CHAPTER 10

IEEE 802.1X ポートベース認証の設定

IEEE 802.1x ポートベース認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。特に明記しない限り、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

コマンドの構文と使用方法の詳細については、Catalyst 3750 のスイッチのコマンド リファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』の「RADIUS Commands」のセクションを参照してください。

また、スイッチは Cisco TrustSec の Security Group Tag（SCT; セキュリティ グループ タグ）Exchange Protocol（SXP）をサポートしています。この機能では、IP アドレスではなく、デバイスのグループに対する ACL ポリシーを定義する Security Group Access Control List（SGACL; セキュリティ グループ アクセス コントロール リスト）がサポートされます。SXP コントロール プロトコルは、ハードウェアのアップグレードを伴わない SCT によるパケットのタギングを可能にし、Cisco TrustSec ドメイン エッジのアクセス レイヤ デバイスと Cisco TrustSec ドメイン内のディストリビューション レイヤ デバイスの間で実行されます。Catalyst 3750-X および 3560-X スイッチは、Cisco TrustSec ネットワーク上でアクセス レイヤ スイッチとして動作します。

Cisco TrustSec の詳細については、次の URL にある『*Cisco TrustSec Switch Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

SXP に関する項では、Catalyst 3750 スイッチでサポートされる機能について定義しています。

この章で説明する内容は、次のとおりです。

IEEE 802.1X ポートベース認証の概要

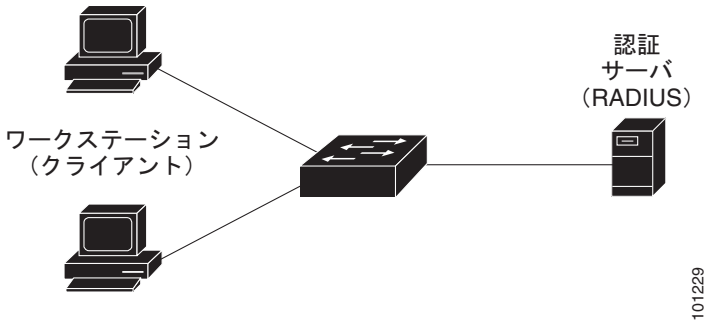
標準では、一般の人がアクセス可能なポートから無許可のクライアントが LAN に接続しないように規制する、クライアント/サーバ型のアクセス制御および認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN のサービスを利用できるようにします。

IEEE 802.1X アクセス制御では、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、および Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックしか許可されません。認証後、通常のトラフィックをポート経由で送受信します。

デバイスの役割

802.1X ポートベース認証を使用するデバイスの役割

図 10-1　802.1X におけるデバイスの役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP OS（オペレーティング システム）に付属しているような 802.1X 準拠のクライアント ソフトウェアを実行する必要があります（クライアントは、802.1X 標準では*サプリカント*といいます）。

  （注） Windows XP のネットワーク接続および 802.1X 認証に関する問題の解決方法については、次の URL にある「Microsoft Knowledge Base」を参照してください。
  http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*：クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

- *スイッチ*（エッジ スイッチまたはワイヤレス アクセス ポイント）：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています（スイッチは、802.1X 標準では*オーセンティケータ*と呼ばれます）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介デバイスとして動作できるものには、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940、またはワイヤレス アクセス ポイントがあります。これらのデバイスでは、RADIUS クライアントおよび 802.1X 認証をサポートするソフトウェアが稼動している必要があります。

認証プロセス

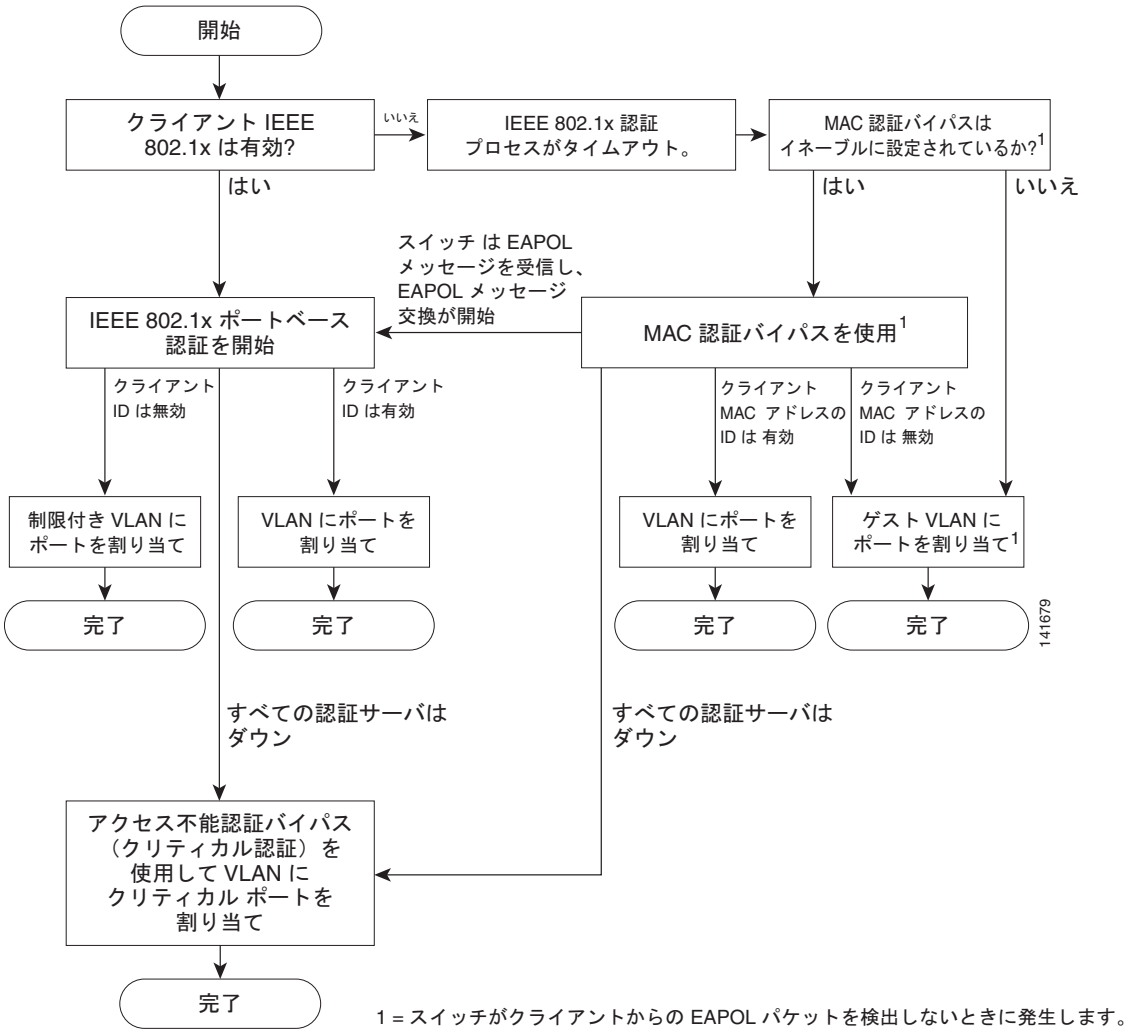
802.1X ポートベース認証がイネーブルであり、クライアントが 802.1X 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1X 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1X 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）失敗ポリシーとも呼ばれます。

図 10-2 に、認証プロセスを示します。

図 10-2　認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用する 802.1X 認証を設定した後、スイッチは、Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS アトリビュート（アトリビュート [27]）は、再認証が発生するまでの時間を指定します。

  Termination-Action RADIUS アトリビュート（アトリビュート [29]）は、再認証中に行うアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。*Initialize* アクションが設定されていると（アトリビュートの値は *DEFAULT*）、802.1X セッションが終了し、再認証中に接続が切断されます。*ReAuthenticate* アクションが設定されていると（アトリビュートの値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力します。

Multidomain Authentication（MDA; マルチドメイン認証）がポートでイネーブルの場合、音声認証に適用可能ないくつかの例外とともにこのフローを使用することができます。MDA の詳細については、「マルチドメイン認証」（P.10-14）を参照してください。

認証の開始およびメッセージ交換

802.1X 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** または **dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにした場合、スイッチはポートのリンク ステートがダウンからアップに変更した時点で、またはポートが認証されてないままアップの状態である限り定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

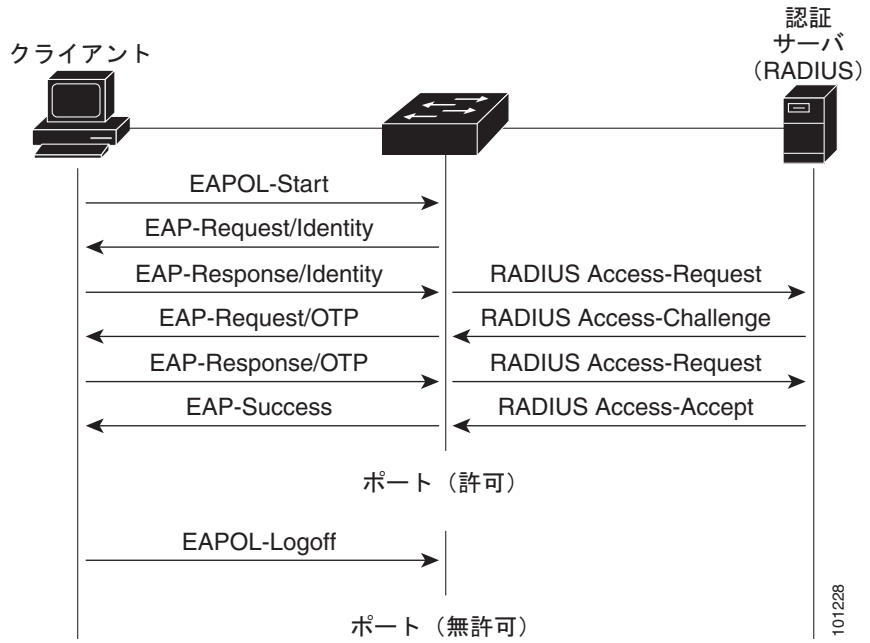
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注） ネットワーク アクセス デバイスで 802.1X 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.10-12）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。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.10-12）を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 10-3 に、クライアントが RADIUS サーバとの間で One-Time-Password（OTP; ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

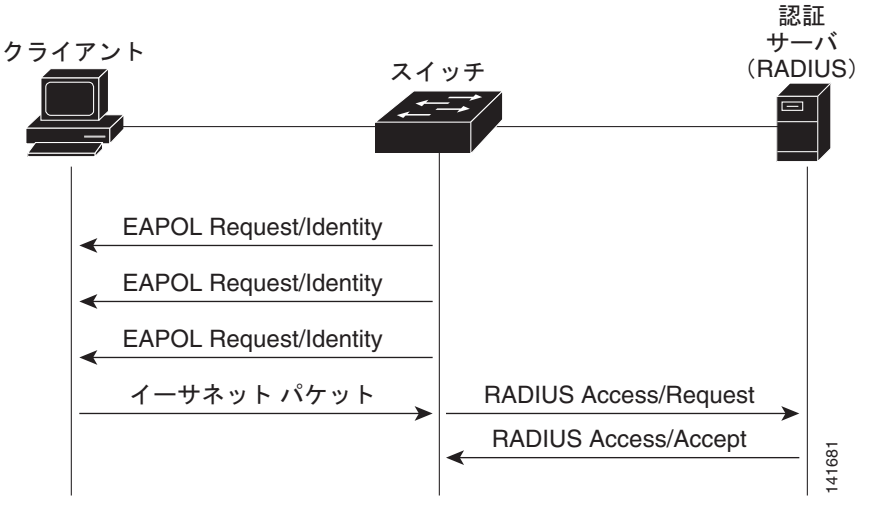
図 10-3　メッセージ交換



EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS アクセス / 要求フレームにこの情報を保存します。サーバがスイッチに RADIUS アクセス / 承認フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1X 認証を停止します。

図 10-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 10-4　MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、このスイッチ上で、および Catalyst 6000 などのその他のネットワーク デバイス上でも、CLI コマンドとメッセージを含め、同じ認証方式を使用できませんでした。個別の認証設定を使用する必要がありました。Cisco IOS Release 12.2(50)SE 以降では、ネットワーク内のすべての Catalyst スイッチ上で、同じ認証方式をサポートしています。

Cisco IOS Release 12.2(55)SE では、認証マネージャからの詳細なシステム メッセージのフィルタリングをサポートしています。詳細については、「認証マネージャの CLI コマンド」（P.10-10）を参照してください。

ポートベース認証

表 10-1 に、これらのホスト モードでサポートされる認証方式を示します。

- シングル ホスト：1 つのポートで 1 つのデータ ホストだけまたは音声ホスト（クライアント）だけが認証されることができます。
- マルチ ホスト：同一のポートで複数のデータホストが認証されることができます（ポートがマルチ ホスト モードで無許可になると、スイッチはすべての接続されたクライアントへのネットワーク アクセスを拒否します）。
- マルチドメイン認証（MDA）：データ装置と音声装置の両方が、同一のスイッチ ポートで認証されることができます。ポートは、データ ドメインと音声ドメインに分けられます。
- マルチ認証：複数のホストがデータ VLAN 上で認証を行えます。このモードでは、音声 VLAN が設定されている場合は、VLAN に 1 つのクライアントも可能です。

表 10-1　802.1X の機能

認証方式	モード			
	シングル ホスト	マルチ ホスト	MDA[1]	マルチ認証[2]
802.1X	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL[4] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id アトリビュート[3] ダウンロード可能な ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id アトリビュート[3] ダウンロード可能な ACL[3] リダイレクト URL[3]
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id アトリビュート[3] ダウンロード可能な ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id アトリビュート[3] ダウンロード可能な ACL[3] リダイレクト URL[3]
スタンドアロン Web 認証[4]	プロキシ ACL、Filter-Id アトリビュート、ダウンロード可能な ACL[2]			
NAC レイヤ 2 IP 検証	Filter-Id アトリビュート[3] ダウンロード可能な ACL リダイレクト URL	Filter-Id アトリビュート[3] ダウンロード可能な ACL リダイレクト URL	Filter-Id アトリビュート[3] ダウンロード可能な ACL リダイレクト URL	Filter-Id アトリビュート[3] ダウンロード可能な ACL[3] リダイレクト URL[3]
フォールバック メソッドとしての Web 認証[5]	プロキシ ACL Filter-Id アトリビュート[3] ダウンロード可能な ACL[3]	プロキシ ACL Filter-Id アトリビュート[3] ダウンロード可能な ACL[3]	プロキシ ACL Filter-Id アトリビュート[3] ダウンロード可能な ACL[3]	プロキシ ACL[3] Filter-Id アトリビュート[3] ダウンロード可能な ACL[3]

1. MDA = マルチドメイン認証。
2. *multiauth* とも呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
5. 802.1X 認証をサポートしないクライアント用です。

ユーザ単位 ACL と Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id は、シングル ホストモードでだけサポートされました。Cisco IOS Release 12.2(50) では、MDA およびマルチ認証がイネーブルであるポートのサポートが追加されました。12.2(52)SE 以降では、マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチ上で設定された Access Control List（ACL; アクセス コントロール リスト）は、Catalyst 6000 スイッチなどの Cisco IOS ソフトウェアを実行している別のデバイスで設定された ACL との互換性がありません。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行している他のデバイスと互換性があります。

（注） ACL では **any** だけをソースとして設定できます。

（注） マルチ ホスト モードに対して設定された ACL では、ステートメントのソース部分は、*any* でなければなりません（たとえば、**permit icmp** *any* **host 10.10.1.1**）。

定義された ACL のソース部分に *any* を指定する必要があります。そうしなければ、ACL は適用できず、認証は失敗します。シングル ホストだけが下位互換性サポートから除外されます。

MDA がイネーブルのポートおよびマルチ認証のポートで、2 つ以上のホストを認証できます。1 つのホストに適用された ACL ポリシーは別のホストのトラフィックに影響を与えません。

マルチホストのポートで 1 つのホストだけが認証され、他のホストは認証なしでネットワーク アクセスを取得した場合、送信元アドレスに *any* を指定することで 1 番めのホストに対する ACL ポリシーを他の接続されたホストにも適用できます。

認証マネージャの CLI コマンド

認証マネージャのインターフェイス コンフィギュレーション コマンドは 802.1X、MAC 認証バイパス、Web 認証などのすべての認証方式を制御します。認証マネージャのコマンドは、接続されたホストに適用される認証方式のプライオリティと順序を決定します。

認証マネージャのコマンドは、ホスト モード、違反モード、認証タイマーなどの汎用認証機能を制御します。汎用認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** インターフェイス コンフィギュレーション コマンドが含まれます。

802.1X 固有のコマンドは **dot1x** キーワードで開始します。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイス上での認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは、グローバルにのみ 802.1X 認証をイネーブルまたはディセーブルにします。

（注） 802.1X 認証がグローバルにディセーブルになっている場合は、そのポートでは Web 認証などの他の認証方式はまだイネーブルになっています。

authentication manager コマンドは、以前の 802.1X コマンドと同じ機能を提供します。

表 10-2　認証マネージャのコマンドおよび以前の 802.1X コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1X コマンド	説明
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	wake-on-LAN（WoL）機能を使用して認証をイネーブルにし、ポート コントロールを双方向または単方向に設定します。
authentication event	**dot1x auth-fail vlan**	ポート上で制限付き VLAN をイネーブルにします。
	dot1x critical (interface configuration)	アクセス不能認証バイパス機能をイネーブルにします。
	dot1x guest-vlan6	アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	認証をサポートしないクライアントのフォールバック メソッドとして Web 認証を使用するようにポートを設定します。
authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	**dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	認証済みポート上で単一のホスト（クライアント）または複数のホストを許可します。
authentication order	**dot1x mac-auth-bypass**	使用される認証方式の順序の定義に柔軟性を与えます。
authentication periodic	**dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。
authentication port-control {**auto** | **force-authorized** | **force-un authorized**}	**dot1x port-control {auto | force-authorized | force-unauthorized}**	ポートの許可ステートの手動での制御をイネーブルにします。
authentication timer	**dot1x timeout**	タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	ポートに新しいデバイスが接続されたとき、またはあるポートに最大数のデバイスが接続された後にそのポートに新しいデバイスが接続されたときに発生する違反モードを設定します。

Cisco IOS Release 12.2(55)SE 以降では、認証マネージャによって生成される詳細なシステム メッセージをフィルタリングできます。フィルタリングされる内容は、通常、認証の成功に関連するものです。802.1x 認証および MAB 認証に関する詳細メッセージをフィルタリングすることもできます。認証方法ごとに、別のコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC Authentication Bypass（MAB; MAC 認証バイパス）の詳細メッセージをフィルタリングします。

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。

許可ステートおよび無許可ステートのポート

802.1X 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1X 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN として設定されている場合、VoIP トラフィックおよび 802.1X プロトコル パケットが許可された後クライアントが正常に認証されます。

802.1X をサポートしていないクライアントが、無許可ステートの 802.1X ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1X 対応のクライアントが、802.1X 標準が稼動していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。また、応答がない場合は、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control または **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します。

- **force-authorized**：802.1X 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- **force-unauthorized**：クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、ポートを介してクライアントに認証サービスを提供できません。
- **auto**：802.1X 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC（メディア アクセス制御）アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可されます。認証に失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

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

802.1X 認証とスイッチ スタック

スイッチがスイッチ スタックで追加または削除されても、RADIUS サーバとスタック間の IP 接続が保たれている限りは、802.1X 認証に影響はありません。このことは、スタック マスターがスイッチ スタックから削除された場合にも当てはまります。スタック マスターに障害が生じると、スタック メンバーが第 5 章「スイッチ スタックの管理」に記載されている選択プロセスを使用して新たなスタック マスターとなり、802.1X 認証プロセスは通常どおり継続されることに注意してください。

サーバに接続されていたスイッチが削除されたり、またはそのスイッチに障害が発生したりといった理由で RADIUS サーバへの IP 接続が切断された場合には、次のイベントが発生します。

- すでに認証済みで定期的な再認証がイネーブル化されていないポートは、認証ステートのままです。RADIUS サーバとの通信は必要ありません。
- すでに認証済みで、定期的な再認証がイネーブル化されているポートは（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用して）、再認証時に認証プロセスに失敗します。ポートは、再認証プロセスで未認証ステートに戻ります。RADIUS サーバとの通信が必要です。

  進行中の認証は、サーバ接続がないため即座に失敗します。

障害の発生したスイッチが再びアップし、スイッチ スタックに参加した場合は、起動時間と、認証が試行されるまでに RADIUS サーバへの接続が再確立されたかどうかによって、認証は失敗することもあります。

RADIUS サーバ接続の切断を回避するには、冗長接続を確立しておく必要があります。たとえば、スタック マスターへの冗長接続とスタック メンバーへの別の冗長接続を確立しておけば、スタック マスターに障害が発生しても、スイッチ スタックは RADIUS サーバへの接続を維持できます。

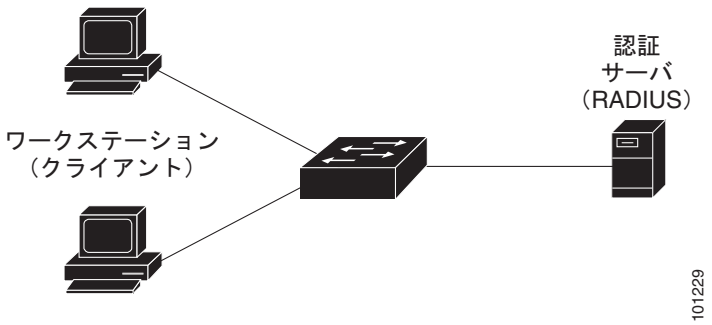
802.1X のホスト モード

I802.1X ポートは、シングルホスト モードまたはマルチホスト モードで設定できます。シングルホスト モード（図 10-1（P.10-3）を参照）では、802.1X 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチホスト 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 10-5（P.10-13）に、ワイヤレス LAN における 802.1X ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチホスト モードがイネーブルの場合、802.1X 認証を使用してポートおよびポート セキュリティを認証し、クライアントを含むすべての MAC アドレスのネットワーク アクセスを管理できます。

図 10-5　　マルチホスト モードの例



このスイッチは、マルチドメイン認証（MDA）をサポートしています。これにより、データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方が、同一のスイッチ ポートに接続できます。詳細については、「マルチドメイン認証」（P.10-14）を参照してください。

マルチドメイン認証

このスイッチは、MDA をサポートしています。これにより、データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方が、同一のスイッチ ポートを認証することができます。ポートは、データ ドメインと音声ドメインに分けられます。

MDA は、デバイス認証の順序を強制しません。しかし、最良の結果を出すには、MDA 対応ポートでは音声デバイスをデータ デバイスの前に認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA 用にスイッチ ポートを設定するには、「ホスト モードの設定」（P.10-46）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る際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 13 章「VLAN の設定」を参照してください。
- Cisco IOS Release 12.2(40)SE 以降のリリースでは、MDA 対応ポートでの音声 VLAN 割り当てをサポートしています。

（注） ダイナミック VLAN を使用して音声 VLAN を Cisco IOS Release 12.2(37)SE の動作する MDA 対応スイッチ ポートに割り当てると、音声デバイスで許可が失敗します。

- 音声デバイスを許可するには、`device-traffic-class=voice` という値を持ったシスコ Attribute-Value（AV; アトリビュート値）ペア アトリビュートを送信するように、AAA サーバを設定する必要があります。この値がない場合、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 および制限付き VLAN 機能は、MDA 対応レポートのデータ デバイスだけに適用されます。スイッチは、許可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。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、errdisable になります。
- デバイスが許可されるまで、ポートでトラフィックがドロップされます。シスコ製以外の IP 電話や音声デバイスがデータおよび音声 VLAN で許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得できます。音声デバイスが 音声 VLAN で送信を開始した後、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック メカニズムとして MAC 認証バイパスを使用して、802.1X 認証をサポートしていないデバイスにスイッチポートを接続することができます。詳細については、「MAC 認証バイパス」（P.10-40）を参照してください。
- *データ*または*音声*デバイスがポートで検出されると、許可に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが無許可である間に 6 つ以上のデバイスが*データ* VLAN で検出された場合や、複数の*音声*デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードがシングルホストまたはマルチホストからマルチドメイン モードに変更される際に、許可済みのデータ デバイスはポートで許可済みのままになります。ただし、ポート音声 VLAN 上の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。

- ポートがシングルホストまたはマルチホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック メカニズムは設定されたままになります。
- マルチドメイン モードからシングルホストまたはマルチホスト モードにポートを切り替えると、ポートからすべての許可済みデバイスが削除されます。
- データ ドメインがまず許可されてゲスト VLAN に配置された場合、802.1X 非対応音声デバイスは認証をトリガーするために音声 VLAN 上のパケットにタグを付ける必要があります。電話はタグ付きトラフィックを送信する必要はありません（802.1X 対応電話も同様です）。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを有する許可済みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。ポート上の 1 つのデバイスだけを使用してユーザ単位 ACL を実行することができます。

詳細については、「ホスト モードの設定」（P.10-46）を参照してください。

802.1X マルチ認証モード

マルチ認証（multiauth）モードは、音声 VLAN 上のデータ VLAN 上の複数の認証済みクライアントを許可します。各ホストは別々に認証されます。音声 VLAN が設定されている場合、このモードでは VLAN 上に 1 つのクライアントが可能です（ポートがその他の音声クライアントを検知すると、その音声クライアントはポートから破棄されますが、違反エラーは発生しません）。

ハブまたはアクセスポイントが 802.1X 対応ポートに接続されている場合、接続されているクライアントは認証される必要があります。

802.1X 非対応デバイスでは、個別のホスト認証が単一のポート上でさまざまな方式によってホスト単位で認証するためのフォールバック メソッドとして MAC 認証バイパスまたは Web 認証を使用できます。

マルチ認証ポート上で認証されるデータ ホストの数に制限はありません。しかし、音声デバイスが設定されている場合は、1 つのデバイスだけが許可されます。違反がトリガーされることを定義されたホストの制限がないため、別の音声デバイスが見つかったときは、何も通知せずに破棄され違反はトリガーされません。

音声 VLAN の MDA 機能の場合、マルチ認証モードは、認証サーバから受信した VSA に応じて認証済みデバイスをデータまたは音声 VLAN のいずれかに割り当てます。

（注） ポートがマルチ認証モードの場合、ゲスト VLAN 機能や認証失敗 VLAN 機能がアクティブになることはありません。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「アクセス不能認証バイパスによる 802.1X 認証」（P.10-26）を参照してください。

ポートのマルチ認証モードの詳細については、「ホスト モードの設定」（P.10-46）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、次の状況で、RADIUS サーバにより提供される VLAN をマルチ認証モードで割り当てることができます。

- ホストが、ポートで許可された最初のホストであり、RADIUS サーバによって VLAN 情報が提供されている。
- 後続のホストが、動作可能な VLAN と一致する VLAN を使用して許可されている。
- 1 つのホストは VLAN の割り当てを持たないポートで認証され、後続のホストは VLAN の割り当てを持たないか、その VLAN 情報が動作可能な VLAN と一致する。

- ポート上で認証された最初のホストはグループ VLAN の割り当てを持ち、後続のホストは VLAN の割り当てを持たないか、そのグループ VLAN がポート上のグループ VLAN と一致する。後続のホストは、VLAN グループの最初のホストと同じ VLAN を使用する必要がある。VLAN リストを使用している場合は、すべてのホストが、その VLAN リストで指定されている条件に従う。
- マルチ認証ポートでは、1 つの音声 VLAN の割り当てだけがサポートされる。
- ポート上のホストに VLAN を割り当てると、後続のホストは、一致する VLAN 情報を持つか、そのポートへのアクセスが拒否される。
- マルチ認証モードでは、ゲスト VLAN や認証失敗 VLAN は設定できない。
- クリティカル認証 VLAN の動作は、マルチ認証モードでは変更されない。ホストが認証を試みたときにサーバに到達できない場合は、設定された VLAN のすべての許可済みホストが再初期化される。

MAC 移動

あるスイッチ ポート上で MAC アドレスが認証されている場合、そのアドレスはスイッチの別の認証マネージャ対応ポート上では許可されません。スイッチが別の認証マネージャ対応ポート上で同一の MAC アドレスを検知すると、そのアドレスは許可されません。

MAC アドレスをあるポートから同一スイッチの別のポートに移動する必要がある場合があります。たとえば、認証されたホストとスイッチポートの間にもう一つのデバイス（ハブや IP 電話など）がある場合、ホストをデバイスから接続解除し、同一スイッチの別のポートに直接接続する場合です。

デバイスが新しいポートで再認証されるように MAC 移動をグローバルにイネーブルにできます。別のポートにホストが移動した場合、1 番めのポート上のセッションは削除され、新しいポート上でホストが再認証されます。

MAC 移動はすべてのホストモードでサポートされます（認証されたホストは、そのポートでイネーブルにされているホストモードにかかわらず、スイッチの任意のポートに移動できます）。

Cisco IOS Release 12.2(55)SE 以降では、ポート セキュリティとともに、MAC 移動をすべてのホストモードで設定できます。

あるポートから別のポートに MAC アドレスを移動すると、元のポート上の認証済みセッションが終了し、新しいポート上で新しい認証シーケンスが開始されます。ポート セキュリティの動作は、MAC 移動を設定している場合でも変わりません。

MAC 移動機能は、音声ホストとデータ ホストの両方に適用されます。

（注）　Open 認証モードでは、MAC アドレスが元のポートから新しいポートにただちに移動されるため、新しいポート上での認証は必要ありません。

詳細については、「MAC 移動のイネーブル化」（P.10-51）を参照してください。

MAC 置換

Cisco IOS Release 12.2(55)SE 以降では、MAC 置換機能を設定して、別のホストによって以前に認証されたポートへの接続をホストが試みたときに発生する違反に対処できます。

（注）　マルチ認証モードでは違反は発生しないため、この機能はマルチ認証モードのポートには適用されません。また、マルチホスト モードでは最初のホストだけに認証が必要になるため、マルチホスト モードのポートにも適用されません。

replace キーワードを使用して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定した場合、マルチドメイン モードのポートでの認証プロセスは次のとおりです。

- 既存の認証済み MAC アドレスを持つポート上で、新しい MAC アドレスが受信されます。
- 認証マネージャが、新しい MAC アドレスを持つポート上の現在のデータ ホストの MAC アドレスを置き換えます。
- 認証マネージャが、その新しい MAC アドレスの認証プロセスを開始します。
- 認証マネージャが、新しいホストは音声ホストであると決定した場合、元の音声ホストは削除されます。

ポートが Open 認証モードである場合は、ただちに新しい MAC アドレスが MAC アドレス テーブルに追加されます。

詳細については、「MAC 置換のイネーブル化」（P.10-52）を参照してください。

802.1X アカウンティング

802.1X 標準では、ユーザのネットワーク 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ています。ただし、ネットワークの使用法についてはトラッキングしません。802.1X アカウンティングは、デフォルトでディセーブルです。802.1X アカウンティングをイネーブルにすると、次のアクティビティを 802.1X 対応のポート上でモニタできます。

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

スイッチは 802.1X アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1X アカウンティング アトリビュート値（AV）ペア

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

AV ペアは、802.1X アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

次の表 10-3 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 10-3　アカウンティング AV ペア

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

1. ホストに対して有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に限り、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

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

802.1X 準備チェック

802.1X 準備チェックは、すべてのスイッチ ポート上で 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続されたデバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。802.1X 機能をサポートしていないデバイスについては、MAC 認証バイパスまたは Web 認証などの認証を変更できます。

この機能は、クライアントのサプリカントが NOTIFY EAP 通知パケットのクエリーをサポートしている場合に限り有効です。クライアントは 802.1X タイムアウト値内に応答する必要があります。

802.1X 準備チェックに関するスイッチ設定の詳細は、「802.1X 準備チェックの設定」（P.10-40）を参照してください。

VLAN 割り当てを使用した 802.1X 認証

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

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されて RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応ポート上でデータ VLAN 割り当てと同じように動作します。詳細については、「マルチドメイン認証」（P.10-14）を参照してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 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、または 802.1X 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN はアクセス ポートに割り当てられた VLAN であることを思い出してください。このポートで送受信されるすべてのパケットはこの VLAN に所属します。
- 802.1X 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。
- 802.1X 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1X ポートでマルチホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1X 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 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 に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします。（アクセス ポートで 802.1X 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID、または VLAN グループ
  - [83] Tunnel-Preference

  アトリビュート [64] は、値 *VLAN*（タイプ 13）でなければなりません。アトリビュート [65] は、値 *802*（タイプ 6）でなければなりません。アトリビュート [81] 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 アトリビュートを使用するスイッチ設定」（P.9-36）を参照してください。

ユーザ単位 ACL を使用した 802.1X 認証の利用

ユーザ単位の Access Control List（ACL; アクセス コントロール リスト）をイネーブルにして、802.1X 認証ユーザに対して異なるレベルのネットワーク アクセスおよびサービスを提供します。RADIUS サーバが 802.1X ポートに接続されたユーザを認証すると、ユーザ ID に基づいて ACL アトリビュートを取得してスイッチに送信します。スイッチは、ユーザ セッションの期間中、そのアトリビュートを 802.1X ポートに適用します。セッションが終了した場合、認証が失敗した場合、またはリンクダウン状態になった場合には、スイッチはユーザ単位の ACL を削除します。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションに保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL の設定およびポート ACL の入力を行うことができます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力済みのルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を避けるために、RADIUS サーバに格納するユーザ プロファイルを慎重に計画します。

RADIUS は、ベンダー固有のアトリビュートなどのユーザ単位アトリビュートをサポートします。これらのベンダー固有のアトリビュート（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#`*n* で、出力方向では `outacl#`*n* です。MAC ACL は、入力方向に限りサポートされます。スイッチは、入力方向に限り VSA をサポートします。このスイッチでは、レイヤ 2 ポートで出力方向のポート ACL はサポートされません。詳細は、第 34 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位の設定を定義します。RADIUS サーバから定義が渡されると、拡張命名規則を使用して作成されます。ただし、Filter-Id アトリビュートを使用する場合、標準 ACL を示すことができます。

Filter-Id アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID アトリビュートは 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してのみサポートされます。

ユーザ単位 ACL の最大サイズは 4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズによって制限されます。

ベンダー固有のアトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」（P.9-36）を参照してください。ACL の設定の詳細については、第 34 章「ACL によるネットワーク セキュリティの設定」を参照してください。

（注） ユーザ単位 ACL は、シングル ホスト モードでだけサポートされます。

ユーザ単位の ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- シングルホスト モードの 802.1X ポートを設定します。

設定の詳細については、「認証マネージャ」（P.10-8）を参照してください。

ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証

ホストの 802.1X 認証または MAC 認証バイパスの間に、RADIUS サーバから ACL とリダイレクト URL をスイッチにダウンロードできます。Web 認証の間にも ACL をダウンロードすることもできます。

（注） ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、ホストがシングルホスト、MDA、またはマルチ認証モードである場合は、スイッチによって ACL の送信元アドレスがホスト IP アドレスに変更されます。

ACL とリダイレクト URL は 802.1X 対応ポートに接続されているすべてのデバイスに適用できます。

802.1X 認証の間に ACL がダウンロードされない場合、スイッチはポート上のスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポート上では、許可ポリシーの一部として、スイッチは電話機だけに ACL を適用します。

Cisco IOS Release 12.2(55)SE 以降では、ポート上にスタティック ACL が存在しない場合は、ダイナミック認証デフォルト ACL が作成され、ポリシーの適用後に、dACL がダウンロードされ、適用されます。

（注）　認証デフォルト ACL は、実行コンフィギュレーションには表示されません。

認証デフォルト ACL は、許可ポリシーを持つホストがポート上で 1 つ以上検出された場合に作成されます。認証デフォルト ACL は、最後に認証されたセッションが終了すると、ポートから削除されます。認証デフォルト ACL を設定するには、**ip access-list extended auth-default-acl** 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。

（注）　認証デフォルト ACL は、シングルホスト モードで Cisco Discovery Protocol（CDP）バイパスをサポートしません。CDP バイパスをサポートするためには、インターフェイス上でスタティック ACL を設定する必要があります。

802.1x 認証および MAB 認証では、*Open* と *Closed* という 2 つの認証モードがサポートされます。*Closed* 認証モードのポート上にスタティック ACL が存在しない場合の動作は次のとおりです。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが適用されるまで、DHCP トラフィックだけを許可します。
- 最初のホストが認証されると、IP アドレスを挿入せずに許可ポリシーが適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、IP アドレスを挿入して最初のセッションおよび後続のセッションのポリシーが適用されます。

Open 認証モードのポート上にスタティック ACL が存在しない場合の動作は次のとおりです。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐため、IP アドレスを挿入してポリシーが適用されます。
- Web 認証は、認証デフォルト ACL-OPEN の影響を受けます。

ディレクティブを設定すると、許可ポリシーを持たないホストのアクセスを制御できます。サポートされているディレクティブの値は *open* および *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブを設定すると、トラフィックはポートによって提供されたアクセスにさらされます。ディレクティブは、AAA サーバまたはスイッチ上にあるユーザ プロファイル内で設定できます。AAA サーバでディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチでディレクティブを設定するには、**epm access-control open** 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。

（注）　ディレクティブのデフォルト値は *default* です。

設定済みの ACL を持たないポート上でホストが Web 認証にフォールバックされた場合の動作は次のとおりです。

- ポートが Open 認証モードである場合は、認証デフォルト ACL-OPEN が作成されます。
- ポートが Closed 認証モードである場合は、認証デフォルト ACL が作成されます。

フォールバック ACL 内の Access Control Entry（ACE; アクセス コントロール エントリ）は、ユーザ単位のエントリに変換されます。設定されたフォールバック プロファイルにフォールバック ACL が含まれない場合、ホストは、ポートに関連する認証デフォルト ACL の影響を受けます。

（注）　Web 認証でカスタム ロゴを使用する場合、カスタム ロゴが外部サーバに格納されているときは、ポート ACL により、認証前に外部サーバへのアクセスを許可する必要があります。その場合は、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更することにより、外部サーバへの適切なアクセスを提供する必要があります。

リダイレクト URL に対する Cisco Secure ACS とアトリビュート値（AV）ペア

スイッチは次の *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP から HTTPS への URL です。
- url-redirect-acl はスイッチ ACL の名前または番号です。

スイッチは、CiscoSecure-Defined-ACL アトリビュート値のペアを使用してエンド ポイント デバイスからの HTTP または HTTPS 要求を代行受信します。その後、スイッチはクライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS 上の url-redirect アトリビュート値のペアには、Web ブラウザのリダイレクト先である URL が含まれます。url-redirect-acl アトリビュート値のペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL 内の許可 ACE に一致するトラフィックがリダイレクトされます。

（注）　スイッチ上の URL リダイレクト ACL とデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバ上のクライアントに対して設定されている場合、接続されたクライアント スイッチ ポート上のデフォルト ポート ACL も設定されている必要があります。

ダウンロード可能な ACL に対する Cisco Secure ACS と AV ペア

RADIUS cisco-av-pair ベンダー固有のアトリビュート（VSA）を使用して Cisco Secure ACS 上の CiscoSecure-Defined-ACL アトリビュート値のペアを設定できます。このペアは、#ACL#-IP-name-number アトリビュートを使用して Cisco Secure ACS 上でダウンロード可能な ACL を指定します。

- *name* は ACL 名です。
- *number* はバージョン番号（たとえば、3f783768）です。

ダウンロード可能な ACL が認証サーバ上のクライアントに対して設定されている場合、接続されたクライアント スイッチ ポート上のデフォルト ポート ACL も設定されている必要があります。

デフォルト ACL がスイッチ上で設定されており、Cisco Secure ACS が host-access-policy をスイッチに送信している場合、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そのポリシーが適用されます。このポリシーが適用されない場合、スイッチはデフォルト ACL を適用します。Cisco Secure ACS がスイッチにダウンロード可能な ACL を送信した場合、この ACL は、スイッチ ポート上で設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信していても、デフォルト ACL が設定されていない場合、許可の失敗が宣言されます。

設定の詳細については、「認証マネージャ」（P.10-8）および「ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定」（P.10-64）を参照してください。

VLAN ID ベースの MAC 認証

ダウンロード可能な VLAN の代わりに、スタティックな VLAN ID に基づいてホストを認証する場合、VLAN ID ベースの MAC 認証を使用できます。スイッチに設定されたスタティック VLAN ポリシーがある場合、認証のために各ホストの MAC アドレスと VLAN 情報が Internet Authentication Service（IAS）（Microsoft）RADIUS サーバに送信されます。接続されたポートに設定された VLAN ID が MAC 認証に使用されます。IAS サーバによる VLAN ID ベースの MAC 認証を使用することで、ネットワーク内に定まった個数の VLAN を所有できます。

この機能は、STP によってモニタされ、処理される VLAN の個数を制限します。ネットワークは固定された VLAN として管理されます。

（注）　この機能は Cisco ACS サーバではサポートされません（ACS サーバは、送信された新しいホストの VLAN-ID を無視し、MAC アドレスだけに基づいて認証します）。

設定手順については、「VLAN ID ベースの MAC 認証の設定」（P.10-67）を参照してください。その他の設定は、「MAC 認証バイパスの設定」（P.10-60）で説明される MAC 認証バイパスと同様です。

ゲスト VLAN を使用した 802.1X 認証

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

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1X ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1X 対応の音声デバイスを許可するときに AAA が使用できない場合、認証は失敗しますが EAPOL パケットの検出は EAPOL 履歴に保存されます。その後 AAA サーバが使用できるようになれば、スイッチはその音声デバイスを認証します。ただし、スイッチは他のデバイスがゲスト VLAN へアクセスすることを許可しなくなります。この状態を回避するには、次のコマンドのいずれかを使用してください。

- **dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続けて **no shutdown** 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、ポートを再起動します。

（注）　インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1X 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1X 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1X 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、802.1X ポート上でシングルホスト モードまたはマルチホスト モードでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

スイッチは、*MAC 認証バイパス*をサポートします。MAC 認証バイパスが 802.1X ポートでイネーブルの場合、スイッチは、802.1X 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1X ポートでクライアントを検出した後、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス / 要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗した場合、ゲスト VLAN が指定されていれば、スイッチはポートをゲスト VLAN に割り当てます。詳細については、「MAC 認証バイパスを使用した 802.1X 認証」（P.10-30）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.10-54）を参照してください。

制限付き VLAN による 802.1X 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 802.1X ポートに対して制限付き VLAN（*認証失敗 VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1X 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効な資格情報を持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注） 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニング ツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることができます。再認証をディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼動しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1X ポート上でシングルホスト モードの場合のみサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポート セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、errdisable ステートに移行します。

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、DHCP スヌーピング、および IP 送信元ガードのような他のポート セキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「制限付き VLAN の設定」（P.10-55）を参照してください。

アクセス不能認証バイパスによる 802.1X 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストが認証されない場合、アクセス不能な認証バイパス機能（*クリティカル認証*または *AAA 失敗ポリシー*ともいう）を使用します。これらのホストを *クリティカル ポート* に接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートへの接続を試みるときは、そのホストはユーザ定義アクセス VLAN *クリティカル VLAN* に移動されます。管理者は制限された認証をホストに与えます。

スイッチがクリティカル ポートに接続されたホストの認証を行う際に、スイッチは設定された RADIUS サーバのステータスを確認します。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースである*クリティカル認証*ステートにします。

マルチ認証ポートに関するサポート

マルチ認証（multiauth）ポートでアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* を使用します。新しいホストがクリティカル ポートに接続する場合、そのポートは再初期化され、接続されているホストはすべてユーザ指定のアクセス VLAN に移動されます。

authentication event server dead action reinitialize *vlan vlan-id* インターフェイス コンフィギュレーション コマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。

- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが改めて利用可能であれば、クリティカル ポートを設定してホストを再初期化し、ホストをクリティカル VLAN の外へ移動できます。これが設定される場合、クリティカル認証ステートのすべてのクリティカル ポートは、自動的に再認証されます。詳細については、このリリースのコマンド リファレンスおよび「アクセス不能認証バイパス機能の設定」（P.10-57）を参照してください。

相互作用機能

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN：アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 802.1X ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN：ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1X アカウンティング：RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）：アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックでは次のとおりです。

- スタック マスターがキープアライブ パケットを送信して RADIUS サーバのステータスを確認します。

  RADIUS サーバのステータスが変化すると、スタック マスターはその情報をスタック メンバーに送信します。これにより、スタック メンバーはクリティカル ポートの再認証の際に RAIDUS サーバのステータスを確認できます。
- 新しいスタック マスターが選ばれると、スイッチ スタックと RADIUS サーバ間のリンクが変更することがあり、新しいスタック マスターは RADIUS サーバのステータスを更新するために、即座にキープアライブ パケットを送信します。

  サーバのステータスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

- スタックにメンバーが追加されると、スタック マスターはそのメンバーにサーバ ステータスを送信します。

音声 VLAN ポートを使用した 802.1X 認証

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

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は 802.1X 認証とは独立して動作できます。

シングルホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチホスト モードでは、サプリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで 802.1X 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

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

シングルホスト モードの 802.1X 対応スイッチ ポートに IP Phone が接続されている場合、スイッチは、それらの電話機を認証せずにネットワーク アクセスを許可します。ポート上でマルチドメイン認証（MDA）を使用して、データ デバイスと音声デバイス（IP Phone など）の両方を認証することを推奨します。

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

音声 VLAN の詳細については、第 15 章「音声 VLAN の設定」を参照してください。

ポート セキュリティを使用した 802.1X 認証

シングルホスト モードまたはマルチホスト モードのどちらでもポート セキュリティを備えた 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があります）。ポートでポート セキュリティおよび 802.1X 認証をイネーブルに設定すると、802.1X 認証はそのポートを認証し、ポート セキュリティはそのクライアントを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、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。

次に、スイッチ上での 802.1X 認証とポート セキュリティ間における相互関係の例を示します。

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

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

  クライアントが認証されてもポート セキュリティ テーブルがいっぱいの場合、セキュリティ違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内でのエントリは他のホストに取って代わられます。

  最初に認証されたホストが原因でセキュリティ違反が発生すると、ポートは errdisable ステートになり、ただちにシャットダウンします。

  セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「セキュリティ違反」（P.25-11）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから 802.1X クライアント アドレスを手動で削除する場合、**dot1x re-authenticate interface** *interface-id* 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、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュア ホスト テーブル内のダイナミック エントリがすべてクリアされます。ここで通常の認証が実行されます。
- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- シングルホスト モードまたはマルチホスト モードのいずれの場合でも、802.1X ポート上でポート セキュリティと音声 VLAN を同時に設定できます。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。
- 新しいデバイスが 802.1X 対応ポートに接続されている場合、または許可されているデバイスの最大数が認証された場合に、ポートがシャットダウン、Syslog エラーの生成、または新しいデバイスからのパケットの廃棄を実行するように **authentication violation** または **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定できます。詳細については、「ポートごとに許可できるデバイスの最大数」（P.10-40）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。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」（P.25-9）を参照してください。

Wake-on-LAN（WoL）機能を使用した 802.1X 認証

802.1X 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1X ポートを通じて接続され、ホストの電源がオフになると、802.1X ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1X 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1X ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注）　PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in または **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 ステートに変わります。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。

authentication control-direction both または **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、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した 802.1X 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 10-2（P.10-5）を参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 802.1X ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1X ポートでクライアントを検出した後、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス / 要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクの存続時間中にインターフェイスで EAPOL パケットが検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであると判断し、インターフェイスを許可するために（MAC 認証バイパスではなく）802.1X 認証を使用します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1X サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS アトリビュート値が DEFAULT であるために前のセッションが終了した場合、スイッチは優先再認証プロセスとして 802.1X 認証を使用します。

MAC 認証バイパスを使用して許可されたクライアントを再認証できます。再認証プロセスは、802.1X を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）に基づいており、Termination-Action RADIUS アトリビュート（アトリビュート [29]）のアクションが *Initialize（初期化）*される場合（アトリビュート値が *DEFALUT*）、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC

認証バイパス機能が 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。AV ペアの詳細については、RFC 3580『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：802.1X ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1X 認証」（P.10-28）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1X 認証」（P.10-28）を参照してください。
- VLAN Membership Policy Server（VMPS）：802.1X および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Admission Control（NAC; ネットワーク アドミッション コントロール）レイヤ 2 IP 検証：この機能は、802.1X ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。

設定の詳細については、「認証マネージャ」（P.10-8）を参照してください。

Cisco IOS Release 12.2(55)SE では、詳細な MAB システム メッセージのフィルタリングをサポートしています。「認証マネージャの CLI コマンド」（P.10-10）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、同一のグループ名を持つユーザを複数の異なる VLAN 間でロード バランスできます。

VLAN は、RADIUS サーバによって提供されるか、または、VLAN グループ名に属するスイッチ CLI によって設定されます。

- ユーザ用の 2 つ以上の VLAN 名を送信するように RADIUS サーバを設定します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1X ユーザ分散は、特定の VLAN のすべてのユーザを追跡し、認証されたユーザを最もユーザ数の少ない VLAN に移動することで、ロード バランシングを達成します。
- ユーザ用の 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。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用することで設定した VLAN グループ名から、選択された VLAN グループ名を検索できます。VLAN グループ名が見つかった場合、最もユーザ数の少ない VLAN を探すために、この VLAN グループ名に属する、対応する VLAN が検索されます。対応する認証されたユーザを該当する VLAN に移動することで、ロード バランシングが達成されます。

（注）　RADIUS サーバは、VLAN ID、VLAN 名、VLAN グループの任意の組み合わせで、VLAN 情報を送信します。

802.1X ユーザ分散設定時の注意事項

- 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。
- 2 つ以上の VLAN を VLAN グループにマップできます。
- VLAN を追加または削除することで VLAN グループを変更できます。
- 既存の VLAN を VLAN グループからクリアした場合、VLAN 内の認証されたポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブな VLAN が VLAN グループにマッピングされているときでも、VLAN グループをクリアできます。VLAN グループをクリアした場合、グループ内の VLAN の認証状態であるポートまたはユーザはクリアされませんが、VLAN グループへのマッピングはクリアされます。

詳細については、「802.1X ユーザ分散の設定」（P.10-61）を参照してください。

NAC レイヤ 2 802.1X 検証

スイッチは NAC レイヤ 2 802.1X 検証をサポートします。これは、デバイス ネットワーク アクセスを許可する前に、エンドポイント システムやクライアントのウイルス対策の状態やポスチャをチェックします。NAC レイヤ 2 802.1X 検証を使用すると、次の作業を実行できます。

- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS アトリビュート（アトリビュート [29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN 番号または名前、または VLAN グループ名のリストを Tunnel Group Private ID（アトリビュート [81]）の値として設定し、VLAN 番号または名前、または VLAN グループ名のプレファレンスを Tunnel Preference（アトリビュート [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（アトリビュート [81]）アトリビュートがリストから選択されます。
- **show authentication** または **show dot1x** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1X 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、802.1X ポートベース認証と似ています。NAC レイヤ 2 802.1X 検証の設定に関する詳細については、「NAC レイヤ 2 802.1X 検証の設定」（P.10-62）および「定期的な再認証の設定」（P.10-47）を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

設定の詳細については、「認証マネージャ」（P.10-8）を参照してください。

柔軟な認証の順序

ポートが新しいホストを認証するために使用する方式の順序を設定する場合に、柔軟な認証の順序を使用できます。MAC 認証バイパスおよび 802.1X はプライマリまたはセカンダリの認証方式にすることができ、Web 認証はこれらのどちらかまたは両方の認証が失敗した場合にフォールバック メソッドにすることができます。詳細については、「認証の順序を柔軟に設定」（P.10-67）を参照してください。

Open1x 認証

Open1x 認証は、デバイスが認証される前にそのデバイスがポートへアクセスすることを許可します。Open 認証が設定されると、ポート上の新しいホストはスイッチにトラフィックだけを送信できます。ホストが認証された後に、RADIUS サーバ上で設定されたポリシーがそのホストに適用されます。

次のシナリオで Open 認証を設定できます。

- Open 認証を使用したシングルホスト モード：認証の前と後で 1 人のユーザのみがネットワークへのアクセスを許可されます。
- Open 認証を使用した MDA モード：音声ドメイン内の 1 人のユーザのみ、およびデータ ドメイン内で 1 人のユーザのみが許可されます。
- Open 認証を使用したマルチホスト モード：任意のホストがネットワークにアクセスできます。
- Open 認証を使用したマルチ認証モード：MDA と同様に、複数のホスト以外を認証できます。

詳細については、「ホスト モードの設定」（P.10-46）を参照してください。

音声認識 802.1X セキュリティの使用

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN にかかわらず、セキュリティ違反が発生した VLAN のみをスイッチの設定でディセーブルにできます。以前のリリースでは、セキュリティ違反を犯したデータ クライアントを認証しようとすると、ポート全体がシャットダウンし、その結果、接続が完全に切られました。

この機能は、PC が IP Phone に接続されている環境で使用できます。データ VLAN でセキュリティ違反が検出されると、そのデータ VLAN のみがシャットダウンされます。音声 VLAN のトラフィックは中断せずに続行します。

音声認識 802.1X セキュリティの設定については、「音声認識 802.1X セキュリティの設定」（P.10-41）を参照してください。

Network Edge Access Topology（NEAT）を使用した 802.1X サプリカント スイッチおよびオーセンティケータ スイッチ

Network Edge Access Topology（NEAT）機能は、（会議室などの）ワイヤリング クローゼットの外側の領域に ID を拡張します。これによって、任意の種類のデバイスがポート上で認証できます。

- 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、別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スイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼットの外側にあり、トランク ポートを通してアップストリーム スイッチに接続されるシナリオで役立ちます。802.1X スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチを使用して認証します。

サプリカント スイッチがポートを正常に認証した後、モードがアクセスからトランクに変更されます。

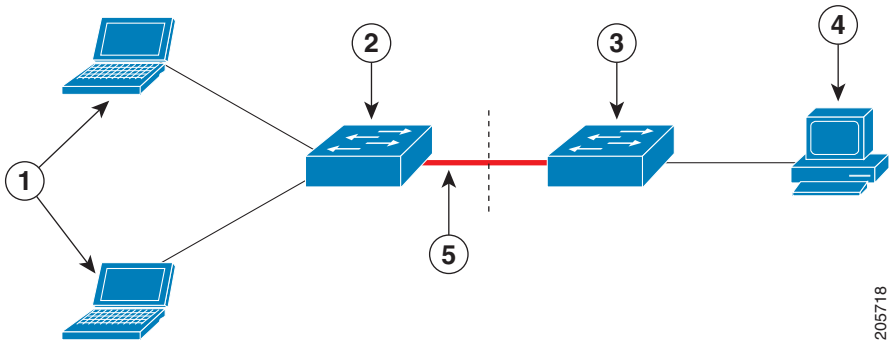
- オーセンティケータ スイッチにアクセス VLAN が設定された場合、認証の正常終了後にトランク ポートのネイティブ VLAN になります。

もう 1 つのサプリカント スイッチに接続しているオーセンティケータ スイッチの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 スイッチのインターフェイスではサポートされません。

サプリカント スイッチで **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを使用して、Network Edge Access Topology（NEAT）をすべてのホストモードで動作させます。

- ホスト許可：確実にネットワーク上で（サプリカントを使用してスイッチに接続している）許可済みのホストからのトラフィックだけが許可されるようにします。スイッチは、Client Information Signalling Protocol（CISP）を使用して、図 10-6 に示すように、サプリカント スイッチにつながる MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル：オーセンティケータ スイッチ上のトランク設定を自動的にイネーブルにし、サプリカント スイッチからの複数の VLAN のユーザ トラフィックを許可します。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します（これは *group* または *user* 設定によって設定できます）。

図 10-6　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 クローゼットの外側）
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		

注意事項

- 他の認証ポートと同一の設定を使用して NEAT ポートを設定できます。サプリカント スイッチが認証する場合、スイッチのベンダー固有のアトリビュート（VSA）に基づいてモードが *アクセスからトランクに*変更されます（device-traffic-class=switch）。
- ネイティブ トランク VLAN に変換される場合は、VSA は、オーセンティケータ スイッチ ポート モードをアクセスからトランクに変更し、802.1X トランク カプセル化およびアクセス VLAN をイネーブルにします。VSA はサプリカントのポート設定を変更しません。

- ホストモードを変更し、かつ、標準ポート設定をオーセンティケータ スイッチ ポートに適用するには、スイッチ VSA の代わりに Auto Smartport ユーザ定義マクロも使用できます。これによって、オーセンティケータ スイッチ ポート上のサポートされない設定を削除でき、ポート モードを *アクセス*から *トランク*に変更できます。これについては、『*AutoSmartports Configuration Guide*』を参照してください。

詳細については、「NEAT を使用したオーセンティケータおよびサプリカント スイッチの設定」（P.10-63）を参照してください。

ACL および RADIUS Filter-Id アトリビュートによる IEEE 802.1X 認証の使用

スイッチは、入力ポートに適用される IP 標準および IP 拡張ポート アクセス コントロール リスト（ACL）をサポートします。

- 管理者が設定した ACL
- Access Control Server（ACS）から入手した ACL

シングル ホスト モードの IEEE 802.1X ポートは、ACS から入手した ACL を使用して、異なるレベルのサービスを IEEE 802.1X 認証済みユーザに提供します。RADIUS サーバは、この種類のユーザとポートを認証し、ユーザ ID に基づいて ACL アトリビュートをスイッチに送信します。スイッチは、ユーザ セッションの期間中、そのアトリビュートをポートに適用します。セッションが終了する、認証が失敗する、または、リンクが失敗すると、ポートは無許可になり、スイッチはポートから ACL を削除します。

ACS から取得した IP 標準 ACL および IP 拡張ポート ACL だけが、Filter-Id アトリビュートをサポートします。Filter-Id アトリビュートは、ACL の名前または番号を指定します。また、Filter-Id アトリビュートは、方向（インバウンドまたはアウトバウンド）およびユーザまたはユーザが所属するグループを指定します。

- ユーザの Filter-Id アトリビュートは、グループの Filter-Id アトリビュートよりも優先されます。
- ACS から入手した Filter-Id アトリビュートが、設定済みの ACL を指定する場合、ユーザ設定の ACL よりも優先されます。
- RADIUS サーバが 2 つ以上の Filter-Id アトリビュートを送信した場合、最後のアトリビュートが適用されます。

Filter-Id アトリビュートがスイッチで定義されていない場合、認証は失敗し、ポートは無許可ステートに戻ります。

共通セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。この ID は、show コマンドや Management Information Base（MIB; 管理情報ベース）など、すべてのレポーティング用途に使用されます。セッション ID はセッション単位の syslog メッセージのすべてと共に表示されます。

セッション ID には次が含まれています。

- Network Access Device（NAD）の IP アドレス
- 単調増加する、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）

次に、**show authentication** コマンドの出力にセッション ID が表示される例を示します。次の例のセッション 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
```

次に、syslog 出力にセッション ID が表示される例を示します。次の例のセッション 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
```

セッション ID は NAD、AAA サーバ、およびその他のレポート分析アプリケーションによってクライアントの特定に使用されます。ID は自動的に表示されます。設定は必要ありません。

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。

- 「NAC レイヤ 2 802.1X 検証の設定」（P.10-62）（任意）
- 「NEAT を使用したオーセンティケータおよびサプリカント スイッチの設定」（P.10-63）
- 「ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定」（P.10-64）
- 「認証の順序を柔軟に設定」（P.10-67）
- 「ポート上での 802.1X 認証のディセーブル化」（P.10-69）（任意）
- 「802.1X 認証設定のデフォルト値へのリセット」（P.10-69）（任意）

802.1X 認証のデフォルト設定

表 10-4 に、802.1X 認証のデフォルト設定を示します。

表 10-4　802.1X 認証のデフォルト設定

機能	デフォルト設定
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。
Authentication、Authorization、Accounting（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。
ホスト モード	シングルホスト モード。
制御方向	双方向制御。
定期的な再認証	ディセーブル。
再認証の間隔（秒）	3600 秒。
再認証回数	2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）。
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数）。
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）。
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）。
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）。
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間）。 タイムアウト期間は、**authentication timer server** または **dot1x timeout server-timeout** インターフェイス コンフィギュレーション コマンドを使用して変更できます。

表 10-4　802.1X 認証のデフォルト設定 （続き）

機能	デフォルト設定
無活動タイムアウト	ディセーブル。
ゲスト VLAN	指定なし。
アクセス不能認証バイパス	ディセーブル。
制限付き VLAN	指定なし。
オーセンティケータ（スイッチ）モード	指定なし。
MAC 認証バイパス	ディセーブル。
音声認識セキュリティ	ディセーブル。

802.1X 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1X 認証」（P.10-38）
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」（P.10-39）
- 「MAC 認証バイパス」（P.10-40）
- 「ポートごとに許可できるデバイスの最大数」（P.10-40）

802.1X 認証

- 802.1X 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1X 対応ポートを（たとえばアクセスからトランクに）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。
- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1X ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 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、音声 VLAN 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 ポート上で 802.1X 認証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 認証はイネーブルになりません。802.1X 対応ポートをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック ポート ：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証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 認証はイネーブルになりません。802.1X 対応ポートをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート ：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1X 認証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 認証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 ：EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにするポートを 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 認証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 認証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; リモート SPAN）宛先ポート ：SPAN または RSPAN 宛先ポートであるポート上で 802.1X 認証をイネーブルにできます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1X 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは、802.1X 認証をイネーブルにできます。

- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1X 認証をグローバルにイネーブルにする前に、802.1X 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降では、802.1x 認証に関連するシステム メッセージのフィルタリングをサポートしています。「認証マネージャの CLI コマンド」（P.10-10）を参照してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1X 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。
- 802.1X 認証をプライベート VLAN ポートに設定できますが、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた 802.1X 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。
- Dynamic Host Configuration Protocol（DHCP）クライアントが接続する 802.1X ポートにゲスト VLAN を設定した後は、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の 802.1X 認証プロセスを再開するための設定を変更することもできます。802.1X 認証プロセスの設定を減らしてください（**authentication timer inactivity** または **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、および **authentication timer reauthentication** または **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド）。設定を減らす量は、接続している 802.1X クライアント タイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングルホスト モードおよびマルチホスト モードの 802.1X ポートでサポートされます。
  - Windows XP を稼動しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントに DHCP が設定されていて、DHCP サーバからの IP アドレスを持つ場合、クリティカル ポート上で EAP 成功メッセージを受信すると、DHCP 設定プロセスが再始動しない場合があります。
  - 802.1X ポート上では、アクセス不能認証バイパス機能および制限付き VLAN を設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。

  - 同じスイッチ ポート上にアクセス不能バイパス機能とポート セキュリティを設定できます。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

MAC 認証バイパス

- 特に明記していない限り、MAC 認証バイパスの注意事項は 802.1X 認証のものと同じです。詳細については、「802.1X 認証」（P.10-38）を参照してください。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが無許可ステートでクライアント MAC アドレスが認証サーバ データベースにない場合、ポートは無許可ステートのままになります。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再認証できます。
- ポートが許可ステートである場合、再認証が発生するまでポートのステートは変わりません。
- MAC 認証バイパスに接続されているものの非アクティブのホストのタイムアウト期間を設定することができます。範囲は 1 ～ 65535 秒です。タイムアウト値を設定する前にポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.25-9）を参照してください。

ポートごとに許可できるデバイスの最大数

802.1X 対応ポートで許可できるデバイスの最大数は、次のとおりです。

- シングルホスト モードでは、1 つのデバイスだけがアクセス VLAN で許可されます。ポートも音声 VLAN で設定されていた場合、音声 VLAN で送受信される Cisco IP Phone は無制限です。
- MultiDomain Authentication（MDA）モードでは、1 つのデバイスだけがアクセス VLAN に許可されます。また、1 つの IP Phone が音声 VLAN に許可されます。
- マルチホスト モードでは、1 つの 802.1X サプリカントだけがポートで許可されます。ただし、非 802.1X ホストはアクセス VLAN で無制限に許可されます。また、デバイスも音声 VLAN で無制限に許可されます。

802.1X 準備チェックの設定

802.1X 準備チェックは、すべてのスイッチ ポート上で 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続されたデバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。

802.1X 準備チェックは、802.1X を設定できるすべてのポートに許可されています。**dot1x force-unauthorized** として設定されているポートでは使用できません。

スイッチで準備チェックをイネーブルにするには、次の事項に注意してください。

- 通常、準備チェックは 802.1X がスイッチでイネーブルになる前に使用します。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用している場合、スイッチ スタックのすべてのポートがテストされます。
- 802.1X 対応のポートに **dot1x test eapol-capable** コマンドを設定してリンクをアップした場合、ポートは 802.1X 機能に関して接続クライアントにクエリーを送信します。クライアントが通知パケットに応答した場合、802.1X に対応していることになります。クライアントがタイムアウト期

間内に応答した場合、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かった場合、そのクライアントは 802.1X に対応していません。そのため、Syslog メッセージも生成されません。

- 準備チェックは、複数のホストを扱うポートにも送信できます（例：IP Phone に接続した PC）。準備チェックに対してタイムアウト期間内に応答したクライアントごとに Syslog メッセージが生成されます。

スイッチ上で 802.1X 準備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 準備チェックをイネーブルにします。 （任意）*interface-id* には、802.1X 準備チェックを行うポートを指定します。 **（注）** **interface** キーワードを省略した場合、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 応答を待機するタイムアウト時間を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 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。

次に、ポートにクエリーを実行するスイッチ上で準備チェックをイネーブルにする方法を示します。また、クエリーを送信したポートから受信した応答も示します。これにより、接続したデバイスが 802.1X に対応しているかどうか確認できます。

```
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
```

音声認識 802.1X セキュリティの設定

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN にかかわらず、セキュリティ違反が発生した VLAN だけをスイッチでディセーブルにできます。この機能は、PC が IP Phone に接続されている IP Phone 環境に役立ちます。データ VLAN でセキュリティ違反が検出されてもシャットダウン対象はそのデータ VLAN だけです。音声 VLAN のトラフィックは中断せずにスイッチを通過できます。

スイッチに音声認識 802.1X セキュリティを設定する場合、次の注意事項に従ってください。

- 音声認識 802.1X セキュリティは、**errdisable detect cause security-violation shutdown vlan** 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イネーブルにします。音声認識 802.1X セキュリティをディセーブルにする場合は、このコマンドの **no** バージョンを使用します。このコマンドはスイッチで 802.1X を設定したすべてのポートに適用されます。

（注） **shutdown vlan** キーワードを指定しない場合、errdisable ステートになった際にポート全体がシャットダウンします。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して errdisabled 回復を設定した場合、ポートは自動的に再度イネーブルになります。errdisable 回復がポートに設定されていない場合、**shutdown** および **no-shutdown** 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、もう一度イネーブルにします。
- **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用すれば、VLAN ごとに再度イネーブルにできます。範囲を指定しない場合、ポート上のすべての VLAN がイネーブルになります。

音声認識 802.1X セキュリティ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	**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	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反が発生したすべての VLAN をシャットダウンします。 （注）　**shutdown vlan** キーワードを指定しない場合、ポート全体が errdisable ステートになり、シャットダウンします。
ステップ 3	**errdisable recovery cause security-violation**	（任意）VLAN ごとの自動エラー回復をイネーブルにします。
ステップ 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	（任意）errdisable ステートの個々の VLAN を再度イネーブルにします。 • *interface-id* には、再度イネーブルにする各 VLAN ポートを指定します。 • （任意）*vlan-list* には、再度イネーブルにする VLAN のリストを指定します。*vlan-list* が指定されていない場合、すべての VLAN が再度イネーブルになります。
ステップ 5	**shutdown** **no-shutdown**	（任意）errdisable ステートの VLAN を再度イネーブルにし、すべての errdisable 状態を回復します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	設定を確認します。
ステップ 8	**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、セキュリティ違反が発生したすべての VLAN をシャットダウンするようにスイッチを設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート Gigabit Ethernet 4/0/2 で errdisable ステートだったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2 vlan
```

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

802.1X 違反モードの設定

802.1X ポートを設定することで、シャットダウン、Syslog エラーの生成、または新規デバイスからのパケットの廃棄を実行できます。実行するための条件は次のとおりです。

- デバイスが 802.1X 対応ポートに接続されている
- 許可するデバイスの最大数がポートで認証された

スイッチ上にセキュリティ違反アクションを設定するには、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*指定されていない*場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。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、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 （注）　**group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**interface** *interface-id*	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードにします。
ステップ 6	**authentication violation shutdown** | **restrict** | **protect** | **replace**} または **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 errdisable ステートにします。 • **restrict**：Syslog エラーを生成します。 • **protect**：そのポートへトラフィックを送信する新規デバイスからのパケットをドロップします。 • **replace**：現在のセッションを削除し、新しいホストを使用して認証します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** または **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 ポートベース認証を設定するには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

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

次に、802.1X の AAA プロセスを示します。

ステップ 1　ユーザがスイッチのポートに接続します。

ステップ 2　認証が実行されます。

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

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

ステップ 5　必要に応じて、再認証が実行されます。

ステップ 6　スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。

ステップ 7　ユーザがポートから切断します。

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

802.1X ポートベース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*指定されていない*場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。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、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 **（注）** **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**dot1x system-auth-control**	スイッチ上で 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）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定がデフォルトです。
ステップ 6	**radius-server host** *ip-address*	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string*	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
ステップ 8	**interface** *interface-id*	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode access**	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** または **dot1x port-control auto**	ポート上で 802.1X 認証をイネーブルにします。 機能の相互作用については、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show authentication** または **show dot1x**	設定を確認します。
ステップ 13	**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。

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、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。デフォルト値は 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 サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵はテキスト ストリングで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。 **（注）** 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず **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。鍵でスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵と一致している必要があります。 複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。
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 サーバをクリアするには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号鍵を RADIUS サーバ上の鍵と同じ *rad123* に設定する例を示します。

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

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」（P.9-36）を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

802.1X 認証済みポート上でシングル ホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。**multi-domain** キーワードを使用して MDA を設定して、ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を、同一スイッチ ポートで認証することができます。

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	**radius-server vsa send authentication**	ベンダー固有のアトリビュート（VSA）を認識し使用するために、ネットワーク アクセス サーバを設定します。
ステップ 3	**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。
ステップ 4	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] または **dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN 上では 1 つのクライアントを、データ VLAN 上では複数の認証されたクライアントを許可します。各ホストは別々に認証されます。 （注）　**multi-auth** のキーワードを使用できるのは、**authentication host-mode** コマンドの場合だけです。 • **multi-host**：シングル ホストの認証後に 802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 • **multidomain**：ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を 1 つの 802.1X 認証済みポートで認証することができます。 （注）　ホスト モードが **multi-domain** に設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 15 章「音声 VLAN の設定」を参照してください。 • **single-host**：802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 指定するインターフェイスで、**authentication port-control** または **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
ステップ 5	**switchport voice vlan** *vlan-id*	（任意）音声 VLAN を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**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。

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** または **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 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

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

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

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、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、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	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。

	コマンド	目的
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate**]} {**restart** ***value***}} または **dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 **authentication timer** のキーワードの意味は次のとおりです。 • **inactivity**：クライアントからアクティビティがない場合、そのクライアントが無許可になるまでの間隔（秒） • **reauthenticate**：自動再認証の試行が開始されるまでの時間（秒） • **restart *value***：無許可ポートを認証する試行が実行されるまでの間隔（秒） **dot1x timeout reauth-period** のキーワードの意味は次のとおりです。 • *seconds*：秒数を 1 ～ 65535 の範囲で設定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **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 authentication periodic** または **no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。再認証の間隔をデフォルトの秒数に戻すには、**no authentication timer** または **no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

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

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

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface *interface-id* 特権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「定期的な再認証の設定」（P.10-47）を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet2/0/1
```

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。クライアントが無効なパスワードを提示した場合、クライアントの認証に失敗する場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、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 quiet-period** *seconds*	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **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。

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

次に、スイッチの待機時間を 30 秒に設定する例を示します。

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

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。

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

スイッチがクライアントからの通知を待機する時間を変更するには、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 tx-period** *seconds*	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 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 authentication** *interface-id* または **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。

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

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

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

スイッチからクライアントへのフレーム再送信回数の設定

（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

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

スイッチからクライアントへのフレーム再送信回数を設定するには、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起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **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。

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

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 5 に設定する例を示します。

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

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

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

再認証回数を設定するには、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*	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **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。

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

次に、ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数として 4 を設定する例を示します。

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

MAC 移動のイネーブル化

MAC 移動はスイッチ上のあるポートから別のポートへの認証されたホストの移動を許可します。

スイッチで MAC 移動をグローバルに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。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	**authentication mac-move permit**	スイッチ上で MAC 移動をイネーブルにします。
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**	（任意）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。

次の例では、スイッチで MAC 移動をグローバルにイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストは、ポート上の認証済みホストを置き換えることができます。

インターフェイス上で MAC 置換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。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	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}	インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。現在のセッションを削除し、新しいホストを使用して認証を開始します。 その他のキーワードの意味は次のとおりです。 • **protect**：予期しない MAC アドレスを持つパケットをドロップします。システム メッセージは生成されません。 • **restrict**：違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown**：予期しない MAC アドレスを受信すると、ポートは errdisable になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	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。

次の例では、インターフェイス上で MAC 置換をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# authentication violation replace
```

802.1X アカウンティングの設定

802.1X アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム 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。サーバは、アクティブな 802.1X セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

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

このストップ 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） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、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。
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）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 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、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

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

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1X 対応でないクライアントはゲスト VLAN に配置されます。802.1X 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングルホスト モードまたはマルチホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5	**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。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**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。

ゲスト VLAN をディセーブルにして削除するには、**no dot1x guest-vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間（秒）を 15 に設定し、802.1X ポートの DHCP クライアント接続時に、VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定すると、認証サーバが有効なユーザ名またはパスワードを受信できない場合、802.1X に準拠したクライアントは制限付き VLAN に移されます。スイッチは、シングルホスト モードに限り制限付き VLAN をサポートします。

制限付き VLAN 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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 8	**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。

制限付き VLAN をディセーブルにして削除するには、**no dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、*VLAN 2* を 802.1X 制限付き VLAN としてイネーブルにする例を示します。

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

ユーザに制限付き VLAN を割り当てる前に、**dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ～ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6	**dot1x auth-fail max-attempts** *max attempts*	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 で、デフォルトは 3 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）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。

設定数をデフォルトに戻すには、**no dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートを制限付き VLAN にするために、認証試行回数を *2* に設定する方法を示します。

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

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）を設定できます。

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、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	**radius-server dead-criteria time** *time* **tries** *tries*	（任意）RADIUS サーバが使用できない、または *dead* と見なされるときを判別するのに使われる条件を設定します。 指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 3	**radius-server deadtime** *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。
ステップ 4	**radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	（任意）次のキーワードを使用して RADIUS サーバ パラメータを設定します。 • **acct-port** *udp-port* : RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1646 です。 • **auth-port** *udp-port* : RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1645 です。 **（注）** RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **test username** *name* : RADIUS サーバ ステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • **idle-time** *time* : スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port** : RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • **ignore-auth-port** : RADIUS サーバ認証ポートのテストをディセーブルにします。 • **key** *string* : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号鍵を指定します。 **（注）** 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず **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。鍵でスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵と一致している必要があります。 **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号鍵を設定できます。

	コマンド	目的
ステップ 5	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}	（任意）アクセス不能認証バイパスのパラメータを設定します。 **eapol**：スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 **recovery delay** *milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。
ステップ 6	**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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 7	**authentication event server dead action [authorize | reinitialize] vlan** *vlan-id*	RADIUS サーバが到達不能である場合、これらのキーワードを使用してポート上のホストを移動します。 • **authorize**：認証を試みる新しいホストをユーザ指定のクリティカル VLAN に移動します。 • **reinitialize**：ポートのすべての認証済みホストをユーザ指定のクリティカル VLAN に移動します。
ステップ 8	**dot1x critical** [**recovery action reinitialize** | **vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。 • **recovery action reinitialize**：回復機能をイネーブルにして、認証サーバが使用可能なとき、回復動作中にポートを認証するように指定します。 • **vlan** *vlan-id*：スイッチがクリティカル ポートに割り当てるアクセス VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 11	**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。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical** {**eapol** | **recovery delay**} 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。アクセス不能認証バイパスをディセーブルにするには、**no 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。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet1/0/2
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
```

```
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1X 認証の設定

WoL を使用した 802.1X 認証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。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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 3	**authentication control-direction {both | in}** または **dot1x control-direction {both | in}**	ポートで WoL を使用して 802.1X 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストとの間でパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単方向に設定します。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **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。

WoL を使用して 802.1X 認証をディセーブルにするには、**no authentication control-direction** または **no dot1x control-direction** 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、WoL を使用した 802.1X 認証をイネーブルにして、ポートを双方向に設定する例を示します。

```
Switch(config-if)# authentication control-direction both
```

または

```
Switch(config-if)# dot1x control-direction both
```

MAC 認証バイパスの設定

MAC 認証バイパス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。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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.10-38）を参照してください。
ステップ 3	**authentication port-control auto** または **dot1x port-control auto**	ポート上で 802.1X 認証をイネーブルにします。
ステップ 4	**dot1x mac-auth-bypass** [**eap** | **timeout activity** {*value*}]	MAC 認証バイパスをイネーブルにします。 （任意）**eap** キーワードを使用して認証用の EAP を使用するようにスイッチを設定します。 （任意）**timeout activity** キーワードを使用して、未認証ステートに移行する前に接続されているホストを非アクティブにすることのできる秒数を設定します。指定できる範囲は 1 ～ 65535 です。 タイムアウト値を設定する前にポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.25-9）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **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。

MAC 認証バイパスをディセーブルにするには、**no dot1x mac-auth-bypass** 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、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Switch(config-if)# dot1x mac-auth-bypass
```

802.1X ユーザ分散の設定

VLAN グループを設定し、VLAN を VLAN グループにマッピングするには特権 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	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定し、単一の VLAN または VLAN 範囲を VLAN 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クリアします。

次の例では、VLAN グループを設定し、VLAN をグループにマッピングし、VLAN グループ設定および指定された VLAN への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 を既存のグループに追加し、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
```

次に、すべての VLAN が VLAN グループから削除され、VLAN グループがクリアされる例を示します。

```
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 グループをクリア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。

NAC レイヤ 2 802.1X 検証の設定

NAC レイヤ 2 802.1X 検証を設定できます。これは、RADIUS サーバを使用した 802.1X 認証とも呼ばれます。

NAC レイヤ 2 802.1X 検証を設定するには、特権 EXEC モードで次の手順を実行します。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 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。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 4	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 キーワードの意味は次のとおりです。 • *seconds*：1 ～ 65535 の秒数を設定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	802.1X 認証の設定を確認します。
ステップ 8	**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、NAC レイヤ 2 802.1X 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

NEAT 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 クローゼット外の 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 スイッチに接続している必要があります。

概要については、「Network Edge Access Topology（NEAT）を使用した 802.1X サプリカント スイッチおよびオーセンティケータ スイッチ」（P.10-33）を参照してください。

（注）　*cisco-av-pairs* 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、インターフェイスは、サプリカントの認証が成功した後に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**	ポートを**アクセス** モードにします。
ステップ 5	**authentication port-control auto**	port-authentication モードを auto に設定します。
ステップ 6	**dot1x pae authenticator**	Port Access Entity（PAE; ポート アクセス エンティティ）オーセンティケータとしてインターフェイスを設定します。
ステップ 7	**spanning-tree portfast**	単一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 ポート上で 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。

次に、スイッチを 802.1X オーセンティケータとして設定する例を示します。

```
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*	Create 802.1X 資格情報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るポートに適用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。

	コマンド	目的
ステップ 5	**password** *password*	新しいユーザ名用のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	強制的に、スイッチがユニキャスト パケットまたはマルチキャスト パケットのいずれかを受信したときにマルチキャスト EAPOL パケット*だけ*を送信するように設定します。 これによって、NEAT はサプリカント スイッチ上ですべてのホスト モードで動作できます。
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**	Port Access Entity（PAE; ポート アクセス エンティティ）サプリカントとしてインターフェイスを設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1X 資格情報プロファイルをインターフェイスに適用します。
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。

次に、スイッチをサプリカントとして設定する例を示します。

```
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
```

Auto Smartport マクロによる NEAT の設定

スイッチ VSA の代わりに Auto Smartport 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できます。これについては、『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定

スイッチ上で 802.1X 認証を設定するほかに、ACS を設定する必要があります。詳細については、『Cisco Secure ACS configuration guides』を参照してください。

（注）　ACS をスイッチにダウンロードする前に、ダウンロード可能な ACL をスイッチ上で設定する必要があります。

ポート上での認証の後、**show ip access-list** 特権 EXEC コマンドを使用して、ダウンロードされた ACL をポート上で表示できます。

ダウンロード可能な ACL の設定

クライアント認証が終了して、IP デバイス トラッキング テーブルにクライアント IP アドレスが追加されると、ポリシーが有効になります。そしてスイッチはダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで実行します。

	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	**ip device tracking**	IP デバイス トラッキング テーブルを設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default group radius**	認証方法を local に設定します。認証方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication**	radius vsa send authentication を設定します。
ステップ 6	**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 7	**ip access-group** *acl-id* **in**	ポート上でデフォルトの ACL を入力方向に設定します。 （注）　*acl-id* は、アクセス リスト名または番号です。
ステップ 8	**show running-config interface** *interface-id*	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。

ダウンロード ポリシーの設定

特権 EXEC モードで実行します。

	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	**access-list** *access-list-number* **deny source** *source-wildcard* **log**	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 access-list-number は、1 ～ 99 または 1300 ～ 1999 の 10 進数です。 **deny** または **permit** を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。 *source* は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 • ドット付き 10 進表記で 32 ビットの値。 • 0.0.0.0 255.255.255.255 という source および source-wildcard 値の省略形を表すキーワード any。source-wildcard 値の入力は不要です。 • source 0.0.0.0 という source および source-wildcard の省略形を表すキーワード host。 （任意）source-wildcard によって、ワイルドカード ビットが source に適用されます。 （任意）log を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	**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	**ip access-group** *acl-id* **in**	ポート上でデフォルトの ACL を入力方向に設定します。 **（注）**　*acl-id* は、アクセス リスト名または番号です。
ステップ 5	**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	**aaa new-model**	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius**	認証方法を local に設定します。認証方法を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**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	**ip device tracking probe** [**count** | **interval** | **use-svi**]	（任意）IP デバイス トラッキング テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信する前に応答を待機する秒数を設定します。指定できる範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。 • **use-svi**：Switch Virtual Intertface（SVI; スイッチ仮想インターフェイス）の IP アドレスを ARP の送信元として使用します。
ステップ 10	**radius-server vsa send authentication**	ベンダー固有のアトリビュートを認識し使用するために、ネットワーク アクセス サーバを設定します。 **（注）**　ダウンロード可能な ACL は動作している必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	**show ip device tracking all**	IP デバイス トラッキング テーブルのエントリについての情報を表示します。
ステップ 13	**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 ポリシー用のスイッチ設定の例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
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)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベースの MAC 認証の設定

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	**mab request format attribute 32 vlan access-vlan**	VLAN ID ベースの MAC 認証をイネーブルにします。
ステップ 3	**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。

VLAN ID ベースの MAC 認証の状態を確認する show コマンドはありません。**debug radius accounting** 特権 EXEC コマンドを使用して RADIUS アトリビュート 32 を確認してください。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次の例では、スイッチで VLAN ID ベースの MAC 認証をグローバルにイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

認証の順序を柔軟に設定

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	**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	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順番を設定します。
ステップ 4	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	（任意）port-priority リストに認証方式を追加します。
ステップ 5	**show authentication**	（任意）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。

次に、ポートが最初に 802.1X 認証を試行し、次にフォールバック メソッドとして Web 認証を試行する設定方法の例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config)# authentication order dot1x webauth
```

Open1x の設定

特権 EXEC モードで実行します。

	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	**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	**authentication control-direction** {**both** | in}	（任意）ポート コントロールを単方向または双方向に設定します。
ステップ 4	**authentication fallback** ***name***	（任意）802.1X 認証をサポートしていないクライアント用に、ポートが Web 認証をフォールバック メソッドとして使用するように設定します。
ステップ 5	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	（任意）ポート上で認証マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順番を設定します。
ステップ 8	**authentication periodic**	（任意）ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}	（任意）ポートの許可ステートの手動制御をイネーブルにします。
ステップ 10	**show authentication**	（任意）設定を確認します。
ステップ 11	**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、ポート上で open 1X を設定する例を示します。

```
Switch# configure terminal
```

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポート上での 802.1X 認証のディセーブル化

802.1X 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1X 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。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	**no dot1x pae**	ポート上で 802.1X 認証をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **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 Port Access Entity（PAE; ポート アクセス エンティティ）オーセンティケータとしてポートを設定するには、**dot1x pae authenticator** 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。この設定では、ポートで 802.1X がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次に、802.1X 認証をポートでディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no dot1x pae authenticator
```

802.1X 認証設定のデフォルト値へのリセット

802.1X 認証設定をデフォルト値に戻すには、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**	802.1X パラメータをデフォルト値に戻します。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **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 の統計情報およびステータスの表示

すべてのポートに関する 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。特定のポートに関する 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。

スイッチに関する 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** | **statistics** | **summary**] 特権 EXEC コマンドを使用します。特定のポートに関する 802.1X 管理および動作ステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

Cisco IOS Release 12.2(55)SE 以降では、**no dot1x logging verbose** グローバル コンフィギュレーション コマンドを使用して詳細な 802.1x 認証メッセージをフィルタリングできます。「認証マネージャの CLI コマンド」（P.10-10）を参照してください。

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