CHAPTER 11

IEEE 802.1x ポートベース認証の設定

この章では、Catalyst 3750-X または 3560-X スイッチで IEEE 802.1x ポートベース認証を設定する方法について説明します。IEEE 802.1x 認証は、無許可デバイス（クライアント）がネットワークにアクセスするのを防ぎます。特に明記しない限り、*スイッチ*という用語は、Catalyst 3750-X または 3560-X スタンドアロン スイッチおよび Catalyst 3750-X スイッチ スタックを意味します。

IP ベース フィーチャ セットまたは IP サービス フィーチャ セットが稼動するスイッチでは、Cisco TrustSec の Security Group Tag（SGT）Exchange Protocol（SxP）もサポートされます。この機能では、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。これは IP アドレスではなく、デバイスのグループに対する ACL ポリシーを定義します。SXP 制御プロトコルでは、アクセス レイヤ デバイスにパケットにタグを付けるためのハードウェア機能がない場合に、Cisco TrustSec ドメインのエッジのアクセス レイヤ デバイス、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 SGT 情報を伝送できます。これらのスイッチは Cisco TrustSec ネットワーク内のアクセス 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 で『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 のセクションでは、スイッチでサポートされる機能を定義します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応する『*Cisco IOS Security Command Reference, Release 12.2*』の「RADIUS Commands」およびコマンド リファレンスを参照してください。

IEEE 802.1x ポートベース認証の概要

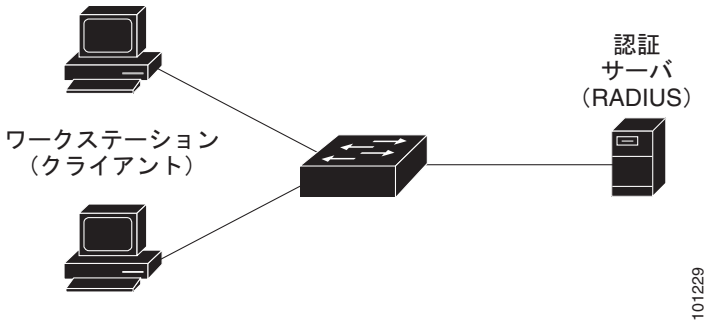
802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

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; シスコ検出プロトコル）、および Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックしか許可されません。認証に成功すると、通常のトラフィックをポート経由で送受信できます。

デバイスの役割

802.1x ポートベース認証では、ネットワーク上のデバイスにはそれぞれ固有の役割があります（図 11-1 を参照）。

図 11-1　802.1x 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 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 認証の問題を解決するには、次の URL にあるマイクロソフト サポート技術情報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透過的に行われます。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*といいます）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われないため、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-X、Catalyst 3750-E、Catalyst 3750、Catalyst 3650-X、Catalyst 3560-E、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ、または無線アクセス 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 IEEE 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。

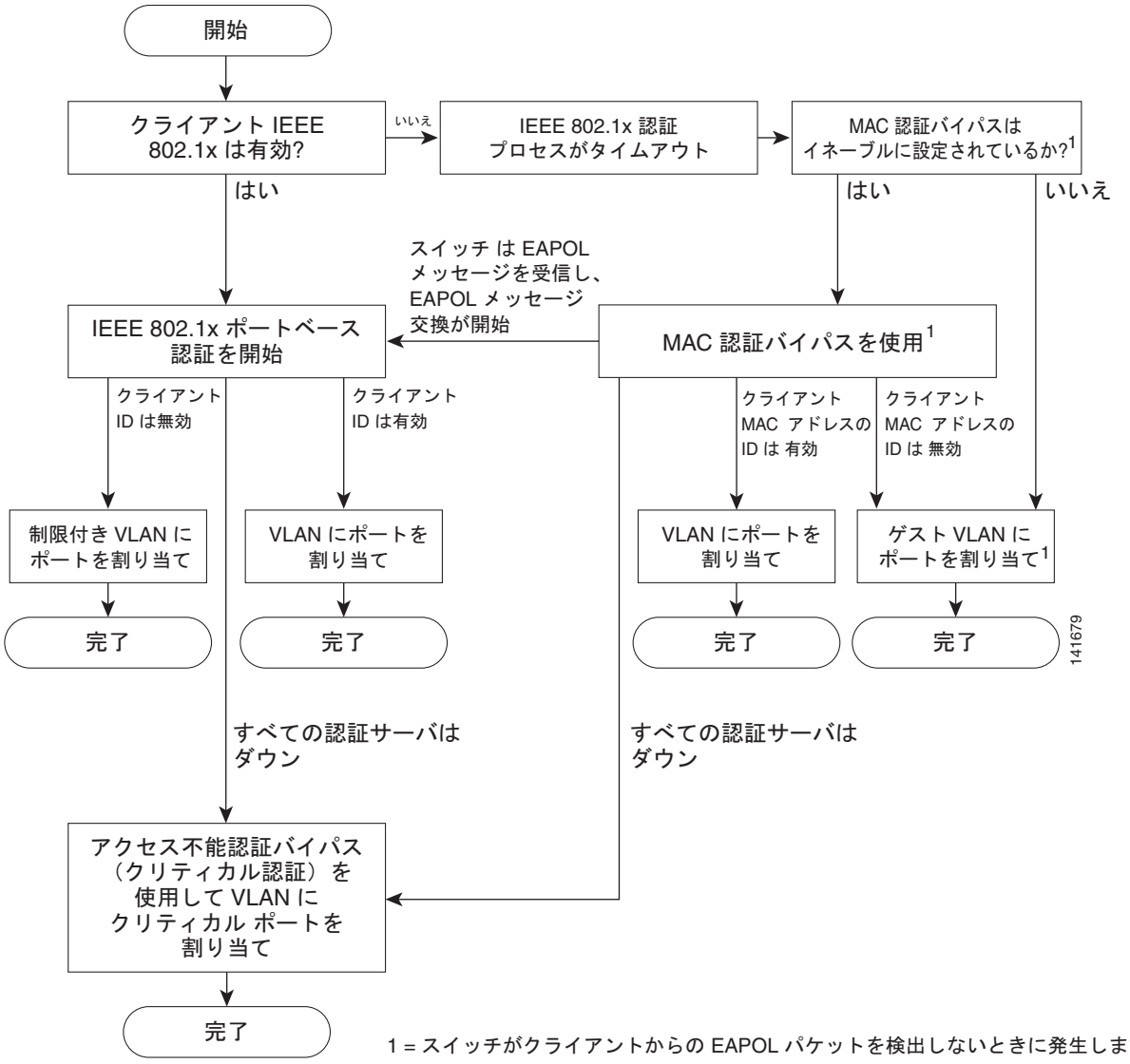
- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN 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、認可、アカウンティング）失敗ポリシーとも呼ばれます。

図 11-2 に、認証プロセスを示します。

ポートで Multi Domain Authentication（MDA）がイネーブルになっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。MDA の詳細については、「MDA」（P.11-30）を参照してください。

図 11-2　認証フローチャート



1 = スイッチがクライアントからの EAPOL パケットを検出しないときに発生します。

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 認証を設定したあと、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* または *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。

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かぎり定期的に、認証を開始しなければなりません。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

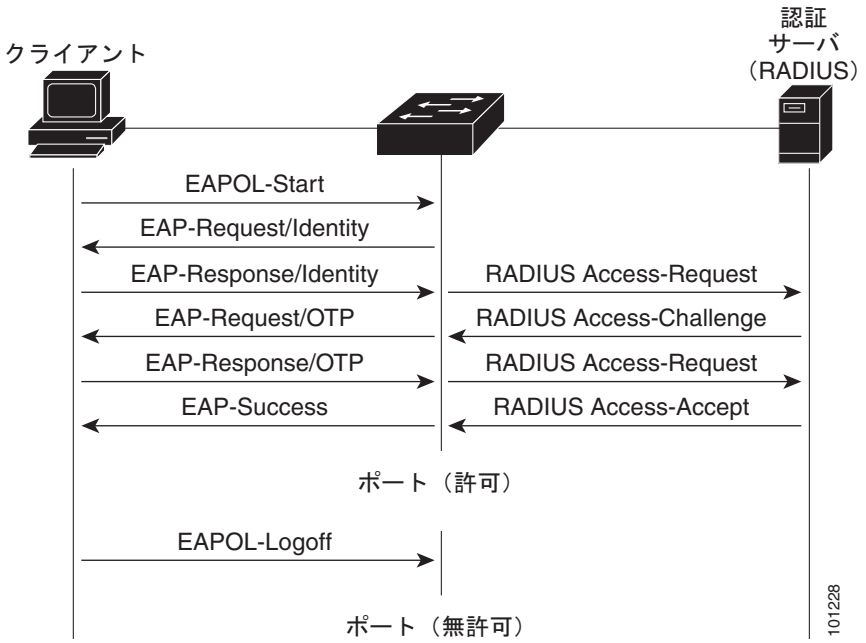
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注） ネットワーク アクセス 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 フレームはすべてドロップされます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが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.11-10）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.11-10）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 11-3 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場合に行われるメッセージ交換を示します。

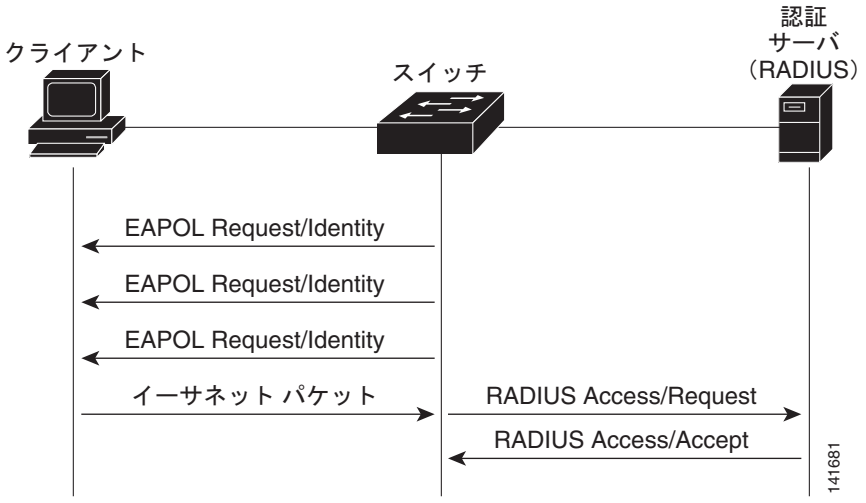
図 11-3　メッセージ交換



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-Access/Request 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-Access/Accept 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、802.1x 認証を停止します。

図 11-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 11-4　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、および、Catalyst 6000 のようなネットワーク デバイス上でも、CLI コマンドおよびメッセージを含み、同じ認証方式は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がサポートされています。

Cisco IOS Release 12.2(55)SE は、認証マネージャからの冗長なシステム メッセージのフィルタリングをサポートします。詳細については、「認証マネージャ CLI コマンド」（P.11-9）を参照してください。

ポートベース認証方式

表 11-1　802.1x 機能

	モード			
認証方式	**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 ACL[3] リダイレクト URL[2]	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL[2] Filter-Id アトリビュート [2] ダウンロード可能 ACL[2] リダイレクト URL[2]	ユーザ単位 ACL[2] Filter-Id アトリビュート [2] ダウンロード可能 ACL[2] リダイレクト URL[2]
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 ACL[2] リダイレクト URL[2]	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL[2] Filter-Id アトリビュート [2] ダウンロード可能 ACL[2] リダイレクト URL[2]	ユーザ単位 ACL[2] Filter-Id アトリビュート [2] ダウンロード可能 ACL[2] リダイレクト URL[2]
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 ACL[2]			
NAC レイヤ 2 IP 検証	Filter-Id アトリビュート [2] ダウンロード可能 ACL リダイレクト URL	Filter-Id アトリビュート [2] ダウンロード可能 ACL リダイレクト URL	Filter-Id アトリビュート [2] ダウンロード可能 ACL リダイレクト URL	Filter-Id アトリビュート [2] ダウンロード可能 ACL[2] リダイレクト URL[2]
フォールバック方式としての Web 認証[4]	プロキシ ACL Filter-Id アトリビュート [2] ダウンロード可能 ACL[2]	プロキシ ACL Filter-Id アトリビュート [2] ダウンロード可能 ACL[2]	プロキシ ACL Filter-Id アトリビュート [2] ダウンロード可能 ACL[2]	プロキシ ACL[2] Filter-Id アトリビュート [2] ダウンロード可能 ACL[2]

1. MDA = Multidomain authentication。
2. *multiauth* とも呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降ではサポートされています。
4. 802.1x 認証をサポートしていないクライアント用です。

ユーザ単位 ACL と Filter-Id

スイッチ上に設定された ACL には、Cisco IOS リリースを実行する他のデバイスとの互換性があります。

ACL にソースとして設定できるのは **any** だけです。

（注） マルチホスト モード用に設定された ACL では、ステートメントのソース部分が *any* である必要があります（たとえば、**permit icmp** *any* **host 10.10.1.1**）。

認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドを使用して、802.1x、MAC 認証バイパス、Web 認証といった、すべての認証方式を制御できます。認証マネージャ コマンドによって、接続されたホストに適用する認証方式のプライオリティと順序を決定できます。

認証マネージャ コマンドによって、ホストモード、違反モード、および認証タイマーなどの、一般的な認証機能を制御できます。一般的な認証コマンドには、**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 コマンドがあります。

802.1x 専用コマンドは、頭に **dot1x** キーワードが付きます。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 コマンドによって、インターフェイス上の認証をイネーブルにできます。しかし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドでは、グローバルでしか、802.1x 認証をイネーブルまたはディセーブルにできません。

（注） 802.1x 認証がグローバルにディセーブルにされても、Web 認証などの他の認証方式は、ポート上でイネーブルのままです。

認証マネージャ コマンドの機能は、旧 802.1x コマンドと同じです。

表 11-2　認証マネージャ コマンドと旧 802.1x コマンド

Cisco IOS Release 12.2(50)SE 以降における認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE よりも前における同等の 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 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	**dot1x auth-fail vlan**	ポート上の制限付き VLAN をイネーブルにします。
	dot1x critical（インターフェイス コンフィギュレーション）	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 802.1x ゲスト VLAN として指定します。

表 11-2　認証マネージャ コマンドと旧 802.1x コマンド （続き）

Cisco IOS Release 12.2(50)SE 以降における認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE よりも前における同等の 802.1x コマンド	説明
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	802.1x 認証をサポートしていないクライアント用に、Web 認証をフォールバック方式として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**}	802.1x 許可ポートで単一のホスト（クライアント）または複数のホストの接続を許可します。
authentication order	**dot1x mac-auth-bypass**	MAC 認証バイパス機能をイネーブルにします。
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制御をイネーブルにします。
authentication timer	**dot1x timeout**	802.1x タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	新しいデバイスがポートに接続する時、または、ポートに接続しているデバイスの数が最大数に達した後に新しいデバイスがそのポートに接続する時に発生する違反モードを設定します。
show authentication	**show dot1x**	スイッチまたは指定されたポートに関する 802.1x の統計情報、管理ステータス、および動作ステータスを表示します。認証マネージャには、旧 802.1x CLI コマンドとの互換性があります。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、認証マネージャで生成された冗長なシステム メッセージをフィルタリングできます。通常、フィルタリングされた内容は、認証の成功と関係しています。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なる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冗長な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 認証の冗長な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）の冗長な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 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あと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。

dot1x port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：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との 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これ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 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かぎりは、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 メンバーは第 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になっているポートは（**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 サーバへの接続が失われないように、冗長接続があることを確認する必要があります。たとえば、冗長接続をスタック マスターに、別の接続をスタック メンバーに確立でき、スタック マスターに障害が発生した場合も、スイッチ スタックは引き続き RADIUS サーバへの接続を維持できます。

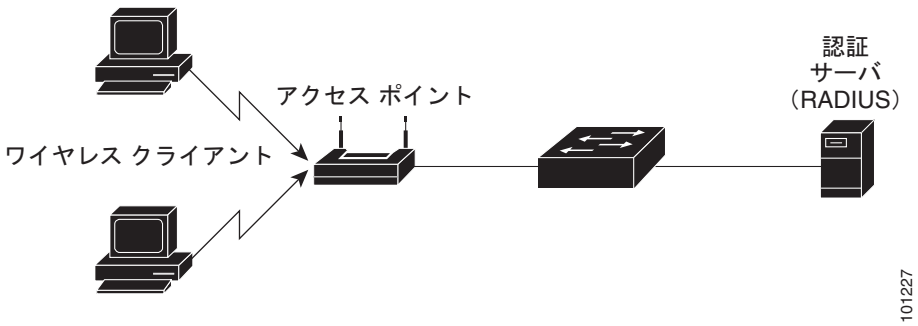
802.1x のホスト モード

802.1x 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 12-1（P.12-2）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 1 つのクライアントだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホストモードでは、1 つの 802.1x 対応ポートに複数のホストを接続できます。図 11-5（P.11-12）に、ワイヤレス LAN における 802.1x ポートベースの認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチホスト モードがイネーブルの場合、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 11-5　　マルチ ホスト モードの例



802.1x マルチ 認証モード

Multiple-authentication（multiauth; マルチ認証）モードでは、音声 VLAN 上に 1 つのクライアントと、データ VLAN 上に複数の認証されたクライアントが許可されます。マルチ認証モードでは、ハブやアクセス ポイントが 802.1x 対応ポートに接続されると、接続されたクライアントごとの認証が要求されることによって、マルチホスト モードに対する強化されたセキュリティが提供されます。非 802.1x デバイスの場合、MAC 認証バイパスまたは Web 認証を、個々のホスト認証のフォールバック方式として使用することで、1 つのポート上で、複数の方式によって複数のホストを一度に認証できます。

マルチ認証モードでは、データ VLAN または 音声 VLAN のどちらか（認証サーバから受信した VSA に基づく）に対して認証されたデバイスを割り当てることによって、音声 VLAN 上の MDA 機能がサポートされます。

（注）　ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、RADIUS サーバにより提供される VLAN を次の条件でマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、運用 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が運用 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- マルチ認証ポート上で、1 つの音声 VLAN 割り当てのみがサポートされている。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。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、許可されたすべてのホストは、設定された VLAN で再初期化される。

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、「802.1x 認証とアクセス不能認証バイパス」（P.11-23）を参照してください。

詳細については、「ホスト モードの設定」（P.11-48）を参照してください。

MAC 移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

状況によっては、同じスイッチ上のあるポートから別のポートに MAC アドレスを移動する必要があります。たとえば、認証されたホストとスイッチ ポートの間に別のデバイス（ハブや IP Phone など）がある場合は、そのデバイスからホストを切断し、同じスイッチの別のポートにホストを直接接続しなければならない場合があります。

MAC 移動をグローバルにイネーブルにすると、新しいポートでデバイスが再認証されます。ホストを 2 つ目のポートに移動すると、1 つ目のポートのセッションは削除され、新しいポート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、ポートでどのホスト モードがイネーブルになっているかに関係なく、スイッチ上の任意のポートに移動できます）。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、MAC 移動は、ポートのセキュリティとともに、すべてのホスト モードで設定できるようになりました。MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。ポートのセキュリティの動作は、MAC 移動を設定するときと変わりません。

MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。

（注）　オープン認証モードでは、MAC アドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「MAC 移動のイネーブル化」（P.11-53）を参照してください。

MAC 置換

Cisco IOS Release 12.2(55)SE 以降のリリースでは、MAC 置換機能を設定して、事前に別のホストが認証されたポートにホストが接続を試みるときに発生する違反に対処できるようになりました。

（注）　違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MAC アドレスはただちに 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.11-53）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、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法は定義されますが、ネットワークの使用方法については監視されません。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、Attribute-Value（AV; アトリビュート値）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 11-3 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 11-3　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動的ホスト制御プロトコル（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だけ、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。

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

802.1x 状態チェック

802.1x 状態チェックは、すべてのスイッチ ポート上の 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に関する情報を表示します。この機能を使用して、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうか判断できます。802.1x 機能をサポートしないデバイス用に、MAC 認証バイパスまたは Web 認証などの別の認証を使用します。

この機能が動作するのは、クライアントのサプリカントが、NOTIFY EAP 通知パケットのあるクエリーをサポートする場合だけです。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。

スイッチへの 802.1x 状態チェックの設定の詳細については、「802.1x 状態チェックの設定」（P.11-42）を参照してください。

VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、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、マルチドメイン ホスト モードでサポートされます。音声デバイスが認証され、RADIUS サーバが許可 VLAN を戻すと、ポート上の音声 VLAN は割り当てられた音声 VLAN のパケットを送受信するよう設定されます。音声 VLAN 割り当ては、MDA 対応ポート上のデータ VLAN 割り当てと同じように動作します。詳細については、「MDA」（P.11-30）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 です。このポート上で送受信されるパケットはすべてこの VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が無効の場合、認証は失敗し、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、設定済みのまたは割り当て済みの 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にしても、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 と設定済み音声 VLAN に戻ります。

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。

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* に変更したりすると、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。

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 名または VLAN ID

  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、IEEE 802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル 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.10-36）を参照してください。

ユーザ単位 ACL を使用した 802.1x 認証

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。設定の競合を避けるには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画する必要があります。

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、入力方向でだけサポートされます。スイッチは、入力方向でだけ 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。詳細については、第 36 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）に対してだけサポートされます。

1 ポートがサポートする 802.1x 認証ユーザは 1 ユーザだけです。マルチ ホスト モードがポートでイネーブルの場合、ユーザ単位 ACL アトリビュートは関連ポートでディセーブルです。

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.10-36）を参照してください。ACL の設定の詳細については、第 36 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。

ユーザ単位 ACL を設定するには、次の手順を実行します。

- 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。

（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。

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

ホストの 802.1x または MAC 認証バイパス中に、RADIUS サーバからスイッチへ、ACL をダウンロードし、URL をリダイレクトできます。Web 認証中にも ACL をダウンロードできます。

（注）　ダウンロード可能 ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

802.1x 対応ポートに接続されたすべてのデバイスに対して、ACL と リダイレクト URL を適用できます。

802.1x 認証中にダウンロードされる ACL がない場合、スイッチによって、ポート上のスタティック デフォルト ACL がホストに適用されます。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト ACL が作成され、dACL がダウンロードされて適用される前にポリシーが実施されます。

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

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して作成できます。

（注）　認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP; シスコ検出プロトコル）バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、*open* および *closed* の 2 つの認証方式がサポートされます。*closed* 認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 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、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

open 認証モードのポートにスタティック ACL がない場合、次のようになります。

- 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に、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *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* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバ上のユーザ プロファイル、または

スイッチ上のいずれかで設定できます。AAA サーバ上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。スイッチ上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。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートが open 認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートが closed 認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL 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 が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。

（注）　Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

リダイレクト URL の Cisco Secure ACS とアトリビュート値ペア

スイッチでは、次の *cisco-av-pair* VSA が使用されます。

- 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 アトリビュート値ペアを使用して、エンド ポイントからの HTTP または HTTPS リクエストを代行受信します。次に、スイッチによって、クライアントの Web ブラウザが、指定されたリダイレクト アドレスに転送されます。Cisco Secure ACS 上の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が格納されます。url-redirect-acl アトリビュート値ペアには、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 と一致するトラフィックは、リダイレクトされます。

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

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

ダウンロード可能 ACL の Cisco Secure ACS とアトリビュート値ペア

Cisco Secure ACS 上の CiscoSecure-Defined-ACL アトリビュート値ペアを、RADIUS cisco-av-pair の vendor-specific attribute（VSA; ベンダー固有属性）を使用して設定できます。このペアによって、#ACL#-IP-name-number 属性が使用されて、Cisco Secure ACS 上のダウンロード可能 ACL の名前が指定されます。

- *name* は、ACL の名前です。
- *number* は、バージョン番号です（たとえば、3f783768 など）。

ダウンロード可能 ACL を認証サーバ上のクライアントに対して設定する場合、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 も設定する必要があります。

デフォルト ACL がスイッチに設定され、Cisco Secure ACS によってホストアクセスポリシーがスイッチに送信される場合、そのポリシーが、スイッチ ポートに接続されたホストからのトラフィックに適用されます。このポリシーが適用されない場合、スイッチによってデフォルト ACL が適用されます。Cisco Secure ACS によって、スイッチに対してダウンロード可能 ACL が送信される場合、この ACL がスイッチ ポートに設定されているデフォルト ACL よりも優先されます。ただし、スイッチが Cisco Secure ACS からのホスト アクセス ポリシーを受信するが、デフォルト ACL が設定されていない場合、認証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.11-8）と「ダウンロード可能 ACL とリダイレクト URL を使用した 802.1x 認証の設定」（P.11-65）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 ではなくスタティック VLAN ID に基づいてホストを認証する場合は、VLAN ID ベースの MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続先のポートに設定された VLAN ID が MAC 認証に使用されます。IAS サーバとともに VLAN ID ベースの MAC 認証を使用することで、ネットワーク内に決まった数の VLAN を設定できます。

この機能は、STP によってモニタおよび処理される VLAN の数も制限します。ネットワークを固定された VLAN として管理できます。

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

設定情報については、「VLAN ID ベースの MAC 認証の設定」（P.11-68）を参照してください。その他の設定は、MAC 認証バイパス（「MAC 認証バイパスの設定」（P.11-61）を参照）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 IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、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 IEEE 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。

スイッチが 802.1x 対応音声デバイスを許可しようとし、AAA サーバが使用できない場合、許可試行は失敗しますが、EAPOL パケットの検出は EAPOL 履歴に保存されます。AAA サーバが使用できるようになると、スイッチは音声デバイスを許可します。ただし、スイッチは他のデバイスによるゲスト VLAN へのアクセスを許可しません。この状況を避けるには、次のコマンド シーケンスのいずれかを使用します。

- ゲスト VLAN へのアクセスを許可するには、**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 コマンドを入力すると、ポートを再起動できます。

制限付き VLAN を使用してネットワーク アクセスの認証に失敗したクライアントを許可するには、**dot1x auth-fail vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力します。

デバイスがリンクの存続時間中にスイッチに 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なくなります。

（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、シングルホスト モードとマルチホスト モードの 802.1x ポートでサポートされます。

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 ポート上でだけサポートされます。

スイッチは、*MAC 認証バイパス*をサポートしています。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、IEEE 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。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。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-Access/Request 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 IEEE 802.1x 認証」（P.11-28）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.11-55）を参照してください。

制限付き VLAN を使用した 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 IEEE 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際限なく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 に変わると、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。制限付き 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 または 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もできますが、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かぎり、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 成功の擬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 モードの場合だけサポートされます。

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 ポート上でだけサポートされます。

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.11-56）を参照してください。

802.1x 認証とアクセス不能認証バイパス

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）は、スイッチが設定済みの RADIUS サーバに到達できず、新しいクライアントを認証できない場合に使用します。そのようなホストを*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 ポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN（*クリティカル VLAN*）に移動されます。管理者はホストに制限付きの認証を提供します。

スイッチはクリティカル ポートに接続されたホストの認証を行う際に、設定済みの 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。

マルチ認証ポートでのサポート

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 ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストが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。

RADUIS サーバが再び利用可能になったときにホストを再初期化してクリティカル VLAN の外にホストを移動するようにクリティカル ポートを設定できます。このように設定すると、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.11-58）を参照してください。

機能の相互作用

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、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。

802.1x ユーザ分散

802.1x ユーザ分散を設定することにより、同じグループ名を持つユーザの負荷を複数の VLAN に分散できます。

VLAN は、RADIUS サーバによって提供されるか、スイッチの CLI によっていずれかの VLAN グループ名に設定されます。

- ユーザに複数の VLAN 名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として複数の VLAN 名を送信できます。802.1x ユーザ分散では、特定の VLAN 内にあるすべてのユーザを追跡し、許可済みユーザをユーザが最も少ない VLAN に移動することでロード バランシングが実現されます。
- ユーザに VLAN グループ名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として VLAN グループ名を送信できます。スイッチの CLI を使用して、設定した VLAN グループ名の中から選択された VLAN グループ名を検索できます。VLAN グループ名が見つかると、その VLAN グループ名に割り当てられた対応する VLAN の中から、ユーザの割り当てが最も少ない VLAN が検索されます。対応する許可済みユーザをその VLAN に移動することで、ロード バランシングが実現されます。

（注） RADIUS サーバは、VLAN ID、VLAN 名、VLAN グループを任意に組み合わせて VLAN の情報を送信できます。

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てください。
- VLAN グループには複数の VLAN をマッピングできます。
- VLAN を追加または削除することによって VLAN グループを変更できます。
- VLAN グループ名から既存の VLAN を消去すると、その VLAN の認証ポートは消去されませんが、マッピングは既存の VLAN グループから削除されます。
- VLAN グループ名から最後の VLAN を消去すると、VLAN グループも消去されます。
- VLAN グループにアクティブな VLAN がマッピングされていても、その VLAN グループを消去できます。VLAN グループを消去すると、グループ内のいずれかの VLAN で認証ステートになっているポートやユーザは消去されませんが、その VLAN グループへの VLAN マッピングは消去されます。

詳細については、「802.1x ユーザ分散」（P.11-25）を参照してください。

音声 VLAN ポートを使用した IEEE 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関係なく、IP Phone は音声トラフィックには VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

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 で認証されたあと、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。

（注） IP Phone と PC がスイッチ ポートに接続されていて、そのポートがシングルホスト モードまたはマルチホスト モードに設定されている場合は、そのポートをスタンドアロンの MAC 認証バイパス モードに設定しないでください。MAC 認証バイパスは、タイムアウト時間がデフォルトの 5 秒に設定された 802.1x 認証へのフォールバック方式としてだけ使用することを推奨します。

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 だけを認識します。音声 VLAN ポートで IEEE 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。

IEEE 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。

（注） 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 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 16 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 IEEE 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 IEEE 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 IEEE 802.1x 認証をイネーブルに設定すると、IEEE 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、IEEE 802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

次に、スイッチ上での IEEE 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 ホストの最大数が静的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.28-10）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから IEEE 802.1x クライアント アドレスを手動で削除する場合、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを使用して、IEEE 802.1x クライアントを再認証する必要があります。
- IEEE 802.1x クライアントがログオフすると、ポートが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、IEEE 802.1x ポート上でポート セキュリティと音声 VLAN を同時に設定できます。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。

ポートが IEEE 802.1x 対応ポートに接続したとき、または最大数の許可デバイスが認証されたとき、**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 コマンドを使用してポートがシャットダウンしたり、Syslog エラーを生成したり、新しいデバイスからのパケットを廃棄したりできます。詳細については、「ポート単位の許可デバイスの最大数」（P.11-42）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.28-9）を参照してください。

WoL 機能を使用した IEEE 802.1x 認証

IEEE 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 IEEE 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、IEEE 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 IEEE 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 IEEE 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。

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。

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 IEEE 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 11-2（P.11-5）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 IEEE 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 IEEE 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 IEEE 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。IEEE 802.1x ポートでクライアントを検出したあと、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-Access/Request 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 IEEE 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）IEEE 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、IEEE 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 IEEE 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、IEEE 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有効で、IEEE 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『IEEE 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。

- IEEE 802.1x 認証：IEEE 802.1x 認証がポートでイネーブルの場合にだけ 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：IEEE 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 IEEE 802.1x 認証」（P.11-26）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した IEEE 802.1x 認証」（P.11-26）を参照してください。
- VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）：IEEE 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 に割り当てることができます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：この機能は、IEEE 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。

詳細については、「認証マネージャ」（P.11-8）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。「認証マネージャ CLI コマンド」（P.11-9）を参照してください。

NAC レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク 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ィルス対策の状態または*ポスチャ*を調べる Network Admission Control（NAC）レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 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。アクションの設定値が *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。
- **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 IEEE 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、IEEE 802.1x ポートベース認証と似ています。NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 IEEE 802.1x 検証の設定」（P.11-63）および「定期的な再認証の設定」（P.11-49）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。詳細については、「認証マネージャ」（P.11-8）を参照してください。

柔軟な認証順序

柔軟な認証順序を使用して、新しいホストを認証するためにポートが使用するメソッドの順序を設定できます。MAC 認証バイパスと 802.1x を、プライマリまたはセカンダリ認証方式にできます。また、それらの認証試行の片方または両方が失敗した場合、Web 認証をフォールバック方式にできます。詳細については、「柔軟な認証順序の設定」（P.11-68）を参照してください。

Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、ポート上の新しいホストが送信できるのは、スイッチに対するトラフィックだけです。ホストが認証されると、RADIUS サーバ上に設定されているポリシーが、そのホストに適用されます。

次のシナリオでオープン認証を設定できます。

- オープン認証を使用したシングルホスト モード：認証の前後に 1 人のユーザだけがネットワークへのアクセスを許可されます。
- オープン認証を使用した MDA モード：音声ドメイン内で 1 人、および、データ ドメイン内で 1 人のユーザだけが許可されます。
- オープン認証を使用したマルチホスト モード：すべてのホストがネットワークにアクセスできます。
- オープン認証を使用したマルチ認証モード：MDA と同様、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.11-48）を参照してください。

MDA

スイッチは、MultiDomain Authentication（MDA）をサポートしています。MDA では、同じスイッチ ポートにおいてデータ デバイスと IP Phone（シスコ製または他社製）などの音声デバイスの両方の認証が可能になります。ポートはデータ ドメインと音声ドメインにわかれています。

MDA はデバイス認証の順序を適用しません。ただし、最適な結果を得るために、MDA 対応ポートではデータデバイスより先に音声デバイスの認証を行うことを推奨します。

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.11-48）を参照してください。
- ホスト モードが multidomain に設定されている場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 16 章「音声 VLAN の設定」を参照してください。
- MDA 対応ポートでの音声 VLAN 割り当てがサポートされます。

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

- 音声デバイスを許可するには、`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 デバイスと見なします。

- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応ポートでのデータ デバイスにだけ適用されます。スイッチは、許可されなかった音声デバイスをデータ デバイスと 見なします。
- ポートの音声ドメインまたはデータ ドメインのいずれかで複数のデバイスが許可を受けようとすると、errdisable になります。
- デバイスが許可されるまで、ポートはトラフィックをドロップします。他社製 IP Phone または音声デバイスは、データ VLAN および音声 VLAN の両方に対して許可されます。データ VLAN では、音声デバイスが DHCP サーバに問い合わせて、IP アドレスを取得し、音声 VLAN 情報を取得することを許可します。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN はブロックされます。
- データ VLAN でバインドされ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 アドレス制限についてはカウントされません。
- データ デバイスにだけ RADIUS サーバからダイナミック VLAN 割り当てを使用できます。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチ ポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。詳細については、「MAC 認証バイパス」（P.11-41）を参照してください。
- ポートで*データ*デバイスまたは*音声*デバイスが検出されると、許可を受けるまでその MAC アドレスはブロックされます。許可を受けられないと、MAC アドレスは 5 分間ブロックされたままになります。
- ポートが許可されないまま、*データ* VLAN で 5 台を超えるデバイスが、または*音声* VLAN で複数の音声デバイスが検出されると、ポートは errdisable ステートになります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとでも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。
- MDA 対応ポートではユーザ単位 ACL は推奨しません。ユーザ単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザ単位 ACL を適用するデバイスは 1 台だけにしてください。

Network Edge Access Topology（NEAT）を使用した 802.1x スイッチ サプリカント スイッチとオーセンティケータ スイッチ

Network Edge Access Topology（NEAT）機能は、ID をワイヤリング クローゼット（会議室など）の外側の領域に拡張します。これにより、ポート上であらゆるタイプのデバイスを認証できるようになります。

- 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して、あるスイッチを他のスイッチに対するサプリカントとして動作するように設定できます。この設定は、スイッチがワイヤリング クローゼットの外にあり、トランク ポートを介してアップストリーム スイッチに接続されてい

る場合などに役に立ちます。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 スイッチを使用した認証を行います。サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変化します。

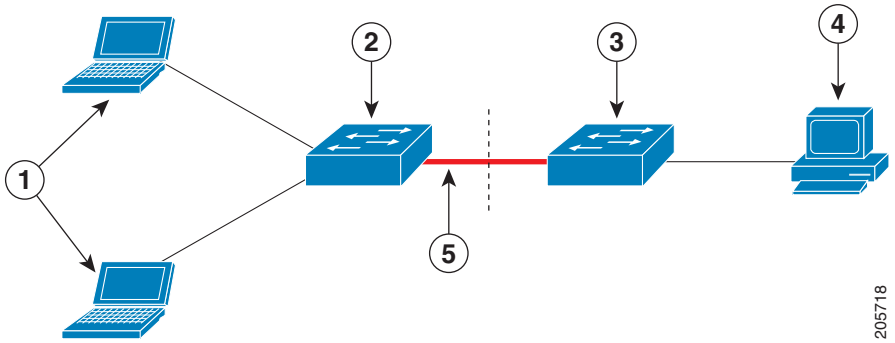
- オーセンティケータ スイッチにアクセス VLAN が設定されている場合は、認証の成功後、そのアクセス VLAN がトランク ポートのネイティブ VLAN になります。

1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA モードまたは multiauth モードをイネーブルにできます。オーセンティケータ スイッチ インターフェイスではマルチホスト モード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 コマンドを使用すると、すべてのホスト モードで Network Edge Access Topology（NEAT）が機能するようになります。

- ホスト認証：必ず（サプリカントを持つスイッチに接続している）許可されたホストからのトラフィックだけがネットワーク上で許可されます。図 11-6 に示すとおり、スイッチでは、サプリカント スイッチに接続している MAC アドレスを、オーセンティケータ スイッチに対して送信するのに、Client Information Signalling Protocol（CISP）が使用されます。
- 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が自動的にイネーブルになり、サプリカント スイッチから来る複数の VLAN からのユーザ トラフィックが許可されます。ACS で、cisco-av-pair を *device-traffic-class=switch* に設定します（これは、*group* 設定値または *user* 設定値で設定できます）。

図 11-6　CISP を使用したオーセンティケータとサプリカント 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）
3	オーセンティケータ スイッチ	**4**	Access Control Server（ACS; アクセス コントロール サーバ）
5	トランク ポート		

注意事項

- NEAT ポートは、他の認証ポートと同じ設定値で設定できます。サプリカント スイッチが認証を行うと、ポート モードがスイッチの Vendor-Specific Attribute（VSA; ベンダー固有のアトリビュート）に基づいて *access* から *trunk* に変化します（device-traffic-class=switch）。
- VSA は、オーセンティケータ スイッチのポート モードを access から trunk に変更し、ネイティブ トランク VLAN に変換されるものがある場合は、802.1x トランク カプセル化とアクセス 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 モードを変更すると*同時に*オーセンティケータ スイッチのポートに標準のポート設定を適用するには、スイッチの VSA ではなく、自動 SmartPort ユーザ定義マクロを使用することもできます。これにより、オーセンティケータ スイッチのポート上でサポートされていない設定を削除し、ポート モードを *access* から *trunk* に変更できます。詳細については、このリリースに対応する『*Auto Smartports 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とサプリカント スイッチの設定」（P.11-64）を参照してください。

音声対応 802.1x セキュリティ

音声対応 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した VLAN だけ（データ VLAN または音声 VLAN）をディセーブルにするようスイッチを設定できます。以前のリリースでは、セキュリティ違反の原因であるデータ 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、接続が完全に切断されます。

PC が IP Phone に接続されている IP Phone 構成でこの機能を使用できます。データ VLAN 上でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンします。音声 VLAN 上のトラフィックは中断することなくスイッチに流れます。

音声対応 802.1x セキュリティの詳細については、「音声対応 802.1x セキュリティの設定」（P.11-43）を参照してください。

共通セッション ID

認証マネージャは、使用する認証方式に関係なく、クライアント用にただ 1 つのセッション ID（共通セッション ID と呼ばれます）を使用します。この ID は、show コマンドや MIB など、すべてのレポートに使用されます。このセッション ID は、セッションごとのすべての syslog メッセージに表示されます。

このセッション ID には、次の要素が含まれています。

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

次に、show authentication コマンドの出力に表示されたセッション ID の例を示します。この例のセッション 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 の出力に表示されたセッション ID の例を示します。この例のセッション 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
```

このセッション 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でクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

Media Access Control Security と MACsec キーの承諾の概要

802.1AE で定義された Media Access Control Security（MACsec; メディア アクセス コントロール セキュリティ）では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA; MACsec キーの承諾）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は 802.1x Extensible Authentication Protocol（EAP; 拡張認証プロトコル）フレームワークの使用に成功した後に実装されます。Cisco IOS Release 12.2(53)SE2 を実行している Catalyst 3750-X スイッチおよび 3560-X スイッチでは、ホスト側のリンク（ネットワーク アクセス デバイスと PC や IP 電話などのエンドポイント デバイスの間のリンク）だけが MACsec を使用してセキュアにすることができます。

MACsec を使用するスイッチでは、クライアントに関連付けられたポリシーに応じて、MACsec フレームまたは非 MACsec フレームを許可します。MACsec フレームは暗号化され、Integrity Check Value（ICV; 整合性チェック値）で保護されます。スイッチはクライアントからフレームを受信すると、MKA によって提供されたセッション キーを使用して暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームがドロップされます。また、スイッチは正しいセッション キーを使用して、ICV を暗号化し、セキュアなポート（セキュアな MAC サービスをクライアントに提供するために使用されるアクセス ポイント）を介して送信されたフレームに追加します。

MKA プロトコルは、基本的な MACsec プロトコルによって使用される暗号化キーを管理します。MKA の基本要件は 802.1x-REV で定義されます。MKA プロトコルでは 802.1x を拡張し、相互認証の確認によってピアを検出し、MACsec 秘密鍵を共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN（EAPOL）パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有される Master Session Key（MSK; マスター セッション キー）を生成します。EAP セッション ID を入力すると、セキュアな Connectivity association Key Name（CKN; 接続アソシエーション キー名）が生成されます。スイッチはオーセンティケータであるため、キー サーバでもあり、ランダムな 128 ビットの Secure Association Key（SAK; セキュア アソシエーション キー）を生成し、クライアント パートナーに送信します。クライアントがキー サーバになることはなく、単一の MKA エンティティであるキー サーバとの対話だけが可能です。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL Protocol Data Unit（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。MKA セッションと参加者は、MKA ライフタイム（6 秒間）が経過しても参加者からの MKPDU を受信していない場合に削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントからの最後の MKPDU を受信した後、6 秒間が経過するまで MKA の動作を継続します。

詳細については、次のセクションを参照してください。

- 「MKA ポリシー」（P.11-35）
- 「仮想ポート」（P.11-35）
- 「MACsec とスタッキング」（P.11-35）
- 「MACsec、MKA および 802.1x ホスト モード」（P.11-36）
- 「MKA 統計情報」（P.11-37）

MKA ポリシー

定義済みの MKA ポリシーをインターフェイスに適用すると、インターフェイス上で MKA がイネーブルになります。MKA ポリシーを削除すると、そのインターフェイス上で MKA がディセーブルになります。次のオプションを設定可能です。

- 16 ASCII 文字未満のポリシー名。
- 物理インターフェイスごとの機密保持（暗号化）オフセット 0 バイト、30 バイト、または 50 バイト。
- 再送保護。許可される順序外のフレームの数によって定義される MACsec ウィンドウ サイズを設定できます。この値は MACsec でセキュリティ アソシエーションをインストールする際に使用されます。値 0 は、フレームが正しい順序で許可されることを意味します。

仮想ポート

1 つの物理ポート上の複数のセキュアな接続アソシエーションに仮想ポートを使用します。各接続アソシエーション（ペア）は仮想ポートを表します。1 つの物理ポートにつき、仮想ポートは最大 2 つです。2 つの仮想ポートのうち、1 つだけをデータ VLAN の一部とすることができます。もう 1 つは、音声 VLAN に対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のために、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチ ホスト モードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非 MACsec ホストでは、マルチ ホスト モードであるため、認証なしでトラフィックを送信できます。

仮想ポートは、接続アソシエーションの任意の ID を表し、MKA プロトコル外の意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は 0x0002 ～ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意の Secure Channel Identifier（SCI; セキュア チャネル ID）を受け取ります。

MACsec とスタッキング

MACsec を実行している Catalyst 3750-X スタック マスターは、MACsec をサポートしているメンバー スイッチ上のポートを示すコンフィギュレーション ファイルを維持します。スタック マスターは、次に示す機能を実行します。

- セキュア チャネルとセキュアなアソシエーションの作成と削除を処理します。
- スタック メンバーにセキュアなアソシエーション サービスを送信します。
- ローカル ポートまたはリモート ポートからのパケット番号とリプレイ ウィンドウ情報を処理し、鍵管理プロトコルを通知します。
- オプションがグローバルに設定された MACsec 初期化要求を、スタックに追加される新しいスイッチに送信します。
- ポート単位の設定をメンバー スイッチに送信します。

メンバー スイッチは、次の機能を実行します。

- スタック マスターからの MACsec 初期化要求を処理します。
- スタック マスターから送信された MACsec サービス要求を処理します。
- スタック マスターにローカル ポートについての情報を送信します。

スタック マスターの切り替えの場合、すべてのセキュアなセッションがダウンし、再確立されます。認証マネージャはセキュアなセッションを認識し、これらのセッションのティアダウンを開始します。

MACsec、MKA および 802.1x ホスト モード

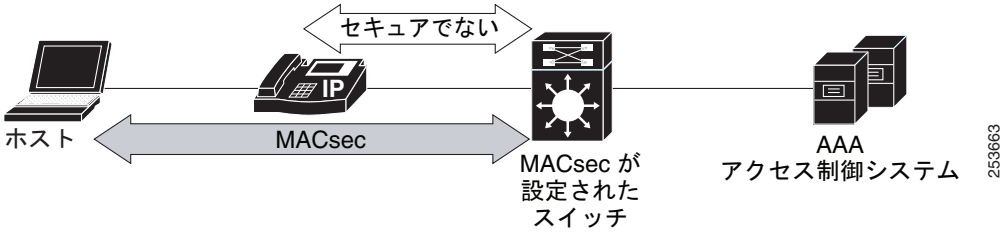
MACsec と MKA プロトコルを 802.1x シングル ホスト モード、マルチ ホスト モード、または Multi Domain Authentication（MDA; マルチドメイン認証）モードで使用できます。マルチ認証モードはサポートされません。

（注）　ソフトウェアでは MDA モードがサポートされますが、MACsec および MKA をサポートする IP 電話はありません。

シングル ホスト モード

図 11-7 に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

図 11-7　セキュアなデータ セッションでのシングル ホスト モードの MACsec

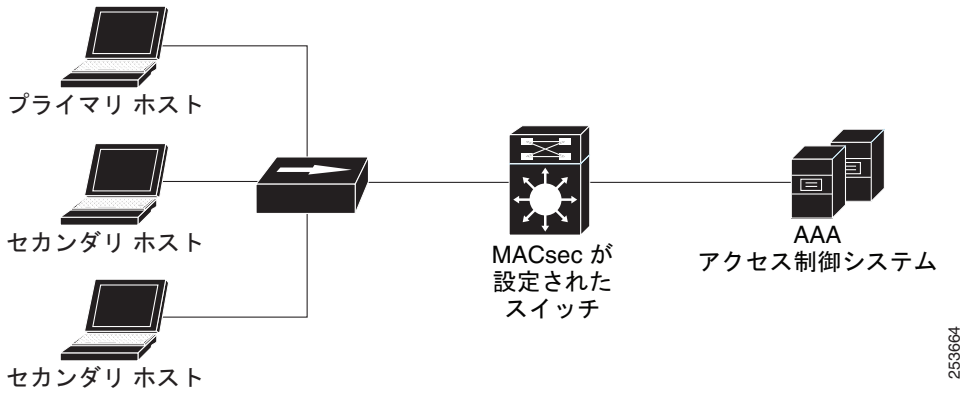


同じスイッチ ポートで、CDP バイパスを使用して、セキュアでない電話セッションをホストします。CDP バイパス モードでは認証をバイパスし、デバイス タイプだけに基づいてアクセスを提供するため、スイッチが電話機との MKA 交換への参加を試行しません。音声 VLAN が設定されている場合、CDP パケットが MAC sec をバイパスします。セキュアな音声アクセスの場合、MDA モードを使用する必要があります。

マルチ ホスト モード

標準（802.1x REV ではない）802 のマルチ ホスト モードでは、ポートが開いているか、1 つの認証に基づいて閉じられています。プライマリ セキュア クライアント サービスのクライアントがホストしている 1 人のユーザが認証される場合、同じポートに接続されているホストに同じレベルのネットワーク アクセスが提供されます。セカンダリ ホストが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ホストは、マルチ ホスト モードであるため、認証なしでネットワークにトラフィックを送信できます。図 11-8 を参照してください。

図 11-8　標準マルチ ホスト モードの MACsec - 非セキュア



MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスについての情報も取得できます。

802.1x 認証の設定

ここでは、次の設定情報について説明します。

- 「802.1x 認証のデフォルト設定」（P.11-38）
- 「802.1x 認証設定時の注意事項」（P.11-39）
- 「802.1x 状態チェックの設定」（P.11-42）（任意）
- 「音声対応 802.1x セキュリティの設定」（P.11-43）（任意）
- 「スイッチおよび RADIUS サーバ間の通信の設定」（P.11-46）（必須）
- 「802.1x 違反モードの設定」（P.11-44）
- 「802.1x 認証の設定」（P.11-45）
- 「ホスト モードの設定」（P.11-48）（任意）
- 「定期的な再認証の設定」（P.11-49）（任意）
- 「ポートに接続するクライアントの手動での再認証」（P.11-50）（任意）
- 「待機時間の変更」（P.11-50）（任意）
- 「スイッチからクライアントへの再送信時間の変更」（P.11-51）（任意）
- 「スイッチからクライアントへのフレーム再送信回数の設定」（P.11-51）（任意）
- 「再認証回数の設定」（P.11-52）（任意）
- 「MAC 移動のイネーブル化」（P.11-53）（任意）
- 「MAC 置換のイネーブル化」（P.11-53）
- 「802.1X アカウンティングの設定」（P.11-54）（任意）
- 「ゲスト VLAN の設定」（P.11-55）（任意）
- 「制限付き VLAN の設定」（P.11-56）（任意）
- 「アクセス不能認証バイパス機能の設定」（P.11-58）（任意）

- 「WoL を使用した 802.1x 認証の設定」（P.11-60）（任意）
- 「MAC 認証バイパスの設定」（P.11-61）（任意）
- 「802.1x ユーザ分散の設定」（P.11-62）（任意）
- 「NAC レイヤ 2 IEEE 802.1x 検証の設定」（P.11-63）（任意）
- 「802.1x 認証設定のデフォルト値へのリセット」（P.11-71）（任意）
- 「ポート上での 802.1x 認証のディセーブル化」（P.11-70）（任意）
- 「NEAT を使用したオーセンティケータとサプリカント スイッチの設定」（P.11-64）（任意）
- 「ダウンロード可能 ACL とリダイレクト URL を使用した 802.1x 認証の設定」（P.11-65）（任意）
- 「VLAN ID ベースの MAC 認証の設定」（P.11-68）（任意）
- 「柔軟な認証順序の設定」（P.11-68）（任意）
- 「Open1x の設定」（P.11-69）（任意）
- 「Web 認証ローカル バナーの設定」（P.11-70）（任意）
- 「ポート上での 802.1x 認証のディセーブル化」（P.11-70）（任意）
- 「802.1x 認証設定のデフォルト値へのリセット」（P.11-71）（任意）
- 「MKA および MACsec の設定」（P.11-71）（任意）

802.1x 認証のデフォルト設定

表 11-4　802.1x 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との 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
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あと、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）

表 11-4　802.1x 認証のデフォルト設定 （続き）

機能	デフォルト設定
最大再送信回数	2 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 **dot1x timeout server-timeout** インターフェイス コンフィギュレーション コマンドを使用すると、このタイムアウト時間を変更できます。
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
認証者（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル
MACsec と MKA	ディセーブル MKA ポリシーは設定されていません。

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.11-39）
- 「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.11-40）
- 「MAC 認証バイパス」（P.11-41）
- 「ポート単位の許可デバイスの最大数」（P.11-42）

802.1x 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 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 access から trunk 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あと、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 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック 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 対応ポートのモード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：アクティブまたはアクティブでない EtherChannel メンバーを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 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の 802.1x 認証をイネーブルにすることができます。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することができます。
- 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。
- IEEE 802.1x 認証において、EAP-Transparent LAN Services（TLS）および EAP-MD5 を実装した Cisco Access Control Server（ACS）アプリケーションを実行しているデバイスを使用している場合、そのデバイスで動作させている ACS バージョンが 3.2.1 以降であることを確認してください。
- IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP 電話などの音声デバイスの両方を認証することを推奨します。

（注）　Catalyst 3750、3560、および 2960 スイッチだけで CDP バイパスがサポートされます。Catalyst 3750-X、3560-X、3750-E、および 3560-E スイッチでは CDP バイパスがサポートされません。

- Cisco IOS Release 12.2(55)SE 以降のリリースでは、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がサポートされています。「認証マネージャ CLI コマンド」（P.11-9）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

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 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。

- 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 IEEE 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 ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を減らしてください（認証タイマーの非アクティブまたは **dot1x timeout quiet-period**、および、認証タイマーの再認証または **dot1x timeout tx-period**）。設定の減少量は、接続された 802.1x クライアントの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。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。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 ポート上でだけサポートされます。

MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、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.11-39）を参照してください。
- ポートが MAC アドレスで許可されたあとに、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。

ポート単位の許可デバイスの最大数

次に、802.1x 対応ポートで許可されたデバイスの最大数を示します。

- 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。ポートが音声 VLAN にも設定されている場合、Cisco IP Phone は数に制限なく、音声 VLAN を介してトラフィックを送受信できます。
- MultiDomain Authentication（MDA）モードでは、アクセス VLAN には 1 つのデバイスだけが許可され、音声 VLAN には 1 つの IP Phone だけが許可されます。
- 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が、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。デバイスは数に制限なく、音声 VLAN で許可されます。

802.1x 状態チェックの設定

802.1x 状態チェックは、すべてのスイッチ ポート上の 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に関する情報を表示します。この機能を使用して、スイッチ ポートに接続されたデバイスが 802.1x 対応であるかどうか判断できます。

802.1x 状態チェックは、802.1x 用に設定できるすべてのポートで許可されます。状態チェックは、**dot1x force-unauthorized** と設定されたポートでは使用できません。

スイッチで状態チェックをイネーブルにするには、次の注意事項に従ってください。

- 状態チェックは一般的に、802.1x がスイッチでイネーブルになる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用する場合、スイッチ スタック上のすべてのポートはテストされます。
- 802.1x 対応ポートに **dot1x test eapol-capable** コマンドを設定し、リンクがアップ状態になると、ポートは 802.1x 機能について接続したクライアントに照会します。クライアントが通知パケットで応答する場合、クライアントは 802.1x 対応です。クライアントがタイムアウト時間内に応答すると、Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- 状態チェックは、複数のホスト（たとえば、IP Phone に接続されている PC）を処理するポート上で送信されます。タイマーの時間内に状態チェックに応答する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 状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチで 802.1x 状態チェックをイネーブルにします。 （任意）*interface-id* では、IEEE 802.1x の状態をチェックするポートを指定します。 **（注）** 任意の **interface** キーワードを省略すると、スイッチ上のすべてのインターフェイスがテストされます。
ステップ 1	**configure terminal**	（任意）グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot1x test timeout** *timeout*	（任意）EAPOL 応答を待つのに使用するタイムアウトを設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 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）変更されたタイムアウト値を確認します。

次に、スイッチ上の状態チェックをイネーブルにしてポートを照会する例を示します。また、照会済みポートから受信した応答も示します。このポートは、接続しているデバイスが 802.1x 対応であることを確認します。

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

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

音声対応 802.1x セキュリティの設定

スイッチ上の音声対応 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した VLAN だけ（データ VLAN または音声 VLAN）をディセーブルにします。PC が IP Phone に接続されている IP Phone 構成でこの機能を使用できます。データ VLAN 上でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンします。音声 VLAN 上のトラフィックは中断することなくスイッチに流れます。

スイッチに音声対応 802.1x 音声セキュリティを設定するには、次の注意事項に従ってください。

- **reducible 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、音声対応 802.1x セキュリティをイネーブルにします。このコマンドの **no** バージョンを入力して、音声対応 802.1x セキュリティをディセーブルにします。このコマンドは、スイッチ内のすべての 802.1x 設定ポートに適用されます。

（注）　**shutdown vlan** キーワードが含まれていない場合、error-disabled ステートになると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 error-disabled 回復を設定する場合、ポートは自動的に再イネーブルになります。error-disabled 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ポートを再イネーブルにします。
- **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用して、個々の VLAN を再イネーブルにできます。範囲を指定しないと、ポート上のすべての VLAN がイネーブルになります。

音声対応 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**	セキュリティ違反エラーが発生した VLAN をすべてシャットダウンします。 （注）　**shutdown vlan** キーワードが含まれていないと、ポート全体が error-disabled 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）自動 VLAN 単位エラー回復をイネーブルにします。

	コマンド	目的
ステップ 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	（任意）error-disabled であった個別の VLAN を再イネーブルにします。 • *interface-id* では、個別の VLAN を再イネーブルにするポートを指定します。 • （任意）*vlan-list* では、再イネーブルにする VLAN のリストを指定します。*vlan-list* が指定されていないと、すべての VLAN が再イネーブルされます。
ステップ 5	**shutdown** **no-shutdown**	（任意）error-disabled になった VLAN を再イネーブルにし、error-disabled 表示をすべてクリアします。
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、セキュリティ違反エラーが発生したすべての VLAN をすべてシャットダウンするようスイッチを設定する例を示します。

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

次に、ポート Gi4/0/2 で error-disabled であったすべての VLAN を再イネーブルにする例を示します。

```
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

次の場合に、802.1x ポートがシャットダウンしたり、Syslog エラーを生成したり、新しいデバイスからのパケットを廃棄したりできるように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した場合
- デバイスの許可された最大数がポートで認証された場合

スイッチ上で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、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *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** キーワード以外のキーワード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。

	コマンド	目的
ステップ 4	**interface** *interface-id*	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 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 error-disabled にします。 • **restrict**：Syslog エラーを生成します。 • **protect**：トラフィックをポートに送信するあらゆる新しい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、新しいホストで認証します。
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。

	コマンド	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *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** キーワード以外のキーワード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。 （注）　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*	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**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だけ、ポートをアクセス モードに設定します。
ステップ 10	**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.11-39）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 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、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。 **（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アイテムとして設定してください。鍵にスペースを使用する場合は、引用符が鍵の一部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に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 サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

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

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

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」（P.10-36）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

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。MDA を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホスト デバイス、および IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチ ポートで許可されます。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] または **dot1x host-mode** {**multi-host** | **multi-domain**}	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。 キーワードの意味は次のとおりです。 • **multi-auth**：音声 VLAN 上の 1 つのクライアント、およびデータ VLAN 上の複数の認証されたクライアントを許可します。 （注）　**multi-auth** キーワードは、**authentication host-mode** コマンドでだけ使用可能です。 • **multi-host**：単一のホストの認証後に、802.1x 許可ポートで複数のホストを許可します。 • **multi-domain**：ホスト デバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。 （注）　ホスト モードが **multi-domain** に設定されている場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 16 章「音声 VLAN の設定」を参照してください。 指定するインターフェイスで、**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 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。

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
```

次に、MDA をイネーブルにして、ポートでホスト デバイスと音声デバイスの両方を許可する方法を示します。

```
Switch(config)# interface gigabitethernet3/0/1
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。
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** キーワードの意味は次のとおりです。 • **inactivity**：クライアントからのアクティビティがない場合に、無許可になるまでのインターバル（秒） • **reauthenticate**：自動再認証が開始するまでの時間（秒単位）。 • **restart** ***value***：認証されていないポートに対する認証試行が実行されるまでのインターバル（秒） **dot1x timeout reauth-period** 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ことにより、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「定期的な再認証の設定」（P.11-49）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、そのあと再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、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あと、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	**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、そのあとフレームを再送信します。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチが 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

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

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

スイッチからクライアントへのフレーム再送信回数を設定するには、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-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。

	コマンド	目的
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 移動によって、認証されたホストをスイッチ上のあるポートから別のポートに移動できます。

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
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。
authentication mac-move permit	イネーブルにします。
end	特権 EXEC モードに戻ります。
show run	設定を確認します。
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、スイッチで MAC 移動をグローバルにイネーブルにする例を示します。

```
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ホストを置換できます。

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。

	コマンド	目的
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。ポートが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。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **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**：ポートは、予期しない MAC アドレスを受信すると 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。

次に、インターフェイス上で MAC 置換をイネーブルにする例を示します。

```
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あと、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.11-39）を参照してください。
ステップ 3	**switchport mode access**	ポートをアクセス モードにします。
	または	または
	switchport mode private-vlan host	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	**dot1x port-control auto**	ポート上で 802.1x 認証をイネーブルにします。

	コマンド	目的
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 を設定している場合、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と、IEEE 802.1x に準拠している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 モードでだけ制限付き 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.11-39）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。

	コマンド	目的
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	**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)# interface gigabitethernet2/0/2
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.11-39）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 秒です。デフォルトは 3 回に設定されています。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
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 分です（24 時間）。デフォルト値は 0 分です。

	コマンド	目的
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あと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* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。 （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アイテムとして設定してください。鍵にスペースを使用する場合は、引用符が鍵の一部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に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。
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.11-39）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 サーバが到達不能な場合は、次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**：認証しようとしてい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**：ポート上で認証されたすべてのホストをユーザ指定のクリティカル VLAN に移動します。

	コマンド	目的
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-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 gigabitethernet 1/0/1
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.11-39）を参照してください。

	コマンド	目的
ステップ 3	**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-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 を使用した 802.1x 認証をディセーブルにするには、**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)# 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.11-39）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**]	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。
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、そのグループに VLAN をマッピングするには、グローバル コンフィギュレーション 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、そのグループに 1 つの VLAN または一定範囲の VLAN をマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list*	VLAN グループ設定または VLAN グループ設定の要素を消去します。

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、その VLAN グループ設定と指定した VLAN へのマッピングを確認する例を示します。

```
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
```

次に、既存の VLAN グループに VLAN を追加し、その VLAN が追加されたことを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10,30
```

次に、VLAN グループから VLAN を削除する例を示します。

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

次に、VLAN グループからすべての VLAN を消去すると、VLAN グループも消去されることを示します。

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

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

次に、すべての VLAN グループを消去する例を示します。

```
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 IEEE 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*：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 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***	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とサプリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼットの外にある 1 つのスイッチを、サプリカントとして設定し、また、認証スイッチに接続する必要があります。

概要については、「Network Edge Access Topology（NEAT）を使用した 802.1x スイッチ サプリカント スイッチとオーセンティケータ スイッチ」（P.11-31）を参照してください。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを auto に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスを Port Access Entity（PAE; 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方法を示します。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1x 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てい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**	新しいユーザ名のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	スイッチがユニキャスト パケットまたはマルチキャスト パケットを受信したときに、マルチキャスト EAPOL パケット*だけ*を強制的に送信します。 またこれによって、サプリカント スイッチのすべてのホスト モードで NEAT が機能するようになります。
ステップ 7	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードにします。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスを Port Access Entity（PAE; ポート アクセス エンティティ）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	インターフェイスに 802.1x 資格情報プロファイルを適用します。
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 マクロを使用した NEAT の設定

スイッチ VSA ではなく Auto SmartPort ユーザ定義マクロを使用して、認証者スイッチを設定することもできます。詳細については、このリリースに対応する『*Auto Smartports Configuration Guide*』を参照してください。

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

スイッチ上での 802.1x 認証の設定に加え、ACS も設定する必要があります。詳細については、次の Web サイトにある『*Configuration Guide for Cisco Secure ACS 4.2*』を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

（注）　ダウンロード可能 ACL は、スイッチにダウンロードする前に設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示します。

ダウンロード可能 ACL の設定

クライアント認証、および IP デバイス トラッキング テーブルへのクライアント IP アドレスの追加が終了した後に、ポリシーが反映されます。次に、スイッチによって、ダウンロード可能 ACL がポートに適用されます。

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	**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 local group radius**	許可の方法をローカルに設定します。許可の方法を削除するには、**no aaa authorization network default local 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**	入力方向にあるポート上でデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
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。

ダウンロード可能ポリシーの設定

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	**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 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のか、それとも許可するのかを指定します。 *source* は、ネットワーク、または、次のようなパケットを送信する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 のワイルドカード ビットを source に適用します。 （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**	入力方向にあるポート上でデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
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**	認証方式を 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までに応答を待機する時間（秒単位）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 Interface（SVI; スイッチ仮想インターフェイス）の IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication**	ベンダー固有属性を認識して使用するようにネットワーク アクセス サーバを設定します。 **（注）**　ダウンロード可能 ACL が動作可能である必要があります。

	コマンド	目的
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip device tracking all**	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。
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、スイッチに対してダウンロード可能ポリシーに関する設定を行う例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local 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 fastEthernet 2/13
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 認証のステータスを確認する show コマンドはありません。RADIUS アトリビュート 32 を確認するには、**debug radius accounting** 特権 EXEC コマンドを使用します。このコマンドの詳細については、次の URL で『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次に、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例を示します。

```
Switch# config 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
```

柔軟な認証順序の設定

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	**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）ポート上で使用される認証方式の順序を設定します。
ステップ 4	**authentication priority dot1x | mab** {**webauth**}	（任意）認証方式をポートプライオリティ リストに追加します。
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 Web 認証をフォールバック方式として試行するように設定する例を示します。

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

Open1x 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	**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）ポート制御を、単一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、Web 認証をフォールバック方式として使用するようにポートを設定します。
ステップ 5	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	（任意）ポート上の認証マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポート上のオープン 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）ポート上で使用される認証方式の順序を設定します。
ステップ 8	**authentication periodic**	（任意）ポート上の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）ポートの認証状態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、ポート上の open 1x を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/1
Switch(config)# authentication control-direction both
```

```
Switch(config)# authentication 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
```

Web 認証ローカル バナーの設定

Web 認証が設定されたスイッチでローカル バナーを設定するには、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	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*]	ローカル バナーをイネーブルにします。 （任意）*C banner-text C* を入力してカスタム バナーを作成します。*C* は区切り文字です。ファイルパスはバナーで表示されるファイルを示します（たとえば、ロゴまたはテキスト ファイル）。
ステップ 3	end	特権 EXEC モードに戻ります。

次に、カスタム メッセージ *My Switch* を使用して、ローカル バナーを設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com の『*Cisco IOS Security Command Reference*』の「Authentication Proxy Commands」を参照してください。

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。

	コマンド	目的
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）認証者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 IEEE 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、ポートの 802.1x 認証を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。
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。

MKA および MACsec の設定

- 「MKA ポリシーの設定」（P.11-72）
- 「インターフェイスでの MACsec の設定」（P.11-72）

MKA ポリシーの設定

MKA プロトコル ポリシーを作成するには、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	**mka policy** *policy name*	MKA ポリシーを指定し、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の最大長は 16 文字です。
ステップ 3	**replay-protection window-size** *frames*	再送保護をイネーブルにして、フレーム数のウィンドウ サイズを設定します。指定できる範囲は 0 ～ 4294967295 です。デフォルトのウィンドウ サイズは 0 です。 ウィンドウ サイズに 0 を入力することと、**no replay-protection** コマンドを入力することとは異なります。ウィンドウ サイズを 0 に設定するには、厳密な順序のフレームで再送保護を使用します。**no replay-protection** を入力すると、MACsec 再送保護がオフになります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mka policy**	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、MKA ポリシー *relay-policy* を設定する例を示します。

```
Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

インターフェイスでの MACsec の設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec 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	**interface** *interface-id*	MACsec インターフェイスを指定し、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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 3	**switchport access vlan** *vlan-id*	このポートのアクセス VLAN を設定します。
ステップ 4	**switchport mode access**	インターフェイスをアクセス ポートとして設定します。
ステップ 5	**macsec**	インターフェイスで 802.1ae MACsec をイネーブルにします。
ステップ 6	**authentication event linksec fail action authorize vlan** *vlan-id*	（任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ資格情報が認識されない認証リンク セキュリティの問題を処理するスイッチを指定します。
ステップ 7	**authentication host-mode multi-domain**	ホストと音声デバイスの両方が、802.1x で認証されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホスト モードはシングルです。
ステップ 8	**authentication linksec policy must-secure**	LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルトは *should secure* です。

	コマンド	目的
ステップ 9	**authentication port-control auto**	ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに切り替えられます。
ステップ 10	**authentication violation protect**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスをドロップするポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。
ステップ 11	**mka policy** *policy name*	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。（**mka policy** 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）MKA ポリシーが設定されていない場合、**mka default-policy** インターフェイス コンフィギュレーション コマンドを入力して、MKA のデフォルトのポリシーをインターフェイスに適用する必要があります。
ステップ 12	**dot1x pae authenticator**	ポートを 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設定します。
ステップ 13	**spanning-tree portfast**	対応するすべての VLAN 内の特定のインターフェイスで、スパニングツリー PortFast をイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。
ステップ 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 16	**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。

これは、インターフェイス上での MACsec の設定と確認の例です。

```
Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication violation protect
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch# show authentication sessions interface gigabitethernet1/0/25
Interface: GigabitEthernet1/0/25
MAC Address: 001b.2140.ec3c
IP Address: 1.1.1.103
User-Name: ms1
Status: Authz Success
Domain: DATA
Security Policy: Must Secure ß--- New
Security Status: Secured ß--- New
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 10
```

```
Session timeout: 3600s (server), Remaining: 3567s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A05783B0000001700448BA8
Acct Session ID: 0x00000019
Handle: 0x06000017
Runnable methods list:
Method State
dot1x Authc Success
```

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、冗長な 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 CLI コマンド」（P.11-9）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。