CHAPTER 9

IEEE 802.1x ポートベースの認証の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチで IEEE 802.1x ポートベースの認証を設定する方法について説明します。LAN がホテルや空港、会社のロビーにまで拡張されて安全でない環境が生じるため、802.1x により無許可の装置（クライアント）によるネットワークへのアクセスを防止します。

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

（注） IEEE 802.1x（**dot1x**）コマンドの中には、スイッチ上に表示されていても、サポートされていないものがあります。サポートされていないコマンドのリストについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

この章で説明する内容は、次のとおりです。

IEEE 802.1x ポートベースの認証の概要

IEEE 802.1x 規格は、クライアント/サーバ ベースのアクセス制御と認証プロトコルについて定義し、不正なクライアントが適切に認証されていない場合は公的にアクセス可能なポートを介した LAN 接続を制限します。認証サーバは、スイッチ ポートに接続された各クライアントを認証してから、スイッチまたは LAN が提供するサービスを利用できるようにします。

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

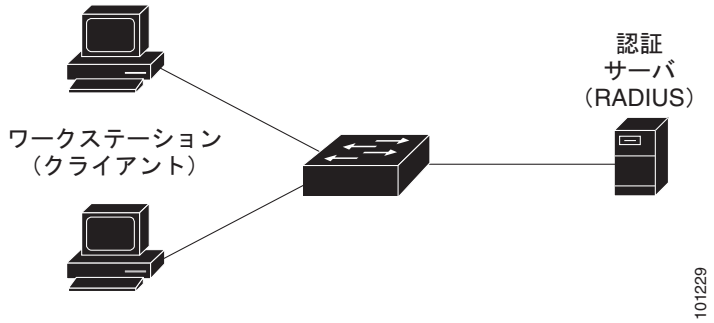
（注） CDP および STP は、Network Node Interface（NNI; ネットワーク ノード インターフェイス）でデフォルトでサポートされます。Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）上で、CDP および STP をイネーブルにできます。User Network Interface（UNI; ユーザ ネットワーク インターフェイス）では、CDP または STP はサポートされていません。

ここでは、802.1x ポートベース認証について説明します。

デバイスの役割

802.1x ポートベース認証を使用すると、ネットワーク内のデバイスは図 9-1 のような特定の役割が割り当てられます。

図 9-1　802.1x デバイスの役割



- *クライアント*：LAN およびスイッチへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムなどで提供されるような、802.1x 準拠のクライアント ソフトウェアが稼動している必要があります （クライアントは、802.1x 規格の *サプリカント*になります）。

（注） Windows XP ネットワーク接続および IEEE 802.1x 認証の問題を解決するには、次の URL にアクセスして Microsoft Knowledge Base Article を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*: 実際にクライアントの認証を行います。認証サーバは、クライアントの ID を確認し、クライアントの LAN およびスイッチ サービスへのアクセスを許可するかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはクライアントにトランスペアレントです。このリリースでサポートされている認証サーバは、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）拡張機能を装備した RADIUS セキュリティ システムだけです。これは、Cisco Secure Access Control Server（ACS）バージョン 3.0 以上に対応しています。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント/サーバ モデルで動作します。
- *スイッチ*（エッジ スイッチまたは無線アクセス ポイント）: クライアントの認証ステータスに基づいてネットワークへの物理アクセスを制御します。スイッチは、クライアントと認証サーバとの間の媒介（プロキシ）として機能し、クライアントに ID 情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには RADIUS クライアントが組み込まれています。RADIUS クライアントは、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの相互作用の役割を果たします。

  スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更が行われず、認証サーバはネイティブのフレーム形式で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、EAP フレームが残ります。これがイーサネット用にカプセル化されてクライアントに送信されます。

認証の開始とメッセージ交換

スイッチまたはクライアントは、認証を開始できます。**dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチは、EAP 要求/ID フレームをクライアントに送信して ID を要求します。フレームの受信後、クライアントは EAP 応答/ID フレームで応答します。

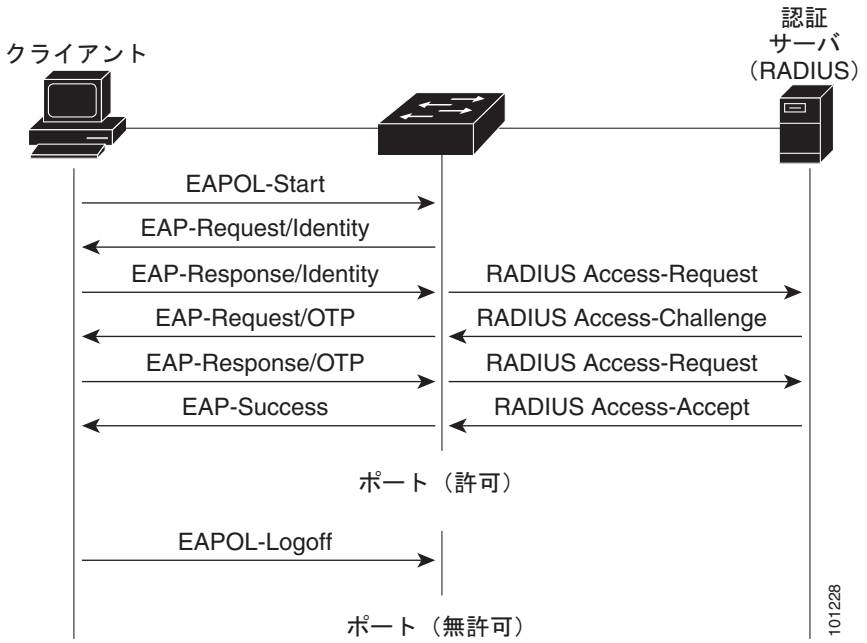
ただし、起動中にクライアントがスイッチから EAP 要求/ID フレームを受信しない場合は、クライアントは、EAPOL 開始フレームを送信して認証を開始できます。これにより、スイッチはクライアントの ID を要求するようになります。

（注） ネットワーク アクセス デバイスで 802.1x がイネーブルになっていないかサポートされていない場合は、クライアントからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもクライアントが EAP 要求/ID フレームを受信しない場合は、クライアントは、ポートが許可ステートであるものとしてフレームを送信します。許可ステートにあるポートは、事実上クライアントが正常に認証されたということを意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-4）を参照してください。

クライアントが自身の ID を提供すると、スイッチは媒介としての役割を開始し、認証が成功または失敗するまでクライアントと認証サーバとの間で EAP フレームを送受信します。認証に成功すると、スイッチのポートは許可された状態になります。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に依存します。図 9-2 に、RADIUS サーバで One Time Password（OTP; ワンタイム パスワード）認証方式を使用するクライアントによって開始されるメッセージ交換を示します。

図 9-2　メッセージ交換



許可ステートおよび無許可ステートのポート

スイッチ ポート ステートに応じて、スイッチはクライアントのネットワークへのアクセスを許可します。ポートは、*無許可*ステートで起動します。このステートでは、ポートは 802.1x、CDP、STP パケット以外の着信および発信トラフィックを許可しません。クライアントが正常に認証されると、ポートは*許可*ステートに移行し、そのクライアントへのすべてのトラフィックは通常のフローが許可されます。

802.1x をサポートしないクライアントが無許可の 802.1x ポートに接続している場合、スイッチはクライアントの ID を要求します。この場合、クライアントは要求に応答できないので、ポートは無許可ステートのままとなり、クライアントはネットワーク アクセスが許可されません。

対照的に、802.1x 対応クライアントが 802.1x 規格を実行していないポートに接続している場合、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答が得られなかった場合、クライアントは要求を一定の回数だけ送信します。応答が得られないので、クライアントはポートが許可ステートにあるものとしてフレームの送信を開始します。

ポートの許可ステートを制御するには、**dot1x port-control** インターフェイス コンフィギュレーション コマンドと次のキーワードを使用します。

- **force-authorized**：IEEE 802.1x 認証をディセーブルにして、認証情報の交換を要求せずにポートを許可ステートに移行させます。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これは、デフォルト設定です。
- **force-unauthorized**：ポートを無許可ステートのままにし、クライアントが認証を試みてもすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1x 認証をイネーブルにして、ポートに無許可ステートで開始させ、EAPOL フレームだけがポート経由で送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、EAPOL 開始フレームを受信すると、認証プロセスが開始されます。スイッチは、クライアントの ID を要求し、クライアントと認証サーバ間で認証メッセージのリレーを開始します。スイッチはネットワークにアクセスしようとする各クライアントを、クライアントの MAC アドレスを使用して一意に識別します。

クライアントが正常に認証されると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントのフレームはすべてそのポート経由で送受信を許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、認証を再試行できます。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。指定された試行回数のあとでもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフすると EAPOL ログオフ メッセージを送信します。これにより、スイッチ ポートは無許可ステートに移行します。

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

802.1x アカウンティング

802.1x 標準は、ネットワーク アクセスに対するユーザの許可および認証方法を定義しますが、ネットワークの使用状況を追跡するものではありません。802.1x アカウンティングは、デフォルトでディセーブルに設定されています。802.1x アカウンティングをイネーブルにすると、802.1x 対応ポートで次のアクティビティを監視できます。

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

スイッチは 802.1x アカウンティング情報をログに記録しません。代わりに、この情報を RADIUS サーバに送信します。RADIUS サーバはアカウンティング メッセージをログに記録するように設定されている必要があります。

802.1x アカウンティングのアトリビュートと値のペア

RADIUS サーバに送信された情報は、アトリビュートと値（AV）のペアという形式で表されます。AV ペアは、さまざまなアプリケーションにデータを提供します （たとえば、課金アプリケーションでは、パケットの Acct-Input-Octets または Acct-Output-Octets の情報が必要となることがあります）。

AV ペアを設定する必要はありません。これらは、802.1x アカウンティングに設定されるスイッチによって、自動的に送信されます。表 9-1 に、スイッチが送信する AV ペアを示します。

表 9-1　アカウンティングの AV ペア

アトリビュート番号	AV ペア名
Attribute [1]	User-Name
Attribute [4]	NAS-IP-Address
Attribute [5]	NAS-Port
Attribute [6]	NAS-Port-Type
Attribute [8]	Framed-IP-Address
Attribute [25]	Class
Attribute [30]	Called-Station-ID
Attribute [31]	Calling-Station-ID

表 9-1　アカウンティングの AV ペア （続き）

アトリビュート番号	AV ペア名
Attribute [40]	Acct-Status-Type
Attribute [41]	Acct-Delay-Time
Attribute [42]	Acct-Input-Octets
Attribute [43]	Acct-Output-Octets
Attribute [44]	Acct-Session-ID
Attribute [45]	Acct-Authentic
Attribute [46]	Acct-Session-Time
Attribute [49]	Acct-Terminate-Cause

スイッチによって送信されている AV ペアを表示するには、**debug radius accounting** または **debug aaa accounting** の各特権 EXEC コマンドを入力します。このコマンドの詳細については、次の URL の『*Cisco IOS Debug Command Reference*』*Release 12.2* を参照してください。

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

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

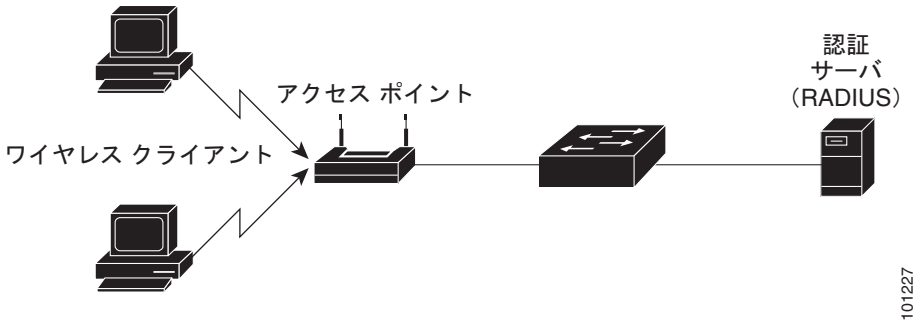
802.1x ホスト モード

802.1x ポートは、単一ホスト モードまたは複数ホスト モードに設定できます。単一ホスト モード（図 9-1（P.9-2）を参照）では、802.1x 対応のスイッチ ポートに接続できるクライアントは 1 台だけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信してクライアントを検出します。クライアントがログオフするか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。図 9-3（P.9-7）は、無線 LAN における 802.1x ポートベース認証を表しています。このモードでは、接続ホストのいずれか 1 つだけが許可されれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL ログオフ メッセージを受信する）、スイッチは、接続しているすべてのクライアントに対するネットワーク 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の場合、802.1x をポートの認証に使用し、クライアントを含むすべての MAC アドレスへのネットワーク アクセスをポート セキュリティが管理します。

図 9-3　複数ホスト モードの例



802.1x 準備状態チェック

802.1x 準備状態チェックでは、すべてのスイッチ ポート上における 802.1x のアクティビティが監視され、802.1x がサポートされているポートに接続されたデバイスに関する情報が表示されます。この機能を使用すれば、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうかを確認できます。802.1x の機能がサポートされていないデバイスに対しては、別の認証を使用します。

この機能が動作するのは、NOTIFY EAP 通知パケットを使用したクエリーがクライアント上のサプリカントによってサポートされている場合だけです。クライアントは、802.1x タイムアウト値の範囲内で応答する必要があります。

802.1x 準備状態チェックに関するスイッチの設定については、「802.1x 準備状態チェックの設定」（P.9-14）を参照してください。

ポート セキュリティを含む 802.1x

単一ホスト モードまたは複数ホスト モードのどちらかで、ポート セキュリティを含む 802.1x ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定する必要もあります）。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 セキュリティがクライアントの MAC アドレスを含むすべての MAC アドレスについてネットワーク アクセスを管理します。この場合、802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

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

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

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

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

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

ポート セキュリティ違反モードは、セキュリティ違反の動作を判別します。詳細については、「セキュリティ違反」（P.23-10）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、802.1x クライアントのアドレスをポート セキュリティ テーブルから手動で削除した場合は、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを使用して 802.1x クライアントを再認証する必要があります。
- 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 エントリが消去されます。ここで通常の認証が実行されます。
- ポートが管理上の理由からシャットダウンされる場合、ポートは無許可ステートになりすべてのダイナミック エントリはセキュア ホスト テーブルから削除されます。
- **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定して、ポートが IEEE 802.1x 対応ポートに接続されている場合や、最大数の許可デバイスが認証されている場合に、ポートがシャットダウンされたり、Syslog エラーが生成されたり、または、新しいデバイスからのパケットが破棄されたりするようにできます。詳細については、「ポート単位の許可デバイスの最大数」（P.9-14）および、このリリースのコマンド リファレンスを参照してください。

スイッチのポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（P.23-8）を参照してください。

VLAN 割り当てを含む 802.1x

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

スイッチと RADIUS サーバで設定されている場合、802.1x と VLAN 割り当てには次のような特性があります。

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

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

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

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

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

VLAN 割り当てを設定するには、次の作業を実行します。

- キーワード **network** 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。
- 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。RADIUS サーバは次のアトリビュートをスイッチに戻す必要があります。
  - [64] トンネル タイプ = VLAN
  - [65] トンネル メディア タイプ = 802
  - [81] トンネル プライベート グループ = VLAN 名または VLAN ID

  アトリビュート [64] は、値 *VLAN*（type 13）とします。アトリビュート [65] は、値 *802*（type 6）とします。アトリビュート [81] には、802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」（P.8-29）を参照してください。

802.1x ユーザ分散

802.1x ユーザ分散を設定して、複数の異なる VLAN を超えて、同じグループ名を持つ各ユーザのロード バランシングができます。

各 VLAN は、RADIUS サーバによって提供されるか、任意の VLAN グループ名で、スイッチ CLI を介して設定されます。

- 1 つのユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。複数の VLAN 名を、ユーザに対する応答の一部として送信できます。802.1x ユーザ分散では、特定の VLAN 内のすべてのユーザを追跡し、許可済みユーザを最もユーザ数の少ない VLAN に移動することによって、ロード バランシングを実現します。
- 1 つのユーザに対して、1 つの VLAN グループ名を送信するように RADIUS サーバを設定します。その VLAN グループ名を、ユーザに対する応答の一部として送信できます。スイッチ CLI を使用して設定した複数の VLAN グループ名の中から、選択した VLAN グループ名を検索できます。その VLAN グループ名が発見されると、最もユーザが少ない VLAN を発見するために、その VLAN グループ名に属する、対応する VLAN が検索されます。対応する許可済みユーザが、その VLAN に移動されることによって、ロード バランシングが実現します。

（注） RADIUS サーバによって、VLAN-ID、VLAN 名、または VLAN グループのどんな組み合せでも、VLAN 情報を送信できます。

802.1x ユーザ分散の設定ガイドライン

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。

- 1 つの VLAN グループに複数の VLAN をマッピングできます。
- VLAN を追加または削除することによって、VLAN グループを変更できます。
- VLAN グループ名から既存の VLAN を消去しても、その VLAN 内のいずれの認証済みポートも消去されることはありませんが、マッピングでは、既存の VLAN グループから削除されます。
- VLAN グループ名から最後の VLAN を消去すると、その VLAN グループは消去されます。
- ある VLAN グループにアクティブな VLAN がマッピングされていても、その VLAN グループを消去できます。VLAN グループを消去しても、そのグループ内のいずれかの VLAN において許可ステートにあるポートまたはユーザは消去されませんが、その VLAN グループに対する VLAN マッピングは消去されます。

詳細については、「802.1x ユーザ分散の設定」（P.9-24）を参照してください。

ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ

Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）機能によって、ID を、ワイヤリング クローゼット（会議室など）の外部の領域に拡張できます。これにより、あらゆるタイプのデバイスに対して、ポート上での認証を許可できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することによって、スイッチを、他のスイッチに対するサプリカントとして動作するように設定できます。この設定は、スイッチがワイヤリング クローゼットの外部にあり、トランク ポートを介してアップストリーム スイッチに接続されているようなシナリオで有用です。802.1x スイッチ サプリカント機能を使用して設定したスイッチでは、アップストリーム スイッチによって認証が行われるので、接続の安全性が確保されます。

  サプリカント スイッチによる認証が成功すると、ポート モードがアクセスからトランクに変更されます。

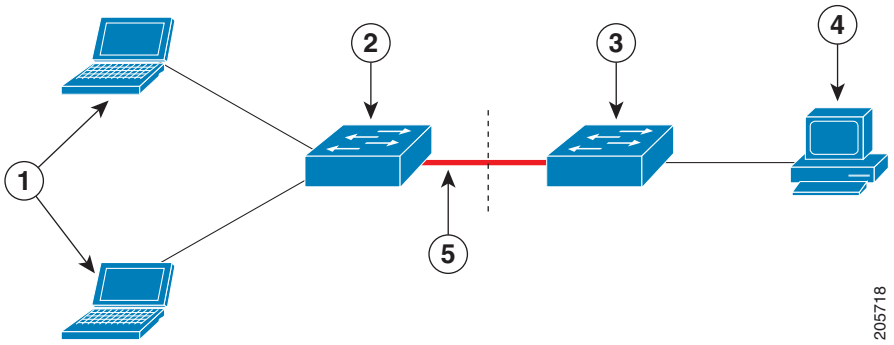
- アクセス VLAN をオーセンティケータ スイッチ上で設定すると、その VLAN は、認証が成功した後に、トランク ポートのネイティブ VLAN になります。

もう 1 つのサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイス上で、MDA またはマルチ認証モードをイネーブルにできます。マルチホスト モードは、オーセンティケータ スイッチ インターフェイスではサポートされていません。

NEAT がすべてのホスト モードで動作するように、サプリカント スイッチ上で、**dot1x supplicant force-multicast** 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。

- ホスト許可：（サプリカントを使用したスイッチに接続している）許可済みホストがネットワーク上で確実に許可されるようにします。各スイッチでは、図 9-4 に示すように、Client Information Signalling Protocol（CISP; クライアント情報シグナリング プロトコル）によって、サプリカント スイッチに接続している MAC アドレスがオーセンティケータ スイッチに送信されます。
- 自動イネーブル化：オーセンティケータ スイッチ上でトランク設定が自動的にイネーブルにされ、オーセンティケータ スイッチから来る、複数の VLAN からのユーザ トラフィックが許可されます。ACS で、cisco-av-pair を *device-traffic-class=switch* に設定します （これは、*group* または *user* 設定で設定できます）。

図 9-4　CISP を使用したオーセンティケータおよびサプリカント スイッチ



1	ワークステーション（クライアント）	2	サプリカント スイッチ（ワイヤリング クローゼットの外部）
3	オーセンティケータ スイッチ	4	Access Control Server（ACS）
5	トランク ポート		

ガイドライン

- NEAT ポートを、他の認証ポートと同じコンフィギュレーションで設定できます。サプリカント スイッチが認証を実行すると、スイッチ ベンダー固有アトリビュート（VSA）に基づいて、ポートモードが *アクセス*から *トランク*に変更されます（device-traffic-class=switch）。
- VSA によって、オーセンティケータ スイッチ ポート モードが、アクセスからトランクに変更され、802.1x トランクのカプセル化およびアクセス VLAN が、ネイティブ トランク VLAN に変換される場合に、イネーブルにされます。VSA によっては、サプリカント上でのポート設定は変更されません。
- ホスト モードを変更し、また、オーセンティケータ スイッチ ポート上で標準ポート設定を適用するには、スイッチ VSA ではなく、AutoSmart ポート ユーザ定義マクロを使用することも可能です。これにより、オーセンティケータ スイッチ ポート上のサポートされていない設定を削除し、ポート モードを *アクセス*から *トランク*に変更できます。詳細については、第 11 章「コマンド マクロの設定」を参照してください。

詳細については、「オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定」（P.9-25）を参照してください。

コモン セッション ID

認証マネージャでは、どの認証方法が使用されるのかに関わらず、クライアントのシングル セッション ID（コモン セッションと呼びます）が使用されます。この ID は、表示コマンドや MIB など、あらゆるレポート用途で使用されます。セッション ID は、セッション単位のすべての Syslog メッセージと共に表示されます。

セッション ID には、次のものがあります。

- Network Access Device（NAD; ネットワーク アクセス デバイス）の IP アドレス
- 単調に増加する一意の 32 ビット整数
- セッション開始タイム スタンプ（32 ビット整数）

この例では、show authentication コマンドの出力内でセッション ID がどのように表示されるのかを示します。この例におけるセッション ID は、160000050000000B288508E5 です。

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

これは、Syslog 出力内でのセッション ID の表示例です。この例におけるセッション ID も、160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

このセッション ID は、クライアントを特定するために、NAD、AAA サーバ、およびその他レポート分析アプリケーションによって使用されます。ID は自動的に表示されます。設定は不要です。

IEEE 802.1x 認証の設定

ここでは、次の設定情報について説明します。

802.1x のデフォルト設定

表 9-2 に、802.1x のデフォルト設定を示します。

表 9-2　802.1x のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル。
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし。 • 1812. • 指定なし。
スイッチの 802.1x イネーブル ステート	ディセーブル。
ポート単位の 802.1x イネーブル ステート	ディセーブル（force-authorized）。 ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
定期的再認証	ディセーブル。
再認証試行間隔	3600 秒
再認証回数	2 回（ポートが未許可ステートになるまでにスイッチが認証プロセスを再開する回数）
待機時間	60 秒（クライアントとの認証交換が失敗したあと、スイッチが待機ステートにとどまる秒数）
再送信時間	30 秒（スイッチが、クライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（スイッチが、認証プロセスを再開するまでに EAP 要求/ID フレームを送信する回数）
ホスト モード	単一ホスト モード
クライアントのタイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが応答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバのタイムアウト時間	30 秒（クライアントの応答を認証サーバにリレーするとき、スイッチが応答を待ち、サーバに応答を送信するまでの時間）。 このタイムアウト時間を変更するには、**dot1x timeout server-timeout** 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。

802.1x 設定時の注意事項

802.1x 認証の設定時の注意事項は次のとおりです。

- 802.1x がイネーブルの場合、ポートは認証されたあとに他のレイヤ 2 またはレイヤ 3 機能がイネーブルになります。
- 802.1x プロトコルは、レイヤ 2 スタティック アクセス ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。

  - トランク ポート：トランク ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバーを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポート上のポートで 802.1x をイネーブルにできます。ただし、ポートが SPAN または RSPAN 宛先ポートとして削除されるまで 802.1x はディセーブルです。SPAN または RSPAN 送信元ポートでは、802.1x をイネーブルにできます。
- RSPAN VLAN または プライベート VLAN 以外のすべての VLAN を設定できます。
- VLAN 割り当て機能付きの 802.1x は、プライベート VLAN ポート、トランク ポート、または VMPS を使用したダイナミック アクセス ポート割り当てではサポートされていません。
- プライベート VLAN ポートでは 802.1x を設定できますが、ポート セキュリティとは同時に設定しないでください。
- **dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x をグローバルにイネーブルにする前に、802.1x と EtherChannel が設定されているインターフェイスで EtherChannel コンフィギュレーションを削除します。

ポート単位の許可デバイスの最大数

これは、802.1x 対応ポート上で許可されるデバイスの最大数です。

- 単一ホスト モードでは、アクセス VLAN 上で許可されるデバイスは 1 つだけです。ポートを音声 VLAN でも設定する場合、音声 VLAN を介してトラフィックを送受信可能な Cisco IP Phone の数に制限はありません。
- マルチホスト モードでは、ポート上で許可される 802.1x サプリカントは 1 つだけですが、アクセス VLAN 上で許可される非 802.1x ホストの数に制限はありません。音声 VLAN 上で許可されるデバイスの数に制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックでは、すべてのスイッチ ポート上における 802.1x のアクティビティが監視され、802.1x がサポートされているポートに接続されたデバイスに関する情報が表示されます。この機能を使用すれば、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうかを確認できます。

802.1x 準備状態チェックは、802.1x 用に設定可能なすべてのポート上で許可されます。準備状態チェックは、**dot1x force-unauthorized** として設定されているポート上では使用できません。

スイッチ上で準備状態チェックをイネーブルにするには、次のガイドラインに従ってください。

- 準備状態チェックは、802.1x をスイッチ上でイネーブルにする前に使用するのが一般的です。
- インターフェイスを指定しないで **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタック上のすべてのポートがテストされます。

- 802.1x 対応ポート上で **dot1x test eapol-capable** コマンドを設定し、リンクが起動する際、ポートによって、接続されたクライアントに対し、その 802.1x 機能に関するクエリーが実行されます。クライアントが通知パケットによって応答する場合、そのクライアントは 802.1x 対応です。クライアントがタイムアウト時間内で応答すると、Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、そのクライアントは非 802.1x 対応です。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホストを処理するポート上（IP 電話に接続された PC など）で送信できます。Syslog メッセージは、タイマー時間内で準備状態チェックに応答するクライアントごとに生成されます。

スイッチ上で 802.1x 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 （任意）*interface-id* には、IEEE 802.1x 準備状態のチェックを実行するポートを指定します。 **（注）** オプションの **interface** キーワードを省略すると、スイッチ上のすべてのインターフェイスがテストされます。
ステップ 1	**configure terminal**	（任意）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	**dot1x test timeout** *timeout*	（任意）EAPOL 応答を待機するために使用されるタイムアウトを設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。
ステップ 3	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	（任意）変更したタイムアウト値を確認します。

次の例では、スイッチ上で準備状態チェックをイネーブルにしてポートにクエリーを実行する方法を示します。また、照会済みポートから受信した応答も示し、接続しているデバイスが 802.1x 対応であることを確認します。

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

802.1x 違反モードの設定

802.1x ポートを、次の場合にシャットダウンされ、Syslog エラーを生成し、新しいデバイスからのパケットを破棄するように設定できます。

- デバイスが 802.1x 対応ポートに接続している
- デバイスに関して許可される最大数がポート上で許可されている

スイッチ上にセキュリティ違反動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定*されない*場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、キーワード **group radius** を入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** コマンドライン ヘルプ ストリングではその他のキーワードが表示されても、サポートされるのは **group radius** キーワードだけです。
ステップ 4	**interface** *interface-id*	クライアントに接続されたポートの中で、IEEE 802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：ポートをエラー ディセーブルにします。 • **restrict**：Syslog エラーを生成します。 • **protect**：トラフィックをポートに送信する新しいデバイスからのパケットを破棄します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show dot1x**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の設定

802.1x ポートベースの認証を設定するには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

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

802.1x AAA プロセスは次のとおりです。

ステップ 1　ユーザがスイッチ上のポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバ設定に基づいて VLAN 割り当てが適切にイネーブルになります。

ステップ 4　スイッチが開始メッセージをアカウンティング サーバに送信します。

ステップ 5　必要に応じて再認証が実行されます。

ステップ 6　再認証結果に基づいて、スイッチが暫定的なアカウンティング アップデートをアカウンティング サーバに送信します。

ステップ 7　ユーザがポートから切断されます。

ステップ 8　スイッチが停止メッセージをアカウンティング サーバに送信します。

802.1x ポートベースの認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが指定*されない*場合に使用されるデフォルトのリストを作成するには、キーワード **default** の後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、キーワード **group radius** を入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** コマンドライン ヘルプ ストリングではその他のキーワードが表示されても、サポートされるのは **group radius** キーワードだけです。
ステップ 4	**dot1x system-auth-control**	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 6	**interface** *interface-id*	クライアントに接続されたポートの中で、802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**dot1x port-control auto**	ポート上で 802.1x 認証をイネーブルにします。 機能の相互作用の詳細については、「802.1x 設定時の注意事項」（P.9-13）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show dot1x**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチと RADIUS サーバ間通信を設定する方法

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、あるいは IP アドレスと特定の UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合せにより、一意の識別子が作成され、これにより、サーバ上の同一の IP アドレスの複数の UDP ポートに RADIUS 要求を送信できます。同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、認証）を設定している場合、あとから設定されたホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。RADIUS のホスト エントリは、設定された順序で試されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* |*ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 です。指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。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）** 先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されるため、鍵は必ず **radius-server host** コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。この鍵は、RADIUS デーモン上で使用する暗号と照合する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し入力してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次の例は、IP アドレスが 172.20.39.46 のサーバを RADIUS サーバとして照合し、ポート 1612 を許可ポートとして使用し、暗号化鍵を RADIUS サーバ上の鍵と *rad123* に設定します。

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

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化鍵の値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバに対する設定」（P.8-29）を参照してください。

さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー ストリングです。詳細については、RADIUS サーバのマニュアルを参照してください。

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにして、その発生間隔を指定できます。再認証の間隔を指定しなかった場合は、再認証は 3600 秒ごとに行われます。

クライアントの定期的な再認証をイネーブルにして、再認証を試行する間隔（秒数）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x reauthentication**	デフォルトではディセーブルに設定されている定期的な再認証をイネーブルにします。
ステップ 4	**dot1x timeout reauth-period** *seconds*	再認証の間隔（秒）を指定します。 指定できる範囲は 1 ～ 65,535 秒で、デフォルトは 3600 秒です。 定期的な再認証がイネーブルに設定されている場合にだけ、このコマンドはスイッチの動作に影響します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

手動によるポート接続クライアントの再認証

dot1x re-authenticate interface *interface-id* 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。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする場合は、「定期的な再認証の設定」（P.9-18）を参照してください。

次に、ポートに接続したクライアントを手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

待機時間の変更

スイッチがクライアントを認証できなかった場合は、スイッチは一定時間アイドル状態を続けたあと、再試行します。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用すると、アイドル時間を制御できます。クライアントが無効なパスワードを提供したため、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力することで、ユーザに対する応答時間を短縮できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**dot1x timeout quiet-period** *seconds*	クライアントとの認証交換が失敗したあと、スイッチが待機ステートにある秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 60 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例では、スイッチ上の待機時間を 30 秒に設定します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

スイッチとクライアント間の再送信時間の変更

クライアントは、スイッチからの EAP 要求/ID フレームに、EAP 応答/ID フレームで応答します。スイッチはこの応答を受信しなかった場合、一定時間（再送信時間）待機してから、フレームを再送信します。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチがクライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1xinterface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例では、スイッチがクライアントからの EAP 要求/ID フレームに対する応答を待ち、要求を再送信するまでの秒数を 60 秒に設定します。

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

スイッチとクライアント間のフレーム再送信回数の設定

スイッチとクライアント間の再送信時間の変更だけでなく、（応答を受信しなかった場合）認証プロセスを再開するまでに、スイッチがクライアントに EAP フレームを送信する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチとクライアント間のフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが、認証プロセスを再開するまでに EAP フレームをクライアントに送信する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例では、認証プロセスを再開するまでに、スイッチが EAP 要求を送信する回数を 5 に設定します。

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

再認証回数の設定

スイッチが、ポートが未許可ステートに変わるまでに認証プロセスを再始動する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが、ポートが未許可ステートに変わるまでに認証プロセスを再始動する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

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

ホスト モードの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	複数のホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x 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）を許可します。 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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

dot1x host-mode single-host インターフェイス コンフィギュレーション コマンドを入力して、インターフェイスを、ポート上の単一ホストを許可するように設定します。

（注）　**dot1x host-mode multi-domain** インターフェイス コンフィギュレーション コマンドは、コマンドライン インターフェイスのヘルプには表示されますが、サポートされていません。インターフェイス上でこのコマンドを設定すると、インターフェイスがエラー ディセーブル ステートになります。

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

次に、802.1x をイネーブルにし、複数のホストを許可する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

```
Switch(config-if)# dot1x host-mode multi-host
```

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、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x アカウンティングの設定

AAA システム アカウンティングと 802.1x アカウンティングをイネーブルにすることにより、ロギング用にシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。これにより、サーバはすべてのアクティブ 802.1x セッションが閉じていることを推測できます。

RADIUS は信頼性のない UDP トランスポート プロトコルを使用するため、ネットワークの状態が悪いとアカウンティング メッセージが消失する場合があります。設定されたアカウンティング要求の再送信回数を超えてもスイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、このシステム メッセージが表示されます。

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

停止メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） 開始、停止、暫定的な更新メッセージ、およびタイム スタンプのロギングなどの、アカウンティング タスクを実行するように RADIUS サーバを設定する必要があります。この機能をオンにするには、RADIUS サーバのネットワーク設定タブにある「Update/Watchdog packets from this AAA client」のロギングをイネーブルにします。次に、RADIUS サーバのシステム設定タブの「CVS RADIUS Accounting」をイネーブルにします。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**aaa accounting dot1x default start-stop group radius**	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting system default start-stop group radius**	（任意）（すべての RADIUS サーバのリストを使用して）システム アカウンティングをイネーブルにして、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

802.1x ユーザ分散の設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、グローバル コンフィギュレーションで次の手順を実行します。

	コマンド	目的
ステップ 1	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定して、単一の VLAN または一連の VLAN をそのグループにマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** ***vlan-group-name*** **vlan-list** ***vlan-list***	VLAN グループ設定、または VLAN グループ設定の要素を消去します。

次の例では、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループの設定と、指定した VLAN に対するマッピングを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
switch# show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
```

次の例では、VLAN を既存の VLAN グループに追加し、その VLAN が追加されたことを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
```

```
-------------                    --------------
eng-dept                         10,30
```

次の例では、VLAN グループから VLAN を削除する方法を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次の例では、VLAN グループからすべての VLAN を消去すると、その VLAN グループが消去されることを示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループを消去する方法を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

オーセンティケータおよび、NEAT を使用したサプリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼットの外部にある 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されていることが必要です。

概要については、「ネットワーク エッジ アクセス トポロジ（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ」（P.9-10）を参照してください。

（注） *cisco-av-pair* は、ACS 上で *device-traffic-class=switch* として設定する必要があります。これにより、サプリカントの認証が成功した後に、インターフェイスがトランクとして設定されます。

スイッチをオーセンティケータとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**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 4	**switchport mode access**	ポート モードを**アクセス**に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを自動に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスを Port Access Entity（PAE）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast**	単一のワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチを 802.1x オーセンティケータとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサプリカントとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1x 証明書プロファイルを作成します。これは、サプリカントとして設定されたポートに付加する必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。
ステップ 5	**password** *password*	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	スイッチによってユニキャストまたはマルチキャスト パケットが受信されたときに、強制的にマルチキャスト EAPOL パケット*だけ*が送信されるように、そのスイッチを設定します。 これにより、すべてのホスト モードで NEAT がサプリカント スイッチ上で動作することも可能となります。
ステップ 7	**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 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスを Port Access Entity（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1x 証明書プロファイルをインターフェイスに付加します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id*	設定を確認します。
ステップ 14	**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。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

ASP を使用した NEAT の設定

スイッチ VSA ではなく、AutoSmart Ports ユーザ定義マクロを使用してオーセンティケータ スイッチを設定することも可能です。詳細については、第 11 章「コマンド マクロの設定」を参照してください。

802.1x 統計情報およびステータスの表示

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

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

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