IEEE 802.1X ポートベースの認証

- 「802.1X 認証の前提条件」（P.83-1）
- 「802.1X 認証の制約事項」（P.83-2）
- 「802.1X ポートベース認証について」（P.83-6）
- 「802.1X ポートベース認証のデフォルト設定」（P.83-31）
- 「802.1X ポートベース認証の設定方法」（P.83-32）
- 「認証のステータスおよび情報の表示」（P.83-58）

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

802.1X 認証の前提条件

なし。

802.1X 認証の制約事項

- 「802.1X 認証」（P.83-2）
- 「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.83-4）
- 「MAC 認証バイパス」（P.83-5）
- 「Web ベース認証」（P.83-5）
- 「ネットワーク エッジ アクセス トポロジ（NEAT）と Client Information Signalling Protocol（CISP）」（P.83-6）

802.1X 認証

- 802.1X 認証をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1X 対応ポートのモードを（たとえばアクセスからトランクに）変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
- 推奨しませんが、ポート セキュリティと 802.1X ポートベース認証は同じポート上に設定できます。

（注）　802.1X 認証は、sticky MAC アドレスまたはスタティック セキュア MAC アドレスによるポート セキュリティと互換性がありません。リリース 15.1(1) SY1 以降では、sticky MAC アドレスまたはスタティック セキュア MAC アドレスによるポート セキュリティと合わせて 802.1X 認証を設定できません。

- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、RADIUS サーバが割り当てた VLAN に割り当てられているポートが、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、ディセーブル化、または削除された場合、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 のスタティック アクセス ポート、音声 VLAN ポート、レイヤ 3 ルーテッド ポートではサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示されてポート モードは変更されません。
  - ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートをダイナミック VLAN 割り当てに変更しようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

  - EtherChannel ポート：EtherChannel のアクティブ メンバであるポートまたはまだアクティブになっていないポートを 802.1X ポートとして設定しないでください。EtherChannel ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートで 802.1X 認証をイネーブルにすることができます。ただし、SPAN または RSPAN 宛先ポートとしてポートが削除されるまで 802.1X 認証はディセーブルです。SPAN または RSPAN 送信元ポートでは 802.1X 認証をイネーブルにできます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1X 認証をグローバルにイネーブルにする前に、802.1X 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- 認証されていないホストからのトラフィックはすべてスイッチ プロセッサに転送されるので、このトラフィックにレート制限を適用することを推奨します。

802.1X ホスト モード

- ポート上でホスト モードが変更されると、ほとんどの場合、そのポート上の既存の 802.1X 認証は削除されます。ただし、シングルホスト モードから他のモードへの変更時とマルチドメイン モードからマルチ認証モードへの変更時は例外です。これら 2 つの場合は、既存の 802.1X 認証が維持されます。
- **authentication open** インターフェイス コンフィギュレーション コマンドを入力すると、認証が成功する前でも、ポートで検出された新しい MAC アドレスは、ネットワークに対して無制限のレイヤ 2 アクセスが許可されます。このコマンドを使用する場合は、デフォルトのスタティック ACL を使用してレイヤ 3 トラフィックを制限する必要があります。詳細については、「認証前オープン アクセス」（P.83-15）を参照してください。
- マルチホスト モードを設定すると、マルチホスト ポートが無許可になった場合（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。
- MDA ホスト モードを設定すると、サードパーティ製 IP Phone の MAC アドレスは最初はデータ VLAN に割り当てられます。タグ付き音声パケットが確認されると、装置はデータ VLAN から削除され、音声 VLAN に配置されます。
- マルチ認証ホスト モードを設定する場合は、次の注意事項に留意してください。
  - マルチ認証ポートの 1 つのクライアントが無許可ステートになった場合（再認証が失敗した場合、またはそのクライアントから EAPOL ログオフ メッセージを受信した場合）、接続された他のクライアントの許可ステータスは変更されません。
  - RADIUS が割り当てた VLAN は、マルチ認証ポートではサポートされません。1 つのデータ VLAN しか持つことができないためです。認証サーバが VLAN 関連の属性を送信した場合、認証は成功しますが、VLAN 割り当ては無視されます。
  - データ VLAN では複数のホストが許可されますが、音声 VLAN で許可されるホストは 1 つだけです。1 つの IP Phone が認証されている場合、同じポートの他の IP Phone は認証を拒否されます。
  - マルチ認証ポートでは、ゲスト VLAN、認証失敗 VLAN、またはクリティカル VLAN はサポートされません。

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 認証がポートでイネーブルになっている場合、音声 VLAN と同じポート VLAN を設定できません。
- VLAN 割り当て機能を使った 802.1X 認証は、トランク ポート上、ダイナミック ポート上、および VMPS を介したダイナミックアクセス ポート割り当てではサポートされません。
- RSPAN VLAN、プライベート プライマリ PVLAN、または音声 VLAN を除き、任意の 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 を設定したあとで、ホスト IP アドレスを DHCP サーバから取得する必要がある場合もあります。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（**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド）の設定を減らします。設定を減らす量は、接続されている 802.1X クライアントのタイプによって異なります。
- 802.1X VLAN ユーザ分散機能を設定する場合は、次の注意事項に従ってください。
  - 最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。
  - 1 つの VLAN を複数の VLAN グループにマッピングできます。
  - VLAN グループにはゲスト VLAN、クリティカル VLAN、または制限 VLAN をマッピングできます。
  - VLAN グループ名を guest VLAN、critical VLAN、または restricted VLAN として指定できません。
  - VLAN グループは VLAN を追加または削除することで変更できますが、少なくとも 1 つの VLAN が VLAN グループにマッピングされている必要があります。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。
  - VLAN グループ名から既存の VLAN を削除した場合、その VLAN にあるポートの認証ステータスは取り消されませんが、マッピングは既存の VLAN グループから削除されます。
  - 既存の VLAN グループ名を削除した場合、そのグループ内の VLAN にあるポートの認証ステータスは取り消されませんが、その VLAN グループへの VLAN マッピングは削除されます。
- 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。
  - アクセス不能認証バイパス機能は、シングルホスト モード、マルチホスト モード、および MDA 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トの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Widows XP クライアントが DHCP 用に設定されていて、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-Success メッセージを受信しても DHCP 設定プロセスが再開されない場合があります。

  - アクセス不能認証バイパス機能とクリティカル VLAN を 802.1X ポートに設定することができます。スイッチがクリティカル VLAN 内のクリティカル ポートを再認証しようとして、すべての RADIUS サーバが利用不能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、ポートはクリティカル VLAN に残ります。
  - アクセス不能認証バイパス機能とポートセキュリティを同じポートに設定できます。
- RSPAN VLAN または音声 VLAN を除き、任意の VLAN を 802.1X 制限 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

- 特記されている場合を除き、MAC 認証バイパスの注意事項は、802.1X 認証の注意事項と同じです。詳細については、「802.1X 認証」（P.83-2）を参照してください。
- ポートが MAC アドレスにより許可されたあと、ポートの MAC 認証バイパスをディセーブルにする場合、ポート ステートに影響はありません。
- EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。
- ポートが未許可ステートであり、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トのままです。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た場合、スイッチは MAC 認証バイパスを使用してポートを再許可します。
- ポートが許可ステートの場合、再許可が発生するまでポートはこのステートのままになります。
- MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。
- 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任意で設定できます。指定できる範囲は 1 ～ 65535 秒ですが、再認証タイムアウトよりも小さい値に設定する必要があります。タイムアウト値を設定する前に、ポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定方法」（P.85-5）を参照してください。

Web ベース認証

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

Web ベース認証の設定方法の詳細については、第 84 章「Web ベース認証」を参照してください。

ネットワーク エッジ アクセス トポロジ（NEAT）と Client Information Signalling Protocol（CISP）

- 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。サプ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 はサプリカントのポート コンフィギュレーションは変更しません。

802.1X ポートベース認証について

- 「802.1X の概要」（P.83-6）
- 「802.1x デバイスの役割」（P.83-7）
- 「ポートベース認証プロセス」（P.83-8）
- 「認証の開始およびメッセージ交換」（P.83-10）
- 「許可ステートおよび無許可ステートのポート」（P.83-12）
- 「802.1X ホスト モード」（P.83-13）
- 「DHCP スヌーピングを使用した 802.1X 認証」（P.83-16）
- 「802.1X アカウンティング」（P.83-16）
- 「VLAN 割り当てを使用した 802.1X 認証」（P.83-17）
- 「VLAN 割り当てでの複数 VLAN および VLAN ユーザ分散」（P.83-19）
- 「ゲスト VLAN を使用した 802.1X 認証」（P.83-19）
- 「制限付き VLAN を使用した 802.1X 認証」（P.83-20）
- 「アクセス不能認証バイパスを使用した 802.1X 認証」（P.83-21）
- 「音声 VLAN ポートを使用した 802.1X 認証」（P.83-22）
- 「ポート セキュリティを使用した 802.1X 認証」（P.83-23）
- 「ACL 割り当てとリダイレクト URL を使用した 802.1X 認証」（P.83-23）
- 「ポート ディスクリプタを使用した 802.1X 認証」（P.83-26）
- 「MAC 認証バイパスを使用した 802.1X 認証」（P.83-26）
- 「Network Admission Control レイヤ 2 IEEE 802.1X 検証」（P.83-27）
- 「Wake-on-LAN を使用した 802.1X 認証」（P.83-28）

802.1X の概要

ここでは、認証、許可、アカウンティング（AAA）の一部として IEEE 802.1X ポートベース認証のロールについて説明します。802.1X 規格は、クライアントおよびサーバ ベースのアクセス コントロールと認証プロトコルについて定義しており、不正なクライアントが公的にアクセス可能なポートを介し

て LAN に接続することを制限しています。認証サーバは、スイッチ ポートに接続する各クライアントを認証し、ポートを VLAN に割り当てたうえで、スイッチや LAN によって提供されるサービスを利用できるようにします。

802.1X アクセス コントロールでは、クライアントが認証されるまで、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）トラフィックだけが許可されます。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

802.1x デバイスの役割

802.1X ポートベース認証では、図 83-1 に示すように、ネットワーク上の装置にはそれぞれ特定のロールがあります。

図 83-1　802.1x デバイスの役割

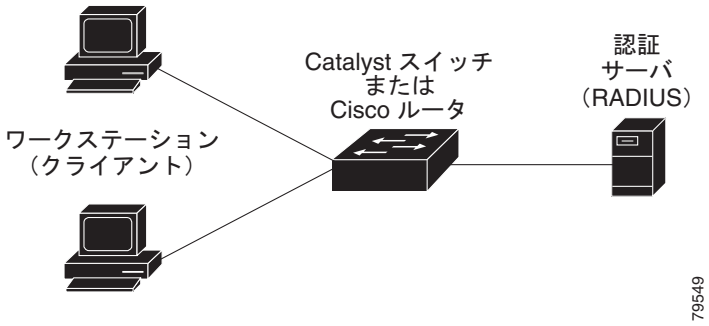


図 83-1 に示す特定の役割は、次のとおりです。

- *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て、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。（クライアントは、IEEE 802.1X 規格では*サプリカント*といいます）。

  （注） Windows XP のネットワーク接続および 802.1X ポートベース認証の問題に関しては、次の URL にある Microsoft Knowledge Base を参照してください。
  http://support.microsoft.com/kb/q303597/

- *認証サーバ*：実際にクライアントの認証を行います。認証サーバはクライアントの識別情報を確認し、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。認証サーバとして、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 システムだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server（ACS）Version 3.0 で使用可能です。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（オーセンティケータおよびバックエンドのオーセンティケータともいう）*：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的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

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

ポートベース認証プロセス

802.1X ポートベース認証をイネーブルにすると、次のようなイベントが発生します。

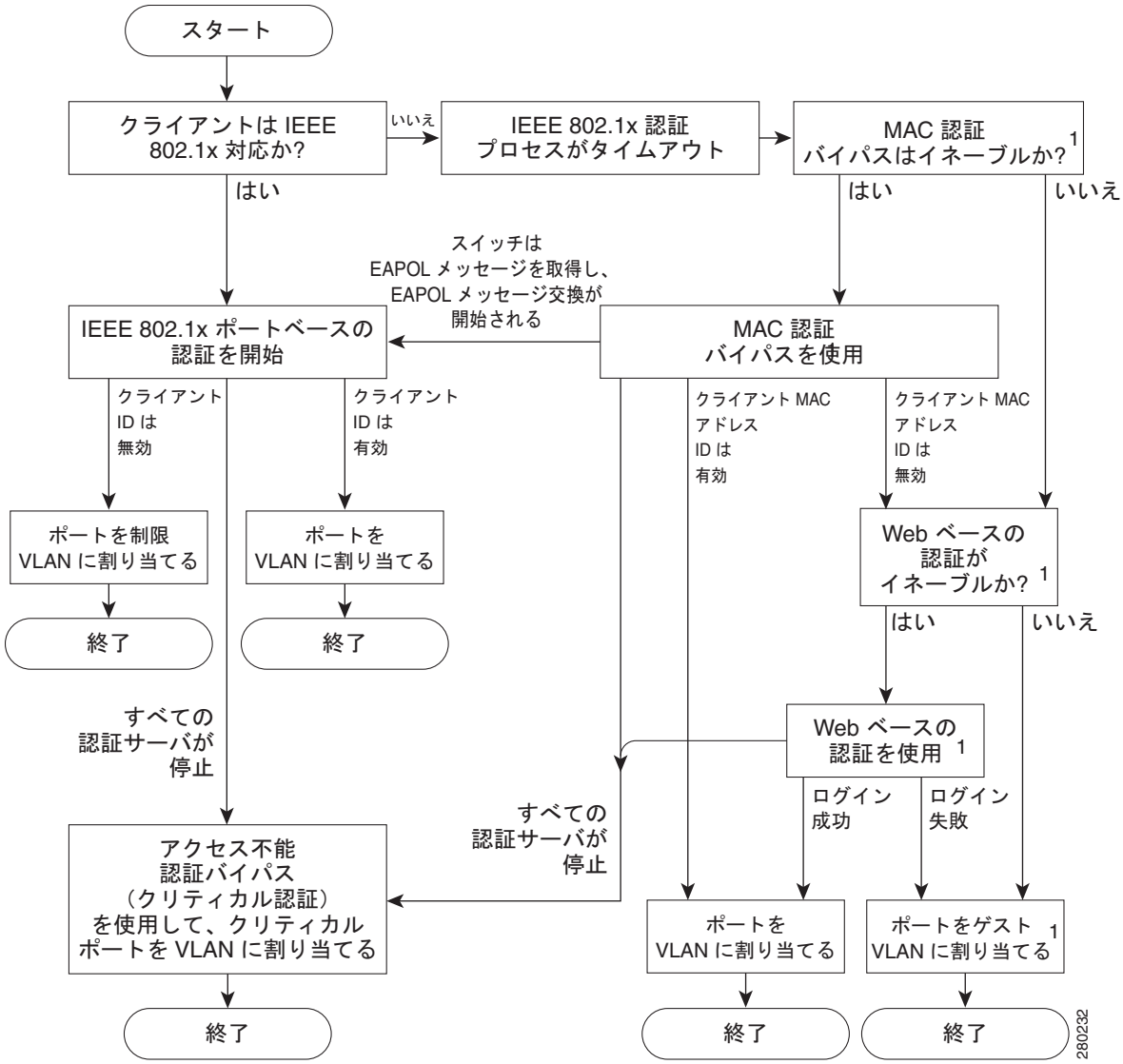
- クライアントが 802.1X 準拠クライアント ソフトウェアをサポートしており、クライアントの ID が有効である場合、802.1X 認証は成功し、スイッチがクライアントに対してネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス（MAB）や Web ベース認証（webauth）などのフォールバック認証方式を使用できます（いずれかまたは両方がイネーブルになっている場合）。
  - MAC 認証バイパスがイネーブルの場合、スイッチは許可のためにクライアントの MAC アドレスを AAA サーバにリレーします。クライアントの MAC アドレスが有効であれば、正常に許可され、スイッチがクライアントに対してネットワークへのアクセスを許可します。
  - Web ベース認証がイネーブルの場合、スイッチは HTTP ログイン ページをクライアントに送信します。スイッチは許可のためにクライアントのユーザ名とパスワードを AAA サーバにリレーします。ログインが成功すると、スイッチがネットワークに対するクライアント アクセスを許可します。

（注）　認証方式のデフォルトの順序は、802.1X、次に MAB、次に Web ベース認証です。順序は変更でき、これらの方式のいずれかをディセーブルにすることもできます。

- フォールバック認証方式がイネーブルになっていない、または成功しない場合、ゲスト VLAN が設定されていれば、スイッチは限定的なサービスを提供するゲスト VLAN にクライアントを割り当てます。
- スイッチが 802.1X 対応クライアントから無効な ID を受信し、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（ダウンして）利用できず、アクセス不能認証バイパスがイネーブルの場合、ユーザ指定のクリティカル VLAN 内でポートをクリティカル認証ステートにすることで、スイッチがクライアントに対してネットワークへのアクセスを許可します。

（注）　アクセス不能認証バイパスは、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。

図 83-2　認証フローチャート



1 = これはスイッチがクライアントから EAPOL パケットを検出できない場合に発生する

スイッチは、次のいずれかの状況が発生するとクライアントを再認証します。

- 定期再認証がイネーブルで、再認証タイマーが満了した場合。

  スイッチ固有の値を使用するか、RADIUS サーバの値に基づいて、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 認証が設定されていると、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]）は、再認証が発生するまでの時間を指定します。

Termination-Action RADIUS 属性（属性 [29]）は、再認証中に実行す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。初期化アクションが設定されている場合（属性値は DEFAULT）、802.1X セッションが終了して、再認証中に接続は失われます。再認証アクションが設定されている場合（属性値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- **dot1x re-authenticate interface** *type slot/port* 特権 EXEC コマンドを入力して、クライアントを手動で再認証した場合。

認証の開始およびメッセージ交換

スイッチまたはクライアントのどちらからでも、認証を開始できます。**dot1x pae authenticator** および **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した場合、スイッチはポートのリンク ステートがダウンからアップに移行したと判断した時点で、認証を開始しなければなりません。次に、スイッチは EAP 要求/アイデンティティ フレームをクライアントに送信して識別情報を要求します（一般に、スイッチは最初のアイデンティティ/要求フレームを送信して、そのあとで 1 つまたは複数の認証情報の要求を送信します）。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

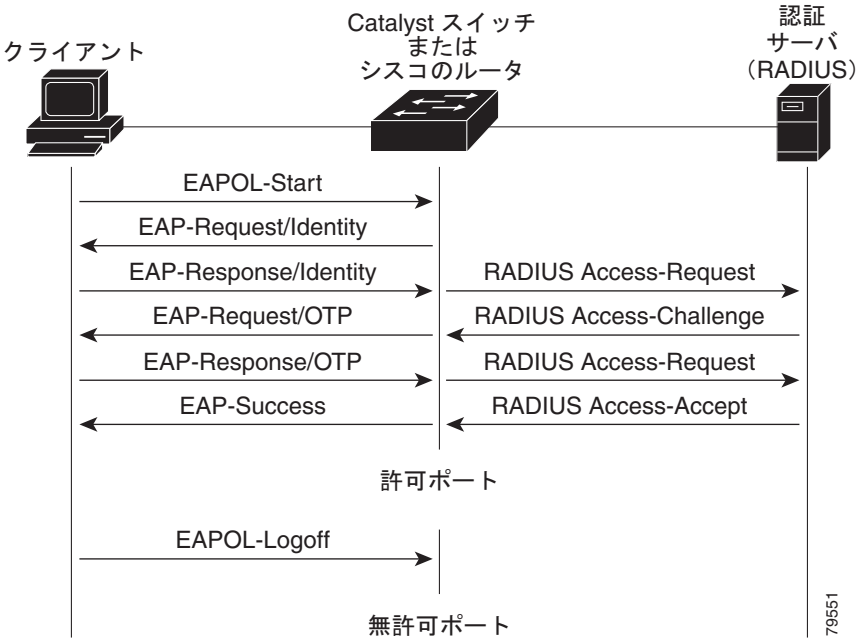
ただし、クライアントが起動時にスイッチから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）ネットワーク アクセス装置で 802.1X がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべてドロップされます。クライアントが認証の開始を 3 回試みても EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.83-12）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポート」（P.83-12）を参照してください。

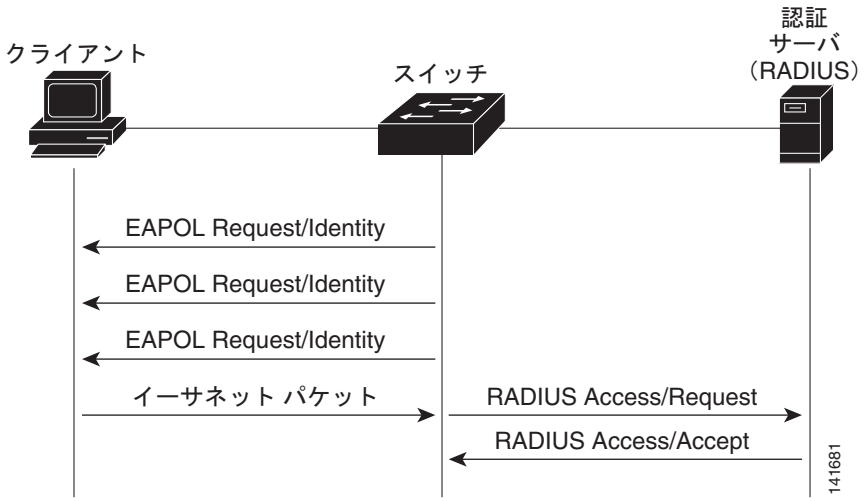
実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 83-3 に、クライアントが RADIUS サーバとの間でワンタイム パスワード（OTP）認証方式を使用する場合に行われるメッセージ交換を示します。

図 83-3　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。MAB 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 認証を開始します。

図 83-4　MAC 認証バイパス中のメッセージ交換



許可ステートおよび無許可ステートのポート

スイッチ ポートのステートによって、クライアントがネットワーク アクセスを許可されているかどうかがわかります。ポートは最初、*無許可*ステートです。ポートはこのステートにある間、802.1X プロトコル パケットを除いてすべての入力トラフィックおよび出力トラフィックを許容しません。クライアントの認証が成功すると、ポートは*許可*ステートに移行し、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。

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 ID 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 プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、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 ポートベースの認証をディセーブルにして、必要な認証交換をせずにポートを許可ステートに移行させます。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートを無許可ステートのままにして、クライアントが認証を試みてもすべて無視します。スイッチはインターフェイス経由でクライアントに認証サービスを提供できません。
- **auto**：802.1x ポートベースの認証をイネーブルにして、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。ネットワークへのアクセスを試行する各クライアントは、クライアントの MAC アドレスを使用してスイッチにより一意に識別されます。

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。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

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

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

802.1X ホスト モード

- 「ホスト モードの概要」（P.83-13）
- 「シングルホスト モード」（P.83-13）
- 「複数ホスト モード」（P.83-13）
- 「マルチドメイン認証モード」（P.83-14）
- 「マルチ認証の VLAN 割り当て」（P.83-15）
- 「マルチ認証モード」（P.83-15）
- 「認証前オープン アクセス」（P.83-15）

ホスト モードの概要

802.1X ポートのホスト モードによって、ポート上で複数のクライアントの認証が可能かどうかと、認証の実行方法が決まります。次の各項で説明する 4 つのホスト モードのいずれかを使用して、802.1X ポートを設定できます。さらに、各モードは、認証前オープン アクセスを許可するように変更される場合もあります。

シングルホスト モード

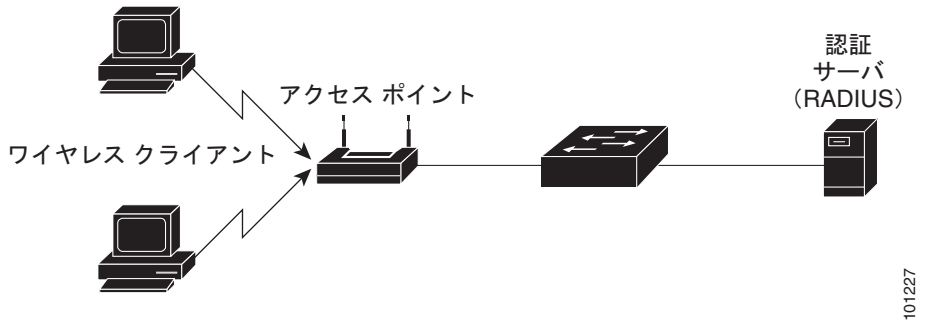
シングルホスト モード（図 83-1（P.83-7）を参照）では、802.1X 対応ポートには、クライアントが 1 つしか接続できません。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

複数ホスト モード

複数ホスト モードでは、複数のホストを 1 つの 802.1X 対応ポートに接続できます。図 83-5 に、ワイヤレス LAN における 802.1x ポート ベースの認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、スイッチは接続されたすべてのクライアントのネットワーク アクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

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

図 83-5　マルチ ホスト モードの例

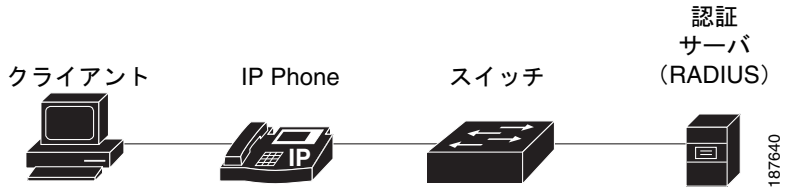


マルチドメイン認証モード

マルチドメイン認証（MDA）モードを使用すると、802.1X、MAC 認証バイパス（MAB）、または Web ベース認証（ホスト用のみ）を使用して、IP Phone（シスコ製またはサードパーティ製）と IP Phone の背後の単一のホストでそれぞれ独立して認証を実行できるようになります。この用途では、マルチドメインは 2 つのドメイン（データと音声）を意味し、ポートあたり 2 つの MAC アドレスだけが許可されます。スイッチではホストをデータ VLAN に、IP Phone を音声 VLAN に配置することができますが、これらは同じスイッチ ポート上にあるように見えます。データ VLAN 割り当ては、認証中に認証、許可、アカウンティング（AAA）サーバから受信されたベンダー固有属性（VSA）から取得することができます。

図 83-6 に、802.1X がイネーブルのポートに接続されている IP Phone に接続された単一ホストがある、典型的な MDA アプリケーションを示します。クライアントはスイッチに直接接続されないため、クライアントの接続が切断されても、スイッチでは、ポート リンクの切断を検出できません。切断されたクライアントの確立済みの認証を別のデバイスが使用する可能性を防ぐために、より最近の Cisco IP Phone は、接続されたクライアントのポートのリンク ステートに変更があったことをスイッチに通知するために、Cisco Discovery Protocol（CDP）のホストの存在を示す Type Length Value（TLV）を送信します。

図 83-6　マルチドメイン認証モードの例



マルチ認証の VLAN 割り当て

マルチ認証の VLAN 割り当てでは、次の状況が発生すると、既存のコマンドを使用してマルチ認証モードの RADIUS サーバから提供された VLAN の割り当てをサポートします。

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

（注）
- 1 つの音声 VLAN だけマルチ認証ポートでサポートされます。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードで設定できません。

マルチ認証モード

マルチ認証モードでは、音声 VLAN 上に 1 つの 802.1X/MAB クライアントと、データ VLAN 上に複数の認証済み 802.1X/MAB/Web 認証クライアントが許可されます。図 83-5 のように、ハブまたはアクセス ポイントが 802.1X ポートに接続される場合、マルチ認証モードでは、接続クライアントごとに認証を要求することで、マルチホスト モードよりもセキュリティが強化されます。802.1X 以外の装置では、個々のホストを認証するフォールバック方式として MAB または Web ベース認証を使用できるので、単一ポート上で異なるホストを異なる方式で認証することが可能になります。

また、マルチ認証では、認証サーバから受信した VSA に従って認証済み装置をデータ VLAN または音声 VLAN に割り当てることで、音声 VLAN での MDA 機能がサポートされます。

認証前オープン アクセス

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

認証前オープン アクセスは、ホスト モードの設定後に **authentication open** コマンドを入力することでイネーブルになり、設定済みのホスト モードの拡張として機能します。たとえば、シングルホスト モードで認証前オープン アクセスをイネーブルにした場合、ポートでは 1 つの MAC アドレスだけが許可されます。認証前オープン アクセスがイネーブルの場合、ポート上に設定されている 802.1X とは別の他のアクセス制限によってのみ、ポート上の初期トラフィックは、制限されます。ポートに 802.1X 以外のアクセス制限が設定されていない場合、クライアント装置は設定されている VLAN 上でフル アクセスが可能です。

DHCP スヌーピングを使用した 802.1X 認証

データ挿入機能を備えた Dynamic Host Configuration Protocol（DHCP）スヌーピングの Option 82 をイネーブルにすると、スイッチがクライアントの 802.1X 認証されたユーザ ID 情報を DHCP ディスカバリ プロセスに挿入でき、DHCP サーバによって別の IP アドレス プールの IP アドレスが別のエンド ユーザのクラスに割り当てられます。この機能により、アカウンティング目的でエンド ユーザに付与する IP アドレスのセキュリティを確保することができ、レイヤ 3 基準に基づいてサービスを許可することができます。

サプリカントと RADIUS サーバとの間で 802.1X 認証が成功すると、スイッチはポートをフォワーディング ステートに設定し、RADIUS サーバから受信した属性を格納します。DHCP スヌーピングを実行している場合、スイッチは DHCP リレー エージェントとして機能し、DHCP メッセージを受信し、別のインターフェイスで送信するためにこれらのメッセージを再度生成します。クライアントが 802.1X 認証後に DHCP ディスカバリ メッセージを送信すると、スイッチはパケットを受信します。スイッチは、保存されたクライアントの RADIUS 属性を含む RADIUS 属性サブオプション セクションをパケットに追加します。スイッチは、その後、ディスカバリ ブロードキャストを再度送信します。DHCP サーバは変更された DHCP ディスカバリ パケットを受信して、IP アドレス リースの作成時に認証済みユーザ ID 情報を使用することができます（設定されている場合）。ユーザと IP アドレスは、1 対 1、1 対多、多対多でマッピングできます。1 対多のマッピングを使用すれば、同一ユーザを複数ポートの 802.1X ホストで認証できます。

スイッチは、802.1X 認証機能とデータ挿入による DHCP スヌーピング Option 82 機能がイネーブルになると、自動的に認証済みユーザ ID 情報を挿入します。データ挿入による DHCP スヌーピング Option 82 を設定するには、「DHCP スヌーピングの Option 82 データ挿入」（P.78-6）を参照してください。

RADIUS 属性サブオプションに挿入されるデータの詳細については、RFC 4014「Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option」を参照してください。

802.1X アカウンティング

IEEE 802.1X 標準には、ネットワーク アクセスに対するユーザの許可と認証方法は定義されていますが、ネットワークの使用状況を追跡するものではありません。IEEE 802.1X アカウンティングは、デフォルトでディセーブルに設定されています。802.1X アカウンティングをイネーブルにすると、802.1X 対応ポートで次のアクティビティをモニタできます。

- 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。
- 再認証の正常な発生
- 再認証の失敗

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

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 セッションの開始時に送信されます。
- INTERIM：既存のセッション中にアップデートのために送信されます。
- STOP：セッション終了時に送信されます。

表 83-1 は AV ペアの一覧で、スイッチによって送信されるタイミングを示しています。

表 83-1　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	条件に応じて送信
			（注） Framed-IP-Address AV ペアは、DHCP スヌーピング バインディング テーブル内のホストに対して有効な DHCP バインディングが存在する場合にだけ送信されます。	
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [26]	Vendor-Specific	—	—	—
	（注） ベンダー固有属性（VSA）は、他の 802.1X 機能によって使用されます。			
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	非送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	非送信	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	非送信	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

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

VLAN 割り当てを使用した 802.1X 認証

ポートの 802.1X 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信してポートを設定します。RADIUS サーバはデータベースにユーザ名と VLAN マッピングを維持し、ポートに接続された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。

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。

- 802.1X 認証がポートでイネーブルになっており、RADIUS サーバからのすべての情報が有効である場合、ポートは認証後に RADIUS サーバが割り当てた VLAN に配置されます。
- マルチホスト モードが 802.1X ポートでイネーブルになっている場合、ポート上のすべてのホストが、最初に認証されたホストと同じ RADIUS サーバが割り当てた VLAN に配置されます。
- マルチ認証モードが 802.1X ポートでイネーブルになっている場合、VLAN 割り当ては無視されます。
- RADIUS サーバから VLAN 番号が提供されなかった場合、認証の成功後にポートはアクセス VLAN 内に設定されます。アクセス VLAN は、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1X 認証がイネーブルになっていても、RADIUS サーバからの VLAN 情報が有効でない場合は、ポートは無許可ステートに戻り、設定されたアクセス VLAN に残ります。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 ポートへの VLAN の指定、誤った VLAN ID、存在しないまたは内部（ルーテッド ポートの）の VLAN ID、あるいは音声 VLAN ID への割り当て試行、などがあります。
- 802.1X 認証がポートでディセーブルになっている場合、ポートは設定済みアクセス VLAN に戻されます。

ポートが強制許可、強制無許可、無許可、またはシャットダウン ステートの場合、ポートは設定済みアクセス VLAN に配置されます。

802.1X ポートが認証され、RADIUS サーバが割り当てた VLAN に配置された場合、ポートのアクセス VLAN 設定に対する変更はすべて有効になりません。

VLAN 割り当て機能を使った 802.1X 認証は、トランク ポート上、ダイナミック ポート上、および VLAN メンバーシップ ポリシー サーバ（VMPS）を介したダイナミックアクセス ポート割り当てではサポートされません。

VLAN 割り当てを設定するには、次の作業を行います。

ステップ 1　**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。

ステップ 2　802.1X 認証をイネーブルにします。

ステップ 3　アクセス ポートでの 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。

ステップ 4　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 名または VLAN ID

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 認証済みユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

VLAN 割り当てでの複数 VLAN および VLAN ユーザ分散

RADIUS が提供する VLAN 割り当てでは、複数の VLAN 間で 802.1X 認証済みユーザを分散してロード バランシングを実行できます。

以前のリリースでは、RADIUS サーバが認証中のユーザの割り当て用に提供できるのは、1 つの VLAN 名または ID でした。RADIUS サーバは、複数の VLAN 名と ID または複数の VLAN を含む VLAN グループの名前を提供できます。次の 2 つの方法のいずれかを使用して、異なる VLAN 間のユーザのロード バランシングを行います。

- 認証中のユーザに対する応答の一部として複数の VLAN ID または VLAN 名を送信するように、RADIUS サーバを設定します。802.1X VLAN ユーザ グループ機能は、特定の VLAN のユーザを追跡し、新たに認証されたユーザを、RADIUS が提供する VLAN ID の追加数が最も少ない VLAN に配置することで、ロード バランシングを実現します。

  「VLAN 割り当てを使用した 802.1X 認証」（P.83-17）に記載された手順を実行します（次の例外を除く）。

  属性 [81] Tunnel-Private-Group-ID は、複数の VLAN 名または VLAN ID を指定します。

- 複数の VLAN を含む VLAN グループを定義します。認証中のユーザに対する応答の一部として、VLAN ID の代わりに VLAN グループ名を提供するように、RADIUS サーバを設定します。提供された VLAN グループ名が定義済みの VLAN グループ名の中に見つかった場合、新たに認証されたユーザは、VLAN グループ内でユーザ追加数が最も少ない VLAN に配置されます。

  「VLAN 割り当てを使用した 802.1X 認証」（P.83-17）に記載された手順を実行します（次の例外を除く）。

  属性 [81] Tunnel-Private-Group-ID は、定義済みの VLAN グループ名を指定します。

詳細については、「VLAN ユーザ分散の設定」（P.83-45）を参照してください。

ゲスト VLAN を使用した 802.1X 認証

スイッチの各 802.1X ポートにゲスト VLAN を設定し、802.1X クライアント ソフトウェアをダウンロードするなど、802.1X に準拠していない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。これらのクライアントは 802.1X 認証用にシステムをアップグレードできる場合もありますが、一部のホストには（Windows 98 システムなど）802.1X 対応でないものもあります。

802.1X ポート上でゲスト VLAN をイネーブルにすると、スイッチが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合や、EAPOL パケットがクライアントから送信されず、フォールバック認証方式がイネーブルになっていない場合に、スイッチはクライアントをゲスト VLAN に割り当てます。

さらに、スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間内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 対応サプリカント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になると EAPOL パケット履歴はクリアされます。

dot1x guest-vlan supplicant グローバル コンフィギュレーション コマンドを使用して、EAPOL パケット履歴に関係なくインターフェイスをゲスト VLAN ステートに変更できるようにします。つまり、そのインターフェイスの前のホストが 802.1X 対応であっても、802.1X 非対応のホストがゲスト VLAN に割り当てられます。

（注） インターフェイスがゲスト VLAN に変更されたあとで EAPOL パケットが検出された場合、インターフェイスは無許可ステートに戻り、802.1X 認証が再開されます。

ポートがゲスト VLAN に移動されると、802.1X 非対応クライアントは数に制限なくアクセスを許可されます。802.1X 対応クライアントが、ゲスト VLAN が設定されたのと同じポートに参加する場合、ポートはユーザ設定のアクセス VLAN 内で無許可ステートになり、認証が再開されます。

802.1X ゲスト VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはマルチホスト モードで機能します。

RSPAN VLAN、プライベート プライマリ PVLAN、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。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、EAPOL メッセージ交換を待機している間に 802.1X 認証がタイムアウトすると、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づい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 認証バイパスを使用した 802.1X 認証」（P.83-26）および「ゲスト VLAN の設定」（P.83-45）を参照してください。

制限付き VLAN を使用した 802.1X 認証

認証に失敗し、ゲスト VLAN にもアクセスできないクライアント向けに限定的なサービスを提供するために、スイッチ上の各 802.1X ポートに制限 VLAN（*認証失敗 VLAN* とも呼ばれます）を設定できます。これらのクライアントは 802.1X 準拠で、認証プロセスに失敗しているため別の VLAN にアクセスすることができません。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の試行と失敗をいつまでも繰り返すことになり、ポートがスパニングツリーのブロッキング ステートのままになります。この機能を使用すると、指定された回数の認証試行のあと、ポートが制限 VLAN となるように設定することができます。

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。RADIUS サーバが Access-Reject EAP 失敗または EAP パケットのない空の応答で応答すると、試行失敗カウントが増加します。このカウントが設定された最大認証試行数を超過すると、ポートは制限 VLAN に移動し、失敗試行カウンタはリセットされ、失敗したクライアントからの後続の EAPOL 開始メッセージは無視されます。

認証に失敗したユーザは、次にスイッチが再認証を試行するまで制限 VLAN に残ります。制限 VLAN のポートは、設定された間隔（デフォルトで 60 秒）で再認証を試行します。再認証に失敗した場合、ポートは制限 VLAN に残ります。再認証に成功した場合、ポートは設定された VLAN または RADIUS サーバによって送信される VLAN に移動します。再認証はディセーブルにすることができます。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される可能性がある場合、再認証をイネーブルのまま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。

802.1X 制限 VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはシングルホスト モードで機能します。認証に失敗したクライアントだけが、そのポートでアクセスを許可されます。例外として、MDA モードで設定されたポートは、制限 VLAN からの音声サプリカントを認証できます。

RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限 VLAN として設定することができます。制限 VLAN 機能はルーテッド ポートやトランク ポートではサポートされておらず、アクセス ポートでだけサポートされています。

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

ダイナミック ARP インスペクション、DHCP スヌーピング、および IP ソース ガードなどの他のポート セキュリティ機能は、制限 VLAN 上で独立して設定できます。

詳細については、「制限付き VLAN の設定」（P.83-46）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

スイッチが設定済み RADIUS サーバに到達できず、ホストが認証できない場合、クリティカル ポートに接続されたホストにネットワーク アクセスできるようスイッチを設定できます。クリティカル ポートは、アクセス不能認証バイパス機能がイネーブルになっています。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。

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

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を試行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、スイッチはユーザ指定のクリティカル VLAN 内で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。
- 認証交換時に RADIUS サーバが使用不能になった場合、現在の交換はタイム アウトになり、スイッチは次の認証試行時にクリティカル ポートをクリティカル認証ステートにします。

ホストを認証できる RADIUS サーバが利用可能な場合、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。

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 8021.x 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 サーバが利用不能で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、ユーザ指定のクリティカル VLAN 内でクリティカル ポートをクリティカル認証ステートにします。

  - 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 サーバが利用不能な場合でもアカウンティングには影響しません。
- プライベート VLAN : プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）: アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1X 認証

マルチ VLAN アクセス ポート（MVAP）は、2 つの VLAN に属しているポートです。音声 VLAN ポートは、ポートの音声トラフィックとデータ トラフィックを異なる VLAN に分離することのできる MVAP です。音声 VLAN ポートは、2 つの VLAN ID に関連付けされています。

- IP Phone との間で音声トラフィックをやりとりする音声 VLAN ID（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 経由でスイッチに接続されたワークステーションへ、またはワークステーションからデータ トラフィックを伝送する Port VLAN ID（PVID）。PVID は、ポートのネイティブ VLAN です。

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、802.1X 認証から独立して IP Phone が動作することができます。

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

IP Phone を認識するために、スイッチは、ポートの許可ステートに関係なく、ポート上の CDP トラフィックを許可します。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 認証がポートでイネーブルになっている場合、音声 VLAN と同じポート VLAN を設定できません。

（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 設定の詳細については、第 18 章「Cisco IP Phone のサポート」を参照してください。

ポート セキュリティを使用した 802.1X 認証

シングルホスト モードまたはマルチホスト モードのいずれかで、802.1X ポートとポート セキュリティを設定できます。（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティも設定する必要があります）。ポート上でのポート セキュリティと 802.1X 認証をイネーブルにすると、802.1X 認証によってポートが認証され、ポート セキュリティによって、クライアントのものを含むすべての MAC アドレスのネットワーク アクセスが管理されます。その場合、802.1X ポートを介してネットワークにアクセス可能なクライアント数またはクライアント グループを制限することができます。

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

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

  クライアントが認証されて手動でポート セキュリティが設定された場合、セキュア ホスト テーブル内のエントリは保証されます。

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

  いずれかのホストでセキュリティ違反が発生した場合、ポートは errdisable ステートになり、ただちにシャットダウンされます。

  セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「ポートでのポート セキュリティ違反モードの設定」（P.85-6）を参照してください。

- **no switchport port-security mac-address** *mac_address* インターフェイス コンフィギュレーション コマンドを使用して、802.1X クライアント アドレスをポート セキュリティ テーブルから手動で削除する場合、**dot1x re-authenticate interface** *type slot/port* 特権 EXEC コマンドを使用して 802.1X クライアントを再認証する必要があります。
- 802.1X クライアントがログオフすると、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリがクリアされます。ここで通常の認証が実行されます。
- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN は、シングルホスト モードまたはマルチホスト モードのいずれの場合でも 802.1X ポート上で同時に設定可能です。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定方法」（P.85-5）を参照してください。

ACL 割り当てとリダイレクト URL を使用した 802.1X 認証

- 「概要」（P.83-24）
- 「Cisco Secure ACS を使用したダウンロード可能 ACL」（P.83-24）

- 「Filter-ID ACL」（P.83-25）
- 「リダイレクト URL」（P.83-25）
- 「ACL のスタティック共有」（P.83-25）

概要

ACL およびリダイレクト URL などのホスト単位のポリシーは、802.1X、MAB、または Web ベース認証交換の終了時に RADIUS Access-Accept パケットで認証サーバ（AS）からスイッチにダウンロードできます。

ホスト単位のポリシーは、認証中に次のようにアクティブ化されます。

- ダウンロード可能 ACL（DACL）は Cisco Secure ACS に定義され、VSA を使用して ACS からスイッチにダウンロードされます。
- Filter-ID ACL はスイッチ上に定義され、ACL 名だけが RADIUS Filter-ID 属性を使用して AS からスイッチにダウンロードされます。
- リダイレクション URL と ACL 名は、VSA を使用して ACS からスイッチにダウンロードされます。リダイレクション ACL はスイッチ上に定義されます。

ホスト単位のポリシーの設定については、「DACL またはリダイレクト URL に関するスイッチの設定」（P.83-53）を参照してください。

Cisco Secure ACS を使用したダウンロード可能 ACL

ホスト認証が成功したあと、Cisco Secure ACS は、VSA を使用して ACL をスイッチにダウンロードすることができます。スイッチは DACL を、ホストが接続されているポート上のデフォルト ACL と結合します。DACL 定義は認証サーバ上にあるので、この機能により、集中型のポリシー管理が可能になります。

DACL の定義方法については、Cisco Secure ACS で次の 2 つの方法が提供されています。

- ダウンロード可能 IP ACL

  DACL のダウンロードは ACS の設定で [Assign IP ACL] を選択することでイネーブルになり、DACL は ACS の [Downloadable IP ACL Content] メニューで定義されます。DACL のサイズには制限がありません。

- ユーザ単位の ACL

  ACS は CiscoSecure-Defined-ACL [009\001 cisco-av-pair] VSA を使用して DACL を送信できます。DACL 全体が 1 つの RADIUS パケットで送信されるので、最大サイズは RADIUS パケットの最大サイズである 4096 バイトに制限されます。DACL は次の形式を使用して ACS 上に定義する必要があります。

  protocol:inacl#*sequence_number=ace*

  次に例を示します。

  ```
  ip:inacl#10=permit ip any 67.2.2.0 0.0.0.255
  ```

DACL の使用時には、次の注意事項が適用されます。

- すべての ACE の送信元アドレスは ANY として定義しておく必要があります。
- ポートの 802.1X ホスト モードが MDA またはマルチ認証の場合、DACL は認証済みホストの IP アドレスを送信元アドレスとして使用するように変更されます。ホスト モードがシングルホストまたはマルチホストの場合、送信元アドレスは ANY として設定され、ダウンロードされた ACL またはリダイレクトがポート上のすべての装置に適用されます。

- ホストの認証中に DACL が提供されなかった場合、ポートに設定されたデフォルトのスタティック ACL がホストに適用されます。音声 VLAN ポートでは、ポートのデフォルトのスタティック ACL だけが電話に適用されます。

Filter-ID ACL

ホスト認証が成功したあと、認証サーバは VSA ではなく、RADIUS Filter-Id 属性（属性 [11]）を使用して、次の形式でスイッチに拡張 ACL 名だけを提供することができます。

acl_name.in

末尾の「.in」は、ACL が受信方向に適用される必要があることを示します。

この方法では、ACL はスイッチ上に定義しておく必要があります。スイッチは、Filter-ID 属性値を、ローカルに設定された ACL の中で Filter-ID と同じ名前または番号を持つものと照合します（たとえば、Filter-ID=101.in は拡張番号付き ACL 101 と一致し、Filter-ID= guest.in は名前付き拡張 ACL「guest」と一致します）。その後は指定された ACL がポートに適用されます。ACL 定義はスイッチ上にあるので、この機能により、ポリシーのローカル バリエーションが可能になります。

Filter-ID ACL の使用時には、次の注意事項が適用されます。

- DACL 使用時の注意事項は Filter-ID ACL にも当てはまります。
- Filter-ID 属性は、番号（100 ～ 199、または 2000 ～ 2699）または名前になります。

リダイレクト URL

ホスト認証が成功したあと、Cisco Secure ACS は、VSA を使用して、認証済みホストからの HTTP または HTTPS 要求を代行受信およびリダイレクトするための情報をスイッチにダウンロードすることができます。ACS はリダイレクション ACL および URL をダウンロードします。ホストからの HTTP または HTTPS 要求が、ダウンロードされた ACL と一致した場合、ホストの Web ブラウザはダウンロードされたリダイレクション URL にリダイレクトされます。

ACS は次の cisco-av-pair VSA を使用してリダイレクションを設定します。

- url-redirect-acl

  この AV ペアは、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 の名前または番号を示します。ACL はスイッチ上に定義しておく必要があり、送信元アドレスは ANY として定義しておく必要があります。この結果、リダイレクト ACL 内の許可エントリに一致するトラフィックがリダイレクトされます。

- url-redirect

  この AV ペアには、Web ブラウザのリダイレクト先となる HTTP または HTTPS URL が含まれます。

ACL のスタティック共有

複数のインターフェイスに同じ PACL および VLAN ベース機能がある場合、スタティック共有機能により、同じ ACL セットを使用するすべてのポートの TCAM 内の PACL および継承された VLAN ベース機能の ACL のコピーが 1 つ格納され、より多くの ACL 用に TCAM の領域を開放します。次のいずれかのイベントが発生したときに、スイッチは自動的にスタティック共有用に設定またはイネーブルにされたすべてのインターフェイスを評価します。

- インターフェイスが設定されたとき。
- インターフェイス上でステートの変化が発生したとき。

次の注意事項および制約事項を考慮してください。

- スタティック共有は、IPv6 をサポートするように設定されたインターフェイスではサポートされません。
- スタティック共有は NAC または 802.1X DACL 機能が設定されたアクセス モードのスイッチ ポートでだけサポートされます。
- スタティック共有は、QoS（VLAN ベースの QoS を除く）がイネーブルになっているスイッチ ポートではサポートされません。
- 802.1X を DACL とともに使用する際には、ポートが認証サーバの応答によってダイナミックに設定されたときにスタティック共有の評価が開始されるのを回避するために、**platform hardware acl dynamic setup static** コマンドを実行することを推奨します。スタティック共有の評価は、ポート/ホストのリンクアップ時間に影響を及ぼす場合があります。
- フォールバック認証がアクティブになっている 802.1X インターフェイスは、フォールバック認証がイネーブルでない、またはアクティブでないインターフェイスと一緒にスタティック共有グループを形成できません。

ポート ディスクリプタを使用した 802.1X 認証

RADIUS サーバ上で Cisco ベンダー固有属性（VSA）**aaa:supplicant-name** を設定すると、説明文を 802.1X クライアントの認証情報と関連付けることができます。ポート上でクライアントの 802.1X 認証が正常に進行している間に、スイッチは RADIUS サーバから Access-Accept パケットの一部として説明情報を受信し、ポートに対して **show interface users** コマンドが入力されたときに、この情報を表示します。ポートが複数の認証済みホストをサポートするモードの場合は、すべての認証済みホストの識別情報がポートの説明とともに表示されます。

MAC 認証バイパスを使用した 802.1X 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 83-4（P.83-12）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、プリンタなどの装置に接続されている 802.1X ポートで、この機能をイネーブルにすることができます。

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。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づい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。

リンクの存続時間内に 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 対応サプ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 サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生した際、Termination-Action RADIUS 属性が DEFAULT であるために前のセッションが終了した場合、スイッチは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていればポートにゲスト VLAN を割り当てます。

再認証が Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）に基づいており、Termination-Action RADIUS 属性（属性 [29]）のアクションが初期化の場合、（属性値は DEFAULT）、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC 認証バイパスがイネーブルで 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許可を開始します。これらの AV ペアの詳細については、RFC 3580「IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines」を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 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.lx 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.83-23）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.83-22）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。
- Network Admission Control（NAC）レイヤ 2 IP 検証：例外リスト内のホストを含む、802.1X ポートが MAC 認証バイパスで認証されたあとにこの機能が有効になります。

Network Admission Control レイヤ 2 IEEE 802.1X 検証

Network Admission Control（NAC）レイヤ 2 IEEE 802.1X 検証は、デバイスにネットワーク アクセスを許可する前に、エンドポイント システムまたはクライアントのウイルス対策の状態または*ポスチャ*を確認します。NAC レイヤ 2 IEEE 802.1X 検証は、認証済みポートを指定の VLAN に割り当てることでポリシーの適用を実行します。これにより、レイヤ 2 で不適切なポスチャのホストを区分および隔離します。

NAC レイヤ 2 IEEE 802.1X 検証の設定は、RADIUS サーバ上でポスチャ トークンを設定する必要があることを除いて、802.1X ポートベース認証の設定に似ています。**show dot1x** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示することができます。NAC レイヤ 2 IEEE 802.1X 検証の設定については、「NAC レイヤ 2 IEEE 802.1X 検証の設定」（P.83-51）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。

NAC エージェントレス監査のサポート

MAB サポートが Cisco NAC 監査アーキテクチャに追加されています。これは、Cisco Trust Agent（CTA）を実行しておらず、NAC クエリーに応答できないクライアントのアンチウイルス ポスチャをチェックするために外部監査サーバを使用するものです。エージェントレス クライアントのアンチウイルス ポスチャを監査およびレポートするためには、NAC 監査サーバはクライアントの IP アドレス

と、そのクライアントがスイッチに接続するための一意のセッション ID を持っている必要があります。エージェントレス クライアントのための NAC 監査アーキテクチャをサポートするには、スイッチはクライアントの IP アドレスをスヌーピングし、エージェントレス クライアント用に一意のセッション ID を作成して割り当て、この情報を RADIUS サーバに渡して NAC 監査サーバと共有できるようにする必要があります。

MAB はレイヤ 2 で動作するので、MAB オーセンティケータは通常、サプリカントの IP アドレスを認識していません。また、サプリカントが最初にオーセンティケータと接触する際、サプリカントには IP アドレスがない可能性があります。DHCP が割り当てた IP アドレスを必要とするサプリカントは、認証の前に DHCP サーバへのアクセスを許可される必要があります。MAB オーセンティケータがサプリカントの IP アドレスを学習できるようにするには、スイッチ上で ARP と DHCP スヌーピングをイネーブルにする必要があります。IP アドレスと一意のセッション ID 情報を NAC 監査サーバと共有できるようにするには、特定の RADIUS 属性の送信をイネーブルにする必要があります。「NAC エージェントレス監査のサポートの設定」（P.83-52）を参照してください。

クライアントの IP アドレスと一意のセッション ID は、次の RADIUS *cisco-av-pair* ベンダー固有属性（VSA）を使用して、RADIUS Access-Request および Access-Accept 内で共有されます。

- Cisco-AVPair="identity-request=*ip-address*"

  ip-address は、ARP または DHCP スヌーピングを使用してスイッチが取得したクライアントの IP アドレスです。

- Cisco-AVPair="audit-session-id=*audit session id string*"

  audit session id string は、スイッチによってネットワーク アクセス サーバ（NAS）の IP アドレス、セッション カウント、およびセッション開始タイムスタンプから引き出された一意の 96 ビット ID の UTF-8 エンコーディングです。

Wake-on-LAN を使用した 802.1X 認証

802.1X 認証と Wake-on-LAN（WoL）機能では、スイッチが *マジック パケット*と呼ばれる特別なイーサネット フレームを受信したときに、休止状態の PC を起動することができます。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 ポートを介して接続されていてホストの電源がオフの場合、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 移動

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

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 移動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 アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。ポート セキュリティの動作は、MAC 移行を設定したときと同じです。

（注）

- MAC 移動はすべてのホスト モードでサポートされます。（認証ホストは、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 移動はポート セキュリティでサポートされます。
- MAC 移動の機能は、音声およびデータ ホストの両方に適用されます。
- オープン認証モードでは、MAC アドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「MAC 移動のイネーブル化」（P.83-54）を参照してください。

MAC 置換

MAC 置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとすると発生する違反に対処するように設定できます。

（注）

- Mac 置換機能は、マルチ認証モードで違反がトリガーされないので、そのモードのポートではサポートされません。
- Mac 置換機能は、マルチ ホスト モードでは最初のホストだけが認証を必要とするため、そのモードのポートではサポートされていません。

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.83-55）を参照してください。

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

NEAT は、ワイヤリング クローゼットの外側の領域（会議室など）に ID を拡大します。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 サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプ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 サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。

  サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。

- 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。

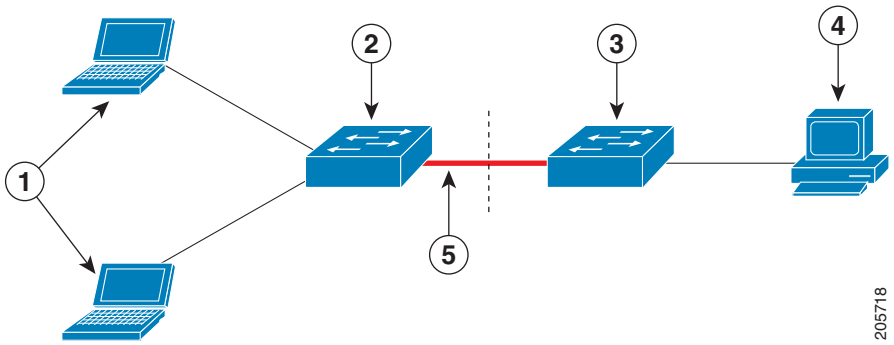
1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。オーセンティケータ スイッチのインターフェイスで、マルチホスト モードがサポートされないため、MDA モードでは音声クライアントはサポートされません。

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）のサプリカント スイッチで使用します。

- ホスト許可：許可済み（サプ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、サプリカント 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 83-7 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、サプリカント 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 83-7　CISP を使用したオーセンティケータまたはサプリカント スイッチ



1	ワークステーション（クライアント）	**2**	サプリカント スイッチ（ワイヤリング クローゼット外）
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		

詳細については、「NEAT オーセンティケータとサプリカント スイッチの設定」（P.83-55）を参照してください。

802.1X ポートベース認証のデフォルト設定

機能	デフォルト設定
802.1X イネーブル ステートの切り換え	ディセーブル
ポート単位の 802.1X イネーブル ステート	ディセーブル（force-authorized） ポートはクライアントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 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
再認証の回数	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（スイッチが要求を再送信するまでに、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数）
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 要求/アイデンティティ 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へ中継する場合、スイッチがクライアントへ要求を再送信するまでに、応答を待機する時間）。
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へ中継する場合、スイッチが認証サーバへ応答を再送信するまでに、返答を待機する時間）。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし

機能	デフォルト設定
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ（スイッチ）モード	指定なし
MAC 認証バイパス	ディセーブル **（注）** EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。

802.1X ポートベース認証の設定方法

- 「802.1X 認証のイネーブル化」（P.83-33）
- 「スイッチ/RADIUS サーバ間通信の設定」（P.83-35）
- 「802.1X オーセンティケータのホスト モードの設定」（P.83-36）
- 「フォールバック認証のイネーブル化」（P.83-36）
- 「定期的な再認証のイネーブル化」（P.83-38）
- 「手動によるポート接続クライアントの再認証」（P.83-39）
- 「ポート接続クライアント認証の初期化」（P.83-40）
- 「802.1X クライアント情報のグローバルな削除」（P.83-40）
- 「インターフェイスからの 802.1X クライアント情報の削除」（P.83-40）
- 「認証セッションのクリア」（P.83-41）
- 「802.1X タイムアウトの変更」（P.83-41）
- 「スイッチ/クライアント間フレーム再送信回数の設定」（P.83-43）
- 「再認証回数の設定」（P.83-43）
- 「IEEE 802.1X アカウンティングの設定」（P.83-44）
- 「VLAN ユーザ分散の設定」（P.83-45）
- 「ゲスト VLAN の設定」（P.83-45）
- 「制限付き VLAN の設定」（P.83-46）
- 「アクセス不能認証バイパス機能の設定」（P.83-48）
- 「MAC 認証バイパスの設定」（P.83-50）
- 「NAC レイヤ 2 IEEE 802.1X 検証の設定」（P.83-51）
- 「NAC エージェントレス監査のサポートの設定」（P.83-52）
- 「DACL またはリダイレクト URL に関するスイッチの設定」（P.83-53）
- 「WoL を使った 802.1X 認証の使用」（P.83-54）
- 「MAC 移動のイネーブル化」（P.83-54）
- 「MAC 置換のイネーブル化」（P.83-55）
- 「NEAT オーセンティケータとサプリカント スイッチの設定」（P.83-55）

- 「ポート上での 802.1X 認証のディセーブル化」（P.83-57）
- 「802.1X 設定をデフォルト値にリセットする方法」（P.83-58）

802.1X 認証のイネーブル化

802.1X ポートベース認証をイネーブルにするには、AAA をイネーブルにして認証方式リストを指定する必要があります。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

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

802.1X AAA 処理は、次のようになります。

1. ユーザがスイッチのポートに接続します。
2. 認証が実行されます。
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。
4. スイッチが開始メッセージをアカウンティング サーバに送信します。
5. 必要に応じて再認証が実行されます。
6. スイッチが、再認証の結果に基づく内部アカウンティング アップデートをアカウンティング サーバに送信します。
7. ユーザがポートから切断します。
8. スイッチが停止メッセージをアカウンティング サーバに送信します。

802.1X ポートベース認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aas new-model`	AAA をイネーブルにします。
ステップ 2	`Router(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1x ポート ベース認証方式リストを作成します。 **aaa authentication** コマンドに名前付きリストが指定されて*いない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 3	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。

	コマンド	目的
ステップ 4	Router(config)# **aaa authorization network {default} group radius**	（任意）VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対してユーザ RADIUS 許可を使用するようにスイッチを設定します。
ステップ 5	Router(config)# **radius-server host** *ip-address*	RADIUS サーバの IP アドレスを指定します。
ステップ 6	Router(config)# **radius-server key** *string*	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される認証および暗号キーを指定します。
ステップ 7	Router(config)# **interface** *type slot/port*	インターフェイス コンフィギュレーション モードを開始し、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 8	Router(config-if)# **switchport mode access**	前の手順で RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 9	Router(config-if)# **authentication port-control auto**	インターフェイスでのポートベース認証をイネーブルにします。 コマンドの **no** 形式を使用すると、インターフェイスでのポートベース認証がディセーブルになります。
ステップ 10	Router(config-if)# **dot1x pae authenticator**	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 11	Router(config)# **end**	特権 EXEC モードに戻ります。

次に、ギガビット イーサネット ポート 5/1 で AAA と 802.1X をイネーブルにする例を示します。

```
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show dot1x all

Sysauthcontrol              Enabled
Dot1x Protocol Version            2

Dot1x Info for GigabitEthernet1/7
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

スイッチ /RADIUS サーバ間通信の設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

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、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）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。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	`Router(config)# radius-server host {hostname | ip_address}`	スイッチに RADIUS サーバ ホスト名や IP アドレスを設定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 3	`Router(config)# radius-server key string`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。

- *hostname* または *ip_address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。
- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号キーに一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、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。
- **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。

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

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46
```

```
Router(config)# radius-server key rad123
```

802.1X オーセンティケータのホスト モードの設定

802.1X 対応ポートは、「802.1X ホスト モード」（P.83-13）の説明にあるように、単一クライアントまたは複数クライアントに対してアクセスを許可することができます。

802.1X 許可ポートのホスト モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# authentication port-control auto`	インターフェイスでのポートベース認証をイネーブルにします。
ステップ 3	`Router(config-if)# dot1x pae authenticator`	インターフェイス上で、802.1X 認証をイネーブルにします。
ステップ 4	`Router(config-if)# authentication host-mode host_mode`	ホスト モードを設定します。*host_mode* の値は次のとおりです。 • **single-host**：許可ポートで単一の認証済みホスト（クライアント）を許可します。 • **multi-host**：1 つのクライアントが認証されると、許可ポートで複数のクライアントを許可します。 • **multi-domain**：単一の IP Phone と単一のデータ クライアントを許可ポートで独立して認証できるようにします。 • **multi-auth**：単一の IP Phone と複数のデータ クライアントを許可ポートで独立して認証できるようにします。
ステップ 5	`Router(config-if)# authentication open`	（任意）認証前オープン アクセスをイネーブルにします。
ステップ 6	`Router(config-if)# end`	特権 EXEC モードに戻ります。

次に、ギガビット イーサネット インターフェイス 5/1 で 802.1X をイネーブルにし、複数のホストを許可する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# authentication host-mode multi-host
```

フォールバック認証のイネーブル化

マルチ認証モードのポートでは、MAB と Web ベース認証のいずれかまたは両方を、802.1X 以外のホスト（EAPOL に応答しないホスト）用のフォールバック認証方式として設定できます。認証方式の順序とプライオリティを設定します。

MAB の設定方法の詳細については、「MAC 認証バイパスの設定」（P.83-50）を参照してください。

Web ベース認証の設定方法の詳細については、第 84 章「Web ベース認証」を参照してください。

フォールバック認証をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **ip admission name** *rule-name* **proxy http**	Web ベース認証の認証ルールを設定します。
ステップ 2	Router(config)# **fallback profile** *profile-name*	Web ベース認証のフォールバック プロファイルを作成します。
ステップ 3	Router(config-fallback-profile)# **ip access-group** *rule-name* **in**	Web ベース認証前にネットワーク トラフィックに適用するデフォルト ACL を指定します。
ステップ 4	Router(config-fallback-profile)# **ip admission name** *rule-name*	IP 許可ルールをプロファイルに関連付け、Web ベース認証で接続するクライアントがこのルールを使用するように指定します。
ステップ 5	Router(config-fallback-profile)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	Router(config-if)# **authentication port-control auto**	ポートで認証をイネーブルにします。
ステップ 8	Router(config-if)# **authentication order** *method1* [*method2*] [*method3*]	（任意）使用される認証方式のフォールバック順序を指定します。*method* の 3 つの値のデフォルト順序は、**dot1x**、**mab**、および **webauth** です。また、指定した順序は、最大から最小まで、再認証の方式の相対的なプライオリティも決定します。
ステップ 9	Router(config-if)# **authentication priority** *method1* [*method2*] [*method3*]	（任意）使用される認証方式の相対プライオリティを上書きします。*method* の 3 つの値は、プライオリティのデフォルト順序で、**dot1x**、**mab**、および **webauth** です。
ステップ 10	Router(config-if)# **authentication event fail action next-method**	認証が失敗した場合には設定された次の認証方式が使用されるように指定します。
ステップ 11	Router(config-if)# **mab** [**eap**]	MAC 認証バイパスをイネーブルにします。任意の **eap** キーワードは、RADIUS 認証中に EAP 拡張機能が使用されるように指定します。
ステップ 12	Router(config-if)# **authentication fallback** *profile-name*	指定されたプロファイルを使用した Web ベースの認証をイネーブルにします。
ステップ 13	Router(config-if)# **authentication violation** [**shutdown** | **restrict**]	（任意）セキュリティ違反が発生した場合のポートのディスポジションを設定します。デフォルトでは、ポートはシャットダウンされます。**restrict** キーワードが設定した場合、ポートはシャットダウンされませんが、違反した MAC アドレスに対するトラップ エントリが設定され、その MAC アドレスからのトラフィックはドロップされます。
ステップ 14	Router(config-if)# **authentication timer inactivity** {*seconds* | **server**}	（任意）MAB および 802.1X に対する無活動タイムアウト値を設定します。デフォルトでは、ポートに対する無活動の長さはディセーブルにされています。 • *seconds*：無活動タイムアウトの期間を指定します。範囲は 1 ～ 65535 秒です。 • server：無活動タイムアウト期間の値が認証サーバから取得されるように指定します。

	コマンド	目的
ステップ 15	Router(config-if)# **authentication timer restart** *seconds*	（任意）無許可ポートの認証を試行するために認証プロセスを再開するまでの期間を指定します。 • *seconds*：再起動期間を指定します。範囲は 1 ～ 65535 秒です。
ステップ 16	Router(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 17	Router(config)# **ip device tracking**	Web ベース認証に必要な IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 18	Router(config)# **exit**	特権 EXEC モードに戻ります。

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

```
Router(config)# ip admission name rule1 proxy http
Router(config)# fallback profile fallback1
Router(config-fallback-profile)# ip access-group default-policy in
Router(config-fallback-profile)# ip admission rule1
Router(config-fallback-profile)# exit
Router(config)# interface gigabit1/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# authentication order dot1x mab webauth
Router(config-if)# mab eap
Router(config-if)# authentication fallback fallback1
Router(config-if)# exit
Router(config)# ip device tracking
Router(config)# exit
```

定期的な再認証のイネーブル化

定期的な 802.1X クライアント再認証をイネーブルにして、その発生間隔を指定できます。再認証を行うまでの期間を手動で指定するか、RADIUS サーバで指定されたセッションタイムアウト期間を使用することができます。期間を指定せずに再認証をイネーブルにする場合、再認証を行う間隔は 3600 秒です。

クライアントの定期的再認証をイネーブルにして、再認証を試行する間隔を秒数で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **authentication periodic**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。

	コマンド	目的
ステップ 3	Router(config-if)# **authentication timer reauthenticate** [*seconds* | **server**]	以下のキーワードを使用して再認証の間隔（秒）を指定します。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて秒数を設定します。 このコマンドがスイッチの動作に影響を与えるのは、定期的再認証がイネーブルに設定されている場合だけです。
ステップ 4	Router(config-if)# **end**	特権 EXEC モードに戻ります。

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

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication periodic
Router(config-if)# authentication timer reauthenticate 4000
```

入力を確認します。

```
Router# show dot1x interface type slot/port
```

手動によるポート接続クライアントの再認証

特定のポートに接続するクライアントを手動で再認証するには、次の作業を行います。

コマンド	目的
Router# **dot1x re-authenticate interface** *type slot/port*	ポートに接続するクライアントを手動で再認証します。 **（注）**　再認証は、すでに認証されているポートのステータスには影響しません。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントを手動で再認証する例を示します。

```
Router# dot1x re-authenticate interface gigabitethernet 5/1
```

入力を確認します。

```
Router# show dot1x all
```

ポート接続クライアント認証の初期化

ポートに接続されているクライアントの認証を初期化するには、次の作業を行います。

コマンド	目的
Router# **dot1x initialize interface** *type slot/port*	ポートに接続されているクライアントの認証を初期化します。 **（注）** 認証の初期化により、既存の認証をディセーブルにしてから、ポートに接続されているクライアントを認証します。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントに対する認証を初期化する例を示します。

```
Router# dot1x initialize interface gigabitethernet 5/1
```

入力を確認します。

```
Router# show dot1x all
```

802.1X クライアント情報のグローバルな削除

スイッチ上のすべてのインターフェイスからすべての既存サプリカントを完全に削除するには、次の作業を行います。

コマンド	目的
Router# **clear dot1x all**	すべてのポートに接続されているすべてのクライアントの 802.1X クライアント情報を削除します。

次に、すべてのポートに接続されているすべてのクライアントの 802.1X クライアント情報を削除する例を示します。

```
Router# clear dot1x all
```

インターフェイスからの 802.1X クライアント情報の削除

すべての既存サプリカントをスイッチのいずれかのインターフェイスまたはすべてのインターフェイスから完全に削除するには、次の作業を行います。

コマンド	目的
Router# **clear dot1x interface** *type slot/port*	指定したポートに接続されているクライアントの 802.1X クライアント情報を削除します。

次に、ギガビット イーサネット ポート 5/1 に接続されているクライアントの 802.1X クライアント情報を削除する例を示します。

```
Router# clear dot1x interface gigabitethernet 5/1
```

認証セッションのクリア

すべての認証セッションまたは選択した認証セッションをクリアするには、次の作業を行います。

コマンド	目的
Router# **clear authentication sessions** [**handle** *handle*] [**interface** *interface*] [**mac** *mac*] [**method** *method*]	現在の認証セッションをクリアします。オプションを指定しない場合、現在のすべてのアクティブ セッションがクリアされます。キーワードを追加したり組み合わせたりすることで、特定のセッションや一部のセッションをクリアすることができます。

次に、ギガビット イーサネット ポート 5/1 に接続されているすべての MAB 認証セッションをクリアする例を示します。

```
Router# clear authentication sessions interface gigabitethernet 5/1 method mab
```

802.1X タイムアウトの変更

インターフェイス コンフィギュレーション モードで **dot1x timeout {attribute}** *seconds* コマンド形式を使用して複数の 802.1X タイムアウト属性を変更することができます。ここでは、待機時間タイムアウトを変更する方法について詳細に説明し、次に同じコマンド形式を使用して他の 802.1X タイムアウトを変更する方法について説明します。

待機時間の設定

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。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、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **dot1x timeout quiet-period** *seconds*	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでいる秒数を設定します。 指定できる範囲は 0 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

次に、スイッチ上の待機時間（quiet period）を 30 秒に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout quiet-period 30
```

スイッチからクライアントへの再送信時間の設定

クライアントはスイッチからの EAP 要求/アイデンティティ フレームに対し、EAP 応答/アイデンティティ フレームで応答します。スイッチはこの応答を受信しなかった場合、一定期間（再送信時間と呼ばれる）待機した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。

スイッチが要求を再送信する前にクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する時間を変更するには、インターフェイス コンフィギュレーション モードで **dot1x timeout tx-period** *seconds* コマンドを使用します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 30 秒です。デフォルトの再送信時間に戻すには、**no dot1x timeout tx-period** コマンドを使用します。

次の例では、要求を再送信する前に、スイッチが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を 60 秒に設定する方法を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout tx-period 60
```

スイッチとクライアント間の EAP 要求フレーム再送信時間の設定

クライアントは EAP 要求フレームを受信したことをスイッチに通知します。スイッチがこの通知を受信できなかった場合、スイッチは所定の時間だけ待機した後、フレームを再送信します。

スイッチが通知を待機する時間を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout supp-timeout** *seconds* コマンドを使用します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 30 秒です。デフォルトの再送信時間に戻すには、**no dot1x supp-timeout** コマンドを使用します。

次に、EAP 要求フレームのスイッチ/クライアント間再送信時間を 25 秒に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout supp-timeout 25
```

スイッチ/認証サーバ間のレイヤ 4 パケット再送信時間の設定

認証サーバは、レイヤ 4 パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、スイッチは所定の時間だけ待機した後、パケットを再送信します。

スイッチから認証サーバへのレイヤ 4 パケットの再送信値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **dot1x timeout server-timeout** *seconds*	スイッチ/認証サーバ間のレイヤ 4 パケットの再送信値を設定します。*seconds* の範囲は 1 ～ 65535 秒です。デフォルトは 30 です。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

次に、スイッチ/認証サーバ間のレイヤ 4 パケットの再送信時間を 25 秒に設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x timeout server-timeout 25
```

スイッチ/クライアント間フレーム再送信回数の設定

スイッチ/クライアント間再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP 要求/アイデンティティ 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/クライアント間のフレーム再送信回数を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# dot1x max-req count`	スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。

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

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x max-req 5
```

再認証回数の設定

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

（注）　このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、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、次の作業を行います。

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

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。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# dot1x max-reauth-req 4
```

IEEE 802.1X アカウンティングの設定

802.1X アカウンティングによる AAA システム アカウンティングをイネーブルにすることにより、ログ用のアカウンティング RADIUS サーバにシステム リロード イベントを送信することができます。その後、すべてのアクティブ 802.1X セッションがクローズしていることをサーバが判別できます。

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-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

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

スイッチ上で AAA をイネーブルにしたあとで 802.1X アカウンティングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aaa accounting dot1x default start-stop group radius`	すべての RADIUS サーバのリストを使用して 802.1X アカウンティングをイネーブルにします。
ステップ 2	`Router(config)# aaa accounting system default start-stop group radius`	（任意）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。

	コマンド	目的
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	Router# **show running-config**	入力を確認します。

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。

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

VLAN ユーザ分散の設定

複数の VLAN を含む VLAN グループを定義できます。さらに、VLAN ロード バランシングのために、802.1X 認証中のユーザに対する応答の一部として VLAN グループ名を提供するように RADIUS サーバを設定できます。提供された VLAN グループ名が定義済みの VLAN グループ名の中に見つかった場合、新たに認証されたユーザは、VLAN グループ内でユーザ追加数が最も少ない VLAN に配置されます。

VLAN グループを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **vlan group** *group-name* **vlan-list** *vlan-list*	VLAN グループを作成するか、既存の VLAN グループに VLAN を追加します。 • *group-name* : VLAN グループの名前です。名前は最大 32 文字で、文字から始める必要があります。 • **vlan-list** *vlan-list* : VLAN グループに属する VLAN です。グループのメンバは、単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲として指定できます。複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

次に、VLAN 7 ～ 9 と 11 を VLAN グループにマッピングする例を示します。

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合、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 アクセスを許可されません。ゲスト VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはマルチホスト モードで機能します。

ゲスト VLAN を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **switchport mode** {**access** | **private-vlan host**}	ポートをアクセス モードに、またはプライベート VLAN ホスト ポートとして設定します。ルーテッド ポートおよびトランク ポートはゲスト VLAN をサポートしません。
ステップ 3	Router(config-if)# **authentication port-control auto**	ポートで認証をイネーブルにします。
ステップ 4	Router(config-if)# **authentication event no-response action authorize vlan** *vlan-id*	アクティブ VLAN をゲスト 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、プライベート プライマリ PVLAN、または音声 VLAN を除き、任意のアクティブ VLAN をゲスト VLAN として設定できます。
ステップ 5	Router(config-if)# {**dot1x pae authenticator** | **mab**}	ポート認証方式を 802.1X にするか、または MAC アドレス バイパスにするかを指定します。
ステップ 6	Router(config-if)# **end**	特権 EXEC モードに戻ります。

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

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# authentication event no-response action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

次に、スイッチにクライアント通知タイムアウトとして 3 秒を設定し、要求を再送信する前にスイッチがクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する秒数として 15 を設定し、802.1X ポートが DHCP クライアントに接続されているときに 802.1X ゲスト VLAN として VLAN 2 をイネーブルにする例を示します。

```
Router(config-if)# dot1x timeout supp-timeout 3
Router(config-if)# dot1x timeout tx-period 15
Router(config-if)# authentication event no-response action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

制限付き VLAN の設定

スイッチに制限付き VLAN を設定すると、認証サーバが有効なユーザ名とパスワードを受信しなかった場合、802.1X 準拠のクライアントが制限付き VLAN に移動します。制限 VLAN として動作する際、ポートに設定されたホスト モードに関係なく、ポートはシングルホスト モードで機能します。

制限 VLAN を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **switchport mode** {**access** | **private-vlan host**}	ポートをアクセス モードに、またはプライベート VLAN ホスト ポートとして設定します。ルーテッド ポートおよびトランク ポートはゲスト VLAN をサポートしません。
ステップ 3	Router(config-if)# **authentication port-control auto**	ポートでのポートベース認証をイネーブルにします。
ステップ 4	Router(config-if)# **authentication event fail** [**retry** *retries*] **action authorize vlan** *vlan-id*	アクティブ VLAN を制限 VLAN として指定します。*vlan-id* の範囲は 1 ～ 4094 です。 （任意）**retry** キーワードは、ポートを制限 VLAN に移動する前に許可される認証試行回数を指定します。
ステップ 5	Router(config-if)# **end**	特権 EXEC モードに戻ります。

制限 VLAN をディセーブルにして削除するには、**authentication event fail** コマンドまたは **dot1x auth-fail** コマンドの **no** 形式を使用します。ポートは無許可ステートに戻ります。

ユーザが制限 VLAN に割り当てられる前に許可される認証試行最大回数を設定できます。**authentication event fail** [**retry** *retries*] **action authorize vlan** コマンドで **retry** キーワードを使用すると、試行回数を設定できます。*retries*（認証試行の許容回数）の範囲は 1 ～ 5 です。デフォルトは 2 回です。

次に、制限 VLAN として VLAN 2 をイネーブルにし、3 回の試行失敗後にホストを割り当てる例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# authentication event fail retry 3 action authorize vlan 2
Router(config-if)# dot1x pae authenticator
```

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てアクセス不能認証バイパス機能をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# radius-server dead-criteria time` *time* **tries** *tries*	（任意）RADIUS サーバが利用不能または*停止*と見なされるときを判別するのに使用される条件を設定します。 指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 2	`Router(config)# 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 3	Router(config)# **radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**key** *string*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]]	（任意）以下のキーワードを使用して RADIUS サーバのパラメータを設定します。 • **acct-port** *udp-port*：RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1646 です。 • **auth-port** *udp-port*：RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルト値は 1645 です。 （注）　RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **key** *string*：スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号キーを指定します。 （注）　**radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。 • **test username** *name*：RADIUS サーバ ステータスの自動化テストをイネーブルにして、使用されるユーザ名を指定します。 • **idle-time** *time*：スイッチがテスト パケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port**：RADIUS サーバのアカウンティング ポートでのテストをディセーブルにします。 • **ignore-auth-port**：RADIUS サーバの認証ポートでのテストをディセーブルにします。
ステップ 4	Router(config)# **dot1x critical eapol**	（任意）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。
ステップ 5	Router(config-if)# **authentication critical recovery delay** *milliseconds*	（任意）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（ポートが毎秒再初期化可能になります）。
ステップ 6	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 7	Router(config-if)# **authentication event server dead action authorize** [**vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにして、AAA サーバに到達できない場合に、指定した VLAN 上のポートが許可されるようにします。VLAN を指定しない場合は、アクセス VLAN が使用されます。 （注）　**vlan** キーワードは、スイッチ ポートでだけ使用できます。
ステップ 8	Router(config-if)# **authentication event server alive action reinitialize**	アクセス不能認証バイパス回復機能を設定し、回復アクションとして、認証サーバが使用可能になったときにポートを認証するように指定します。
ステップ 9	Router(config-if)# **end**	特権 EXEC モードに戻ります。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical** {**eapol**} 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 authorize**（または **no dot1x critical**）インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Router(config)# radius-server dead-criteria time 30 tries 20
Router(config)# radius-server deadtime 60
Router(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 key abc1234 test
username user1 idle-time 30
Router(config)# dot1x critical eapol
Router(config)# authentication critical recovery delay 2000
Router(config)# interface gigabitethernet 0/1
Router(config-if)# authentication event server dead action authorize vlan 123
Router(config-if)# authentication event server alive action reinitialize
```

MAC 認証バイパスの設定

インターフェイス上で MAC 認証バイパスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **authentication port-control** {**auto** | **force-authorized** | **force-unauthorized**}	ポートでの 802.1X 認証をイネーブルにします。 キーワードの意味は次のとおりです。 • **auto**：認証が成功するまで EAPOL トラフィックだけを許可します。 • **force-authorized**：すべてのトラフィックを許可し、認証は不要です。 • **force-unauthorized**：どのトラフィックも許可しません。

	コマンド	目的
ステップ 3	Router(config-if)# **mab** [**eap**]	インターフェイス上で MAC 認証バイパスをイネーブルにします。 • （任意）**eap** キーワードを使用して、スイッチが許可に EAP を使用するように設定します。 • EAP を使った MAC 認証バイパスがインターフェイス上でイネーブルになっている場合は、その後にインターフェイス上で実行される **default interface** コマンドによってディセーブルになることはありません。 • MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。
ステップ 4	Router(config-if)# **end**	特権 EXEC モードに戻ります。

次に、ポートで MAC 認証バイパスをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication port-control auto
Router(config-if)# mab
```

NAC レイヤ 2 IEEE 802.1X 検証の設定

NAC レイヤ 2 IEEE 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 IEEE 802.1X の設定は 802.1X の設定と同じですが、RADIUS サーバでポスチャ トークンと VLAN 割り当てを設定する手順が追加されます。

NAC レイヤ 2 IEEE 802.1X 検証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **authentication port-control auto**	インターフェイスでのポートベース認証をイネーブルにします。
ステップ 3	Router(config-if)# **authentication periodic**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。

	コマンド	目的
ステップ 4	Router(config-if)# **authentication timer reauthenticate** [*seconds* | **server**]	以下のキーワードを使用して再認証の間隔（秒）を指定します。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて秒数を設定します。 このコマンドがスイッチの動作に影響を与えるのは、定期的再認証がイネーブルに設定されている場合だけです。
ステップ 5	Router(config-if)# **end**	特権 EXEC モードに戻ります。

次に、NAC レイヤ 2 IEEE 802.1X 検証を設定する例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config)# authentication port-control auto
Router(config-if)# authentication periodic
Router(config-if)# authentication timer reauthenticate server
```

NAC エージェントレス監査のサポートの設定

エージェントレス クライアントのための NAC 監査アーキテクチャをサポートするには、スイッチは認証中の 802.1X クライアントの IP アドレスをスヌーピングし、エージェントレス クライアント用に一意のセッション ID を作成して割り当て、この情報を RADIUS サーバに渡して NAC 監査サーバと共有できるようにする必要があります。スイッチがこの情報を取得して共有できるようにするには、スイッチ上で ARP と DHCP スヌーピングをイネーブルにし、特定の RADIUS 属性の送信をイネーブルにする必要があります。

NAC エージェントレス監査をサポートするための RADIUS およびトラッキング設定を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **radius-server attribute 8 include-in-access-req**	access-request または accounting-request パケットで Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。
ステップ 2	Router(config)# **radius-server vsa send authentication**	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）（特に audit-session-id）を認識して使用するようにネットワーク アクセス サーバを設定します。
ステップ 3	Router(config)# **radius-server vsa send accounting**	後続の RADIUS Accounting-Request に VSA を含めることができるようにします。
ステップ 4	Router(config)# **ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。

DACL またはリダイレクト URL に関するスイッチの設定

接続されたホストの認証中に RADIUS サーバからの DACL またはリダイレクト URL を受け入れるようにスイッチ ポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **config 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	Router(config)# **radius-server vsa send authentication**	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにネットワーク アクセス サーバを設定します。 **（注）** この手順は、リダイレクト URL を使用する場合、または DACL が Filter-ID 属性ではなく VSA を使用してダウンロードされる場合にだけ必要となります。
ステップ 3	Router(config)# **ip device tracking**	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 4	Router(config)# **ip access-list extended** *dacl-name*	VSA または Filter-ID 属性によって参照される ACL を設定します。 **（注）** この手順は、RADIUS サーバで定義され、VSA を使用してダウンロードされる DACL には必要ありません。
ステップ 5	Router(config-std-nacl)# {**permit** | **deny**} ...	ACL を定義します。 **（注）** 送信元アドレスは ANY にする必要があります。
ステップ 6	Router(config-std-nacl)# **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 7	Router(config)# **ip access-list extended** *acl-name*	ポート用のデフォルト ACL を定義します。
ステップ 8	Router(config-std-nacl)# {**permit** | **deny**} ...	ACL を定義します。
ステップ 9	Router(config-std-nacl)# **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 10	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	Router(config-if)# **ip access-group** *acl-name* **in**	インターフェイスでデフォルトのスタティック ACL を適用します。
ステップ 12	Router(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。

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。

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# radius-server vsa send authentication
Router(config)# ip device tracking
Router(config)# ip access-list extended my_dacl
Router(config-ext-nacl)# permit tcp any host 10.2.3.4
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended default_acl
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface fastEthernet 2/13
Router(config-if)# ip access-group default_acl in
```

```
Router(config-if)# exit
```

WoL を使った 802.1X 認証の使用

Wake-on-LAN（WoL）を使った 802.1X 認証をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **authentication control-direction** {**both** | **in**}	ポートでの WoL を使った 802.1X 認証をイネーブルにし、以下のキーワードを使用してポートを双方向または単一方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホスト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 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

WoL を使った 802.1X 認証をディセーブルにするには、**no authentication control-direction**（または **no dot1x control-direction**）インターフェイス コンフィギュレーション コマンドを使用します。

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

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# authentication control-direction both
```

MAC 移動のイネーブル化

スイッチで MAC 移動をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **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	Router(config)# **authentication mac-move permit**	スイッチで MAC 移動をイネーブルにします。
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	Router# **show running-config**	（任意）入力を確認します。
ステップ 5	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

MAC 置換のイネーブル化

インターフェイスの MAC 置換をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# 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	`Router(config)# interface interface-id`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-if)# authentication violation {protect | replace | restrict | shutdown}`	インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • **restrict**：違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown**：ポートは、予期しない MAC アドレスを受信すると errdisable になります。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	入力を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で MAC 置換をイネーブルにする例を示します。

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

NEAT オーセンティケータとサプリカント スイッチの設定

- 「NEAT オーセンティケータの設定」（P.83-56）
- 「NEAT サプリカントの設定」（P.83-56）

（注）
- NEAT では、1 台のスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続する必要があります。
- 概要については、「Network Edge Access Topology（NEAT）を使用した 802.1x サプリカントおよびオーセンティケータ スイッチ」（P.83-30）を参照してください。
- cisco-av-pairs 値は、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、サプリカントが正常に認証されたあとでトランクとしてインターフェイスを設定します。

NEAT オーセンティケータの設定

オーセンティケータとしてスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **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	Router(config)# **cisp enable**	CISP をイネーブルにします。
ステップ 3	Router(config)# **interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# **switchport mode access**	ポート モードを **access** に設定します。
ステップ 5	Router(config-if)# **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	Router(config-if)# **dot1x pae authenticator**	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 7	Router(config-if)# **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	Router(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 9	Router# **show running-config interface** *interface-id*	設定を確認します。
ステップ 10	Router# **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。

```
Router# configure terminal
Router(config)# cisp enable
Router(config)# interface gigabitethernet1/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# spanning-tree portfast trunk
```

NEAT サプリカントの設定

サプリカントとしてスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **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	Router(config)# **cisp enable**	CISP をイネーブルにします。
ステップ 3	Router(config)# **dot1x credentials** *profile*	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 4	Router(config)# **username** *suppswitch*	ユーザ名を作成します。
ステップ 5	Router(config)# **password** *password*	新しいユーザ名のパスワードを作成します。

	コマンド	目的
ステップ 6	Router(config)# **dot1x supplicant force-multicast**	ユニキャスト パケットまたはマルチキャスト パケット受信した場合に、スイッチにマルチキャスト EAPOL パケット*だけ*を送信するように強制すると、NEAT はすべてのホスト モードのサプリカント スイッチで機能できます。
ステップ 7	Router(config)# **interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	Router(config-if)# **switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	Router(config-if)# **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	Router(config-if)# **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）サプリカントとして設定します。
ステップ 11	Router(config-if)# **dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルをインターフェイスに対応付けます。
ステップ 12	Router(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 13	Router# **show running-config interface** *interface-id*	設定を確認します。
ステップ 14	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチをサプリカントとして設定する方法を示します。

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

ポート上での 802.1X 認証のディセーブル化

no dot1x pae インターフェイス コンフィギュレーション コマンドを使用して、ポートでの 802.1X 認証をディセーブルにすることができます。

ポートでの 802.1X 認証をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **no dot1x pae authenticator**	ポートでの 802.1X 認証をディセーブルにします。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

802.1X をポートでイネーブルにするもののポートに接続されているクライアントを許可できないようにする 802.1X Port Access Entity（PAE）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。

次にポートでの 802.1X 認証をディセーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/1
Router(config-if)# no dot1x pae authenticator
```

802.1X 設定をデフォルト値にリセットする方法

802.1X 設定をデフォルト値にリセットするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type slot/port*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	Router(config-if)# **dot1x default**	設定可能な 802.1x パラメータをデフォルト値にリセットします。
ステップ 3	Router(config-if)# **end**	特権 EXEC モードに戻ります。

次に、ポートの 802.1X 認証設定をデフォルト値にリセットする例を示します。

```
Router(config)# interface gigabitethernet 3/27
Router(config-if)# dot1x default
```

認証のステータスおよび情報の表示

- 「802.1X ステータスの表示」（P.83-58）
- 「認証の方式およびステータスの表示」（P.83-59）
- 「MAC 認証バイパスのステータスの表示」（P.83-62）

802.1X ステータスの表示

スイッチのグローバルな 802.1X 管理ステータスおよび動作ステータスを表示したり、個別のポートの 802.1X 設定を表示したりするには、次の作業を行います。

コマンド	目的
Router# **show dot1x** [**all** | **interface** *type slot/port*]	スイッチのグローバルな 802.1X 管理ステータスおよび動作ステータスを表示します。 （任意）**all** キーワードを使用して、802.1X 認証を使用するすべてのインターフェイスのグローバルな 802.1X ステータスと 802.1X 設定を表示します。 （任意）**interface** キーワードを使用して、特定のインターフェイスの 802.1X 設定を表示します。

次に、グローバルな 802.1X ステータスを表示する例を示します。

```
Router# show dot1x
Sysauthcontrol              Disabled
Dot1x Protocol Version             2
Critical Recovery Delay          100
Critical EAPOL              Disabled

Router#
```

次に、802.1X 認証を使用するすべてのインターフェイスのグローバルな 802.1X ステータスと 802.1X 設定を表示する例を示します。

```
Router# show dot1x all
Sysauthcontrol              Disabled
Dot1x Protocol Version             2
Critical Recovery Delay          100
Critical EAPOL              Disabled

Dot1x Info for GigabitEthernet3/27
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Router#
```

認証の方式およびステータスの表示

認証の方式およびステータスを表示するには、次のいずれかの作業を行います。

コマンド	目的
Router# **show authentication registrations**	登録済みのすべての方式の詳細を表示します。
Router# **show authentication interface** *interface*	特定のインターフェイスの認証情報を表示します。
Router# **show authentication method** *method*	指定した方式を使用して許可された現在の認証セッションを一覧表示します。
Router# **show authentication sessions** [**handle** *handle*] [**interface** *interface*] [**mac** *mac*] [**method** *method*] [**session-id** *session-id*]	現在の認証セッションに関する情報を表示します。オプションを指定しない場合、現在のすべてのアクティブ セッションが一覧表示されます。キーワードを追加したり組み合わせたりすることで、特定のセッションや一部のセッションに関する詳細情報を表示することができます。

表 83-2　認証セッションのステート

ステート	説明
Idle	セッションが初期化されました。方式はまだ実行されていません。
Running	このセッションの方式が実行中です。
No methods	このセッションの結果を出した方式はありません。
Authc Success	ある方式で、このセッションの認証成功の結果が提供されました。
Authc Failed	ある方式で、このセッションの認証失敗の結果が提供されました。
Authz Success	このセッションでは、すべての機能が正常に適用されました。
Authz Failed	このセッションで、機能の適用に失敗しました。

表 83-3　認証方式のステート

ステート	説明
Not run	指定した方式はこのセッションで実行されていません。
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次に、登録済みの認証方式を表示する例を示します。

```
Router# show authentication registrations
Auth Methods registered with the Auth Manager:
  Handle  Priority  Name
    3        0       dot1x
    2        1       mab
    1        2       webauth
```

次に、特定のインターフェイスに関する認証の詳細を表示する例を示します。

```
Router# show authentication interface gigabitethernet 1/23
Client list:
  MAC Address     Domain   Status              Handle          Interface
  0123.4567.abcd  DATA     Authz Success  0xE0000000  GigabitEthernet1/23

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

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Router# show authentication sessions

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

次に、指定の認証方式を使用して許可されたセッションを表示する例を示します。

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

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Router# show authentication sessions interface gigabitethernet 1/47

Interface:  GigabitEthernet1/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000

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

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

            Interface:  GigabitEthernet1/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001

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

次に、指定のセッション ID の認証セッションを表示する例を示します。

```
Router# show authentication sessions session-id 0B0101C70000004F2ED55218
```

```
            Interface:  GigabitEthernet9/2
           MAC Address:  0000.0000.0011
            IP Address:  20.0.0.7
              Username:  johndoe
                Status:  Authz Success
                Domain:  DATA
        Oper host mode:  multi-host
      Oper control dir:  both
         Authorized By:  Critical Auth
           Vlan policy:  N/A
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  0B0101C70000004F2ED55218
       Acct Session ID:  0x00000003
                Handle:  0x91000001

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

次に、指定の認証方式によって許可されたすべてのクライアントを表示する例を示します。

```
Router# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Router# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

MAC 認証バイパスのステータスの表示

MAB のステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show mab** {**all** | **interface** *type slot/port*} [*detail*]	すべてのインターフェイスまたは特定のインターフェイスに関する MAB 認証の詳細を表示します。

表 83-4　MAB 認証ステート

ステート	説明
INITIALIZE	許可セッションは初期化されています。
ACQUIRING	セッションはクライアントの MAC アドレスを取得中です。
AUTHORIZING	セッションは MAC ベースの許可を待機中です。
TERMINATE	許可セッションの結果が取得されました。

次に、単一のインターフェイスに関する簡単な MAB ステータスを表示する例を示します。

```
Router# show mab interface fa1/1

MAB details for GigabitEthernet1/1
```

```
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
```

次に、単一のインターフェイスに関する詳細な MAB ステータスを表示する例を示します。

```
Router# show mab interface fa1/1 detail

MAB details for GigabitEthernet1/1
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する