



IEEE 802.1x ポートベース認証の設定

IEEE 802.1x ポートベース認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。IE 3010 スイッチのコマンド リファレンスと、『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」に、コマンドの構文と使用方法の情報が 있습니다。

この章で説明する内容は、次のとおりです。

- 「IEEE 802.1x ポートベース認証の概要」 (P.10-1)
- 「802.1x 認証の設定」 (P.10-32)
- 「802.1x の統計情報およびステータスの表示」 (P.10-65)

IEEE 802.1x ポートベース認証の概要

IEEE 802.1x 規格では、一般の人がアクセス可能なポートからクライアントが LAN に接続しないように規制する、クライアント/サーバベースのアクセス コントロールおよび認証プロトコルを規定しています。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 サービスを利用できるようにします。

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

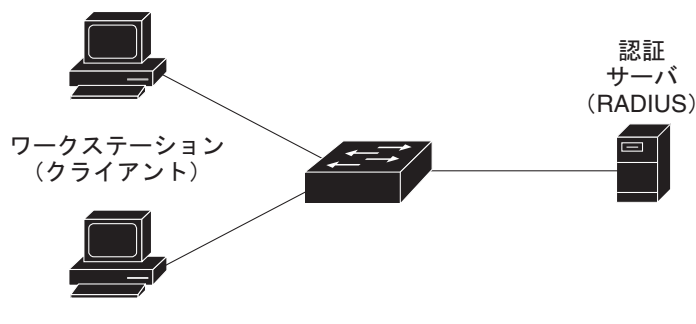
- 「デバイスの役割」 (P.10-2)
- 「認証プロセス」 (P.10-3)
- 「認証の開始およびメッセージ交換」 (P.10-5)
- 「認証マネージャ」 (P.10-7)
- 「許可状態および無許可状態のポート」 (P.10-10)
- 「802.1x のホスト モード」 (P.10-11)
- 「マルチドメイン認証」 (P.10-12)
- 「802.1x 複数認証モード」 (P.10-13)
- 「MAC Move」 (P.10-13)
- 「MAC 置換」 (P.10-14)
- 「802.1x アカウンティング」 (P.10-14)
- 「802.1x アカウンティング属性値ペア」 (P.10-15)
- 「802.1x 準備状態チェック」 (P.10-16)

- 「VLAN 割り当てを使用した 802.1x 認証」 (P.10-16)
- 「ユーザ単位 ACL を使用した 802.1x 認証の使用」 (P.10-17)
- 「ゲスト VLAN を使用した 802.1x 認証」 (P.10-21)
- 「制限付き VLAN を使用した 802.1x 認証」 (P.10-22)
- 「アクセス不能認証バイパスを使用した 802.1x 認証」 (P.10-23)
- 「音声 VLAN ポートを使用した 802.1x 認証」 (P.10-25)
- 「ポートセキュリティを使用した 802.1x 認証」 (P.10-25)
- 「Wake-on-LAN を使用した 802.1x 認証」 (P.10-25)
- 「MAC 認証バイパスによる 802.1x 認証」 (P.10-26)
- 「802.1x ユーザ ディストリビューション」 (P.10-27)
- 「Network Admission Control レイヤ 2 802.1x 検証」 (P.10-28)
- 「柔軟な認証の順序設定」 (P.10-28)
- 「Open1x 認証」 (P.10-29)
- 「音声認識 802.1x セキュリティの使用」 (P.10-29)
- 「Network Edge Access Topology (NEAT) を使用した 802.1x サプリカントおよびオーセンティケータ」 (P.10-29)
- 「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証」 (P.10-19)
- 「ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用」 (P.10-31)
- 「コモンセッション ID」 (P.10-31)

デバイスの役割

802.1X ポートベースの認証での装置の役割：

図 10-1 802.1x におけるデバイスの役割



101229

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



(注) Windows XP のネットワーク接続と 802.1x 認証の問題を解決するには、次の URL にある「Microsoft Knowledge Base」を参照してください。
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- 認証サーバ：クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対して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えます）。

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 をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、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。

仲介装置として動作できる装置は、IE 3010、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 の各スイッチや、ワイヤレス アクセス ポイントなどです。これらのデバイスでは、RADIUS クライアントおよび 802.1x 認証をサポートするソフトウェアが稼働している必要があります。

認証プロセス

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

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

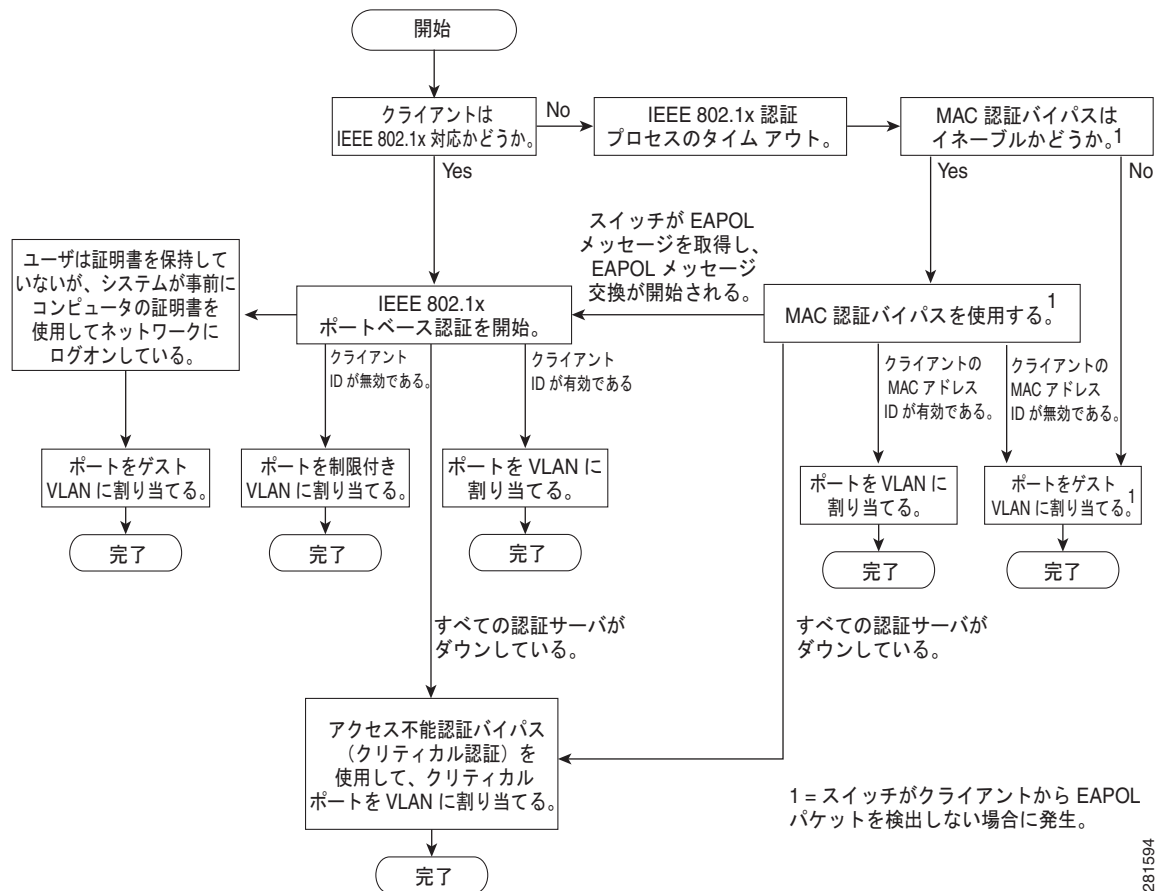
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。



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

図 10-2 に、認証プロセスを示します。

図 10-2 認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

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

RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性 (属性 [27])、および Termination-Action RADIUS 属性 (属性 [29]) に基づいてタイマーを使用します。

Session-Timeout RADIUS 属性 (属性 [27]) には再認証が行われるまでの時間を指定します。

Termination-Action RADIUS 属性 (属性 [29]) には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize* (属性値は *DEFAULT*) を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate* (属性値は RADIUS-Request) を設定した場合、セッションは再認証による影響を受けません。

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

Multidomain Authentication (MDA; マルチドメイン認証) がポートでイネーブルにされている場合、このフローが使用されます。ただし、音声許可の場合はいくつかの例外があります。MDA の詳細については、「[マルチドメイン認証](#)」(P.10-12) を参照してください。

認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステータスがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに 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 EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。



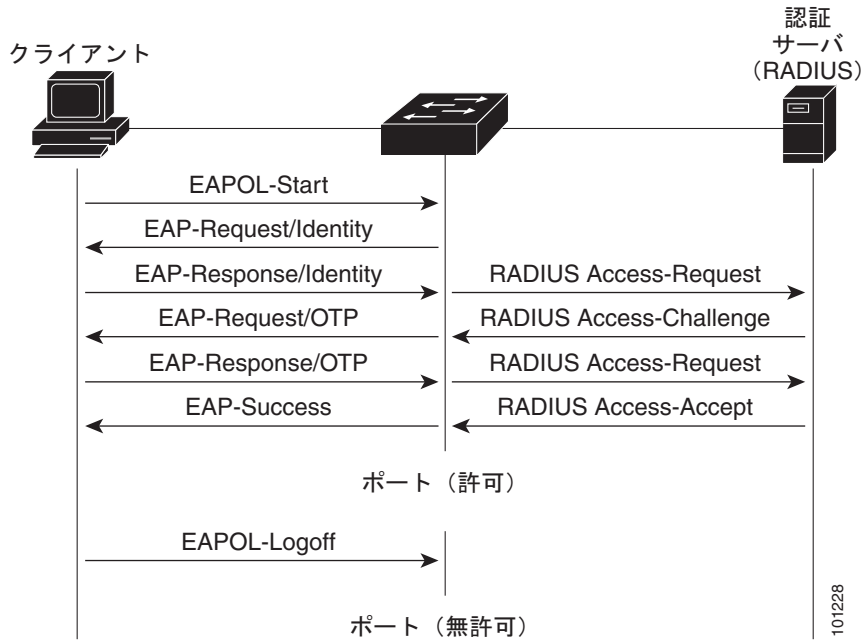
(注)

ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステータス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タス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、「[許可ステータスおよび無許可ステータスのポート](#)」(P.10-10) 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タスになります。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、「[許可ステータスおよび無許可ステータスのポート](#)」(P.10-10) 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 10-3 に、クライアントが RADIUS サーバとの間で OTP (ワンタイム パスワード) 認証方式を使用する際に行われるメッセージ交換を示します。

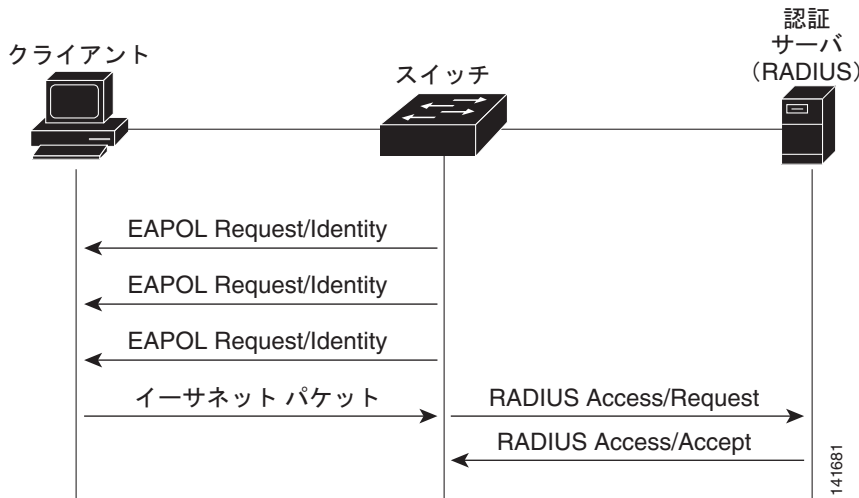
図 10-3 メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS 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 プロセスを停止して、802.1x 認証を停止します。

図 10-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 10-4 MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、スイッチ上および Catalyst 6000 などの他のネットワーク デバイス上で、CLI コマンドおよびメッセージなど、同じ認証方法を使用することができず、異なる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、ネットワークのすべての Catalyst スイッチで同じ認証方法を使用できます。

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.10-9) を参照してください。

- 「[ポートベースの認証方法](#)」(P.10-7)
- 「[ユーザ単位 ACL および Filter-Id](#)」(P.10-8)
- 「[認証マネージャ CLI コマンド](#)」(P.10-9)

ポートベースの認証方法

表 10-1 に、これらのホスト モードでサポートされている認証方法を示します。

- シングル ホスト：ポートで認証できるデータまたは音声ホスト（クライアント）は 1 つだけです。
- マルチ ホスト：同じポートで複数のデータ ホストを認証できます（ポートがマルチ ホスト モードで無許可になると、スイッチは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）。
- マルチドメイン認証（MDA）：同じスイッチ ポートでデータ デバイスと音声デバイスの両方を認証できます。ポートはデータ ドメインと音声ドメインに分割されます。
- 複数認証：複数のホストがデータ VLAN で認証できます。このモードでは、音声 VLAN が設定されている場合、VLAN で 1 クライアントだけ使用できます。

表 10-1 802.1x の機能

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ⁴ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
スタンドアロン Web 認証 ⁴	プロキシ ACL、Filter-Id 属性、ダウンロード可能な ACL ²			

表 10-1 802.1x の機能 (続き)

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²
NAC レイヤ 2 IP 検証	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
フォールバック メソッドとしての Web 認証 ⁵	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³

1. MDA = マルチドメイン認証。
2. *multiauth* とも呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
5. 802.1x 認証をサポートしていないクライアントの場合。

ユーザ単位 ACL および Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id がサポートされているのは、シングル ホスト モードだけでした。Cisco IOS Release 12.2(50) では、MDA および複数認証 (multiauth) をイネーブルにしたポートのサポートが追加されました。12.2(52)SE 以降では、マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、Catalyst 6000 スイッチなど、Cisco IOS ソフトウェアを実行する別のデバイスで設定された ACL と互換性がありませんでした。

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



(注) **any** は、ACL の発信元としてだけ設定できます。



(注) マルチ ホスト モードで設定された ACL では、ステートメントの発信元部分は **any** でなければなりません (たとえば、**permit icmp any host 10.10.1.1**)。

定義された ACL の発信元ポートには **any** を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。

マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに **any** を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

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 コマンドは、802.1x、MAC 認証バイパス および Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。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** または **authentication** 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 コマンドは、インターフェイスでの認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。



(注) 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

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

表 10-2 認証マネージャ コマンドおよび以前の 802.1x コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {both in}	dot1x control-direction {both in}	Wake-on-LAN (WoL) 機能を使用した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 dot1x critical (インターフェイス コンフィギュレーション) dot1x guest-vlan6	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback <i>fallback-profile</i>	dot1x fallback <i>fallback-profile</i>	認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
authentication host-mode [multi-auth multi-domain multi-host single-host]	dot1x host-mode {single-host multi-host multi-domain}	認可ポートでシングル ホスト (クライアント) またはマルチ ホストを許可します。
authentication order	dot1x mac-auth-bypass	使用される認証方法の順序を柔軟に定義できるようにします。
authentication periodic	dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
authentication port-control {auto force-authorized force-unauthorized}	dot1x port-control {auto force-authorized force-unauthorized}	ポートの許可ステータスの手動制御をイネーブルにします。

表 10-2 認証マネージャ コマンドおよび以前の 802.1x コマンド (続き)

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication timer	dot1x timeout	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後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、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せん。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 (仮想 LAN) ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは *許可ステート*に変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

802.1x 認証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 標準が稼働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。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

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

- **force-authorized** : 802.1x 認証をディセーブルにし、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全フレームがポート経由での送受信を許可されます。認証が失敗すると、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。指定された回数試行してもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

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。

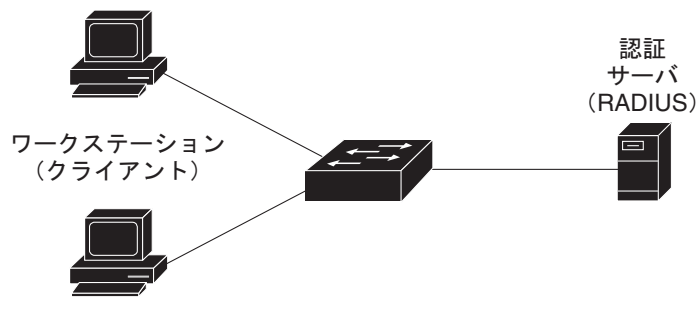
ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1x 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 10-1 \(P.10-2\)](#) 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クライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。[図 10-5 \(P.10-11\)](#) に、ワイヤレス LAN における 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 10-5 マルチ ホスト モードの例



(注)

ポートベース認証が設定された場合は、認可の前に、すべてのホスト モードに対してラインプロトコルがアップ状態になります。

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方を同じスイッチ ポートに接続できます。詳細については、「[マルチドメイン認証](#)」(P.10-12) を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定するには、「[ホスト モードの設定](#)」(P.10-42) を参照してください。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、[第 14 章「VLAN の設定」](#)を参照してください。
- 音声デバイスを許可するには、値 `device-traffic-class=voice` の Cisco Attribute Value (AV; 属性値) ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、`errordisable` になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポートセキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック方法として MAC 認証バイパスを使用して、IEEE 802.1x 認証をサポートしていないデバイスにスイッチポートを接続できます。詳細については、「[MAC 認証バイパス](#)」(P.10-36) を参照してください。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは `errordisable` になります。
- ポートのホスト モードがシングル ホストまたはマルチホストからマルチドメイン モードに変更される場合、許可済みのデータ デバイスはポートで許可済みのままになります。ただし、ポート音声 VLAN の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。
- ポートがシングルまたはマルチ ホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック方法は設定されたままになります。
- マルチドメイン モードからシングル ホストまたはマルチ ホスト モードにポートを切り替えると、ポートからすべての認証済みデバイスが削除されます。

- データ ドメインがまず許可されてゲスト VLAN に配置された場合、IEEE 802.1x 非対応音声デバイスは認証をトリガーするために音声 VLAN 上のパケットにタグを付ける必要があります。電話機はタグ付きトラフィックを送信する必要はありません (802.1x 対応電話の場合も同様です)。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーがある許可済みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。使用する場合、ポート上の 1 デバイスだけでユーザ単位 ACL が実行されます。

詳細については、「[ホスト モードの設定](#)」(P.10-42) を参照してください。

802.1x 複数認証モード

複数認証 (multiauth) モードでは、データ VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは、VLAN で 1 クライアントだけ認証できます (ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません)。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。

802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 台だけです。ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。

音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取った VSA に応じて、認証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。



(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。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「[アクセス不能認証バイパスを使用した 802.1x 認証](#)」(P.10-23) を参照してください。

ポートでのマルチ認証モードの設定の詳細については、「[ホスト モードの設定](#)」(P.10-42) を参照してください。

MAC Move

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。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス (ハブまたは IP Phone など) がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC Move をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。

MAC Move はすべてのホスト モードでサポートされます（認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。

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。

MAC Move 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 Move のイネーブル化](#)」(P.10-47) 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.10-48) 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を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 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。その代わりに、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 アカウンティング属性値ペア

RADIUS サーバに送信された情報は、Attribute Value (AV; 属性値) 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 属性の情報が必要です)。

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

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

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

表 10-3 アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [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
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	常時送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	常時送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	常時送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol (DHCP) バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にのみ、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 『802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサブリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

802.1x 準備状態チェックのスイッチの設定については、「[802.1x 準備状態チェックの設定](#)」(P.10-36)を参照してください。

VLAN 割り当てを使用した 802.1x 認証

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

音声デバイスが認可されているときに、RADIUS サーバから認可された VLAN が返された場合、このポートの音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されています。音声 VLAN 割り当ては、マルチドメイン認証 (MDA) 対応のポートでのデータ VLAN 割り当てと同じように機能します。詳細については、「[マルチドメイン認証](#)」(P.10-12)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 とは、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 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッドポートの VLAN、間違った VLAN ID、存在しないまたは内部 (ルーテッドポート) VLAN ID、RSPAN VLAN、シャットダウンまたは一時停止している VLAN の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行 (またはその逆) のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。

- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN (RADIUS サーバにより指定) に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
 - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致なくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
 - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

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

トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server (VMPS; VLAN メンバーシップ 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 認証をイネーブルにし、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属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
 - [64] Tunnel-Type = VLAN
 - [65] Tunnel-Medium-Type = 802
 - [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID または VLAN-Group
 - [83] Tunnel-Preference

属性 [64] は、値 *VLAN* (タイプ 13) でなければなりません。属性 [65] は、値 *802* (タイプ 6) でなければなりません。属性 [81] は、802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(P.9-36) を参照してください。

ユーザ単位 ACL を使用した 802.1x 認証の使用

ユーザ単位 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、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 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポート

に適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。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は保存しません。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。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート 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には、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザプロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。Vendor-Specific Attribute (VSA; ベンダー固有属性) は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。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コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、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 属性は 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。

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 の最大サイズにより制限されます。

ベンダー固有属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(P.9-36) を参照してください。ACL の設定の詳細については、第 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。



(注)

ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、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。
- 802.1x ポートをシングル ホスト モードに設定します。

設定の詳細については、「認証マネージャ」(P.10-7) を参照してください。

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

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。



(注) ダウンロード可能な ACL は *dACL* と呼ばれます。

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。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、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) 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、オープンおよびクローズの 2 つの認証方式がサポートされます。クローズ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。

オープン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せす。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。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ (ACE) は、ユーザ単位のエン트리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 ログを使用し、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、ステティック 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。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- *url-redirect* は HTTP to HTTPS URL です。
- *url-redirect-acl* はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL 属性値ペアを使用して、エンドポイント デバイスからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS の *url-redirect* 属性値ペアには、Web ブラウザがリダイレクトされる URL が含まれます。*url-redirect-acl* 属性値ペアには、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 の permit ACE と一致するトラフィックがリダイレクトされます。



(注) スイッチの URL リダイレクト ACL およびデフォルト 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。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

RADIUS の *cisco-av-pair* Vendor-Specific Attribute (VSA; ベンダー固有属性) を使用すると、Cisco Secure ACS で CiscoSecure-Defined-ACL Attribute Value (AV; 属性値) ペアを設定できます。このペアは、*#ACL#-IP-name-number* 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

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

ダウンロード可能な ACL が認証サーバ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。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホストアクセスポリシーをスイッチに送信すると、スイッチは、スイッチポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホストアクセスポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

設定の詳細については、「[認証マネージャ](#)」(P.10-7) および「[ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定](#)」(P.10-60) を参照してください。

VLAN ID ベース 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、VLAN ID ベース MAC 認証を使用できます。スイッチにスタティック VLAN ポリシーが設定されていると、認証する各ホストの MAC アドレスとともに VLAN の情報が IAS (Microsoft) RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

この機能を使用すると、STP によりモニタリングおよび処理される VLAN の数も制限されます。ネットワークは、固定 VLAN として管理できます。



(注)

この機能は Cisco ACS Server ではサポートされていません (ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います)。

設定の詳細については、「[VLAN ID ベース MAC 認証の設定](#)」(P.10-62) を参照してください。追加設定は、同様の MAC 認証バイパスです («[MAC 認証バイパスの設定](#)」(P.10-56) を参照してください)。

ゲスト VLAN を使用した 802.1x 認証

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

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

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

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

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンドシーケンスを使用します。

- **authentication event no-response action authorize 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、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。



(注)

インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステータスに戻って 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 で無許可ステータスになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッド ポート) またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは **MAC 認証バイパス** をサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1X ポートでクライアントを検出したあと、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 アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、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。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます (指定されていない場合)。詳細については、「[MAC 認証バイパスによる 802.1x 認証](#)」(P.10-26) を参照してください。

詳細については、「[ゲスト VLAN の設定](#)」(P.10-49) 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、スイッチの各 802.1X ポートに対して制限付き VLAN (認証失敗 VLAN と呼ばれることもあります) を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ (通常、企業にアクセスするユーザ) に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。



(注)

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

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

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

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

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

ダイナミック ARP インスペクション、DHCP スヌーピング、および IP 送信元ガードのような他のセキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「[制限付き VLAN の設定](#)」(P.10-50) を参照してください。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、*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。これらのホストを *クリティカル ポート*に接続するようにスイッチを設定できます。

新しいホストが *クリティカル ポート*に接続しようとする、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。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、*クリティカル ポート*に接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。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。

複数認証ポートのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホスト モードに設定され、*クリティカル VLAN*に移動されます。マルチ認証 (multiauth) ポートで、この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** コマンドを使用します。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、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 に移動されません。

このコマンドは、すべてのホスト モードでサポートされます。

認証結果

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

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイムアウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカル ポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。詳細については、このリリースのコマンドリファレンスおよび「[アクセス不能認証バイパス機能の設定](#)」(P.10-52) 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 と異なら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。

音声 VLAN ポートを使用した 802.1x 認証

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

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

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

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

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

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



(注)

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

音声 VLAN の詳細については、第 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 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x がポートごとに（または IP テレフォニーに MDA が設定されている場合は VLAN ごとに）単一の MAC アドレスを強制するため、ポート セキュリティが冗長になり、正常な IEEE 802.1x 操作が妨害される場合もあります。

Wake-on-LAN を使用した 802.1x 認証

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

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

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



(注)

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

authentication control-direction in 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、そのポートはスパンニングツリー フォワーディング ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンド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 認証バイパスによる 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス (図 10-2 (P.10-4) を参照) に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 802.1x ポートでこの機能をイネーブルにできます。

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

MAC 認証バイパス機能が 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1x ポートでクライアントを検出したあと、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 アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、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。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サブリカントであることを確認し、(MAC 認証バイパス機能ではなく) 802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1x サブ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。Termination-Action RADIUS 属性の値が DEFAULT であるという理由で直前のセッションが終了した場合、スイッチは再認証時に、802.1x 認証を優先再認証プロセスとして使用します。

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

再認証が Session-Timeout RADIUS 属性 (属性 [27])、および Termination-Action RADIUS 属性 (属性 [29]) に基づいて行われるときに、Termination-Action RADIUS 属性 (属性 [29]) のアクションが Initialize (属性値は DEFAULT) である場合、MAC 認証バイパス セッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能がイネーブルで、802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。AV ペアの詳細については、RFC 3580 『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1x 認証：802.1x 認証がポートでイネーブルの場合にだけ 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：802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1x 認証」(P.10-25) を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1x 認証」(P.10-25) を参照してください。
- VLAN メンバーシップ ポリシー サーバ (VMPS)：802.1x および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- シスコ ネットワーク アドミッションコントロール (NAC) レイヤ 2 IP 検証：この機能は、802.1x ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。
- Network Edge Access Topology (NEAT)：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

設定の詳細については、「認証マネージャ」(P.10-7) 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.10-9) を参照してください。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。



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

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。

- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

詳細については、「[802.1x ユーザ ディストリビューションの設定](#)」(P.10-56) を参照してください。

Network Admission Control レイヤ 2 802.1x 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の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャをチェックする Network Admission Control (NAC) レイヤ 2 802.1x 検証をサポートしています。NAC レイヤ 2 802.1x 検証を使用すると、次の作業を実行できます。

- Session-Timeout RADIUS 属性 (属性 [27]) と Termination-Action RADIUS 属性 (属性 [29]) を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性 (属性 [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 属性 (属性 [29]) を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID (属性 [81]) の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference (属性 [83]) の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID (属性 [81]) 属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、802.1x ポートベース認証と似ています。NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「[NAC レイヤ 2 802.1x 検証の設定](#)」(P.10-57) および「[定期的な再認証の設定](#)」(P.10-43) を参照してください。

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

設定の詳細については、「[認証マネージャ](#)」(P.10-7) を参照してください。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法的順序を設定できます。MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。詳細については、「[柔軟な認証順序の設定](#)」(P.10-63) 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、新しいホストはポートに定義されているアクセスコントロールリスト (ACL) に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバ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。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

詳細については、「[ホスト モードの設定](#)」(P.10-42) を参照してください。



(注)

オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

音声認識 802.1x セキュリティの使用

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、データ クライアントを認証しようとしてセキュリティ違反が発生すると、ポート全体がシャットダウンされ、接続が完全に切断されていました。

この機能は、PC が IP Phone に接続されている場合に使用できます。この機能を使用した場合、データ VLAN 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され、音声 VLAN のトラフィックは中断することなく処理を続行できます。

音声認識 802.1x セキュリティの設定については、「[音声対応 802.1x セキュリティの設定](#)」(P.10-37) を参照してください。

Network Edge Access Topology (NEAT) を使用した 802.1x サブリカントおよびオーセンティケータ

Network Edge Access Topology (NEAT) 機能は、ワイヤリング クローゼット (会議室など) 外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サブリカント：802.1x サブリカント機能を使用することで、別のスイッチのサブリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、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る場合に役に立ちます。802.1x スイッチ サブ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 スイッチで認証します。

サブリカント 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更されません。

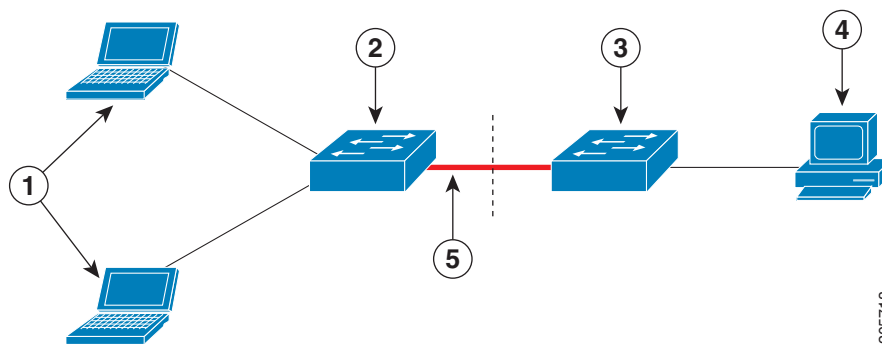
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

1 つ以上のサブリカント 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 または **multiauth** モードをイネーブルにできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

すべてのホスト モードで機能するように **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 Network Edge Access Topology (NEAT) のサブリカント スイッチで使用します。

- ホスト許可：許可済み（サブリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol (CISP) を使用して、サブリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します（図 10-6 を参照してください）。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サブリカント スイッチから着信する複数の VLAN 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** として設定します（この設定は **group** または **user** 設定で行うことができます）。

図 10-6 CISP を使用したオーセンティケータまたはサブリカント スイッチ



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

注意事項

- NEAT ポートは、他の認証ポートと同じコンフィギュレーションで設定できます。サブリカント スイッチが認証すると、ポート モードはベンダー固有属性 (VSA) に基づいてアクセスからトランクに変更されます (**device-traffic-class=switch**)。
- VSA はオーセンティケータ スイッチ ポート モードをアクセスからトランクに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします (任意の VLAN がネイティブ トランク VLAN に変換される場合)。VSA はサブリカントのポート コンフィギュレーションは変更しません。

- ホスト モードを変更して、オーセンティケータ スイッチ ポートの標準ポート コンフィギュレーションを適用するには、スイッチ VSA ではなく、Auto 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 ポートでサポートされていないコンフィギュレーションを削除して、ポート モードをアクセスからトランクに変更できます。詳細については、『*AutoSmartports Configuration Guide*』を参照してください。

詳細については、「NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定」(P.10-58) を参照してください。

ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用

スイッチは、入力ポートの IP 標準および IP 拡張ポートの Access Control List (ACL; アクセス コントロール リスト) の両方をサポートします。

- 設定する ACL
 - Access Control Server (ACS) からの ACL

シングル ホスト モードでの IEEE 802.1x ポートは、ACS からの ACL を使用して、異なるレベルのサービスを IEEE 802.1x 認証ユーザに提供します。RADIUS サーバは、このタイプのユーザおよびポートを認証する場合、ユーザ ID に基づいた ACL 属性をスイッチに送信します。送信された属性は、ユーザ セッション期間中、ポートに適用されます。セッションが終了、認証が失敗、またはリンクで故障が発生した場合、ポートは無許可になり、スイッチは ACL をポートから削除します。

ACS からの IP 標準および IP 拡張ポート ACL だけが Filter-Id 属性をサポートします。これは ACL の名前または番号を指定します。Filter-id 属性は、方向 (インバウンドまたはアウトバウンド)、およびユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id 属性は、グループの Filter-Id 属性よりも優先されます。
- ACS からの Filter-Id 属性が、すでに設定されている ACL を指定する場合、これは、ユーザ設定 ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id 属性を送信する場合、最後の属性だけが適用されます。

Filter-Id 属性がスイッチで定義されていない場合、認証が失敗し、ポートが無許可ステータスに戻ります。

コモン 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、表示コマンドや Management Information Base (MIB; 管理情報ベース) などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

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

次に、**show authentication** コマンドの出力にセッション ID が表示される例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```
Switch# show authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Fa4/0/4	0000.0000.0203	mab	DATA	Authz Success	160000050000000B288508E5

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

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

セッション ID は、NAD、AAA サーバ、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。

802.1x 認証の設定

ここでは、次の設定について説明します。

- 「802.1x 認証のデフォルト設定」 (P.10-33)
- 「802.1x 認証設定時の注意事項」 (P.10-34)
- 「802.1x 準備状態チェックの設定」 (P.10-36) (任意)
- 「音声対応 802.1x セキュリティの設定」 (P.10-37) (任意)
- 「802.1x 違反モードの設定」 (P.10-38) (任意)
- 「スイッチおよび RADIUS サーバ間の通信の設定」 (P.10-41) (必須)
- 「ホスト モードの設定」 (P.10-42) (任意)
- 「定期的な再認証の設定」 (P.10-43) (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.10-44) (任意)
- 「待機時間の変更」 (P.10-44) (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.10-45) (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.10-46) (任意)
- 「再認証回数の設定」 (P.10-46) (任意)
- 「802.1X アカウンティングの設定」 (P.10-48) (任意)
- 「MAC Move のイネーブル化」 (P.10-47) (任意)
- 「MAC 置換のイネーブル化」 (P.10-48) (任意)
- 「ゲスト VLAN の設定」 (P.10-49) (任意)
- 「制限付き VLAN の設定」 (P.10-50) (任意)
- 「アクセス不能認証バイパス機能の設定」 (P.10-52) (任意)
- 「WoL を使用した 802.1x 認証の設定」 (P.10-55) (任意)
- 「MAC 認証バイパスの設定」 (P.10-56) (任意)
- 「NAC レイヤ 2 802.1x 検証の設定」 (P.10-57) (任意)
- 「NEAT を使用したオーセンティケータ スイッチおよびサブリケータ スイッチの設定」 (P.10-58)
- 「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定」 (P.10-60)
- 「柔軟な認証順序の設定」 (P.10-63)

- 「ポート上での 802.1x 認証のディセーブル化」(P.10-64) (任意)
- 「802.1x 認証設定のデフォルト値へのリセット」(P.10-65) (任意)

802.1x 認証のデフォルト設定

表 10-4 に、802.1x 認証のデフォルト設定を示します。

表 10-4 802.1x 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル (force-authorized) ポートはクライアントとの 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 <ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • Key 	<ul style="list-style-type: none"> • 指定なし • 1812 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔 (秒)	3600 秒
再認証回数	2 回 (ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数)
待機時間	60 秒 (スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数)
再送信時間	30 秒 (スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数)
最大再送信回数	2 回 (スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数)
クライアント タイムアウト時間	30 秒 (認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間)
認証サーバ タイムアウト時間	30 秒 (クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間) authentication timer server 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。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ (スイッチ) モード	指定なし

表 10-4 802.1x 認証のデフォルト設定 (続き)

機能	デフォルト設定
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1x 認証」(P.10-34)
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」(P.10-35)
- 「MAC 認証バイパス」(P.10-36)
- 「ポートあたりのデバイスの最大数」(P.10-36)

802.1x 認証

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポート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後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルータード 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、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、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、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、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。
- 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.10-9) 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

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- 802.1X 認証をプライベート VLAN ポートに設定できますが、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた 802.1X 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッド ポート) または トランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- 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 を設定した後、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軽減します (**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、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 を稼働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タスの場合、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 クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
 - 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 ステータスをクリティカル認証ステータスに変更し、制限付き VLAN に残ります。

- 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

- 特に明記していない限り、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。詳細については、「802.1x 認証」(P.10-34) を参照してください。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポートステータスに影響はありません。
- ポートが未許可ステータスであり、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、ポートは未許可ステータスのままです。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ると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステータスにない場合、再認証が行われるまでポートはこのステータスを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ~ 65535 秒です。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングルホストモードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証 (MDA) モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホストモードの場合、1 台の 802.1x サブリカントだけがポートで許可されます。ただし、アクセス VLAN で許可される 802.1x 非対応ホストの数には制限はありません。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされ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と、スイッチスタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに回答すると、802.1x 対応です。クライアントがタイムアウト時間内に回答すると 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回答しない場合、クライアントは 802.1x に対応していません。Syslog メッセージは生成されません。

- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

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

	コマンド	目的
ステップ 1	dot1x test eapol-capable [interface interface-id]	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 (任意) <i>interface-id</i> には、802.1x 準備状態チェックを実行するポートを指定します。 (注) オプションの interface キーワードを省略した場合、スイッチ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 2	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 3	dot1x test timeout timeout	(任意) EAPOL 応答の待機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。デフォルトは 10 秒です。
ステップ 4	end	(任意) 特権 EXEC モードに戻ります。
ステップ 5	show running-config	(任意) 変更したタイムアウト値を確認します。

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

```
switch# dot1x test eapol-capable interface gigabitethernet0/2
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/2 is EAPOL capable
```

音声対応 802.1x セキュリティの設定

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

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

- errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。



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

- **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、errdisable リカバリを設定すると、ポートは自動的に再びイネーブルにされます。errdisable リカバリがポートで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びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface interface-id vlan [vlan-list]** 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause security-violation shutdown vlan	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 (注) shutdown vlan キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。
ステップ 3	errdisable recovery cause security-violation	(任意) 自動 VLAN 単位エラー リカバリをイネーブルにします。
ステップ 4	clear errdisable interface interface-id vlan [vlan-list]	(任意) errdisable になっている個々の VLAN を再びイネーブルにします。 <ul style="list-style-type: none"> • <i>interface-id</i> の場合、個々の VLAN を再びイネーブルにするポートを指定します。 • (任意) <i>vlan-list</i> の場合、再びイネーブルにする VLAN のリストを指定します。<i>vlan-list</i> を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	shutdown no-shutdown	(任意) errdisable の VLAN を再びイネーブルにして、すべての errdisable 指示をクリアします。
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任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

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

次の例では、errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet0/2 vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 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
- ポートで認証されるデバイスの最大数に達した

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication dot1x {default} method1</code>	802.1x 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用方法になっている方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 <i>method1</i> には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ スtring に表示されますが、サポートされていません。
ステップ 4	<code>interface interface-id</code>	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	<code>switchport mode access</code>	ポートをアクセス モードにします。
ステップ 6	<code>authentication violation {shutdown restrict protect replace}</code>	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。 <ul style="list-style-type: none"> • shutdown : ポートを errordisable 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すべての新しいデバイスから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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show authentication</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(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、認証、許可、アカウントिंग (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トング 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。

802.1x 認証の設定

- ステップ 6** スイッチが仮のアカウントिंग アップデートを、再認証結果に基づいたアカウントिंग 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トिंग 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	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication dot1x {default} method1</code>	802.1x 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用している方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 <i>method1</i> には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ スtringに表示されますが、サポートされていません。
ステップ 4	<code>dot1x system-auth-control</code>	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	<code>aaa authorization network {default} group radius</code>	(任意) ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定は、デフォルトです。
ステップ 6	<code>radius-server host ip-address</code>	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7	<code>radius-server key string</code>	(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キーを指定します。
ステップ 8	<code>interface interface-id</code>	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	<code>switchport mode access</code>	(任意) ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10	<code>authentication port-control auto</code>	ポート上で 802.1x 認証をイネーブルにします。 機能の相互作用については、「802.1x 認証設定時の注意事項」(P.10-34)を参照してください。
ステップ 11	<code>dot1x pae authenticator</code>	インターフェイスのポートアクセス エンティティを、オーセンティケータとしてのみ動作し、サブリカント用のメッセージは無視するように設定します。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show authentication</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(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	<code>configure terminal</code>	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	<code>radius-server host {hostname ip-address} auth-port port-number key string</code>	<p>RADIUS サーバ パラメータを設定します。</p> <p><code>hostname ip-address</code> 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。</p> <p><code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 です。指定できる範囲は 0 ~ 65536 です。</p> <p><code>key string</code> には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。<code>key</code> は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。</p> <p>(注) キー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、キーは必ず <code>radius-server host</code> コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。</p> <p>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。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、IP アドレス 172.20.39.46 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、暗号キーを RADIUS サーバ上のキーと同じ `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
```

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

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

ホスト モードの設定

802.1X 認証済みポート上でシングルホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。**multi-domain** キーワードを使用して、マルチドメイン認証（MDA）を設定し、同じスイッチ ポート上の IP Phone（シスコ製品または他社製品）など、ホストと音声デバイスの両方の認証をイネーブルにします。

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 vsa send authentication	VSA（Vendor-Specific Attribute; ベンダー固有属性）を認識し使用するために、ネットワーク アクセス サーバを設定します。
ステップ 3	interface interface-id	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	authentication host-mode [multi-auth multi-domain multi-host single-host]	<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> multi-auth : 音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。各ホストは個別に認証されます。 <p>(注) multi-auth キーワードを使用できるのは、authentication host-mode コマンドだけです。</p> <ul style="list-style-type: none"> multi-host : シングル ホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。 multi-domain : IP Phone（シスコ製または他社製）など、ホストおよび音声の両方のデバイスを 802.1x 許可ポートで認証できるようにします。 <p>(注) ホスト モードが multi-domain に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 16 章「音声 VLAN の設定」を参照してください。</p> <ul style="list-style-type: none"> single-host : 802.1x 許可ポートでシングル ホスト（クライアント）の接続を許可します。 <p>指定するインターフェイスで、authentication port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。</p>
ステップ 5	switchport voice vlan vlan-id	(任意) 音声 VLAN を設定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface interface-id	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート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 gigabitethernet0/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにして、ポートでホストおよび音声デバイスの両方を許可する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication 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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>authentication periodic</code>	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。 (注) デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチで RADIUS-provided セッション タイムアウトを使用するには、 <code>authentication timer reauthenticate</code> コマンドを入力します。
ステップ 4	<code>authentication timer {{{inactivity reauthenticate}}} {restart value}}</code>	再認証の試行の間隔（秒）を設定します。 <code>authentication timer</code> キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> inactivity : クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位）。 reauthenticate : 自動再認証が開始するまでの時間（秒単位）。 restart value : 無許可ポートの認証を試行するまでの間隔（秒単位）。 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show authentication interface interface-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの再認証試行間隔に戻すには、**no 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)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 4000
```

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface interface-id 特権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブまたはディセーブルにする方法については、「[定期的な再認証の設定](#)」(P.10-43)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 gigabitethernet0/2
```

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer inactivity** インターフェイス コンフィギュレーション コマンドは、アイドル時間を制御します。クライアント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	authentication timer inactivity seconds	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの待機時間に戻すには、**no authentication timer inactivity** 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)# authentication timer inactivity 30
```

スイッチからクライアントへの再送信時間の変更

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



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

スイッチがクライアント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	authentication timer reauthenticate 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 interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの再送信時間に戻すには、**no authentication timer reauthenticate** 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)# authentication timer reauthenticate 60
```

スイッチからクライアントへのフレーム再送信回数の設定

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



(注)

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

スイッチ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。デフォルト値は 2 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	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-reauth-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下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	dot1x max-req count	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォルトは 2 です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show authentication interface interface-id	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。

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

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

MAC Move のイネーブル化

MAC Move を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC Move をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	authentication mac-move permit	スイッチで MAC Move をイネーブルにします。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	(任意) 設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>authentication violation {protect replace restrict shutdown}</code>	<p>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。</p> <p>他のキーワードは、次のような機能があります。</p> <ul style="list-style-type: none"> • 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 <code>errdisable</code> になります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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トリングタスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>aaa accounting dot1x default start-stop group radius</code>	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	<code>aaa accounting system default start-stop group radius</code>	(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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.10-34) を参照してください。

	コマンド	目的
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	ポート上で 802.1x 認証をイネーブルにします。
ステップ 5	authentication event no-response action authorize vlan <i>vlan-id</i>	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 <i>interface-id</i>	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 authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステータスに戻ります。

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 gigabitethernet0/2
Switch(config-if)# authentication event no-response action authorize 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)# authentication timer inactivity 3
Switch(config-if)# authentication timer reauthenticate 15
Switch(config-if)# authentication event no-response action authorize vlan 2
```

制限付き VLAN の設定

スイッチ上に制限付き VLAN を設定している、認証サーバが有効なユーザ名またはパスワードを受信できない場合と、802.1X に準拠した場合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 モードでのみ制限付き 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 <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.10-34) 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。

	コマンド	目的
ステップ 4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
ステップ 5	authentication event fail action authorize vlan-id	アクティブ VLAN を 802.1x 制限付き 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 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 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 authentication event fail action authorize 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 IEEE 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 gigabitethernet0/2
Switch(config-if)# authentication event fail action authorize 2
```

ユーザに制限付き VLAN を割り当てる前に、**authentication event retry retry count** 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。指定できる認証試行回数は 1 ~ 3 回です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1x 認証設定時の注意事項 」(P.10-34) 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	ポート上で 802.1x 認証をイネーブルにします。
ステップ 5	authentication event fail action authorize vlan-id	アクティブ VLAN を 802.1x 制限付き 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 制限付き VLAN として設定できます。
ステップ 6	authentication event retry retry count	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ~ 3 です。デフォルトは 3 です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show authentication interface 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。

デフォルト値に戻すには、**no authentication event retry** 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)# authentication event retry 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 <i>dead</i> 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 <i>time</i> の範囲は 1 ~ 120 秒です。スイッチは、デフォルトの <i>seconds</i> 値を 10 ~ 60 秒の間で動的に決定します。 指定できる <i>tries</i> の範囲は 1 ~ 100 です。スイッチは、デフォルトの <i>tries</i> パラメータを 10 ~ 100 の間で動的に決定します。
ステップ 3	radius-server deadtime minutes	(任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ~ 1440 分 (24 時間) です。デフォルト値は 0 分です。

コマンド	目的
ステップ4 radius-server host <i>ip-address</i> [acct-port <i>udp-port</i>] [auth-port <i>udp-port</i>] [test username <i>name</i> [idle-time <i>time</i>] [ignore-acct-port] [ignore-auth-port] [key <i>string</i>]	(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。 <ul style="list-style-type: none"> • acct-port <i>udp-port</i> : 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 <i>udp-port</i> : 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。 <ul style="list-style-type: none"> • test username <i>name</i> : 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 <i>time</i> : スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ~ 35791 分です。デフォルトは 60 分 (1 時間) です。 • ignore-acct-port : RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • ignore-auth-port : RADIUS サーバ認証ポートのテストをディセーブルにします。 • key <i>string</i> : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号キーを指定します。 (注) キー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、キーは必ず radius-server host コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 <p>radius-server key {0 <i>string</i> 7 <i>string</i> <i>string</i>} 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キーを設定できます。</p>
ステップ5 dot1x critical { eapol recovery delay <i>milliseconds</i> }	(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。 <p>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。</p> <p>recovery delay <i>milliseconds</i> : 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)。</p>
ステップ6 interface <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1x 認証設定時の注意事項 」(P.10-34) を参照してください。
ステップ7 authentication event server dead action [authorize reinitialize] vlan <i>vlan-id</i>	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 <ul style="list-style-type: none"> • authorize : 認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。 • reinitialize : ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。

	コマンド	目的
ステップ 8	authentication event server dead action {authorize reinitialize} vlan <i>vlan-id</i>	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。 <ul style="list-style-type: none"> • authorize : ポートを認証します。 • reinitialize : すべての許可済みのクライアントを再初期化します。
ステップ 9	authentication server dead action authorize [vlan]	ACS サーバがダウンしている場合は、アクセス VLAN または設定された VLAN (VLAN が指定されている場合) のスイッチを許可します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show authentication interface <i>interface-id</i>	(任意) 設定を確認します。
ステップ 12	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をデフォルトの設定に戻すには、**no authentication event server dead action {authorize | reinitialize}** 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 authentication event server dead action** 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 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	<code>configure terminal</code>	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	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1x 認証設定時の注意事項 」(P.10-34) を参照してください。
ステップ 3	<code>authentication control-direction {both in}</code>	<p>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。</p> <ul style="list-style-type: none"> both : ポートを双方向に設定します。ポートは、ホストに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、ホストにパケットを送信できますが、受信はできません。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show authentication interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 authentication control-direction** インターフェイス コンフィギュレーション コマンドを使用します。

次に、WoL を使用した 802.1x 認証をイネーブルにして、ポートを双方向に設定する例を示します。

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

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.10-34) を参照してください。
ステップ 3	authentication 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	authentication order [mab] {webauth}	認証方式の順序を設定します。 <ul style="list-style-type: none"> • mab : 認証方式の順序に MAC Authentication Bypass (MAB; MAC 認証バイパス) を追加します。 • webauth : 認証方式の順序に Web 認証を追加します。
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 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 authentication order** 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)# authentication order
```

802.1x ユーザ ディストリビューションの設定

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

	コマンド	目的
ステップ 1	vlan group vlan-group-name vlan-list vlan-list	VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。
ステップ 2	show vlan group all vlan-group-name	設定を確認します。
ステップ 3	no vlan group vlan-group-name vlan-list vlan-list	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

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、VLAN グループ コンフィギュレーションおよび指定 VLAN と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、VLAN を既存の VLAN グループに追加し、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 を VLAN グループから削除する例を示します。

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

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

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

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

次の例では、すべての VLAN グループをクリアする方法を示します。

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

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

NAC レイヤ 2 802.1x 検証の設定

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

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	authentication event no-response action authorize 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	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	authentication timer reauthenticate	クライアントに対する再認証試行を設定します (1 時間に設定)。 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。

	コマンド	目的
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 <i>interface-id</i>	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 IEEE 802.1x 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
```

NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサブリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

概要については、「[Network Edge Access Topology \(NEAT\) を使用した 802.1x サブリカントおよびオーセンティケータ](#)」(P.10-29) を参照してください。



(注)

cisco-av-pairs は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サブリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

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) を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 <i>interface-id</i>	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

```
Switch# configure terminal
Switch(config)# cisp enable
```

```
Switch(config)# interface gigabitethernet0/1
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
```

スイッチをサブ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 クレデンシヤル プロファイルを作成します。これは、サブリカントとして設定されるポートに接続する必要があります。
ステップ 4	username suppswitch	ユーザ名を作成します。
ステップ 5	password password	新しいユーザ名のパスワードを作成します。
ステップ 6	dot1x supplicant force-multicast	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。これにより、NEAT がすべてのホスト モードでのサブリカントスイッチで機能できるようにもなります。
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ポート アクセス エンティティ (PAE) をサブリカントとして設定します。
ステップ 11	dot1x credentials profile-name	802.1x クレデンシヤル プロファイルをインターフェイスに接続します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show running-config interface interface-id	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチをサブリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet0/1
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、オーセンティケータ スイッチを設定することもできます。詳細については、『*Auto Smartports Configuration Guide*』を参照してください。

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

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。詳細については、[Cisco Secure ACS コンフィギュレーション ガイド](#)を参照してください。



(注) スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で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。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキング テーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip device tracking</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa authorization network default group radius</code>	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、 <code>no aaa authorization network default group radius</code> コマンドを使用します。
ステップ 5	<code>radius-server vsa send authentication</code>	<code>radius vsa send authentication</code> を設定します。
ステップ 6	<code>interface interface-id</code>	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	<code>ip access-group acl-id in</code>	ポートの入力方向のデフォルト ACL を設定します。 (注) <code>acl-id</code> はアクセス リストの名前または番号です。
ステップ 8	<code>show running-config interface interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで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	送信元アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。 access-list-number には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は deny 、許可する場合は permit を指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビット長の値。 source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。source-wildcard 値を入力する必要はありません。 source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。 (任意) source-wildcard ビットを送信元アドレスに適用します。 (任意) ログを入力して、エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します。
ステップ3	interface interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ip access-group acl-id in	ポートの入力方向のデフォルト 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	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 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。 <ul style="list-style-type: none"> count count : スイッチが ARP プロ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。デフォルトは 3 です。 interval interval : スイッチが ARP プロ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使用するために、ネットワーク アクセス サーバを設定します。 (注) ダウンロード可能な ACL が機能する必要があります。

	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、ダウンロード ポリシーのスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default 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 gigabitethernet0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベース 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 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 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。**debug radius accounting** 特権 EXEC コマンドを使用して RADIUS 属性 32 を確認できます。このコマンドの詳細については、『Cisco IOS Debug Command Reference, Release 12.2』を参照してください。
http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

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

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

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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>authentication order [dot1x mab] {webauth}</code>	(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	<code>authentication priority [dot1x mab] {webauth}</code>	(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	<code>show authentication</code>	(任意) 設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 認証を試行してから Web 認証をフォールバック方法として設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>authentication control-direction {both in}</code>	(任意) ポート制御を単一方向モードまたは双方向モードに設定します。
ステップ 4	<code>authentication fallback name</code>	(任意) 802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 5	<code>authentication host-mode [multi-auth multi-domain multi-host single-host]</code>	(任意) ポート上で認証マネージャ モードを設定します。
ステップ 6	<code>authentication open</code>	(任意) ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	<code>authentication order [dot1x mab] {webauth}</code>	(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	<code>authentication periodic</code>	(任意) ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 9	<code>authentication port-control {auto force-authorized force-un authorized}</code>	(任意) ポートの許可ステータスの手動制御をイネーブルにします。

	コマンド	目的
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。

次の例では、ポートの Open1x を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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
```

ポート上での 802.1x 認証のディセーブル化

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

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no dot1x pae	ポート上で 802.1x 認証をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x Port Access Entity (PAE; ポート アクセス エンティティ) オーセンティケータとしてポートを設定するには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで 802.1x がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次の例では、ポートの 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x default</code>	802.1x パラメータをデフォルト値に戻します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show authentication interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x の統計情報およびステータスの表示

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

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

Cisco IOS Release 12.2(55)SE 以降では、`no dot1x logging verbose` グローバル コンフィギュレーション コマンドを使用して、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.10-9) 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。

