CHAPTER 39

802.1X 認証の設定

この章では、Catalyst 6500 シリーズ スイッチ上で IEEE 802.1X 認証を設定する方法について説明します。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

（注） MAC（メディア アクセス制御）アドレス認証バイパスの設定については、第 40 章「MAC 認証バイパスの設定」を参照してください。

（注） イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合に、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティ機能を使用する手順についても説明します。

（注） Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

（注） Network Admission Control（NAC）の設定については、第 42 章「NAC の設定」を参照してください。

この章で説明する内容は、次のとおりです。

- 802.1X 認証の機能（p.39-2）
- 認証のデフォルト設定（p.39-11）
- 認証設定時の注意事項（p.39-12）
- スイッチ上での 802.1X 認証の設定（p.39-13）

802.1X 認証の機能

802.1X 規格では、クライアント / サーバベースのアクセス制御および認証プロトコルを定義しています。このプロトコルは、無許可の装置が公的にアクセス可能なポートから LAN にアクセスするのを制限します。802.1X は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。一方のアクセス ポイントが未制御のポートで、もう一方は制御ポートです。1 つのポートを通過するトラフィックはすべて、両方のアクセス ポイントで利用できます。802.1X は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。802.1X アクセス制御によりデバイスが認証されるまでは、Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけしか、そのデバイスの接続ポートを通過できません。認証に成功すると、通常のトラフィックがポートを通過できるようになります。双方向のトラフィックまたは着信トラフィックのみを制限できます。

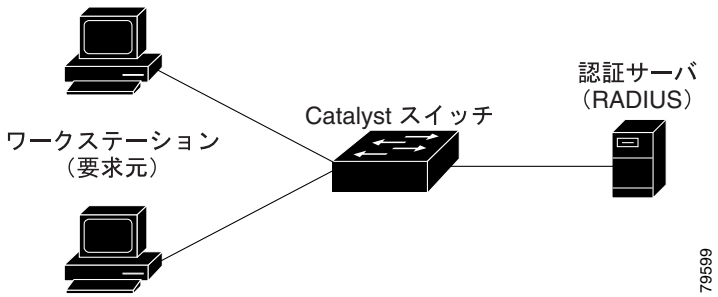
ここでは、次の内容について説明します。

- デバイスの役割（p.39-2）
- 認証の開始とメッセージ交換（p.39-3）
- 許可および無許可ステートのポート（p.39-4）
- 認証サーバ（p.39-6）
- スイッチに設定可能な 802.1X パラメータ（p.39-6）
- RADIUS サーバを使用した 802.1X VLAN 割り当ての概要（p.39-6）
- DHCP での 802.1X 認証の機能（p.39-7）
- 補助 VLAN トラフィック用に設定されたポート上での 802.1X 認証の概要（p.39-8）
- ゲスト VLAN に対する 802.1X 認証の概要（p.39-8）
- ポート セキュリティでの 802.1X 認証の機能（p.39-9）
- ARP トラフィック検査での 802.1X 認証の機能（p.39-10）

デバイスの役割

802.1X ポートベース認証を使用すると、ネットワーク内のデバイスには特定の役割が割り当てられます（図 39-1 を参照）。

図 39-1　802.1X デバイスの役割



- *要求元* — LAN およびスイッチ サービスへのアクセスを要求し、スイッチの要求に応答します。ワークステーションは、802.1X 準拠のソフトウェアを実行している必要があります。

（注）　802.1X では、*クライアント*または*ホスト*に対して*要求元*という用語を使用します。Catalyst 6500 シリーズ CLI の構文では*ホスト*が使用されるので、このマニュアルでは、*要求元*ではなく*ホスト*を使用します。

- *認証サーバ* — 実際にホストの認証を行います。認証サーバは、ホストの ID を確認し、LAN およびスイッチ サービスへのホストのアクセスを許可するかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはホストにトランスペアレントです。このリリースでは、Extensible Authentication Protocol（EAP）拡張機能搭載の Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムが唯一のサポート対象認証サーバです。Cisco Secure Access Control Server バージョン 3.0 で利用できます。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。
- *スイッチ* — ホス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なアクセスを制御します。スイッチは、ホストと認証サーバとの間の媒介（プロキシ）として機能し、ホストに ID 情報を要求し、その情報を認証サーバで確認し、ホストに応答をリレーします。スイッチは RADIUS クライアントと対話します。RADIUS クライアントは EAP フレームのカプセル化およびカプセル化解除を行い、認証サーバと対話します。

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

認証の開始とメッセージ交換

スイッチまたはホストは、認証を開始できます。**set port dot1x** *mod/port* **port-control auto** コマンドを使用してポート上で認証をイネーブルにする場合、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ことを確認したときに、認証を開始する必要があります。スイッチは、EAP-Request/Identity フレームをホストに送信して ID を要求します（一般に、スイッチは最初の ID/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）。ホストは、フレームを受信すると EAP-Response/Identity フレームを送信します。

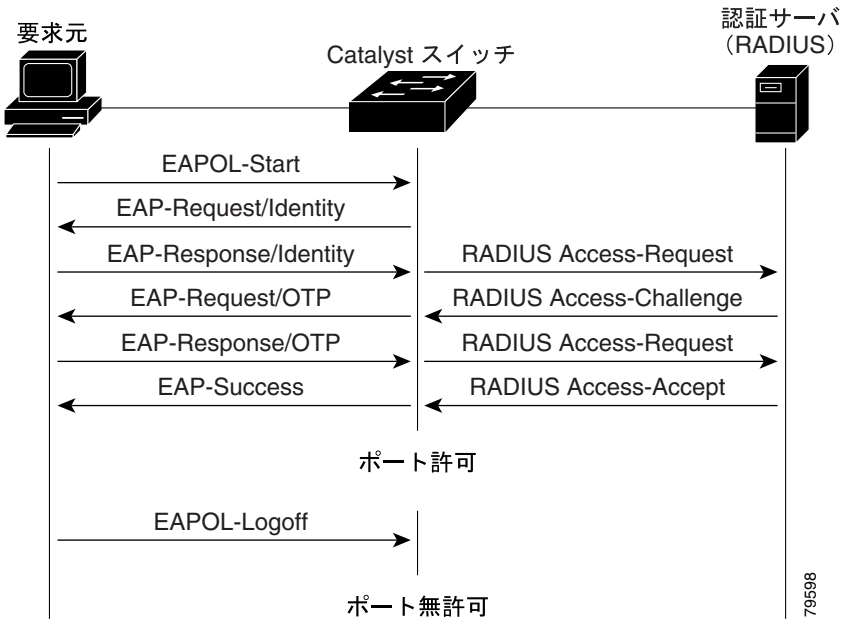
起動中に、ホストがスイッチから EAP-Request/Identity フレームを受信しない場合は、ホストは EAPOL-Start フレームを送信して認証を開始できます。これにより、スイッチはホストの ID を要求するようになります。

（注）　ネットワーク アクセス装置で 802.1X がイネーブルになっていないかサポートされていない場合は、ホストからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもホストが EAP-Request/Identity フレームを受信しない場合は、ホストはポートが許可ステートにあるかのようにフレームを送信します。許可ステートにあるポートは、ホストが正常に認証されたということです。詳細については、「許可および無許可ステートのポート」（p.39-4）を参照してください。

ホストが ID を供給すると、スイッチは媒介として動作し、認証が成功または失敗するまでホストと認証サーバとの間で EAP フレームを受け渡します。認証が成功すると、スイッチのポートは許可された状態になります。詳細については、「許可および無許可ステートのポート」（p.39-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に左右されます。図 39-2 に、RADIUS サーバで One Time Password（OTP; ワンタイム パスワード）認証方式を使用するホストによって開始されるメッセージ交換を示します。

図 39-2　メッセージ交換



許可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、ホストがネットワーク 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、*無許可*ステートで開始します。このステートでは、ポートは、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可していません。ホストが正常に認証されると、ポートは*許可*ステートに移行し、そのホストへのすべてのトラフィックは通常のフローが許可されます。

802.1X をサポートしていないホストが無許可の 802.1X ポートに接続している場合は、スイッチはホストに ID を要求します。この場合、ホストは要求に応答できないので、ポートは無許可ステートのままで、ホストはネットワーク アクセスが許可されません。

802.1X 対応ホストが 802.1X プロトコルを実行していないポートに接続している場合、ホストは EAPOL-Start フレームを送信して認証プロセスを開始します。応答が得られなかった場合、ホストは要求を固定回数だけ送信します。応答が得られないので、ホストはポートが許可ステートにあるかのようにフレームの送信を開始します。

ポートの許可ステートを制御するには、**set port dot1x** *mod/port* **port-control** コマンドと以下のキーワードを使用します。

- **force-authorized —** 802.1X 認証をディセーブルにして、認証交換なしでポートを許可ステートに移行させます。ポートは、ホストの 802.1X ベースの認証なしで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、ホストが認証を試みてもすべて無視します。スイッチは、インターフェイスを介してホストに認証サービスを提供できません。
- **auto —** 802.1X 認証をイネーブルにして、ポートに無許可ステートを開始させ、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、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、ホストの ID を要求し、ホストと認証サーバ間で認証メッセージのリレーを開始します。ネットワークにアクセスしようとする各ホストは、ホストの MAC アドレスを使用して一意に識別されます。

ホストが正常に認証されると（認証サーバから Accept フレームを受信する）、ポート ステートが許可に切り替わり、認証されたホストのフレームはすべてそのポートを通じて許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、認証を再試行できます。スイッチは、認証サーバにアクセスできない場合、要求を再送信できます。指定された試行回数のあとでもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

ホストがログオフすると、サーバは EAPOL-Logoff メッセージを送信し、スイッチ ポートを無許可ステートに移行させます。

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-Logoff メッセージを受信した場合は、ポートは無許可ステートに戻ります。

表 39-1 に、802.1X の用語の説明を示します。

表 39-1　802.1X の用語

用語	定義
認証者 PAE[1]	ポイントツーポイント LAN セグメントの一端のエンティティで、ホストの認証を実行します（「認証者」エンティティともいいます）。認証者は実際の認証方式からは独立しており、認証交換のパススルーとしてのみ機能します。認証者はホストと対話し、ホストからの情報を認証サーバに引き渡し、認証サーバから指示されればホストを認証します。
認証サーバ	認証者 PAE に対して認証サービスを提供するエンティティ。ホスト PAE の証明書を確認してから、ホスト PAE が LAN/ スイッチ サービスへのアクセスを許可するかどうかを、クライアントである認証者 PAE に通知します。
許可ステート	ホスト PAE が許可されたあとのポートのステータス
両方	未許可のスイッチ ポートでの着信および発信の双方向のフロー制御
制御ポート	セキュリティ保護されているアクセス ポイント
EAP	Extensible Authentication Protocol
EAPOL[2]	LAN MAC サービスで直接処理できる、カプセル化された EAP メッセージ
In	未許可スイッチ ポートでの着信フレームに限ったフロー制御
ポート	LAN インフラストラクチャへの単一ポイント接続（MAC ブリッジ ポートなど）
PAE	特定のシステム ポートに対応するポート アクセス エンティティ プロトコル オブジェクト
PDU	プロトコル データ ユニット
RADIUS	Remote Access Dial-In User Service
要求元[3] PAE	LAN/ スイッチ サービスへのアクセスを要求し、認証者からの情報要求に応答するエンティティ
未許可ステート	認証要求元 PAE が許可される前のポートのステータス
未制御ポート	セキュリティ保護されていないアクセス ポイントであり、制御されていない PDU の交換を許可します。

1. PAE = Port Access Entity（ポート アクセス エンティティ）
2. EAPOL = Extensible Authorization Protocol over LAN
3. 802.1X では、*クライアント*または*ホスト*に対して*要求元*という用語を使用します。Catalyst 6500 シリーズ CLI の構文では*ホスト*が使用されるので、このマニュアルでは、*要求元*ではなく*ホスト*を使用します。

認証サーバ

認証者と認証サーバとの間で交換されたフレームは、認証メカニズムによって異なるので、802.1X 規格では定義されていません。他のプロトコルを使用できますが、特に認証サーバがリモートに配置されているときは認証には RADIUS の使用を推奨します。RADIUS には、内蔵の EAP フレームのカプセル化をサポートする拡張機能が搭載されているためです。

スイッチに設定可能な 802.1X パラメータ

スイッチ上で設定できる 802.1X パラメータは、次のとおりです。

- Force-Authorized、Force-Unauthorized、または自動 802.1X ポート制御を指定
- 単一認証、複数認証、および複数ホスト認証を指定
- システム認証制御のイネーブル化およびディセーブル化
- 待機時間の指定
- 認証者からホストへの再送信時間の指定
- バックエンド認証者からホストへの再送信時間の指定
- バックエンド認証者から認証サーバへの再送信時間の指定
- バックエンド認証者からホストに再送信されるフレーム数の指定
- ホストの自動的な再認証時間の指定
- セキュリティ違反後のポート シャットダウン タイムアウト時間の指定
- ホストの自動的な再認証のイネーブル化およびディセーブル化

RADIUS サーバを使用した 802.1X VLAN 割り当ての概要

Release 7.2(2) より前のスーパバイザ エンジン ソフトウェア リリースでは、802.1X クライアントが認証されると、そのクライアントは NVRAM（不揮発性 RAM）に設定された VLAN に加入します。Release 7.2(2) 以降のソフトウェア リリースでは、認証後に 802.1X ホストはその VLAN 割り当てを RADIUS サーバから受信できます。

この VLAN 割り当て機能によって、特定の VLAN に対するユーザ アクセスを制限できます。たとえば、ゲスト ユーザはネットワークへのアクセスが制限された VLAN に割り当てることが可能です。

802.1X 認証を受けたポートは、そのポートに接続されているホストのユーザ名に基づいて、VLAN に割り当てられます。この機能は、ユーザ名と VLAN のマッピングが保存されている RADIUS サーバと連動します。

あるポートの 802.1X 認証が完了すると、RADIUS サーバから VLAN が送信され、ユーザはその VLAN へのアクセス権を与えられます。VLAN 割り当て機能に関連した 802.1X ポートの動作は以下のとおりです。

- リンク確立時、802.1X ポートは NVRAM に設定されている元の VLAN に配置されています。
- リンク確立後、RADIUS が提供する VLAN が有効であり、管理ドメイン内でアクティブな状態であれば、ポートは RADIUS 提供の VLAN に割り当てられます。
- ポートが別の VLAN に属している場合、そのポートは RADIUS が提供する VLAN に移動します。
- RADIUS が提供する VLAN が管理ドメイン内でアクティブな状態でない場合、そのポートは非アクティブ ステートになります。
- RADIUS 提供の VLAN が無効であるか、またはポートのハードウェアに問題がある場合、そのポートは 802.1X 未許可ステートになります。

- 1 つの 802.1X ポートに対して複数ホスト オプションをイネーブルにした場合は、最初の認証済みユーザが受信した RADIUS 提供 VLAN と同じ VLAN にすべてのホストが入ります。
- 802.1X 設定モジュールがダウン状態の場合は、802.1X ポートのすべての Enhanced Address Recognition Logic（EARL）エントリが消去されます。
- 802.1X 設定モジュールがアップ状態に戻ると、すべての 802.1X ポートが NVRAM に設定されている VLAN に割り当てられます。
- 802.1X 設定モジュールのコンフィギュレーションが消去された場合、すべての 802.1X ポートが NVRAM 設定 VLAN に移動し、802.1X ポートの EARL エントリはすべて消去されます。
- 802.1X ポートが許可ステートから未許可ステートに移行すると、そのポートは NVRAM に設定された VLAN に移動します。

「RADIUS サーバを使用した 802.1X VLAN の割り当て」の機能を正常に完了させるには、RADIUS サーバによって以下の 3 つの RFC 2868 属性を認証者（認証ホストと接続しているシスコ製スイッチ）に戻す必要があります。

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-Id = VLAN NAME

属性 [64] には、[VLAN] 値（タイプ 13）が含まれる必要があります。属性 [65] には、[802] 値（タイプ 6）が含まれる必要があります。属性 [81] では、正常に認証された 802.1X 認証ホストを割り当てた VLAN 名を指定します。

（注）　VLAN は、番号ではなく名前で指定する必要があります。

DHCP での 802.1X 認証の機能

802.1X 認証は Dynamic Host Configuration Protocol（DHCP）をサポートしており、認証済みユーザの ID を DHCP 検出プロセスに付加することによって、DHCP サーバが異なるエンド ユーザのクラスに IP アドレスを割り当てることを可能にします。これを利用すれば、エンド ユーザに付与された IP アドレスをアカウンティングのために保護したり、レイヤ 3 の基準に準拠したサービスを提供したりできます。RADIUS サーバが要求元を認証すると、DHCP サーバは IP アドレスのリースに関連付けられた認証済みユーザの ID を保持します。この認証済みユーザの ID は、DHCP 検出プロセスに付加されます。それにより、異なるユーザのクラスごとに異なるアドレスを割り当てることができます。

要求元と 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。この属性は、DHCP サーバ内のアドレス プールへのマッピングに使用されます。スイッチは DHCP リレー エージェントとして機能できるため、DHCP メッセージを受け取り、そのメッセージを他のインターフェイスで伝送するために再生成できます。要求元が（認証後に）DHCP を検出すると、スーパバイザ エンジン上の DHCP リレー エージェントがパケットを受信し、RADIUS サーバから受信して格納した属性を DHCP 発見パケットに付加し、再びブロードキャストします。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、同じユーザが複数のポートの 802.1X ホストを通じて認証できます。

補助 VLAN トラフィック用に設定されたポート上での 802.1X 認証の概要

Multiple VLAN Access Port（MVAP）の 802.1X をイネーブルにできます。また、802.1X ポートの補助 VLAN ID をイネーブルにできます。

802.1X 認証および補助 VLAN 用に設定されたポートを単一ホスト認証モードにして、IP Phone からの補助 VLAN タグ付きパケットを転送する必要があります。IP Phone にはホスト PAE 機能が装備されていないので、802.1X 認証用に設定されたポート上で IP Phone からの補助 VLAN タグ付きパケットを受信したときは、パケットは許可トラフィックとして転送されます。

IP Phone の先に接続されているホスト PAE は認証されます。IP Phone の先のホスト PAE からのトラフィックだけが認証後に転送されます。

（注）　802.1X 対応 VLAN ポートに接続した IP Phone にホスト PAE を接続した場合は、古いホストを取り外したあとで新しいホスト PAE が認証されます。新しいホスト PAE からのトラフィックだけが認証後に転送されます。

ゲスト VLAN に対する 802.1X 認証の概要

ここでは、ゲスト VLAN に対する 802.1X 認証について説明します。

ゲスト VLAN 機能によって、802.1X 非対応ホストは 802.1X 認証を使用するネットワークにアクセスできます。802.1X 認証をサポートするようにシステムをアップグレードしているときに、ゲスト VLAN を使用できます。

802.1X ゲスト VLAN として VLAN を設定すると、802.1X 非対応ホストはすべてこの VLAN に入れられます。どのような VLAN（プライベート VLAN と RSPAN VLAN を除く）もゲスト VLAN として設定できます。ポートがすでにゲスト VLAN で転送を行っているときに、そのホストのネットワーク インターフェイス上での 802.1X サポートをイネーブルにすると、ポートはただちにゲスト VLAN から除外され、認証者は認証発生待ちとなります。

ポート上での 802.1X 認証をイネーブルにすると、802.1X プロトコルが実行されます。ホストが一定時間内に認証者からのパケットに応答できない場合、認証者はそのホストをゲスト VLAN に入れます。

ゲスト VLAN は、単一認証と複数ホスト モードの両方でサポートされています。

（注）　ゲスト VLAN 機能を認証失敗 VLAN 機能と対比させてください。従来型の 802.1X ポートでは、スイッチはポートに接続された要求元の ID 情報が認証サーバで検証されて認証されるまで、ネットワークへのアクセスを提供しません。認証失敗 VLAN 機能を使用すれば、ポート単位で認証失敗 VLAN を設定できます。要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。

認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。

詳細については、「認証失敗 VLAN の設定」（p.39-37）を参照してください。

Windows XP ホストでのゲスト VLAN に対する 802.1X 認証の際の使用上の注意事項

ここでは、Windows XP ホストでのゲスト VLAN に対する 802.1X 認証を設定する際の注意事項について説明します。

- ゲスト VLAN がポートでイネーブルの場合、そのポートは単一方向のポートとして設定できません。また、その逆に単一方向ポートをゲスト VLAN に設定できません。
- ホストが認証者に応答できない場合、ポートは 180 秒間接続されたままです。180 秒が経過すると、ログイン / パスワード ウィンドウはホストに表示されません。解決策はユーザに接続を解除させ、ネットワーク インターフェイス ケーブルを再接続することです。
- 不正なログイン / パスワードにより応答するホストは、認証を失敗し、ゲスト VLAN に割り当てられません。ホストが初めて認証に失敗すると、待機時間タイマーが始動し、稼働している間はアクティビティが一切発生しません。待機時間タイマーが満了すると、ホストにログイン / パスワード ウィンドウが表示されます。ホストが 2 度めも認証に失敗すると、待機時間タイマーが再度始動し、稼働している間はアクティビティが一切発生しません。ホストに 3 度めのログイン / パスワード ウィンドウが表示されます。3 度めも失敗すると、ポートは接続しているが未許可ステートに入れられます。この問題の解決策はユーザに接続を解除させ、ネットワーク インターフェイス ケーブルを再接続することです。
- ホストが認証者 PAE からのユーザ名およびパスワード認証要求に応答しない場合、それはゲスト VLAN に配置されます。

（注）　ゲスト VLAN はローカル スイッチに限定され、VTP を通じて伝播されることはありません。

ポート セキュリティでの 802.1X 認証の機能

802.1X 認証はポート セキュリティ機能と互換性があります（詳細については、第 37 章「ポート セキュリティの設定」を参照）。特定ポートの 1 つだけの MAC アドレスのポート セキュリティをイネーブルにした場合は、その MAC アドレスだけが RADIUS サーバを介して認証されます。それ以外の MAC アドレスを通じて接続しているユーザはすべて、アクセスが拒否されます。複数の MAC アドレスのポート セキュリティをイネーブルにしている場合は、各アドレスは 802.1X RADIUS サーバを介して認証が必要です。

（注）　警告 CSCin25663 のため、ポート セキュリティ用に設定する MAC アドレスから logoff メッセージを受信した場合、またはその特定の MAC アドレスの再認証に失敗した場合、その MAC アドレスは削除されます。この問題は今後のソフトウェア リリースで解決されます。

（注）　802.1X 認証とポート セキュリティが任意の 802.1X ポート上でイネーブルになっているときは、ポート上では 802.1X 認証がポート セキュリティに優先されます。まずホストが認証され、それからポート セキュリティによって保護されます。

802.1X モード（単一認証モード、複数ホスト モード、または複数認証モード）に対してポート セキュリティをイネーブルにできます。1 つのポート上で一度にイネーブルにできるのは 1 つのモードだけです。デフォルトのポート モードは単一認証モードです。

単一認証モードおよび複数ホスト モードのポート セキュリティをディセーブルにできます。ただし、複数認証モードのポート セキュリティはディセーブルにできません。

MAC アドレス ベースのポート セキュリティについてイネーブルに設定されているポートで、802.1X 認証もイネーブルにすると、最大許容数の MAC アドレスを設定していないかぎりは、ポート上で 802.1X 認証は発生しません。802.1X 単一ホスト モード認証もイネーブルに設定されているポートに対して、最大許容数未満の MAC アドレスを設定すると、設定済みの MAC アドレスを削除するかどうかを尋ねるシステム メッセージが表示されます。このメッセージに [yes] と応答すると、MAC アドレス ベースのポート セキュリティに対して設定された MAC アドレスは削除され、ポートは 802.1X 認証を使用して認証されます。その他のモードに対して 802.1X 認証がイネーブルに設定されている場合は、メッセージは表示されず、MAC アドレスは保持されます。

複数認証モードでは、すべての接続ホストは 802.1X を使用して認証され、ポート セキュリティを使用して保護されています。802.1X は、MAC アドレスを認証してから MAC アドレスにポート セキュリティを施して保護します。MAC アドレスが EAPOL-Logoff パケットを送信すると、ポート セキュリティ テーブルから MAC アドレスが削除されます。

ARP トラフィック検査での 802.1X 認証の機能

（注）　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

（注）　ARP トラフィック検査と 802.1X の設定は相互に排他的な関係にあります。

ARP トラフィック検査によって、セキュリティ ACL（VACL）フレームワーク内に順序依存型の一連のルールを設定して ARP テーブルへの攻撃を防止できます。ARP トラフィック検査は 802.1X ポート認証プロトコルを補完するもので、認証されたクライアントの MAC アドレスをポートにバインドしてから、IP/MAC アドレスのバインドを追加することで追加のスプーフ検査に対する MAC アドレスのスプーフィングの可能性を排除します。

ARP トラフィック検査を 802.1X 認証と併用することにより、悪意のあるユーザ / ホストが他のホストの ARP テーブルを破壊する可能性を排除し、ポートおよびユーザのセキュリティを強化できます。要求元の 802.1X 認証が成功したあと、ARP トラフィック検査（要求元の IP アドレスおよび MAC アドレスをバインドします）が実行され、スプーフィングの可能性を排除します。

ARP は認証メカニズムを備えていない簡易プロトコルで、ARP 要求および応答が正しいかどうかを確認する方法がありません。認証メカニズムがなければ、悪意のあるユーザ / ホストによってレイヤ 2 ネットワークまたはブリッジ ドメインにある同じ VLAN 上の他のホストの ARP テーブルが破壊される可能性があります。

たとえば、ユーザ / ホスト A（悪意のあるユーザ）が、デフォルト ルータの IP アドレスとホスト A の MAC アドレスで、非送信請求 ARP 応答（不必要な ARP パケット）をサブネット上の他のホストに送信することがあります。従来の OS（オペレーティング システム）では、デフォルト ルータのスタティック ARP エントリがホストにすでにある場合でも、ホスト A からの新たにアドバタイズされたバインディングが学習されます。ホスト A が IP 転送をイネーブルにし、すべてのパケットを「スプーフィングされた」ホストとルータ間でやり取りする場合、ホスト A は（たとえば dsniff プログラムを使用して）man-in-the-middle 攻撃を実行できます。スプーフィングされたホストでは、そのトラフィックのすべてにスニッフィングが行われていることを認識しません。

また、ARP 検査を実行することで、（イーサネット ヘッダーにある）送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄できます。**set security acl arp-inspection match-mac** {**enable** [**drop** [**log**]] | **disable**} コマンドを CLI から入力することで、この機能をイネーブル（またはディセーブル）にできます。

ARP トラフィック検査の設定については、「ARP トラフィックの検査」（p.15-30）を参照してください。

認証のデフォルト設定

表 39-2 に、802.1X 認証のデフォルト設定を示します。

表 39-2　802.1X 認証のデフォルト設定

機能	デフォルト値
PAE 機能	認証者のみ
プロトコル バージョン	1
802.1X ポート制御	Force-Authorized
802.1X 複数ホスト	ディセーブル
802.1X システム認証制御	イネーブル
802.1X 待機時間	60 秒
802.1X 認証者からホストへの再送信時間	30 秒
802.1X バックエンド認証者からホストへの再送信時間	30 秒
802.1X バックエンド認証者から認証サーバへの再送信時間	30 秒
バックエンド認証者からホストに再送信される 802.1X フレーム数	2
802.1X ホストの自動再認証時間	3600 秒
802.1X 認証者によるホストの自動再認証	ディセーブル
802.1X シャットダウン タイムアウト時間	300 秒
802.1X RADIUS アカウンティング	ディセーブル
802.1X RADIUS VLAN 割り当て	イネーブル
802.1X RADIUS キープアライブ ステート	イネーブル

認証設定時の注意事項

ここでは、スイッチ上で 802.1X 認証を設定する際の注意事項について説明します。

- 802.1X は他のプロトコルでも機能しますが、リモートに配置された認証サーバでは RADIUS を使用することを推奨します。
- 802.1X はイーサネット ポート上でのみサポートされています。
- Release 7.5(1) では、2 つの帯域内管理インターフェイスの sc0 と sc1 をサポートしています。802.1X 認証は、RADIUS サーバと通信するときは、常に認証者の ID として sc0 インターフェイスを使用します。sc1 インターフェイスでは 802.1X 認証はサポートされていません。
- 802.1X をトランク ポート上でイネーブルに設定するには、そのポートのトランキングをオフにする必要があります。802.1X ポート上でトランキングをイネーブルに設定することはできません。
- 802.1X をダイナミック ポート上でイネーブルに設定するには、そのポートのダイナミック VLAN をオフにする必要があります。802.1X ポート上でダイナミック VLAN をイネーブルに設定することはできません。
- 802.1X をチャネリング ポート上でイネーブルに設定するには、そのポートのチャネリングをオフにする必要があります。802.1X ポート上でチャネリングをイネーブルに設定することはできません。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポート上では 802.1X をイネーブルに設定することはできません。また、802.1X ポート上で SPAN 宛先を設定することはできません。ただし、802.1X ポートを SPAN 送信元ポートとして設定することはできます。
- 補助 VLAN を **dot1p** または **untagged** に設定できません。また、補助 VLAN は 802.1X 対応ポート上のネイティブ VLAN と同じにしてはなりません。
- 802.1X 対応補助 VLAN ポート上では、複数認証オプションをイネーブルにできません。802.1X 対応 AUX ポート上で複数ホスト オプションをイネーブルにすることは推奨できません。
- 802.1X 対応補助 VLAN ポートは、ポート上の補助 VLAN がゲスト VLAN と同じ場合は、ゲスト VLAN に入れられないので、補助 VLAN と同じゲスト VLAN を割り当てないでください。
- 802.1X 対応ポートでは、管理上設定された VLAN は補助 VLAN と同じにすることはできません。
- プライベート VLAN および 802.1X の設定は相互に排他的な関係にあります。
- PFC3A/PFC3B/PFC3BXL を使用することにより、**set rate-limit l2port-security** コマンドを使用してスイッチ上で 802.1X ポート セキュリティ レート リミッタをグローバルにイネーブル、ディセーブル、または設定できます。レート制限設定の詳細については、「スイッチ上でのレイヤ 2 PDU レート制限の設定」（p.8-65）を参照してください。

スイッチ上での 802.1X 認証の設定

ここでは、スイッチ上で 802.1X 認証を設定する手順について説明します。

（注）　VLAN 割り当てに関する RADIUS サーバの使用については、「RADIUS サーバを使用した 802.1X VLAN 割り当ての概要」（p.39-6）を参照してください。

- 802.1X 認証のグローバルなイネーブル化（p.39-13）
- 802.1X 認証のグローバルなディセーブル化（p.39-14）
- 各ポートに対する 802.1X 認証のイネーブル化（p.39-14）
- アクセス不可能認証バイパスでの 802.1X のイネーブル化（p.39-15）
- 複数 802.1X 認証のイネーブル化（p.39-16）
- ホストの自動再認証の設定およびイネーブル化（p.39-17）
- 手動でのホストの再認証（p.39-18）
- 複数ホストのイネーブル化（p.39-18）
- 複数ホストのディセーブル化（p.39-18）
- 待機時間の設定（p.39-19）
- シャットダウン タイムアウト時間の設定（p.39-19）
- 認証者からホストへの EAP-Request/Identity フレーム再送信時間の設定（p.39-19）
- バックエンド認証者からホストへの EAP-Request フレーム再送信時間の設定（p.39-20）
- バックエンド認証者から認証サーバへのトランスポート レイヤ パケット再送信時間の設定（p.39-20）
- バックエンド認証者からホストへの再送信フレーム数の設定（p.39-21）
- 802.1X コンフィギュレーション パラメータのデフォルト値へのリセット（p.39-21）
- DHCP リレー エージェントでの 802.1X 認証のイネーブル化（p.39-22）
- DHCP リレー エージェントでの 802.1X 認証のディセーブル化（p.39-23）
- 802.1X ゲスト VLAN へのホストの追加（p.39-23）
- 802.1X 単一方向制御ポートの設定（p.39-24）
- ACL 割り当てでの 802.1X の設定（p.39-25）
- 802.1X ユーザ分散の設定（p.39-32）
- 802.1X RADIUS アカウンティングとトラッキングのイネーブル化およびディセーブル化（p.39-34）
- 認証済み ID とポート説明のマッピングの設定（p.39-35）
- RADIUS サーバ設定の DNS レゾリューションの設定（p.39-36）
- 認証失敗 VLAN の設定（p.39-37）
- RADIUS サーバ フェールオーバーの設定（p.39-38）
- show コマンドの使用方法（p.39-39）

802.1X 認証のグローバルなイネーブル化

各ポートに対して 802.1X 認証を設定するには、先にシステム全体でイネーブルに設定する必要があります。802.1X 認証をグローバルにイネーブルにすると、802.1X 認証の要求する特定の要件を各ポートが満たしていれば、各ポートに 802.1X 認証を設定できます。各ポートに 802.1X 認証を設定する手順については、「各ポートに対する 802.1X 認証のイネーブル化」（p.39-14）を参照してく

ださい。

802.1X 認証をグローバルにイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
802.1X 認証をグローバルにイネーブルにします。	**set dot1x system-auth-control enable**

次に、802.1X 認証をグローバルにイネーブルにする例を示します。

```
Console> (enable) set dot1x system-auth-control enable
dot1x system-auth-control enabled.
```

802.1X 認証のグローバルなディセーブル化

802.1X 認証をシステム全体に対してイネーブルに設定しているときは、これをグローバルにディセーブルにできます。802.1X 認証をグローバルにディセーブルにすると、(それまで 802.1X 認証を設定していたポートを含め)、どのポートでも 802.1X 認証を利用できなくなります。

802.1X 認証をグローバルにディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
802.1X 認証をグローバルにディセーブルにします。	**set dot1x system-auth-control disable**

次に、802.1X 認証をグローバルにディセーブルにする例を示します。

```
Console> (enable) set dot1x system-auth-control disable
dot1x system-auth-control disabled.
```

各ポートに対する 802.1X 認証のイネーブル化

802.1X 認証をグローバルにイネーブルにすると、コンソールから各ポートに対して 802.1X 認証をイネーブルにする必要があります。802.1X 認証をグローバルにイネーブルに設定する手順については、「802.1X 認証のグローバルなイネーブル化」(p.39-13) を参照してください。

(注) スイッチ上で 802.1X 認証をイネーブルにする前に、少なくとも 1 つの RADIUS サーバを指定する必要があります。詳細については、第 21 章「AAA によるスイッチ アクセスの設定」を参照してください。

スイッチへのアクセスに 802.1X 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で 802.1X 制御をイネーブルにします。	**set port dot1x** *mod/port* **port-control auto**
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、モジュール 3 のポート 1 上で 802.1X 認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port dot1x 3/1 port-control auto
Port 3/1 dot1x port-control is set to auto.
Trunking disabled for port 3/1 due to Dot1x feature.
Spantree port fast start option enabled for port 3/1.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------- -----------------   ----------------   ---------------
 3/1  SingleAuth    disabled            disabled           Both    Both
Console> (enable)
```

（注）　新しい認証のために現状のマシンを消去するには、**set port dot1x** *mod/port* **initialize** コマンドを入力します。

アクセス不可能認証バイパスでの 802.1X のイネーブル化

802.1X アクセス不可能認証バイパスをポート単位でイネーブルにできます。この機能により、ポートをクリティカルとして指定できます。ポートがクリティカルとして指定された場合、802.1X は通常の方法でこのポートを認証しようとします。認証サーバに到達できないポートでも、管理上設定された VLAN またはポートのネイティブ VLAN 内のネットワークにアクセスできます。ポートが単一認証モードの場合に限り、ポートをクリティカルとして設定できます。

クリティカル ポートがネットワークへのアクセス権を取得して、認証サーバが使用可能になると、クリティカル ポートは無許可ステートに戻り、通常の認証プロセスが再開します。クリティカル ポートが認証されると、RADIUS サーバが指定した VLAN に移行します。この時点で、**set port dot1x** *mod/port* **initialize** コマンドを使用して、ポートを手動で初期化する必要があります。

ホストが通常の認証プロセスにより認証されたあとで認証サーバがダウンした場合、スイッチはこのポートがクリティカル ポートかどうかを確認します。スイッチがこのポートをクリティカル ポートと判断した場合、このポートに対する通常の再認証プロセスは一時的にディセーブルになります。ポートは、認証サーバがアクティブになり認証プロセスを再開するまで、ネットワークへのアクセス権が与えられます。

ポートをクリティカル ポートとして指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポートをクリティカル ポートとして指定します。	**set port dot1x** *mod/port* **critical** {**enable** | **disable**}
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、クリティカル ポートとしてポートを指定する例を示します。

```
Console> (enable) set port dot1x 5/48 critical enable
Port 5/48 critical-port option is enabled
Console> (enable)
```

次に、802.1X の設定を確認する例を示します。

```
Console> (enable) show port dot1x 5/48
Port  Auth-State           BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 5/48 -                   -          force-authorized    -

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 5/48 SingleAuth    disabled            disabled           Both    -

Port  Posture-Token Critical Termination action Session-timeout
----- ------------ -------- ------------------ ---------------
 5/48 -            YES      -                  -
Console> (enable)
```

複数 802.1X 認証のイネーブル化

複数のホストが 802.1X ポートにアクセスできるように、複数認証を指定できます。シスコ独自の複数認証では、1 つのポート上で複数の dot1x ホストの認証が可能で、すべてのホストが別個に認証されます。複数 802.1X 認証をイネーブルにする際は次の注意事項に従ってください。

- 複数の認証済みポートの非 802.1X ホストからのトラフィックはブロックされます。
- ゲスト VLAN は、複数の認証済みポート上でイネーブルにできません。
- MVAP 上では複数認証はイネーブルにできません。
- 複数の認証済みポートはポート VLAN になり、RADIUS 指定の VLAN にはなりません。
- ポート上で複数認証をイネーブルにするには、先にポート セキュリティをポート上でイネーブルにする必要があります。
- 複数の認証済みポート上では、ポート セキュリティをディセーブルにできません。
- ポート セキュリティ タイマーは、複数の認証済みポートで使用します。再認証タイマーは、複数の認証済みポートでは使用しません。

複数 802.1X 認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定のポート上で複数 802.1X 認証をイネーブルにします。	**set port dot1x** *mod*/*port* **multiple-authentication** {**enable** | **disable**}
ステップ 2	802.1X の設定を確認します。	**show port dot1x** *mod*/*port*

次に、モジュール 3 のポート 1 上で複数 802.1X 認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-authentication enable
PortSecurity should be enabled on port 3/1, before enabling Multiple-authentication
Port Security not enabled on 3/1.
Console> (enable) set port security 3/1 enable
Port 3/1 security enabled.
Console> (enable) set port dot1x 3/1 multiple-authentication enable
Port 3/1 Multiple-authentication option enabled
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 3/1  MultiAuth    disabled            disabled           Both    Both
Console> (enable)
```

ホストの自動再認証の設定およびイネーブル化

802.1X ホストの自動再認証をイネーブルに設定する前であれば、802.1X 認証がホストを再認証する頻度を指定できます。ホストの自動再認証をイネーブルに設定する前に期間を指定しない場合は、802.1X は 3600 秒をデフォルト設定とします（有効な値は 1 ～ 65,535 秒です）。

特定ポートに接続したホストの 802.1X ホスト自動再認証をイネーブルにできます。特定ポートに接続したホストを手動で再認証する手順については、「手動でのホストの再認証」（p.39-18）を参照してください。

802.1X 認証がホストを再認証する頻度を設定し、802.1X 自動再認証をイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホストの再認証の時間定数を設定します。	**set dot1x re-authperiod** *seconds*
ステップ 2	再認証をイネーブルにします。	**set port dot1x** *mod/port* **re-authentication enable**
ステップ 3	802.1X の設定を確認します。	**show port dot1x** *mod/port*

次に、自動再認証を 7,200 秒に設定し、ポート 3/1 で 802.1X 再認証をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable) set port dot1x 3/1 re-authentication enable
Port 3/1 Dot1x re-authentication enabled.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 3/1  MultiAuth    enabled             disabled           Both    Both
Console> (enable)
```

手動でのホストの再認証

特定のポートに接続したホストは、いつでも手動で再認証できます。802.1X ホストに自動再認証の設定をする場合は、「ホストの自動再認証の設定およびイネーブル化」（p.39-17）を参照してください。

特定のポートに接続したホストを手動で再認証するには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポートに接続したホストを手動で再認証します。	**set port dot1x** *mod/port* **re-authenticate**

次に、モジュール 3 のポート 1 に接続したホストを手動で再認証する例を示します。

```
Console> (enable) set port dot1x 3/1 re-authenticate
Port 3/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 3/1 authorized.
Console> (enable)
```

複数ホストのイネーブル化

特定ポートをイネーブルにして複数ユーザのアクセスを可能にします。ポートが複数のユーザに対してイネーブルで、そのポートに接続したホストが正常に許可されているとき、MAC アドレスを持つホストはすべて、そのポートに対してトラフィックを送受信することができます。そのあとでハブを介して複数のホストをそのポートに接続すると、そのポートのセキュリティ レベルを低くすることができます。

特定のポート上で複数ホストのアクセスをイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポート上で複数ホストをイネーブルにします。	**set port dot1x** *mod/port* **multiple-host enable**

次に、モジュール 3 のポート 1 上で複数ホストのアクセスをイネーブルにする例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-host enable
Port 3/1 Multiple-host option enabled.
Console> (enable)
```

複数ホストのディセーブル化

イネーブルに設定されているポート上で複数ユーザのアクセスをディセーブルに設定できます。

特定のポート上で複数ホストのアクセスをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
特定のポート上で複数ホストをディセーブルにします。	**set port dot1x** *mod/port* **multiple-host disable**

次に、モジュール 3 のポート 1 上で複数ホストのアクセスをディセーブルにする例を示します。

```
Console> (enable) set port dot1x 3/1 multiple-host disable
Port 3/1 Multiple-host option disabled.
Console> (enable)
```

待機時間の設定

認証者がホストを認証できないときは、一定時間のアイドル状態を経て再試行します。アイドル時間は、quiet-period の値によって決まります（デフォルトの設定は 60 秒です）。この値は、0 ～ 65,535 秒の範囲で設定できます。

待機時間の値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
待機時間の値を設定します。	**set dot1x quiet-period** *seconds*

次に、待機時間を 45 秒に設定する例を示します。

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
Console> (enable)
```

シャットダウン タイムアウト時間の設定

セキュリティ違反のためにポートがシャットダウンした場合、手動で再度イネーブルにするか、シャットダウン タイムアウト時間を設定してポートが再びイネーブルになるようにする必要があります。

セキュリティ違反のあとにポートがディセーブルになる期間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
シャットダウン タイムアウト時間を設定します。	**set dot1x shutdown-timeout** *1 – 65535 seconds*

次に、シャットダウン タイムアウト時間を設定する例を示します。

```
Console> (enable) set dot1x shutdown-timeout 300
dot1x shutdown-timeout set to 300 seconds.
Console> (enable)
```

認証者からホストへの EAP-Request/Identity フレーム再送信時間の設定

ホストは、EAP-Request/Identity フレームを受信したことを認証者に通知します。認証者は、この通知を受信しないときは、一定時間待機してから、フレームを再送信します。認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

認証者からホストへの EAP-Request/Identity フレームの再送信時間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証者からホストへの EAP-Request/Identity フレームの再送信時間を設定します。	**set dot1x tx-period** *seconds*

次に、認証者からホストへの EAP-Request/Identity フレームの再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
Console> (enable)
```

バックエンド認証者からホストへの EAP-Request フレーム再送信時間の設定

ホストは、EAP-Request フレームを受信したことをバックエンド認証者に通知します。バックエンド認証者は、この通知を受信しないときは、一定時間待機してから、フレームを再送信します。バックエンド認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

バックエンド認証者からホストへの EAP-Request フレーム再送信時間を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者からホストへの EAP-Request フレーム再送信時間を設定します。	**set dot1x supp-timeout** *seconds*

次に、バックエンド認証者からホストへの EAP-Request フレーム再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
Console> (enable)
```

バックエンド認証者から認証サーバへのトランスポート レイヤ パケット再送信時間の設定

認証サーバは、トランスポート レイヤ パケットを受信するたびにバックエンド認証者に通知します。バックエンド認証者は、パケットの送信後この通知を受信 *しない* ときは、一定時間待機してから、パケットを再送信します。バックエンド認証者が通知を待つ時間を 1 ～ 65,535 秒の範囲で設定できます（デフォルトの設定は 30 秒です）。

バックエンド認証者から認証サーバへのトランスポート レイヤ パケットの再送信時間の値を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者から認証サーバへの、トランスポート レイヤ パケットの再送信時間を設定します。	**set dot1x server-timeout** *seconds*

次に、バックエンド認証者から認証サーバへの、トランスポート レイヤ パケットの再送信時間を 15 秒に設定する例を示します。

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
Console> (enable)
```

バックエンド認証者からホストへの再送信フレーム数の設定

認証サーバは、一定数のフレームを受信するたびにバックエンド認証者に通知します。バックエンド認証者は、フレーム送信後にこの通知を受信しないときは、一定時間待機してから、そのフレームを再送信します。バックエンド認証者が再送信するフレーム数を 1 ～ 10 の範囲（デフォルトは 2）で設定できます。

バックエンド認証者からホストに再送信されるフレーム数を設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バックエンド認証者からホストへの再送信フレーム数を設定します。	**set dot1x max-req** *count*

次に、バックエンド認証者からホストに再送信されるフレーム数を 4 に設定する例を示します。

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
Console> (enable)
```

802.1X コンフィギュレーション パラメータのデフォルト値へのリセット

1 つのコマンドで、802.1X コンフィギュレーション パラメータをデフォルト値に戻すことができます。これは 802.1X をグローバルにディセーブルにすることにもなります。

802.1X コンフィギュレーション パラメータをデフォルト値に戻すには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	802.1X コンフィギュレーション パラメータをデフォルト値に戻し、802.1X をグローバルにディセーブルにします。	**clear dot1x config**
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、802.1X コンフィギュレーション パラメータをデフォルト値に戻し、設定を確認する例を示します。

```
Console> (enable) clear dot1x config
This command will disable dot1x on all ports and take dot1x parameter values back to
factory defaults.
Do you want to continue (y/n) [n]?
Console> (enable) show dot1x
PAE Capability              Authenticator Only
Protocol Version            1
system-auth-control         enabled
max-req                     2
quiet-period                45 seconds
radius-accounting           disabled
radius-vlan-assignment      enabled
radius-keepalive state      enabled
re-authperiod               7200 seconds
server-timeout              30 seconds
shutdown-timeout            300 seconds
supp-timeout                30 seconds
tx-period                   30 seconds

Console> (enable)
```

DHCP リレー エージェントでの 802.1X 認証のイネーブル化

DHCP リレー エージェントが特定の VLAN の 802.1X パラメータを DHCP サーバに送信できるようにするには、イネーブル モードで次の作業を行います。

（注）　管理 VLAN（sc0 または sc1 インターフェイスで設定されている VLAN）を、dot1x-dhcp Access Control Entry（ACE; アクセス制御エントリ）のある Access Control List（ACL; アクセス制御リスト）にマッピングできません。VLAN 1 または VLAN 2 が dot1x-dhcp ACE のある ACL にマッピングされる際に、**clear config interface** コマンドを使用できません。

	作業	コマンド
ステップ 1	DHCP リレー エージェントの 802.1X 認証をイネーブルにします。 （注）　このコマンドは、指定された ACL 名で ACE エントリを生成します。この ACL は他の ACE エントリを持つこともできますが、DHCP の ACE エントリが優先されます。	**set security acl ip** *acl_name* **permit dot1x-dhcp**
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、802.1X の DHCP リレー トラフィック用の ACL エントリを作成する例を示します。

```
Console> (enable) set security acl ip dhcp_relay permit dot1x_dhcp
Successfully configured Dot1x Dhcp ACL for dhcp_relay. Use 'commit' command to save
changes
```

次に、既存の ACL エントリ上で DHCP 以外のトラフィックを許可するように ACL を設定する例を示します。

```
Console> (enable) set security acl ip dhcp_relay permit any
dhcp_relay editbuffer modified. Use 'commit' command to apply changes.
console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl dhcp_relay
Commit operation in progress
ACL 'dhcp_relay' successfully committed.
```

次に、dhcp-relay-acl に適用する VLAN をマッピングする例を示します。

```
Console> (enable) set security acl map dhcp_relay 1-3,20
Mapping in progress...
ACL dhcp_relay successfully mapped to VLAN 1.
ACL dhcp_relay successfully mapped to VLAN 2.
ACL dhcp_relay successfully mapped to VLAN 3.
ACL dhcp_relay successfully mapped to VLAN 20.
```

クライアントからサーバに転送される DHCP パケットには、DHCP リレー エージェント情報フィールドが追加されます。[dhcp-relay-acl] にマッピングされていない VLAN とすべての DHCP パケットは変更なく従来どおりスイッチされます。

DHCP リレー エージェントでの 802.1X 認証のディセーブル化

DHCP リレー エージェントが特定の VLAN の 802.1X パラメータを DHCP サーバに送信しないようにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	DHCP リレー エージェントの 802.1X 認証をディセーブルにします。	**clear security acl map dhcp_relay** *vlan_ID*
ステップ 2	802.1X の設定を確認します。	**show dot1x**

次に、VLAN1 ～ 3 および 20 の 802.1X 認証パラメータを送信しないように DHCP リレー エージェントを設定し、設定を確認する例を示します。

```
Console> (enable) clear security acl map dhcp_relay 1-3,20
Successfully cleared mapping between ACL dhcp_relay and VLAN 1.
Successfully cleared mapping between ACL dhcp_relay and VLAN 2.
Successfully cleared mapping between ACL dhcp_relay and VLAN 3.
Successfully cleared mapping between ACL dhcp_relay and VLAN 20.
```

802.1X ゲスト VLAN へのホストの追加

一般的に、ゲスト VLAN は最小限のサービスをサポートし、最小限のネットワーク アクセスを行います。ホストは、**set port dot1x** *mod/port* **port-control auto** コマンド オプションが使用された場合にだけ、ゲスト VLAN に追加されます。**set port dot1x** *mod/port* **port-control** コマンド オプションを **auto** から **force-authorized** または **force-unauthorized** に変更すると、ホストはゲスト VLAN から削除され、ポート VLAN に戻されます。

ポートを 802.1X ゲスト VLAN に追加するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	アクティブ VLAN を 802.1X ゲスト VLAN として設定します。	**set port dot1x** *mod/port* **guest-vlan** {*vlan* | **none**}
ステップ 2	ポートごとに 802.1X ゲスト VLAN 設定を確認します。	**show port dot1x guest-vlan**

次に、ポート 3/1 を 802.1X ゲスト VLAN 200 に追加する例を示します。

```
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 is Multiple-authentication enabled, guest-vlan can not be enabled
Console> (enable) set port dot1x 3/1 multiple-authentication disable
Port 3/1 Multiple-authentication option disabled
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 Guest Vlan is set to 200
Console> (enable) show port dot1x guest-vlan
Guest-Vlan    Status   Mod/Ports
------------- -------- ------------------
200           active   3/1
none          none     2/1-2,3/2-48,8/1-8
Console> (enable)
```

次に、ポートをゲスト VLAN から削除する例を示します。

```
Console> (enable) set port dot1x 3/1 guest-vlan none
Port 3/1 Guest Vlan is cleared
Console> (enable)
```

802.1X 単一方向制御ポートの設定

802.1X により、スイッチに接続されているホストにおける無人システムのバックアップまたはソフトウェア アップグレードを実行するために、ウェイクオン LAN テクノロジー（リモート ウェイクアップともいう）を使用できます。

単一方向制御ポートが設定されている場合、ホスト認証の前にポートは発信方向のみのトラフィックを許可します。この動作により、管理ステーションは選択されたホストへウェイクオン LAN フレームを送信できます。このフレームは、ホストに対して電源投入とブート、認証、およびその後の無人操作を実行するトリガとなります。

（注）　ウェイクオン　LAN　テクノロジーではホストに特定のハードウェアが必要ですが、これはこのマニュアルの範囲ではありません。

Release 8.3(1) より前のソフトウェア リリースでは、デフォルトで 802.1X ブリッジ ポートが双方向ステートに設定されています。このステートでは制御は無許可のポートで双方向のプロトコル交換に影響します。単一方向制御ポート機能により、**set port dot1x** *mod/port* **port-control-direction** コマンドを使用して、802.1X 対応ポートを単一方向（**in** キーワード）または双方向（**both** キーワード）ステートに設定できます。

単一方向ステート

ポートを単一方向ポート（**in** キーワード）として設定して **set port dot1x** *mod/port* **port-control auto** コマンドを使用してポートを **auto** に設定する場合、ブリッジ ポートはスパニングツリー フォワーディング ステートに移行します。この場合、ポートに向かうすべてのトラフィックがスーパバイザ エンジンに転送されて処理されます。ウェイクオン LAN 機能により、接続ホストがスリープ モードまたは電源切断ステートの場合、ホストはネットワークの他のデバイスとトラフィックを交換しません。単一方向ポートと接続されたホストはトラフィックをネットワーク外に送信できず、ネットワーク内の他のデバイスからのトラフィックのみを受信できます。単一方向ポートが何らかの入力トラフィックを認識した場合、ポートは双方向ステート（デフォルト）に戻ってスパニング ツリー ステートがブロッキング モードに移行し、入出力トラフィックが廃棄されます。ポートの認証者システムが初期化ステートに移行し、EAPOL パケット交換以外のトラフィックは許可されません。ポートが双方向ステートに戻る際、5 分タイマーが起動してタイマーが切れるまでにポートが認証されなかった場合、ポートは単一方向ステートに戻ります。

双方向ステート

ポートを双方向ポート（**both** キーワード）として設定して **set port dot1x** *mod/port* **port-control auto** コマンドを使用してポートを **auto** に設定する場合、ポートは双方向でアクセス制御されます。このステートは、ポートでの入力パケットの受信および出力パケットの伝送をディセーブルにします。ポートが双方向ポートとして設定される場合、Release 8.3(1) より前のソフトウェア リリースのように動作し、ポートはスパニング ツリー ブロッキング ステートになり通常の認証プロセスに従います。

設定時の注意事項

ここでは、802.1X 単一方向ポートを設定する上での注意事項を説明します。

- 補助 VLAN — ポートを単一方向ポートとして設定する際にポートで補助 VLAN をサポートするには、接続された IP Phone が確実に即座に動作するよう補助 VLAN がスパニング ツリー フォワーディング ステートに移行します。入力トラフィックの障害を避けるために、まずポート VLAN もスパニング ツリー フォワーディング ステートに移行し、トラフィックがポート VLAN で確認されたら、ポートはすべての追加トラフィックを廃棄するためにスパニング ツリー ブロッキング ステートに移行します。そこで接続ホストはトラフィックの送信許可を得るように要求されます。
- ゲスト VLAN — ゲスト VLAN は、双方向ポートとして設定されているポートでのみサポートされます。ゲスト VLAN がポートでイネーブルの場合、そのポートは単一方向のポートとして設定できません。また、その逆に単一方向ポートをゲスト VLAN に設定できません。
- ポート モード — 単一方向ポートとして設定されているポートのポート モード（単一認証モード、複数ホストモード、または複数認証モード）は単一認証モード（デフォルトのポート モード）でなければなりません。

CLI を使用した 802.1X 単一方向または双方向ポートの設定

in キーワードを指定する場合、すべての入力トラフィックは廃棄されて出力トラフィックは許可されます。**both** キーワード（デフォルト）を指定した場合、ポート上のすべての受信トラフィックおよび送信トラフィックが廃棄されます。ポートを 802.1X 単一方向ポートまたは双方向ポートとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートを 802.1X 単一方向ポートまたは双方向ポートとして設定します。	**set port dot1x** *mod/port* **port-control-direction** [**both** | **in**]

次に、ポートを単一方向または双方向ステートに設定して設定を変更する例を示します。

```
Console> (enable) set port dot1x 3/1 port-control-direction both
Port 3/1 Port Control Direction set to Both.
Console> (enable) set port dot1x 3/1 port-control-direction in
Port 3/1 Port Control Direction set to In.
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 3/1  SingleAuth    enabled             disabled           In      Both
Console> (enable)
```

ACL 割り当てでの 802.1X の設定

ここでは、ACL 割り当てでの 802.1X を設定する手順について説明します。

- 概要（p.39-26）
- ACL 割り当てでの 802.1X 設定時の注意事項（p.39-26）
- CLI を使用した ACL 割り当てでの 802.1X の設定（p.39-27）
- QoS ACL での 802.1X の設定（p.39-28）

概要

ACL 割り当てで 802.1X を設定する場合、ユーザの 802.1X 認証に基づいてアクセス制御ポリシーをインターフェイスに動的に割り当てるのに ID ベースの ACL が使用されます。この機能は、ユーザを特定のネットワーク セグメントに限定し、機密性の高いサーバへのアクセスを制限し、使用可能なプロトコルとアプリケーションを制限します。また、この機能を使用すると、ユーザの移動性に支障が出たり、管理上のオーバーヘッドが大幅に増加したりすることなく、ごく特定の ID ベースのセキュリティを提供できます。

ACL 割り当てで 802.1X を設定する場合、ユーザが物理的な位置を変更するたびに発生する、IP アドレスまたは MAC アドレスに基づいたアクセス制御ポリシーの作成、変更、削除における問題を解消できます。この機能によって、VLAN-based Policy（VACL; VLAN ベース ポリシー）や Port-based Policy（PACL; ポートベース ポリシー）の代わりに ID ベースのセキュリティ アクセス ポリシーを作成する際に、ユーザの移動性を損なうことなくポリシーを作成できます。この機能を使用することで、ユーザの物理的な位置を変更したり、ネットワーク接続を変更したりするたびに、ユーザはアクセス ポリシーの変更についてネットワーク管理者に依存する必要はありません。

新しい **group** *group_name* キーワードは、ポリシーをグループとして分類するのに使用します。グループとは、ポリシーを適用するユーザ（IP アドレス）のセットです。この機能を実行する前に、ユーザ セットへの IP アクセスを許可したい場合、ACL ACE に各ユーザの IP アドレスを指定する必要があります。ACE ごとに設定可能な IP アドレスは 1 つだけです。この新しい機能を使用する場合、**set security acl ip** *grpacl* **permit ip group** *ip-permit-group* **any** のように、ACE に *group_name* を指定します。*ip-permit-group* はグループで、そのグループ内のすべてのユーザは認証されます。ユーザ認証が成功してユーザの IP アドレスが取得されたら、ユーザがグループに属している場合、ユーザの IP アドレスがグループに追加され、新しい ACE が作成されてハードウェア（PFC）にインストールされます。ACL はユーザ認証およびログオフにより動的に伸縮します。すなわち ACL は動的で、ポリシーは認証済みで有効なユーザに対してのみインストールされます。

ACL 割り当てで 802.1X を設定する場合、ユーザが認証されるたびに自動的に Quality of Service（QoS; サービス品質）ACL および VACL をユーザに設定できます。RADIUS サーバは、認証成功パケットとともに QoS VLAN ベース ACL、QoS ポートベース ACL、または VACL ポリシー名を送信します。ポリシー名に関連付けられたポリシーは、すでに CLI を使用してスイッチに設定されています。ポリシーは ACE のセットに変換されて、スイッチにインストールされます。

IP アドレスに ACL を適用できます。802.1X 認証がユーザ名で実行され MAC アドレスと結びついているものの IP アドレスは認証時には認識されていないため（認証に成功したあとでのみ DHCP がホストで開始されます）、ACE のインストールが実行されるのは、DHCP スヌーピングまたはダイナミック ARP 検査を通じて IP アドレスが認識されたあとになります。

ACL 割り当てで 802.1X を設定する場合、主に次の 2 種類の設定作業があります。

- RADIUS サーバ内にあるユーザのグループ名の関連付けと設定
- スイッチの CLI を使用したスイッチ上のグループの設定、コミット、ACL のマッピング

802.1X ACL 割り当てが設定されると、スイッチは次の作業を実行します。

- ユーザの認証
- DHCP スヌーピングまたはダイナミック ARP 検査を使用したユーザの IP アドレスの取得
- IP アドレスを使用した ACL の拡張と PFC のプログラミング

ACL 割り当てでの 802.1X 設定時の注意事項

ここでは、ACL 割り当てで 802.1X を設定する上での注意事項を説明します。

- ACL 割り当てでの 802.1X に設定されているポートのポート モード（単一認証モード、複数ホストモード、または複数認証モード）は単一認証モード（デフォルトのポート モード）でなければなりません。
- （DHCP スヌーピングまたはダイナミック ARP 検査を通じて取得した）動的に学習された IP アドレスは、グループ名を拡張するのに使用します。ACL 割り当てでの 802.1X は、スタティック IP アドレスでもサポートされています（スタティック IP アドレスが RADIUS サーバにも設定されている必要があります）。
- グループはポリシー グループです。ポリシー グループの例としては、IP アドレスのセットに対する「http アクセスの拒否」などのポリシーです。
- ユーザは永続的にグループと結びついているわけではなく、ユーザは同時に複数のポリシー グループに属することができます。複数のポリシーを定義したい場合、たとえば、「http アクセスの拒否」と「FTP アクセスの拒否」の両方を定義したい場合、2 つのポリシー グループ（1 つは「http アクセスの拒否」を定義したグループ、もう 1 つは「FTP アクセスの拒否」を定義したグループ）を定義できます。
- RADIUS サーバは、認証成功パケット内の特定のユーザに適用されなければならないすべてのポリシーを送信でき、ユーザはこれらのグループをすべてスイッチに追加できます。RADIUS サーバが送信したポリシー グループはスイッチに設定されていませんが、ポリシーは無視されるか、ポートが無許可ステートになります。RADIUS サーバがスイッチの ACL 内に存在しないグループ ID を送信すると、認証が失敗します。
- Release 8.3(1) 以降のソフトウェア リリースでは、1 つのグループ名に設定されている 802.1X 認証済みユーザを VLAN 間で均一に分散することにより、負荷を分散できます。詳細については、「802.1X ユーザ分散の設定」（p.39-32）を参照してください。

CLI を使用した ACL 割り当てでの 802.1X の設定

（注）　ここでは、ACL 割り当てでの 802.1X の設定に使用する、Release 8.3(1) で導入された CLI について説明します。ACL 設定の詳細については、第 15 章「アクセス制御の設定」を参照してください。

ACL 割り当てで 802.1X をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 割り当てで 802.1X を設定します。	**set security acl ip** {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num*/*port_num*}} [**ip**] {*src_ip_spec* | [**group** {*group_name*}} {*dest_ip_spec* | [**group**} [**precedence** {*precedence*}] [**tos** {*tos*}] [**fragment**] [**capture**] [**log**] [**before** {*editbuffer_index*} | **modify** {*editbuffer_index*}]

次に、802.1X グループのグループ名を指定してグループが設定済みであることを確認する例を示します。

```
Console> (enable) set security acl ip grpacl permit ip group ip-permit-group any
grpacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl grpacl
ACL commit in progress.

ACL 'grpacl' successfully committed.
Console> (enable)

Console> (enable) show dot1x group all
Group Manager Info

Current Group Count = 1

------------------------------------------------------------
Info of Group ip-permit-group
User Count  = 0
Console> (enable)
```

QoS ACL での 802.1X の設定

ここでは、QoS ACL で 802.1X を設定する手順について説明します。

- QoS ACL での 802.1X 設定時の注意事項（p.39-28）
- QoS ACL での 802.1X 設定例（p.39-29）
- RADIUS サーバの設定（p.39-31）

RADIUS サーバは、ポリシー名を 802.1X クライアントに送信します。ポリシーはすでにスイッチに定義されていてコミットされています。ユーザは、QoS ポリシーを設定する際にすべての既存の QoS 機能を完全に利用できます。802.1X クライアントは、QoS サブシステムと対話して認証が行われたあとにインターフェイスにポリシーを適用します。ポリシーは、認証済みクライアントがインターフェイスから脱退する際に削除されます。802.1X がインターフェイスにポリシーを付加した場合でも、スイッチの CLI から直接ポリシーのマッピングを解除できます。

QoS ACL での 802.1X 設定時の注意事項

ここでは、QoS ACL で 802.1X を設定する上での注意事項を説明します。

- QoS ポリシーの設定に誤りがあり 802.1X がインターフェイスでユーザを認証しようとした場合、認証が失敗します。
- 802.1X がインターフェイスで適切に認証されたあとに QoS ポリシーを誤って設定した場合、同じ QoS ポリシーを使用してインターフェイスで再認証が行われる際に、認証が失敗します。
- 複数の QoS ポリシー（入力および出力ポリシー）が同時に適用される場合、QoS ポリシーが失敗すると、認証も失敗します。
- ポートベース ポリシーおよび VLAN ベース ポリシーを同じインターフェイスに適用すると、認証が失敗します。
- 802.1X ユーザがログインする際にのみ、802.1X セキュリティおよび QoS ポリシーが適用されます。スイッチまたは RADIUS サーバで 802.1X セキュリティ ポリシーと QoS ポリシーの一方または両方を変更する場合、802.1X ユーザが再認証されるまで変更は適用されません。再認証がイネーブル（デフォルトでない）の場合、ポリシーは通常 1 時間以内に有効になります。再認証がディセーブル（デフォルト）の場合、各 802.1X ユーザがログアウトし、再びログインするまでポリシー変更は有効になりません。
- 既存の QoS コマンドは、QoS ポリシー情報の作成と表示に使用されます。コマンドは **set qos enable**、**set qos acl**、および **commit qos acl** ですが、これに限定されません。スケジューリング コマンドおよびポートベース QoS コマンドもダイナミック QoS ポリシーの作成に使用できます。

- QoS ポリシーをスイッチに定義したあとは、（**set qos acl map** コマンドを使用して）ポリシーを VLAN またはポートにマッピングし、さらにポリシー マッピングが成功したことを確認する必要があります。確認後、ACL マッピングを消去して 802.1X をインターフェイスに設定します。

（注）　QoS ACL の名前付けには注意してください。QoS ACL 名は、RADIUS サーバに指定されているポリシー名と一致する必要があります。

QoS ACL での 802.1X 設定例

次の例では、QoS がイネーブルで [Dot1xDscp5Policy] という 802.1X QoS ポリシーが作成されます。その後、ポリシーはコミットされます。さらに、同じポリシー名（Dot1xDscp5Policy）が RADIUS サーバに作成されます。一定期間が経過したあと、802.1X がクライアントを認証してポリシーが適用されたあとでそのポリシーがポート 3/1 に適用されたことが確認できます。ポリシー マッピングがマッピング コマンドのコンフィギュレーション（config）画面に表示されないことを確認できます。これは、実行コンフィギュレーションでのみ表示されます。

RADIUS サーバの AV ペアには [qos:inpacl=Dot1xDscp5Policy] という入力が必要です。ポート 3/1 の要求元認証を実行後、ポート 3/1 に対する QoS ランタイム マッピングが実行されます。

AV ペアに対する他のオプションは、qos:invacl=<policy-name> および qos:outpacl=<policy-name> です。

AV ペアのポリシー名がスイッチのポリシー名と一致しない場合、要求元は認証されません。

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable) set qos acl ip Dot1xDscp5Policy dscp 5 any
Dot1xDscp5Policy editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit qos acl all

QoS ACL 'Dot1xDscp5Policy' successfully committed.
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable)

<<< Dot1x Authenticates a client on 3/1 and applies Dot1xDscp5Policy >>>

Console> (enable) show qos acl map runtime Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP 3/1
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
ACL name                        Type Ports
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
QoS ACL mappings on output side:
ACL name                        Type Vlans
------------------------------- ---- --------------------------------
Dot1xDscp5Policy                  IP
Console> (enable)
```

次の例では、**show qos acl map** コマンドを使用してダイナミック QoS ポリシー情報が表示されます。**runtime** キーワードを使用すると、どのダイナミック ポリシーがどのインターフェイスに適用されるかを確認できます。**config** キーワードではダイナミック QoS ポリシー マッピングを表示できません。

```
Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
ACL name                         Type Ports
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
QoS ACL mappings on output side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
Console> (enable) show qos acl map runtime Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
ACL name                         Type Ports
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP 3/1
QoS ACL mappings on output side:
ACL name                         Type Vlans
-------------------------------- ---- --------------------------------
Dot1xDscp5Policy                   IP
Console> (enable)
```

RADIUS サーバの設定

Cisco Secure Access Control Server（ASC）3.x 以降を使用する場合、認証済みクライアントと関連付けられる QoS ポリシー名を設定する必要があります。RADIUS サーバを設定するには、ACS のホームページから次の手順を実行します。

ステップ 1　**network configuration** を選択します。

ステップ 2　NAS IP をクリックして、属性の RADIUS IOS/PIX スタイルをオンにします。Authenticate Using（認証使用）フィールドが表示されます。

ステップ 3　**IOS/PIX** オプションを選択して実行します。

ステップ 4　**interface config** を選択します。

ステップ 5　**RADIUS (IOS/PIX)** を選択します。

ステップ 6　AV ペア オプションの前にある両方のチェック ボックスをオンにします。最初のオプションは AV ペアです。

AV ペア ボックスがすべてのユーザに表示されます。チェック ボックスをオンにして AV ペア文字列をウィンドウに入力します。この場合の文字列は、各ユーザに関連付ける QoS ポリシー名を表します。複数の AV ペア文字列を送信する場合、各 AV ペアを別の 26/9/1 属性として送信できるように別の行に分ける必要があります。

802.1X ユーザ分散の設定

802.1X ユーザ分散を設定することにより、同じグループ名を持つユーザを複数の VLAN に分散できます。Release 8.3(1) より前のソフトウェア リリースでは、802.1X でサポートされていた RADIUS VLAN 割り当て機能は RADIUS サーバから取得した VLAN 番号を使用し、すべてのユーザをその VLAN に追加しました。Release 8.3(1) 以降のソフトウェア リリースでは、1 つのグループ名に設定されている 802.1X 認証済みユーザを VLAN 間で均一に分散することにより、負荷を分散できます。

これらの 2 つの方法は、異なる VLAN でユーザのロード バランシングを実現するために使用します。VLAN は RADIUS サーバから提供されるか、スイッチの CLI を通じて VLAN グループ名に設定されます。

- ユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として複数の VLAN 名を送信できます。802.1X ユーザ分散では、特定の VLAN 内にあるすべてのユーザを追跡し、許可済みユーザをユーザが最も少ない VLAN に移動することでロード バランシングを実現しています。
- ユーザに VLAN グループ名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として VLAN グループ名を送信できます。選択された VLAN グループ名は、Catalyst CLI を使用して設定された VLAN グループ名の中から検索されたものです（「CLI を使用した 802.1X ユーザ分散の設定」[p.39-33] を参照）。VLAN グループ名が見つかると、この VLAN グループ名の下に設定された対応する VLAN が検索されてユーザの割り当てが最も少ない VLAN を探し、対応する許可済みユーザをその VLAN に移動することでロード バランシングを実現します。

802.1X ユーザ分散の設定の注意事項

ここでは、802.1X ユーザ分散機能を設定する際の注意事項について説明します。

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。
- 複数の VLAN を VLAN グループにマッピングできます。
- 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。
- VLAN グループ名から既存の VLAN を削除する場合、VLAN に認証されたポートは消去されませんが、マッピングは既存の VLAN から削除されます。
- VLAN グループ名から最後の VLAN を消去すると、VLAN グループが削除されます。
- アクティブ VLAN がグループにマッピングされていても VLAN グループを消去できます。VLAN グループを消去する際、グループ内のいずれかの VLAN にある認証ステートのポートまたはユーザは消去されませんが、VLAN グループへの VLAN マッピングは消去されます。
- **set dot1x radius-vlan-assignment disable** コマンドを入力すると、RADIUS サーバから送信された VLAN 情報は無視されて、ポートは NVRAM 設定 VLAN のままになります。このコマンドは、VLAN 割り当て機能をグローバルにイネーブルまたはディセーブルにするのに使用します。このコマンドがイネーブルの場合、スイッチはトンネル属性を使用して RADIUS アクセス受入れメッセージ内の VLAN 名を抽出します。このコマンドは、デフォルトではイネーブルです。

CLI を使用した 802.1X ユーザ分散の設定

VLAN グループを設定してそれに VLAN をマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN グループを設定して単一 VLAN または VLAN の範囲をそれにマッピングします。	**set dot1x vlan-group** {*vlan-group-name*} {*vlans*}
設定を確認します。	**show dot1x vlan-group** [**all** | {*vlan-group-name*}]
VLAN グループ設定または VLAN グループのエレメントを消去します。	**clear dot1x vlan-group** [**all** {*vlan-group-name*} [{*vlans*}]]

次に、VLAN グループを設定し、VLAN をグループにマッピングし、VLAN グループが設定されていて特定の VLAN にマッピングされていることを確認する例を示します。

```
Console> (enable) set dot1x vlan-group eng-dept 10
Vlan group name eng-dept is successfully configured and mapped to vlan 10
Console> (enable) set dot1x vlan-group hr-dept 20
Vlan group name hr-dept is successfully configured and mapped to vlan 20
Console> (enable) show dot1x vlan-group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
Console> (enable) show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
Console> (enable)
```

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

```
Console> (enable) set dot1x vlan-group eng-dept 30
Vlan 30 is successfully mapped to vlan group eng-dept.
Console> (enable) show dot1x vlan-group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10,30
Console> (enable)
```

次に、VLAN を VLAN グループから消去する例を示します。

```
Console> (enable) clear dot1x vlan-group eng-dept 10
Vlan 10 is successfully cleared from vlan group eng-dept.
Console> (enable)
```

次に、すべての VLAN が VLAN グループから消去された場合に VLAN グループが消去される例を示します。

```
Console> (enable) clear dot1x vlan-group eng-dept 30
Vlan 30 is successfully cleared from vlan group eng-dept.
Warning: No more vlans mapped to this group, vlan group is cleared.
Console> (enable) show dot1x vlan-group eng-dept
Vlan group eng-dept doesn't exist, can not display.
Console> (enable)
```

次に、すべての既存の VLAN グループを消去する例を示します。

```
Console> (enable) clear dot1x vlan-group all
Console> (enable) show dot1x vlan-group all
No vlan groups are present for display.
Console> (enable)
```

802.1X RADIUS アカウンティングとトラッキングのイネーブル化およびディセーブル化

802.1X RADIUS アカウンティングおよびトラッキングを使用して、802.1X ユーザ アカウンティング情報を RADIUS サーバに送信できます。この機能は UDP ポート番号 1813 を使用します。

802.1X アカウンティング パケットは、次の情報を RADIUS サーバに提供できます。

- ユーザが正常に認証した時
- ユーザがログオフした時
- リンクが 802.1X ポートでダウンした時
- 再認証が成功した時
- 再認証が失敗した時

アカウンティング パケットの属性は次のとおりです（オプションの属性もあります）。

- 属性 [1] USERNAME — 認証されようとしているユーザ名
- 属性 [4] NAS-IP — 認証およびアカウント セッションを開始するスイッチの IP アドレス（通常、sc0 インターフェイス IP アドレス）
- 属性 [40] ACCT-STATUS-TYPE — START/STOP/INTERIM
  - 認証が成功してポートが許可ステートに移行する際に START が送信されます。
  - ユーザが logoff を送信するか、リンクがダウンするか、再認証が失敗した場合に STOP が送信されます。
  - 再認証が成功すると、INTERIM が送信されます。
- 属性 [44] ACCT-SESSION-ID — すべてのアカウンティング セッションに関連付けられた固有のセッション IDT

アカウンティング パケット フォーマットは次のとおりです。

```
<NAS-IP> <user-id> <date> <time> <random16bit#>
```

アカウンティング パケット フォーマットの例は次のとおりです。

```
9.9.150.140 rameshp 31/07/2003 12:40:00 12345
```

上記に挙げた属性は、（START/STOP/INTERIM の）ACCT-STATUS-TYPE の属性に関係なく、共通です。

INTERIM アップデートに固有の属性は次のとおりです。

- 属性 [8] FRAMED-IP-ADDRESS — ユーザに割り当てられた IP アドレス（このアドレスはスタティック割り当てまたは DHCP を通じて取得可能）
- 属性 [81] TUNNEL-PRIVATE-GROUP-ID — RADIUS サーバが送信する実際の VLAN 名

  [Interim Accounting Request] 内の上記の属性とともに送信される CISCO-AV-PAIRS は次のとおりです。
  - AAA:ip-addr-method — IP 割り当てが DHCP を通じたものか静的に設定されるかを送信します。
  - AAA:vlan-assign-method — ローカル デバイスまたは RADIUS による割り当て

RADIUS サーバが VLAN を送信しない場合のタイプは「ローカル デバイス」になります。この場合、管理上設定されたポート VLAN はユーザの VLAN です。RADIUS サーバが VLAN を送信した場合、タイプは「RADIUS による割り当て」になります。

STOP パケットに固有の属性は次のとおりです。

- 属性 [49] ACCT-TERMINATION-CAUSE — 原因はユーザのログオフ、ポートのダウン、再認証失敗などが考えられます。
- CISCO-AV-PAIRS
  - Cisco:Input-Octets — ポートで受信される入力トラフィックのバイト数を指定する 64 バイトの整数
  - Cisco:Output-Octet — ポートから転送された出力トラフィックのバイト数を指定する 64 バイトの整数

CLI を使用した 802.1X RADIUS アカウンティングおよびトラッキングのイネーブル化およびディセーブル化

802.1X RADIUS アカウンティングおよびトラッキングをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います（デフォルトはディセーブル）。

作業	コマンド
802.1X RADIUS アカウンティングとトラッキングをグローバルにイネーブルまたはディセーブルにします。	**set dot1x radius-accounting** {**enable** | **disable**}

次に、802.1X RADIUS アカウンティングとトラッキングをグローバルにイネーブルまたはディセーブルにする例を示します。

```
Console> (enable) set dot1x radius-accounting enable
dot1x radius-accounting enabled.
Console> (enable) set dot1x radius-accounting disable
dot1x radius-accounting disabled.
Console> (enable)
```

認証済み ID とポート説明のマッピングの設定

認証済み ID とポート説明のマッピングを使用して、RADIUS サーバから受信した情報に基づいてポート名を 802.1X ポートに割り当てることができます。この機能は AV ペア「要求元名」を使用して一意に認証済みユーザのポート名を割り当てます。現在サポートされているのは、認証サーバから送信されるシスコのサポートする AV ペアのみで、他のベンダー固有の AV ペアは無視されます。

RADIUS サーバから受信されるポート名を表示するには、**show port** コマンドを入力します。スイッチが 20 文字以上の認証済みポート名を受信する場合、名前は 19 文字に切り捨てられて # 記号が名前に付加されます（合計で 20 文字が許可され、**set port name** コマンドと互換性があります）。**set port name** コマンドを入力する場合、最終結果は、認証済み ID とポート説明のマッピング機能を使用した場合と同じですが、この機能は 802.1X 認証で動的に名前を割り当てるところが異なっています。動的に割り当てられたポート名の例は次のとおりです。

```
Console> (enable) show port 4/1
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 4/1  rmanam-test-supplic# connected  1          a-full       a-100 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status
----- ------------- --------------
 4/1  none          none

.
.
.
Console> (enable)
```

RADIUS サーバ設定の DNS レゾリューションの設定

RADIUS サーバ用の Domain Name System（DNS; ドメイン ネーム システム）レゾリューションを設定する場合、IP アドレスに加えて DNS 名を使用して RADIUS サーバを設定できます。DNS 名と IP アドレスを関連付けるのに設定された DNS サーバを使用して、スイッチが自動的に DNS 名を解決します。設定済みの DNS 名は、プライマリまたはセカンダリとして設定された他の IP アドレスと共存できます。DNS 名は NVRAM に保存されます。DNS レゾリューションが機能するために、RADIUS キープアライブ機能をイネーブルにする必要があります。DNS レゾリューション機能により、スイッチの知識なしに RADIUS サーバの IP アドレスを透過的に変更できます。次に、スイッチは修正された IP アドレスを使用して DNS 名を解決します。

スイッチは、DNS 名の初期設定時、802.1X がディセーブルまたはイネーブルになるとき、802.1X ポート認証中、または RADIUS サーバへの要求がタイムアウトの場合に、IP アドレスに対する DNS 名のレゾリューションを再び実行します（2 回めの解決）。このレゾリューションは、DNS 名と IP アドレスのマッピングが DNS サーバ側で変更されていないかをチェックします。

DNS 名が RADIUS サーバの IP アドレスの代わりに設定されている場合に、**show config** または **show radius** コマンドを入力して DNS 名を表示します。最大 3 つの RADIUS サーバを設定できます。設定済みの RADIUS サーバ パラメータを表示するには、次のように **show radius** コマンドを入力します。

```
Console> (enable) show radius
RADIUS Deadtime:              0 minutes
RADIUS Key:                   cisco
RADIUS Retransmit:            2
RADIUS Timeout:               5 seconds
Framed-Ip Address Transmit:  Disabled

RADIUS-Server                     Status  Auth-port Acct-port Resolved IP Address
--------------------------------- ------- --------- --------- -------------------
9.9.150.16                        primary 1812      1813
cat6k-sup2                                1812      1813      9.9.150.20
cat6k-sup3                                1812      1813      9.9.150.21
Console> (enable)
```

認証失敗 VLAN の設定

従来型の 802.1X ポートでは、スイッチはポートに接続された要求元の ID 情報が認証サーバで検証されて認証されるまで、ネットワークへのアクセスを提供しません。認証失敗 VLAN 機能を使用すれば、ポート単位で認証失敗 VLAN を設定できます。要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。

（注）　認証失敗 VLAN 機能をゲスト VLAN 機能と対比させてください。ゲスト VLAN 機能によって、802.1X 非対応ホストは 802.1X 認証を使用するネットワークにアクセスできます。802.1X 認証をサポートするようにシステムをアップグレードしているときに、ゲスト VLAN を使用できます。一般的に、ゲスト VLAN は最小限のサービスをサポートし、最小限のネットワーク アクセスを行います。

認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。

詳細については、「ゲスト VLAN に対する 802.1X 認証の概要」（p.39-8）を参照してください。

認証失敗 VLAN 設定時の注意事項および制限事項

ここでは、認証失敗 VLAN の設定時の注意事項および制限事項について説明します。

- 要求元による 802.1X 認証が 3 回失敗すると、ポートは要求元からのネットワーク アクセスが可能な認証失敗 VLAN に移動されます。3 回の試行では、ポートが認証失敗 VLAN でイネーブルにされ、EAP 成功パケットが要求元に送信されるまで 3 分間の遅延が生じます（失敗したあとにデフォルト待機時間の 60 秒に基づいて、それぞれの失敗で 1 分間の遅延が生じます）。
- 失敗した 802.1X 認証の回数は、リンク確立後からポートが認証失敗 VLAN に移動するまで数えられます。ポートが認証失敗 VLAN に移動すると、失敗回数カウンタがリセットされます。
- 認証に失敗したユーザだけが認証失敗 VLAN に移動されます。
- 認証失敗 VLAN は、単一認証モード（デフォルト ポート モード）でのみサポートされています。
- 認証失敗 VLAN は、単一方向ポートとして設定されたポートではサポートされていません。
- 要求元の MAC アドレスが CAM テーブルに追加され、この MAC アドレスだけが認証失敗 VLAN ポートで許可されます。ポートに新たに現れる MAC アドレスは、セキュリティ違反として扱われます。
- 認証失敗 VLAN ポートを RSPAN VLAN またはプライベート VLAN の一部にすることはできません。
- Multiple VLAN Access Port（MVAP）では、認証失敗 VLAN と補助 VLAN を同じにすることはできません。
- 認証失敗 VLAN およびポート セキュリティ機能は、相互に競合しません。さらに、Dynamic ARP Inspection（DAI）、DHCP スヌーピング、および IP ソース ガードなどの他のセキュリティ機能を認証失敗 VLAN で個別にイネーブルまたはディセーブルにできます。
- 認証失敗 VLAN は、ゲスト VLAN とは無関係です。ただし、ゲスト VLAN と認証失敗 VLAN を同じ VLAN にすることができます。802.1X 非対応ホストと認証失敗ホストを区別しない場合は、両方を同じ VLAN（ゲスト VLAN または認証失敗 VLAN）に設定できます。
- 認証失敗 VLAN では、ハイ アベイラビリティがサポートされています。

認証失敗 VLAN の作成および 802.1X ポートの追加

認証失敗 VLAN を作成し、VLAN に 802.1X ポートを追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証失敗 VLAN を作成し、VLAN に 802.1X ポートを追加します。	**set port dot1x** *mod/ports* **auth-fail-vlan** {**none** | *vlan*}

次に、認証失敗 VLAN（VLAN 81）を作成し、ポート 3/33 を追加する例を示します。

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan 81
Port 3/33 Auth Fail Vlan is set to 81
Console> (enable)
```

次に、認証失敗 VLAN の設定を表示する例を示します。

```
Console> (enable) show port dot1x auth-fail-vlan
Auth-Fail-Vlan Status   Mod/Ports
-------------- -------- ------------------
81             active   3/33
none           none     1/1-2,2/1-2,3/1-32,3/34-48
Console> (enable)
```

次に、認証失敗 VLAN からポートを消去する例を示します。

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan none
Port 3/33 Auth Fail Vlan is cleared
Console> (enable)
```

次に、認証失敗 VLAN のアクティブ ユーザおよびポートを表示する例を示します。

```
Console> (enable) show dot1x auth-fail-users
Username       Mod/Port   Auth-Fail-Vlan
--------       --------   --------------
testuser       3/33       81
Console> (enable)
```

RADIUS サーバ フェールオーバーの設定

Release 8.4(1) より前のソフトウェア リリースでは、アクティブ RADIUS サーバがダウンまたは到達不能になった場合に、バックアップ RADIUS サーバがアクティブになる前に 802.1X 認証がタイムアウトしていました。Release 8.4(1) およびこれ以降のソフトウェア リリースでは、一部の RADIUS サーバ タイマー値を設定することが可能で、**show radius** コマンドはアクティブ RADIUS サーバを表示するように拡張されました。

RADIUS サーバ フェールオーバーを回避するには、次のコマンドを入力します。

- **set dot1x max-req —** ステート マシンが認証セッションをタイムアウトするまでに、ステート マシンが要求元に EAP-Request フレームを再送信する最大回数を指定します。有効な値は、1 ～ 10 です。デフォルトは 2 です。次に例を示します。

  ```
  Console> (enable) set dot1x max-req 8
  dot1x max-req set to 8.
  Console> (enable)
  ```

- **set dot1x server-timeout —** バックエンド認証者から認証サーバへのパケット再送信の時間定数を指定します。有効な値は、1 ～ 65535 秒です。認証サーバがバックエンド認証者に特定のパケットを受信したことを通知しない場合、バックエンド認証者は一定期間（**server-timeout** *seconds* パラメータを入力して設定）待機してから、パケットを再送信します。デフォルトは 30 です。次に例を示します。

```
Console> (enable) set dot1x server-timeout 100
dot1x server-timeout set to 100 seconds.
Console> (enable)
```

次に、**show radius** コマンドを入力して、RADIUS サーバ コンフィギュレーションを表示し、アクティブな RADIUS サーバを確認する例を示します。

```
Console> (enable) show radius
Active RADIUS Server:        81.81.81.20
RADIUS Deadtime:             1 minutes
RADIUS Key:                  cisco
RADIUS Retransmit:           2
RADIUS Timeout:              5 seconds
Framed-Ip Address Transmit:  Disabled

RADIUS-Server                    Status  Auth-port Acct-port Resolved IP Address
-------------------------------- ------- --------- --------- -------------------
81.81.81.20                      primary 1812      1813
10.6.89.200                              1812      1813
10.6.98.35                               1812      1813
Console> (enable)
```

show コマンドの使用方法

802.1X 認証とその設定に関する情報を表示するには、**show** コマンドを使用します。

- **show port dot1x ?**
- **show port dot1x**
- **show port dot1x statistics**
- **show dot1x**
- **show cam static**

show port dot1x コマンドの使用方法のオプションを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
show port dot1x コマンドの使用方法のオプションを表示します。	**show port dot1x ?**

次に、**show port dot1x** コマンドの使用方法のオプションを表示する例を示します。

```
Console> (enable) show port dot1x ?
  guest-vlan                Show Port guest vlan information
  statistics                Show statistic information
  <mod>                     Module number
  <mod/port>                Module number and Port number(s)
  |                         Output modifiers
  <cr>
```

特定モジュールの特定ポート上での認証者 PAE およびバックエンド認証者に関するすべてのパラメータの値を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定モジュールの特定ポート上での、認証者 PAE およびバックエンド認証者に関するすべての設定可能なパラメータ値および現在のステート パラメータ値を表示します。	**show port dot1x** *mod/port*

次に、モジュール 3 のポート 1 上での認証者 PAE およびバックエンド認証者に関するすべてのパラメータ値を表示する例を示します。

```
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  connecting          idle       auto                unauthorized

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------ -----------------   ----------------   ---------------
 3/1  SingleAuth    enabled             disabled           In      Both
Console> (enable)
```

特定モジュールの特定ポート上で認証者によって送受信される EAP フレーム別の統計情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
特定モジュールの特定ポート上で認証者によって送受信される EAP フレーム別の統計情報を表示します。	**show port dot1x statistics** *mod/port*

次に、モジュール 3 のポート 1 上で認証者によって送受信される EAP フレーム別の統計情報を表示する例を示します。

```
Console> (enable) show port dot1x statistics 3/1
Port   Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logoff Rx_Resp/Id Rx_Resp
-----  --------- ------ -------- -------- --------- ---------- -------
 3/1   43        0      43       0        0         0          0

Port   Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
-----  ---------- ---------- -------- --------------- -------------------
 3/1   2          0          2        0               00-00-00-00-00-00
Console> (enable)
```

グローバル 802.1X パラメータを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PAE 機能、プロトコルのバージョン、system-auth-control、およびその他のグローバル dotlx パラメータを表示します。	**show dot1x**

次に、グローバル 802.1X パラメータを表示する例を示します。

```
Console> (enable) show dot1x
PAE Capability              Authenticator Only
Protocol Version            1
system-auth-control         enabled
max-req                     2
quiet-period                60 seconds
radius-accounting           disabled
radius-vlan-assignment      enabled
radius-keepalive state      enabled
re-authperiod               7200 seconds
server-timeout              30 seconds
shutdown-timeout            300 seconds
supp-timeout                30 seconds
tx-period                   30 seconds

Console> (enable)
```

802.1X 認証 MAC アドレスを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
802.1X 認証 MAC アドレスを表示します。	**show cam static**

次に、802.1X 認証 MAC アドレスを表示する例を示します。この例では、802.1X とポート セキュリティの両方がイネーブルに設定されています。

```
Console> (enable) show cam static 8/17
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
12    00-40-ca-13-ae-bf  $          8/17
17    00-30-94-c2-c3-c1  X          8/17
Total Matching CAM Entries Displayed  =2
Console> (enable)
```