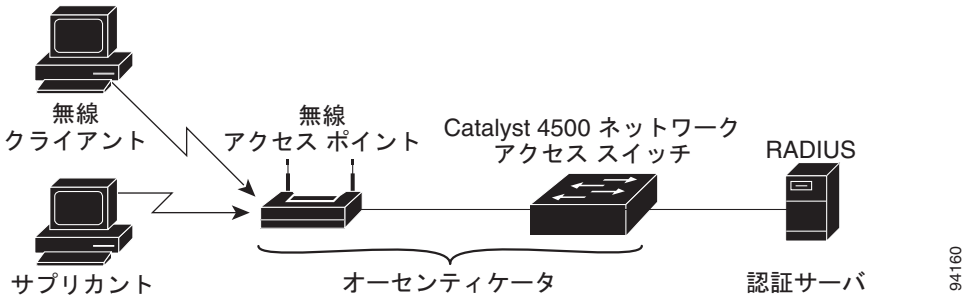
- ポイントツーポイント
- 無線 LAN

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。クライアントが脱退するか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

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.34-66）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、無線アクセス 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、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

図 34-7　　無線 LAN の例



802.1X ポートベース認証の設定

（注） ここに記載されている認証コマンドの使用が推奨されていますが、12.2(46)SG 以前のリリースで使用されていた 802.1X コマンドも使用できます。

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.34-24）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.34-27）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.34-63）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.34-45）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」（P.34-23）
- 「802.1X 設定時の注意事項」（P.34-24）
- 「802.1X 認証のイネーブル化」（P.34-24）（必須）
- 「スイッチ/RADIUS サーバ通信の設定」（P.34-27）（必須）
- 「複数ドメイン認証および複数認可の設定」（P.34-29）
- 「ACL 割り当てとリダイレクト URL を使用した 802.1X 認証の設定」（P.34-32）
- 「ユーザ単位の ACL とフィルタ ID ACL を使用した 802.1X 認証の設定」（P.34-38）
- 「RADIUS によるセッション タイムアウトの設定」（P.34-45）（任意）
- 「ゲスト VLAN を使用した 802.1X 認証の設定」（P.34-46）（任意）
- 「MAC 認証バイパスを使用した 802.1X 認証の設定」（P.34-48）（任意）

- 「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.34-50）（任意）
- 「単方向制御ポートを使用した 802.1X 認証の設定」（P.34-52）（任意）
- 「認証失敗の場合の 802.1X 認証の設定」（P.34-53）（任意）
- 「音声 VLAN に対する 802.1X 認証の設定」（P.34-54）（任意）
- 「VLAN 割り当てを使用した 802.1X 認証の設定」（P.34-55）
- 「フォールバック認証のイネーブル化」（P.34-57）
- 「定期的再認証のイネーブル化」（P.34-60）（任意）
- 「複数ホストのイネーブル化」（P.34-62）（任意）
- 「待機時間の変更」（P.34-63）（任意）
- 「スイッチ/クライアント間の再送信時間の変更」（P.34-63）（任意）
- 「スイッチ/クライアント間のフレーム再送信回数の設定」（P.34-64）（任意）
- 「手動によるポート接続クライアントの再認証」（P.34-66）（任意）
- 「802.1X 認証ステートの初期化」（P.34-66）
- 「802.1X クライアント情報の削除」（P.34-66）
- 「802.1X 設定をデフォルト値にリセットする方法」（P.34-66）（任意）

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
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1645 • 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、クライアントの 802.1X ベース認証なしで通常のトラフィックを送受信します。
定期的再認証	ディセーブル
再認証の試行間隔	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あと、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。

表 34-1　802.1X のデフォルト設定（続き）

機能	デフォルト設定
最大再送信回数	2 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
クライアントのタイムアウト時間	30 秒 認証サーバからの要求をクライアントにリレーするとき、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。
認証サーバのタイムアウト時間	30 秒 クライアントの応答を認証サーバにリレーするとき、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 プロトコルは、レイヤ 2 スタティック アクセス、PVLAN ホスト ポート、およびレイヤ 3 ルーテッド ポートでのみサポートされます。その他のポート モードには 802.1X を設定できません。
- VLAN 割り当を使用する場合、この機能では一般的な AAA コマンドが使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.34-24）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、定義された方式を使い果たすまで続きます。このサイクルのいずれかのポイントで認証が失敗すると、認証プロセスは停止し、他の認証方式は試行されません。

（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応するように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。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 次のキーワードを少なくとも 1 つ入力します。 • **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.34-23）を参照してください。
ステップ 9	`Switch(config-if)# authentication 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)# authentication port-control auto
Switch(config-if)# end

Switch# show authentication sessions interface f9/2
            Interface:  FastEthernet9/2
          MAC Address:  0007.e95d.83c4
           IP Address:  Unknown
               Status:  Running
               Domain:  UNKNOWN
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A050B160000009505106398
     Acct Session ID:  0x0000009B
              Handle:  0x0D000095

Runnable methods list:
       Method   State
       dot1x    Running
       mab      Not run
```

次に、ポートが認可されるときの例を示します。

```
Switch# show authentication sessions  int G4/5
            Interface:  GigabitEthernet4/5
          MAC Address:  0015.e981.0531
           IP Address:  Unknown
            User-Name:  ctssxp
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A053F0F00000004041E6B0C
     Acct Session ID:  0x00000021
              Handle:  0x2C000004

Runnable methods list:
       Method   State
       dot1x    Authc Success

Switch# show dot1x interface G4/5 details

Dot1x Info for GigabitEthernet4/5
```

```
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0015.e981.0531
Session ID                = 0A053F0F00000004041E6B0C
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

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り、一意の識別子が作成され、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 2 つの異なるホスト エントリが同じサービス（認証など）に対して設定されている場合、2 番めに設定されたホスト エントリは、最初のエントリのフェールオーバー時のバックアップとして機能します。RADIUS のホストエントリは、設定された順序で試行されます。

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,* s 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。 指定された RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。 **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。デフォルト値は 1645 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 1646 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化キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。 **（注）** キーの先行スペースは無視されますが、キーの途中と最後のスペースは有効なため、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、キーの一部として引用符を使用する場合を除いて、キーを引用符で囲まないでください。このキーは、RADIUS デーモン上で使用する暗号と一致する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し使用してください。
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 を認証ポートとして指定し、暗号化キーを 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 g3/2
Switch(config)# end
Switch#
```

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化キーの値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** のグローバル コンフィギュレーション コマンドを使用します。

さらに、RADIUS サーバで AAA クライアントも作成する必要があります。この設定には、スイッチの IP アドレス、およびサーバとスイッチで共用するキー文字列などがあります。

複数ドメイン認証および複数認可の設定

MDA および複数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)# 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] authentication host-mode {single-host | multi-host | multi-domain} | multi-auth}`	キーワードにより、次のものが許可されます。 • **single-host**：IEEE 802.1X 認可ポートの単一ホスト（クライアント）が許可されます。 • **multi-host**：単一ホストの認証後に 802.1X 認可ポートの複数ホストが許可されます。 • **multi-domain**：1 つのホストおよび（IP Phone、Cisco、または Cisco 以外などの）1 つの音声デバイスの両方が、IEEE 802.1X 認可ポートで認証されます。 **（注）** ホスト モードが**マルチドメイン**に設定されているときは、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 32 章「音声インターフェイスの設定」を参照してください。 • **multi-auth**：複数のホストおよび IP Phone（Cisco または Cisco 以外）などの 1 つの音声デバイスが、IEEE 802.1X 認可ポートで認証されるようにします。このキーワードでは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースが必要です。 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 authentication host-mode {multi-host | multi-domain | multi-auth}** インターフェイス コンフィギュレーション コマンド（これよりも前のリリースでは、**no dot1x host-mode** {**multi-host** | **multi-domain**} 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)# authentication port-control auto
Switch(config-if)# authentication 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 terminal
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)# authentication port-control auto
Switch(config-if)# authentication 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)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# mab eap
Switch(config-if)# no shut
Switch(config-if)# end
```

次に、ファスト イーサネット インターフェイス 3/1 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#
```

次に、MDA をイネーブルにし、IEEE 802.1x 認可ポート上で複数ホストと 1 つの音声デバイスを認証する例を示します。

```
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)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-auth
Switch(config-if)# map eap
Switch(config-if)# no shut
Switch(config-if)# end
```

ACL 割り当てとリダイレクト URL を使用した 802.1X 認証の設定

次の内容について説明します。

ダウンロード可能な ACL

ダウンロード可能な ACL 機能を使用すると、認証サーバからデバイス固有の認可ポリシーをダウンロードできます。これらのポリシーは、該当するクライアントに対する認証に成功し、クライアントの IP アドレスが IP デバイス トラッキング テーブルに入力された後で、アクティブにされます（ポートが認証され、IP デバイス トラッキング テーブルに IP アドレス エントリが入力されると、ダウンロード可能な ACL がポート上で適用されます）。

次のセクションでは、関連する認証（802.1X または MAB）の設定を補うために必要な設定について説明します（スイッチ上では独自の設定作業は不要です。設定のすべては ACS 上に存在します）。認証に成功後、**show ip access-list** コマンドを入力して、ダウンロード可能な ACL を表示します。

スイッチの設定

ステップ 1　IP デバイス トラッキング テーブルを設定します。

```
Switch(config)# ip device tracking
```

ステップ 2　認証を転送するよう、RADIUS VSA を設定します。

```
Switch(config)# radius-server vsa send authentication
```

ステップ 3　インターフェイスにスタティック ACL（PACL）を設定します。

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

インターフェイス設定のサンプル

```
Switch# show running-configuration interface g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab eap
 dot1x pae authenticator
end

Switch#
Switch# show ip access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

DACL のデバッグ コマンド

IP デバイス トラッキング テーブルには、ARP または DHCP を介して認識されたホスト IP アドレスが含まれています。

次のコマンドにより、IP デバイス トラッキング テーブルでの制限が表示されます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------
50.0.0.12       0015.60a4.5e84 GigabitEthernet2/9     ACTIVE
```

次のコマンドにより、ACS からダウンロードされた DACL が Policy Enforced Module（EPM）セッションに含まれることが表示されます。

```
Switch# show epm session ip 50.0.0.12
Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-auth-48b79b6e
```

次のコマンドにより、ダウンロード可能な ACL の内容が表示されます。

```
Switch# show ip accesslists xACSACLx-IP-auth-48b79b6e
Extended IP access list xACSACLx-IP-auth-48b79b6e (per-user)
    10 permit udp any any
```

```
Switch(config)#
```

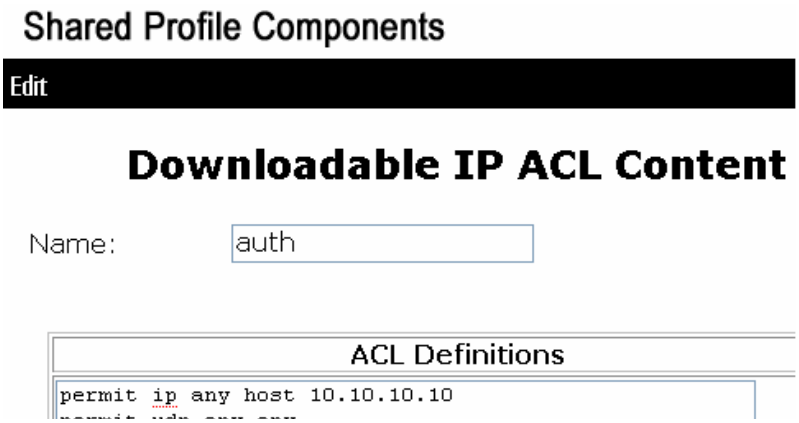
Cisco ACS での DACL の設定

（注）　DACL は、Cisco ACS のみでサポートされます。

DACL に必要な ACS が正しく動作するように設定する手順は、次のとおりです。

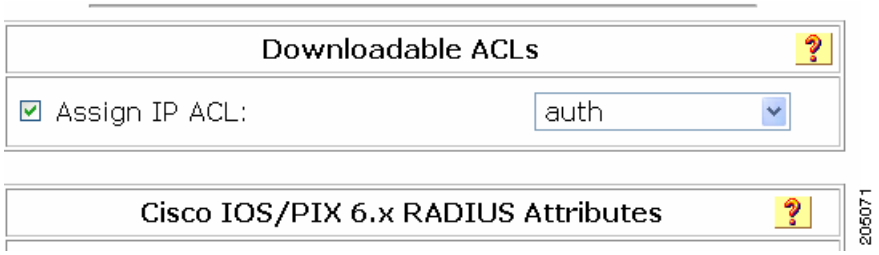
ステップ 1　[Radius Shared Profile] > [Downloadable IP ACL Content] を選択すると表示されるウィンドウで、ダウンロード可能な IP ACL を設定します。

図 34-8　　共有プロファイル コンポーネント



ステップ 2　[User] > [DACLs] を選択すると表示されるウィンドウを使用して、ユーザでこの DACL を接続します。

図 34-9　　ダウンロード可能な ACL



URL のリダイレクト

この設定には、ACS に 1 つ、スイッチ上に 1 つ、2 つの設定が含まれます。

ACL の設定

2 つの Cisco-AV ペアを設定するには、ユーザまたはグループの Cisco IOS/PIX 6x RADIUS アトリビュートで次のステートメントを追加します。

```
url-redirect-acl=urlacl
url-redirect=http://www.cisco.com
```

（注）　デフォルト ポート **ACL** は、インターフェイス上で設定する必要があります。

スイッチの設定

URL リダイレクトのためにスイッチを設定するには、次の手順を実行します。

ステップ 1　IP デバイス トラッキング テーブルを設定します。

```
Switch(config)# ip device tracking
```

ステップ 2　**send authentication** コマンドで、RADIUS を設定します。

```
Switch(config)# radius-server vsa send authentication
```

ステップ 3　URL リダイレクトの ACL（URLACL）を設定します。

```
Switch# ip access-list urlacl
    10 permit tcp any any
Switch#
```

ステップ 4　インターフェイスにスタティック ACL（PACL）を設定します。

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

インターフェイス設定のサンプル

```
Switch# show running-configuration int g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab
 dot1x pae authenticator
end

Switch#
```

```
Switch# show access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

次のコマンドで、URL リダイレクトを確認します。

show ip device tracking コマンドにより、IP デバイス トラッキング テーブルでの制限が示されます。

```
Switch(config)# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------
50.0.0.12       0015.60a4.5e84 GigabitEthernet2/9     ACTIVE
```

show epm session ip コマンドにより、特定のホストの EPM セッションが表示されます。ACS からダウンロードされる URL のリダイレクト ACL 情報および URL リダイレクト URL 情報を確認します。

```
Switch# show epm session ip 50.0.0.12
Admission feature       : DOT1X
AAA Policies            :
URL Redirect ACL        : urlacl
URL Redirect            : http://www.cisco.com
```

Cisco IOS ソフトウェアでサポートされる AV ペアの詳細については、
AAA クライアント上で実行されているソフトウェア リリースに関する ACS コンフィギュレーションおよびコマンド リファレンス マニュアルを参照してください。

DACL と URL リダイレクトの注意事項および制約事項

ダウンロード可能な ACL または URL リダイレクトについては、ACL ソースを ANY
（許可 TCP ANY ホスト 1.1.1.1 eq 80 または許可 TCP ANY ホスト 1.1.1.1 eq 443）にする必要があります。

ダウンロード可能なポリシーの設定

ダウンロード可能なポリシーを設定するには、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)# access-list` *access-list-number* **{deny | permit}** *source* [*source-wildcard*] [**log**]	ソース アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。 *access-list-number* は、1 から 99 または 1300 から 1999 の十進数です。 条件が一致した場合にアクセスを拒否するか許可するかを指定するには、**deny** または **permit** を入力します。 *source* は、パケットの送信元となるネットワークまたはホストのアドレスで、次の形式で指定します。 • ドット付き 10 進数形式の 32 ビットの値 • source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形としてキーワード any source-wildcard の値は必要ではありません。 • source および source-wildcard の値の source 0.0.0.0 の省略形としてキーワード host （任意）ソースのワイルドカード ビットには、source-wildcard を適用します。 （任意）コンソールに送信されるエントリに一致するパケットに関する情報ロギング メッセージを発生させるために、ログを入力します。
ステップ 3	`Switch(config-if)# 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 4	`Switch(config-if)# ip access-group` **{***access-list-number* | *name***} in**	指定されたインターフェイスへのアクセスを制御します。 この手順は、ダウンロードされたポリシーを動作させるために必須です。
ステップ 5	`Switch(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	`Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 7	`Switch(config)# aaa authorization network default local`	認可形式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default local** コマンドを使用します。
ステップ 8	`Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** 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 9	`Switch(config)# ip device tracking` [**probe** {**count** *count* | interval *interval*}]	（任意）IP デバイス トラッキング テーブルで、これらのパラメータを設定します。 • **count**：スイッチが ARP プローブに送信する回数。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval**：ARP プローブの応答前にスイッチが応答待ちする秒数。指定できる範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。

	コマンド	目的
ステップ 10	`Switch(config)# radius-server vsa send authentication`	ネットワーク アクセス サーバが、ベンダー固有の属性を認識して使用するように設定します。 **（注）**　ダウンロード可能な ACL が動作可能な状態です。
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 ip device tracking {all | interface interface-id | ip ip-address | mac mac-address}`	IP デバイス トラッキング テーブルにあるエントリの情報を表示します。
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、ダウンロード可能なポリシーに関するスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

ユーザ単位の ACL とフィルタ ID ACL を使用した 802.1X 認証の設定

次の内容について説明します。

- 「ユーザ単位の ACL とフィルタ ID ACL」（P.34-38）
- 「ユーザ単位の ACL とフィルタ ID ACL の設定」（P.34-44）

ユーザ単位の ACL とフィルタ ID ACL

Cisco IOS Release 12.2(52)SG よりも前のリリースでは、Cat4K プラットフォームでのみ、ダウンロード可能な ACL がサポートされます。これは、Cisco ACS サーバでは動作しますが、サードパーティ AAA サーバでは動作しません。Cisco IOS Release 12.2(52)SG では、Catalyst 4500 スイッチからフィルタ ID/ユーザ単位の ACL 拡張機能が提供されます。これにより、サードパーティ製 AAA サーバを使用した ACL ポリシーの実施が可能になります。

フィルタ ID 機能により、次の機能が実行できるようになります。

フィルタ ID オプションを使用すると、管理者は、IETF 規格の Radius アトリビュートを使用して、AAA サーバ上で ACL 名を定義できます。ACL そのものは、スイッチ上で事前にローカルに定義する必要があります。

ユーザ単位の ACL 機能により、次の機能が実行できるようになります。

ユーザ単位の ACL を使用すると、管理者は、Cisco Radius AV ペアを使用して、AAA サーバ上でユーザ単位の ACL を定義できます。これにより、Cisco Radius ディクショナリをロードすることによって、サードパーティ AAA サーバ上での相互動作が可能になります。Cisco Radius ディクショナリには、VSA として設定された **Cisco Radius AV ペア** が含まれています。

（注）　Radius のベンダー固有属性（VSA）を使用すると、ベンダーは、標準 RADIUS アトリビュートに含まれない独自の専用 RADIUS アトリビュートをサポートできます。

スイッチの設定

ステップ 1　IP デバイス トラッキング テーブルを設定します。

```
Switch(config)# ip device tracking
```

ステップ 2　インターフェイスにスタティック ACL（PACL）を設定します。

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

インターフェイス設定のサンプル

```
Switch# show running-configuration interface g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab eap
 dot1x pae authenticator
end

Switch#
Switch# show ip access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

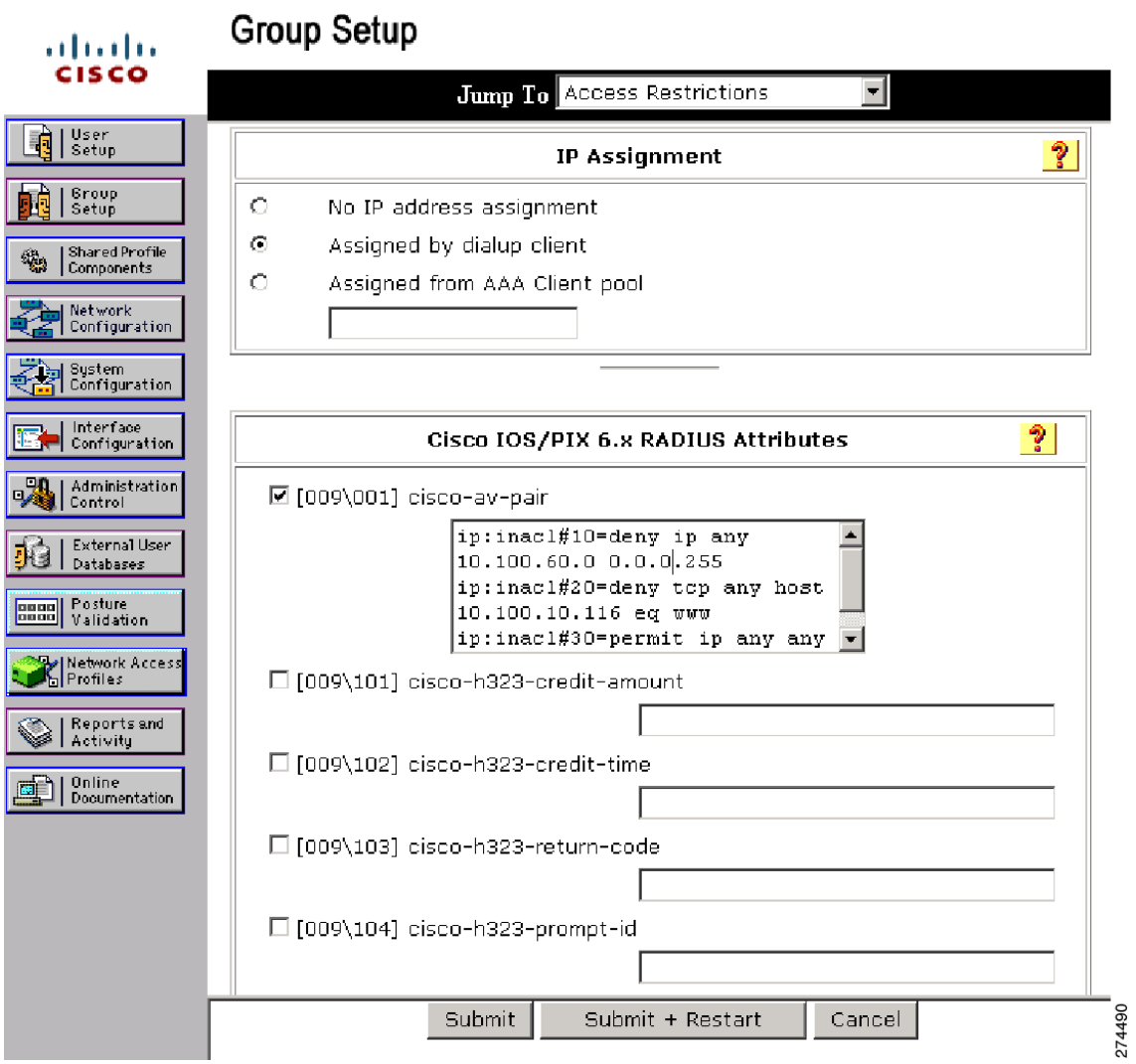
ACS でのユーザ単位の ACL の設定

[Group/User Setting] ページで、[Cisco IOS/PIX 6.x RADIUS Attributes] セクションまでカーソルを移動します。[[009\001] cisco-av-pair] の横のボックスを選択し、ユーザ単位の ACL の要素を入力します。ユーザ単位の ACL の形式は、次のとおりです。

```
<protocol>:inacl#<sequence number>=<ACE>
<protocol> can be either "ip" for IP-based ACLs or "mac" for MAC-based ACLs.
```

次の例では、設定しているグループのメンバは、10.100.60.0 サブネットに対するすべてのアクセスが拒否され、10.100.10.116 にあるサーバに対する http アクセスが拒否され、他のすべての場所へのアクセスが許可されます。

図 34-10　　ユーザ単位の ACL での ACE の定義



（注）　出力 ACL（outacl）はサポートされません。

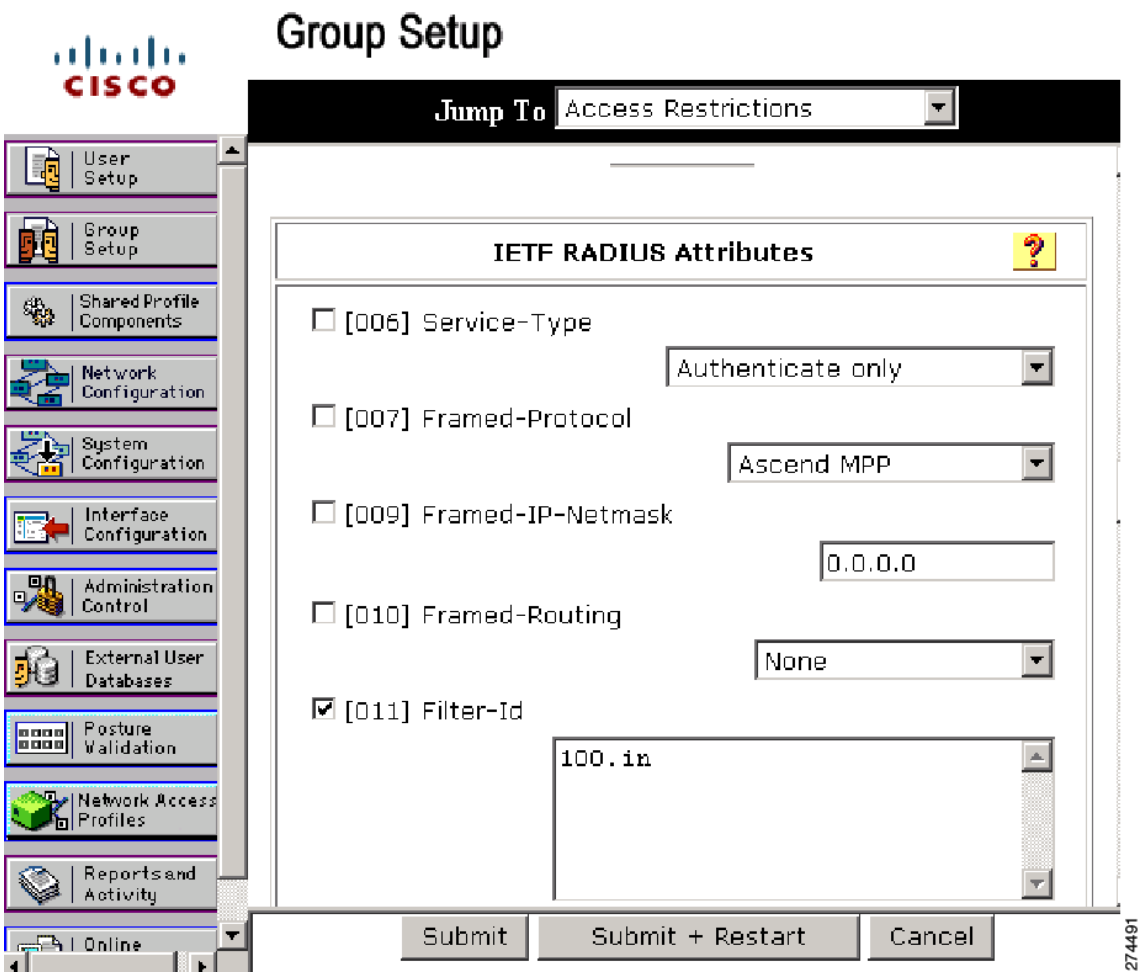
ACS でのフィルタ ID の設定

[Group/User Setting] ページで、[IETF RADIUS Attributes] セクションまでカーソルを移動します。[[011] Filter-Id] の横のボックスを選択し、このグループのメンバに適用する ACL を入力します（図 34-11）。

フィルタ ID の形式は、次のとおりです。

```
<ACL>.in
<ACL> is the number of the ACL that was configured on the switch in the previous step
```

図 34-11　フィルタ ID アトリビュートの設定



（注）　出力 ACL（たとえば "100.out" など）はサポートされません。

ユーザ単位の ACL とフィルタ ID ACL のデバッグ コマンド

IP デバイス トラッキング テーブルには、ARP または DHCP を介して認識されたホスト IP アドレスが含まれています。次のコマンドにより、IP デバイス トラッキング テーブルでの制限が表示されます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
IP Address MAC Address Interface STATE
-----------------------------------------------------------
50.0.0.12 0015.60a4.5e84 GigabitEthernet2/9 ACTIVE
```

次のコマンドにより、ACS からのユーザ単位の ACL が Policy Enforced Module（EPM）セッションに含まれることが表示されます。

```
Switch# show epm session ip 50.0.0.12
Admission feature : DOT1X
AAA Policies :
Per-User ACL            : deny ip any host 20.20.10.10
```

次のコマンドにより、ユーザ単位の ACL の内容が表示されます（前述のユーザ単位の ACL はインターフェイス上に設定されるデフォルト ポート ACL で、次の例では、151 がデフォルト ポート ACL です）。

```
Switch# show access-list
Extended IP access list 151

     deny ip host 20.20.0.3 host 20.20.10.10

    10 permit ip any any (57 estimate matches)
```

次のコマンドにより、セッション数と、対応するクライアント IP アドレスが表示されます。

```
Switch# show epm session summary
EPM Session Information

-----------------------

Total sessions seen so far : 1

Total active sessions      : 1

Session IP Address :

-------------------

50.0.0.12
```

次のコマンドにより、ACL（ACS からの IP と MAC ACL の両方）が Policy Enforced Module（EPM）セッションに含まれることが表示されます。

```
Switch# show epm session ip 50.0.0.12
Admission feature : DOT1X
AAA Policies :
Per-User ACL            : deny ip any host 20.20.10.10
Per-User ACL            : deny any host 0000.AAAA.AAAA
```

次のコマンドにより、ユーザ単位の ACL の内容が表示されます（前述のユーザ単位の ACL はインターフェイス上に設定されるデフォルト ポート ACL で、次の例では、151 がデフォルト ポート ACL です）。

```
Switch# show access-list
Extended IP access list 151

     deny ip host 20.20.0.3 host 20.20.10.10

    10 permit ip any any (57 estimate matches)
..
..
..(check for the mac access-list created)..
..
Extended MAC access list PerUser_MAC_ACL-589079192 (per-user)
    deny   any host 0000.aaaa.aaaa
..
```

次のコマンドにより、ACS からのフィルタ ID 155 が Policy Enforced Module（EPM）セッションに含まれることが表示されます。

（注） 156 IP 拡張 ACL はスイッチ上で事前に設定されるもので、これによってポリシー実行を発生させることができます。

```
Switch# show ip access-list 156
Extended IP access list 156
    10 deny ip any host 155.155.155.156
    20 deny ip any 156.100.60.0 0.0.0.255
    30 deny tcp any host 156.100.10.116 eq www

Switch# show epm session ip 50.0.0.12
Admission feature : DOT1X
AAA Policies :
Filter-Id               : 155
```

次のコマンドにより、インターフェイスに適用されるフィルタ ID の内容が表示されます。

```
Switch# show ip access-list int <gi6/3>

Switch# show ip access-list interface gi6/3
     deny ip host 20.20.0.2 host 155.155.155.156
     deny ip host 20.20.0.2 156.100.60.0 0.0.0.255
     deny tcp host 20.20.0.2 host 156.100.10.116 eq www
```

ユーザ単位の ACL とフィルタ ID ACL の注意事項および制約事項

ユーザ単位の ACL およびフィルタ ID ACL については、ACL ソースを ANY（許可 TCP ANY ホスト 1.1.1.1 eq 80 または許可 TCP ANY ホスト 1.1.1.1 eq 443）にする必要があります。

ユーザ単位の ACL とフィルタ ID ACL の設定

ユーザ単位の ACL およびフィルタ ID ACL 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)# access-list` *access-list-number* **{deny | permit}** *source* [*source-wildcard*] [**log**]	ソース アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。 *access-list-number* は、1 から 99 または 1300 から 1999 の十進数です。 条件が一致した場合にアクセスを拒否するか許可するかを指定するには、**deny** または **permit** を入力します。 *source* は、パケットの送信元となるネットワークまたはホストのアドレスで、次の形式で指定します。 • ドット付き 10 進数形式の 32 ビットの値 • source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形としてキーワード any source-wildcard の値は必要ではありません。 • source および source-wildcard の値の source 0.0.0.0 の省略形としてキーワード host （任意）ソースのワイルドカード ビットには、source-wildcard を適用します。 （任意）コンソールに送信されるエントリに一致するパケットに関する情報ロギング メッセージを発生させるために、ログを入力します。
ステップ 3	`Switch(config-if)# 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 4	`Switch(config-if)# ip access-group` **{***access-list-number* | *name***} in**	指定されたインターフェイスへのアクセスを制御します。 この手順は、ダウンロードされたポリシーを動作させるために必須です。
ステップ 5	`Switch(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	`Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 7	`Switch(config)# aaa authorization network default local`	認可形式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default local** コマンドを使用します。
ステップ 8	`Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** 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 9	`Switch(config)# ip device tracking` [**probe** {**count** *count* | interval *interval*}]	（任意）IP デバイス トラッキング テーブルで、これらのパラメータを設定します。 • **count**：スイッチが ARP プローブに送信する回数。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval**：ARP プローブの応答前にスイッチが応答待ちする秒数。指定できる範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。
ステップ 10	`Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	Switch# **show ip device tracking** {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	IP デバイス トラッキング テーブルにあるエントリの情報を表示します。
ステップ 12	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、ダウンロード可能なポリシーに関するスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

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.34-23）を参照してください。
ステップ 5	Switch(config-if)# **authentication timer reauthenticate** {*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)# authentication timer reauthenticate 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#
```

ゲスト VLAN を使用した 802.1X 認証の設定

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、認証サーバで EAPOL 要求（または ID フレーム）に対する応答が受信されなかった場合、または、EAPOL パケットがクライアントから送信されなかった場合に、Catalyst 4500 シリーズ スイッチによってクライアントがゲスト VLAN に割り当てられます。

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。
		有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。

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.34-23）を参照してください。
ステップ 5	`Switch(config-if)# authentication event no-response action authorize 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 authentication event no-response action authorize vlan** インターフェイス コンフィギュレーション コマンド（これよりも前のリリースでは、**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)# authentication 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)# authentication event no-response action authorize vlan 50
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

次に、セカンダリ PVLAN 100 を PVLAN 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)# authentication port-control auto
Switch(config-if)# authentication event no-response action authorize 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# 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。 スイッチ上でサプリカント 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`
	または
	`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。
		有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。

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.34-23）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)# authentication 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。
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 gigabitethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication event no-response action authorize vlan 5
Switch(config-if)# authentication 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

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。

	コマンド	目的
ステップ 3	Switch(config-if)# **switchport mode access** または 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。 有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。
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.34-23）を参照してください。
ステップ 5	Switch(config-if)# **authentication 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)# **mab [eap]**	スイッチの MAB をイネーブルにします。 **eap** オプションは、標準の RADIUS Access-Request、Access-Accept 通信に対して、完全な EAP 通信を使用する必要があることを指定します。デフォルトでは、**eap** オプションは MAB でイネーブルになっています。
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 mab 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、ポートの認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認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認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)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# end
Switch# show mab int g3/3 details
MAB details for GigabitEthernet3/3
--------------------------------------
Mac-Auth-Bypass            = Enabled

MAB Client List
---------------
Client MAC                 = 0001.0001.0001
Session ID                 = C0A8016F0000002304175914
MAB SM state               = TERMINATE
Auth Status                = AUTHORIZED
```

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.34-27）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)# authentication 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に 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)# authentication 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`
	または
	`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。
		有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。

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.34-23）を参照してください。
ステップ 7	`Switch(config-if)# authentication 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)# authentication event server dead action authorize [vlan` *vlan-id*`]`	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 authentication event server dead action authorize vlan** インターフェイス コンフィギュレーション コマンド（これよりも前のリリースでは、**dot1x critical** 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 9	`Switch(config-if)# authentication event server alive 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 10	`Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	`Switch# show dot1x interface interface-id details`	（任意）入力を確認します。
ステップ 12	`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.34-24）および「スイッチ /RADIUS サーバ通信の設定」（P.34-27）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 1645 を、アカウンティングには 1646 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 1645 acct-port 1646 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)# authentication port-control auto
Switch(config-if)# authentication event server dead action authorize vlan 17
Switch(config-if)# end
Switch# show dot1x int fastethernet 3/1 details

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

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。
		有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになることを指定します。

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.34-23）を参照してください。
ステップ 5	`Switch(config-if)# authentication 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)# authentication control-direction {in | both}`	各ポートで単方向ポート制御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）　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。単方向制御ポートとスパニング ツリー Portfast は、ホストに接続されたスイッチ ポート上で設定する必要があります。このような 2 つのポートがイーサネット ケーブルで接続されている場合は、2 つのポート間でホスト学習がフラッピングするため、CPU の使用率が増加する可能性があります。

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)# authentication port-control auto
Switch(config-if)# authentication control-direction in
Switch(config-if)# end
Switch# show dot1x int g3/3
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                        = AUTHENTICATOR
PortControl                = AUTO
ControlDirection           = In
HostMode                   = SINGLE_HOST
ReAuthentication           = Disabled
```

```
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Switch#
```

認証失敗の場合の 802.1X 認証の設定

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（Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）、DHCP スヌーピング、IP ソース ガードなど）と一緒に使用します。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)# authentication 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)# authentication event fail action authorize 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 authentication event fail action authorize 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)# authentication event fail retry` *max-attempts* `action` [`authorize vlan` *vlan-id* | `next-method`]	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 pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication event fail retry 5 action authorize vlan 40
Switch(config-if)# end
Switch# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
Switch#
```

音声 VLAN に対する 802.1X 認証の設定

（注） 802.1X と音声 VLAN を同時に設定する必要があります。

（注） 同一ポート上に、認証失敗 VLAN と音声 VLAN の両方は設定できません。これら 2 つの機能を同じポート上で設定しようとすると、Syslog メッセージが表示されます。

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.34-23）を参照してください。
ステップ 7	`Switch(config-if)# authentication 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)# authentication port-control auto
Switch(config-if)# end
Switch(config# end
Switch#
```

VLAN 割り当てを使用した 802.1X 認証の設定

ダイナミック VLAN 割り当てをイネーブルにするには、スイッチで必要な追加設定はありません。MDA または複数認証を設定するには、39-29 ページの「複数ドメイン認証および複数認可の設定」セクションを参照してください。VLAN 割り当てをイネーブルにするには、Cisco ACS サーバで対応する設定を行う必要があります。

VLAN 割り当てで 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-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)# authentication host-mode multi-domain`	インターフェイスで MDA をイネーブルにします。
ステップ 7	`Switch(config-if)# authentication 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 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.34-23）を参照してください。
ステップ 9	`Switch(config)# end`	特権 EXEC モードに戻ります。
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、インターフェイス上に MDA を設定し、認証メカニズムとして 802.1X を設定する例を示します。

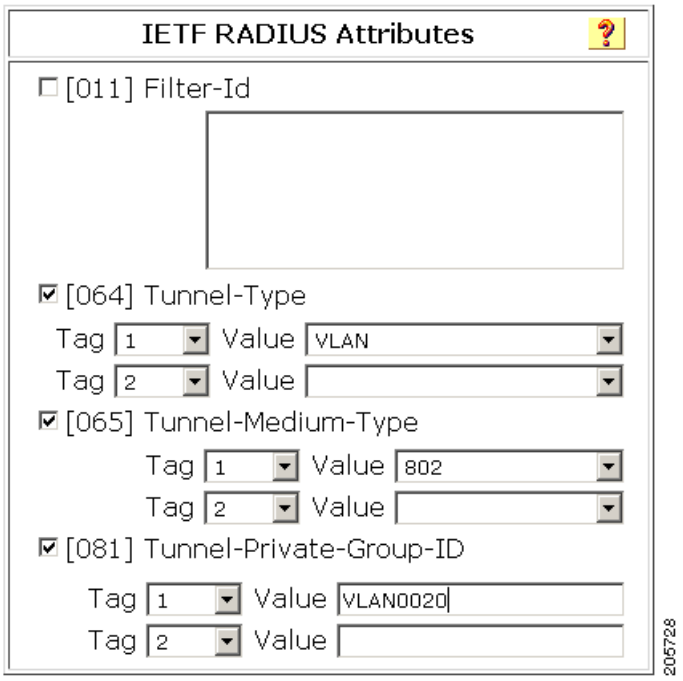
（注）　ACS サーバで VLAN 割り当てを設定する必要があります。スイッチ上では、設定の変更は不要です。

```
Switch(config)# interface FastEthernet3/3
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 16
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Cisco ACS での VLAN 割り当ての設定

音声 VLAN 割り当てを使用して MDA をイネーブルにする手順は、1 つの手順を除いて、MDA をアクティブにする手順と同じです。その 1 つの手順とは、[User] > [IETF RADIUS] アトリビュートを選択後に、VLAN をダイナミック VLAN 割り当て用に設定する手順です（図 34-12 を参照）。この手順では、ダイナミック VLAN 割り当てに必要な ACS 設定が正しく機能するように設定されます。

図 34-12　　ユーザ設定



（注）　手順は音声デバイスと同じですが、AAA サーバが Cisco Attribute-Value（AV）ペア アトリビュートを device-traffic-class=voice にして送信するように設定する必要がある点が異なります。

フォールバック認証のイネーブル化

マルチ認証モードのポート上では、MAB および Web ベース認証のいずれか一方または両方を、非 802.1X ホスト（EAPOL に対して応答しないホスト）に対するフォールバック認証方式として設定できます。認証方式の順序とプライオリティを設定します。

MAB の設定方法の詳細については、「MAC 認証バイパスを使用した 802.1X 認証の設定」（P.34-48）を参照してください。

Web ベース認証の設定方法の詳細については、第 35 章「Web ベース認証の設定」を参照してください。

（注）　MDA またはマルチ認証ポート上で、Webauth およびその他の認証方式が設定されている場合、ポートに接続されているすべてのデバイスで、ダウンロード可能な ACL ポリシーを設定する必要があります。

フォールバック認証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(config)# ip admission name rule-name proxy http`	Web ベース認証の認証ルールを設定します。
ステップ 2	`Switch(config)# fallback profile profile-name`	Web ベース認証のフォールバック プロファイルを作成します。
ステップ 3	`Switch(config-fallback-profile)# ip access-group rule-name in`	Web ベース認証前にネットワーク トラフィックに適用するデフォルト ACL を指定します。
ステップ 4	`Switch(config-fallback-profile)# ip admission name rule-name`	IP 許可ルールをプロファイルに関連付け、Web ベース認証によって接続しているクライアントでこのルールが使用されるよう指定します。
ステップ 5	`Switch(config-fallback-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	`Switch(config)# interface type slot/port`	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。 *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 7	`Switch(config-if)# authentication port-control auto`	ポートで認証をイネーブルにします。
ステップ 8	`Switch(config-if)# authentication order method1 [method2] [method3]`	（任意）使用される認証方式のフォールバック順序を指定します。*method* の 3 つの値のデフォルト順序は、**dot1x**、**mab**、および **webauth** です。指定された順序により、再認証の（最も高いプライオリティから最も低いプライオリティへの）相対プライオリティも決定されます。
ステップ 9	`Switch(config-if)# authentication priority method1 [method2] [method3]`	（任意）使用される認証方式の相対プライオリティを上書きします。*method* の 3 つの値は、プライオリティのデフォルト順序で、**dot1x**、**mab**、および **webauth** です。
ステップ 10	`Switch(config-if)# authentication event fail action next-method`	認証に失敗した場合に適用される次の認証方式を指定します。

	コマンド	目的
ステップ 11	Switch(config-if)# **mab** [**eap**]	MAC 認証バイパスをイネーブルにします。オプションの **eap** キーワードは、RADIUS 認証中に使用される EAP 拡張機能を指定します。
ステップ 12	Switch(config-if)# **authentication fallback** *profile-name*	指定されたプロファイルを使用した Web ベースの認証をイネーブルにします。
ステップ 13	Switch(config-if)# **authentication violation** [**shutdown** | **restrict**]	（任意）セキュリティ違反が発生した場合のポートのディスポジションを設定します。デフォルトでは、ポートはシャットダウンされます。**restrict** キーワードが設定されている場合、ポートはシャットダウンされず、違反 MAC アドレスに対してトラップ エントリがインストールされ、MAC アドレスからのトラフィックは廃棄されます。
ステップ 14	Switch(config-if)# **authentication timer inactivity** {*seconds* | **server**}	（任意）MAB および 802.1X に対する無活動タイムアウト値を設定します。デフォルトでは、ポートに対する無活動の長さはディセーブルにされています。 • *seconds*：無活動タイムアウトの期間を指定します。指定できる範囲は 1 ～ 65535 秒です。 • server：認証サーバから無活動タイムアウト期間の値を取得することを指定します。
ステップ 15	Switch(config-if)# **authentication timer restart** *seconds*	（任意）無認可ポートの認証の試行で、認証プロセスを再起動するまでの期間を指定します。 • *seconds*：再起動期間を指定します。指定できる範囲は 1 ～ 65535 秒です。
ステップ 16	Switch(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 17	Switch(config)# **ip device tracking**	Web ベース認証に必要な IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 18	Switch(config)# **exit**	特権 EXEC モードに戻ります。
ステップ 19	Switch# **show dot1x interface** *type slot/port*	入力を確認します。

次に、MAB への 802.1X フォールバックをイネーブルにし、続いて、802.1X がイネーブルにされたポートで Web ベース認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit5/9
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication order dot1x mab webauth
Switch(config-if)# mab eap
Switch(config-if)# authentication fallback fallback1
Switch(config-if)# exit
Switch(config)# ip device tracking
Switch(config)# exit
```

ポート上でフォールバック認証が設定されている場合に、802.1X を使用してホストが認証されたかどうかを特定するには、次のコマンドを入力します。

```
Switch# show authentication sessions interface g7/2

            Interface:  GigabitEthernet7/2
          MAC Address:  0060.b057.4687
           IP Address:  Unknown
            User-Name:  test2
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013F0000000901BAB560
      Acct Session ID:  0x0000000B
               Handle:  0xE8000009

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

Switch# show dot1x interfaces g7/2 detail

Dot1x Info for GigabitEthernet7/2
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_AUTH
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 2

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0060.b057.4687
Session ID                = C0A8013F0000000901BAB560
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

ポート上でフォールバック認証が設定されている場合に、MAB を使用してホストが認証されたかどうかを特定するには、次のコマンドを入力します。

```
Switch# show authentication sessions interface g7/2

            Interface:  GigabitEthernet7/2
          MAC Address:  0060.b057.4687
           IP Address:  192.168.22.22
            User-Name:  0060b0574687
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013F0000000B01BBD278
```

```
      Acct Session ID:  0x0000000D
               Handle:  0xF500000B

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

Switch# show mab interface g7/2 detail

MAB details for GigabitEthernet7/2
--------------------------------------
Mac-Auth-Bypass           = Enabled


MAB Client List
---------------
Client MAC                = 0060.b057.4687
Session ID                = C0A8013F0000000B01BBD278
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

ポート上でフォールバック認証が設定されている場合に、Web ベース認証を使用してホストが認証されたかどうかを特定するには、次のコマンドを入力します。

```
Switch# show authentication sessions interface G4/3
           Interface:  GigabitEthernet4/3
         MAC Address:  0015.e981.0531
          IP Address:  10.5.63.13
              Status:  Authz Success
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A053F0F0000000200112FFC
     Acct Session ID:  0x00000003
              Handle:  0x09000002

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Failed over
       webauth  Authc Success

Switch# show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
 Client IP 10.5.63.13 Port 4643, timeout 1000, state ESTAB
```

定期的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してい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.34-63）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.34-23）を参照してください。
ステップ 5	`Switch(config-if)# authentication periodic`	クライアントの定期的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）。 定期的再認証をディセーブルにするには、**no authentication periodic** インターフェイス コンフィギュレーション コマンド（これよりも前のリリースでは、**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。
ステップ 6	`Switch(config-if)# authentication timer reauthenticate {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 authentication timer reauthenticate** グローバル コンフィギュレーション コマンド（これよりも前のリリースでは、**dot1x timeout reauth-attempts** 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)# authentication 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)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 4000
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

複数ホストのイネーブル化

図 34-7（P.34-22）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、無線アクセス 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.34-23）を参照してください。
ステップ 5	`Switch(config-if)# authentication host-mode multi-host`	802.1X 許可ポート上で、複数のホスト（クライアント）を許容します。 **（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 authentication 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（これよりも前のリリースでは、**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 6	`Switch(config-if)# authentication 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、ファスト イーサネット インターフェイス 5/9 上で 802.1X をイネーブルにし、複数のホストを許容する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

待機時間の変更

スイッチがクライアントを再認証できないとき、スイッチは一定時間アイドルのままになり、そのあと再試行します。アイドル時間は、**quiet-period** の値によって決まります。クライアントが無効なパスワードを提供したことにより、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力すると、ユーザに応答するまでの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.34-23）を参照してください。
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)# authentication 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 fastethernet4/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

スイッチ/クライアント間の再送信時間の変更

クライアントは、スイッチからの EAP-Request/Identity フレームに、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.34-23）を参照してください。
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)# authentication 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 fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

スイッチ/クライアント間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 またはどちら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.34-23）を参照してください。
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かったりする場合に）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。 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)# authentication 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 fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# authentication 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

dot1x re-authenticate interface 特権 EXEC コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。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、「定期的再認証のイネーブル化」（P.34-60）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 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。

認証の詳細の表示

ここでは、次の内容について説明します。

Auth Manager に登録されている認証方式の確認

次のように入力します。

```
Switch# show authentication registrations
Handle  Priority  Name
      3         0       dot1x
      2         1       mab
      1         2       webauth
```

インターフェイスの Auth Manager サマリーの表示

次に、802.1X より高いプライオリティ（より低い値）で MAB を設定する例を示します。

```
Switch# show authentication int gi1/5
Client list:
Interface  MAC Address     Method   Domain   Status         Session ID
  Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
  Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94

Available methods list:
  Handle  Priority  Name
    3         0      dot1x
    2         1      mab
Runnable methods list:
  Handle  Priority  Name
    2         0      mab
    3         1      dot1x
```

スイッチ上のすべての Auth Manager セッションの概要の表示

次のように入力します。

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

特定の認証方式で認可されたスイッチ上でのすべての Auth Manager セッションの概要の表示

次のように入力します。

```
Switch# show authentication method dot1x
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

インターフェイスの Auth Manager セッションの確認

Auth 管理セッションは、**show authentication sessions** コマンドで確認できます。

```
Switch# show authentication sessions int gi1/5
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab Authc Success
----------------------------------------
Interface: GigabitEthernet1/5
MAC Address: 0014.bf5d.d26d
IP Address: 20.0.0.7
User-Name: johndoe
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
```

```
Idle timeout: N/A
Common Session ID: 0A3462B10000000E29811B94
Acct Session ID: 0x00000010
Handle: 0x1100000E
Runnable methods list:
Method State
dot1x Authc Success
mab Not run
```

個々の出力は、**handle**、**interface**、**MAC**、**session-id**、または **method** の各キーワードで改善できます。

```
Switch# show authentication sessions mac 000f.23c4.a401
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab Authc Success

Switch# show authentication sessions session-id 0A3462B10000000D24F80B58
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab uthc Success

Switch# show authentication session method dot1x int gi1/5
Interface: GigabitEthernet1/5
MAC Address: 0014.bf5d.d26d
IP Address: 20.0.0.7
User-Name: johndoe
Status: Authz Success
Domain: DATA
```

```
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000E29811B94
Acct Session ID: 0x00000010
Handle: 0x1100000E
Runnable methods list:
Method State
dot1x Authc Success
mab Not run
```

MAB の詳細の表示

次のいずれかのコマンドを入力します。

```
Switch# show mab all
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

Switch# show mab all detail
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED

Switch# show mab int fa5/9
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

Switch# show mab int fa5/9 detail
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

EPM ロギング

EPM ロギングを使用すると、グローバル コンフィギュレーション モードの **epm logging** コマンドで、EMP ロギング メッセージを表示します。EPM ロギングをディセーブルにするには、**no epm logging** コマンドを入力します。

ロギング メッセージは、次のイベント中に表示されます。

POLICY_APP_SUCCESS：名前付き ACL、プロキシ ACL、およびサービス ポリシー、URL リダイレクト ポリシーでの、正常実行されるポリシー アプリケーション イベント

POLICY_APP_FAILURE：未設定ポリシー、誤ったポリシー、ダウンロード要求の失敗、および AAA からのダウンロードの失敗などの、ポリシー アプリケーションの失敗条件

IPEVENT：IP 割り当て、IP リリース、および、クライアント待ちの IP イベント

AAA：AAA イベント（ダウンロード要求、または AAA からのダウンロードの正常終了など）

例 1

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# epm logging
Switch# clear dot1x all
Switch#
*May 15 08:31:26.561: %EPM-6-POLICY_REQ: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C000000030004956C| AUTHTYPE=DOT1X|
        EVENT=REMOVE
*May 15 08:31:26.581: %AUTHMGR-5-START: Starting 'dot1x' for client (0000.0000.0001) on
Interface Fa9/25
*May 15 08:31:26.681: %DOT1X-5-SUCCESS: Authentication successful for client
(0000.0000.0001) on Interface Fa9/25
*May 15 08:31:26.681: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for
client (0000.0000.0001) on Interface Fa9/25
```

例 2

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# epm logging
Switch(config)# int f9/25
Switch(config-if)# shut
Switch(config-if)# no shut
*May 15 08:41:56.329: %EPM-6-IPEVENT: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C0000026108FB7924| AUTHTYPE=DOT1X|
        EVENT=IP-RELEASE
*May 15 08:41:56.333: %EPM-6-IPEVENT: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C0000026108FB7924| AUTHTYPE=DOT1X|
        EVENT=IP-WAIT
```

Cisco IOS XE 3.1.0 SG リリースにおける Cisco IOS セキュリティ機能

このマニュアルでは、Cisco IOS XE 3.1.0 SG でサポートされているセキュリティ ソフトウェア機能について説明します。機能マニュアルへのリンクが掲載されています。

機能ガイドには、複数の機能に関する情報が含まれている場合があります。機能ガイドで特定の機能に関する情報を検索する場合は、巻末の機能情報表を参照してください。

機能ガイドには、さまざまなソフトウェア リリースとプラットフォームでサポートされている機能が掲載されています。ご使用のシスコ ソフトウェア リリースまたはプラットフォームで、機能ガイドに記載されたすべての機能がサポートされているとは限りません。巻末の機能情報表で、ご使用のソフトウェア リリースでサポートされている機能に関する情報を確認してください。プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

ロールベース アクセス制御 CLI コマンド

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_role_base_cli.html

HTTP 用の認証プロキシ アカウンティング

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy.html

拡張パスワード セキュリティ

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_sec_4cli.html

IEEE 802.1X：柔軟な認証

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy.html

イメージ検証

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_image_verifctn.html

TFTP 経由の登録の手動認証

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.html

Ipsec VPN の事前フラグメンテーション

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_pre_frag_vpns.html

ルータ セキュリティ監査の管理容易性

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtaudlog.html

信頼できるルート認証機関

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/dtrustrt.html