802.1X の設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1X ポートベースの認証を設定する手順について説明します。

この章は、次の項で構成されています。

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

802.1X の概要

802.1X では、クライアント 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を定義し、許可されていないクライアントが公にアクセス可能なポートを経由してLANに接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

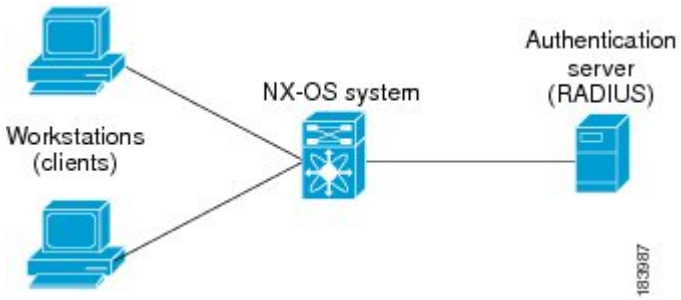
802.1Xアクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

デバイスのロール

802.1X ポート ベースの認証では、ネットワーク上のデバイスにそれぞれ特定のロールがあります。

次の図は、802.1X のデバイスのロールを示しています。

図 *1*：*802.1X* デバイスのロール



特定のロールは次のとおりです。

サプリカント

LAN および Cisco NX-OS デバイス サービスへのアクセスを要求し、Cisco NX-OS デバイスからの要求に応答するクライアント デバイスです。ワークステーションでは、Microsoft Windows XP が動作するデバイスで提供されるような、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。

（注） Windows XP のネットワーク接続および Cisco 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 サポート技術情報の記事を参照してください。http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

認証サーバ

サプリカントの実際の認証を行います。認証サーバはサプリカントの識別情報を確認し、LAN および Cisco NX-OS デバイスのサービスへのアクセスをサプリカントに許可すべきかどうかを Cisco NX-OS デバイスに通知します。Cisco NX-OS デバイスはプロキシとして動作するので、認証サービスはサプリカントに対しては透過的に行われます。認証サーバとして、拡張認証プロトコル（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティデバイス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 バージョン 3.0 で使用可能です。RADIUS はサプリカント サーバ モデルを使用し、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。

オーセンティケータ

サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。オーセンティケータは、サプリカ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、サプリカントから識別情報を要求し、得られた識別情報を認証サーバに確認し、サプリカントに応答をリレーします。オーセンティケータには、EAP フレームのカプセル化/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。

オーセンティケータが EAPOL フレームを受信して認証サーバにリレーする際は、イーサネット ヘッダーを取り除き、残りの EAP フレームを RADIUS 形式にカプセル化します。このカプセル化のプロセスでは EAP フレームの変更または確認が行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。オーセンティケータは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 ヘッダーを削除し、残りの EAP フレームをイーサネット用にカプセル化してサプリカントに送信します。

（注） Cisco NX-OS デバイスがなれるのは、802.1X オーセンティケータだけです。

認証の開始およびメッセージ交換

オーセンティケータ（Cisco NX-OS デバイス）とサプリカント（クライアント）のどちらも認証を開始できます。ポート上で認証をイネーブルにした場合、オーセンティケータはポートのリンク ステートがダウンからアップに移行した時点で、認証を開始する必要があります。続いて、オーセンティケータは EAP-Request/Identity フレームをサプリカントに送信して識別情報を要求します（通常、オーセンティケータは 1 つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サプリカントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

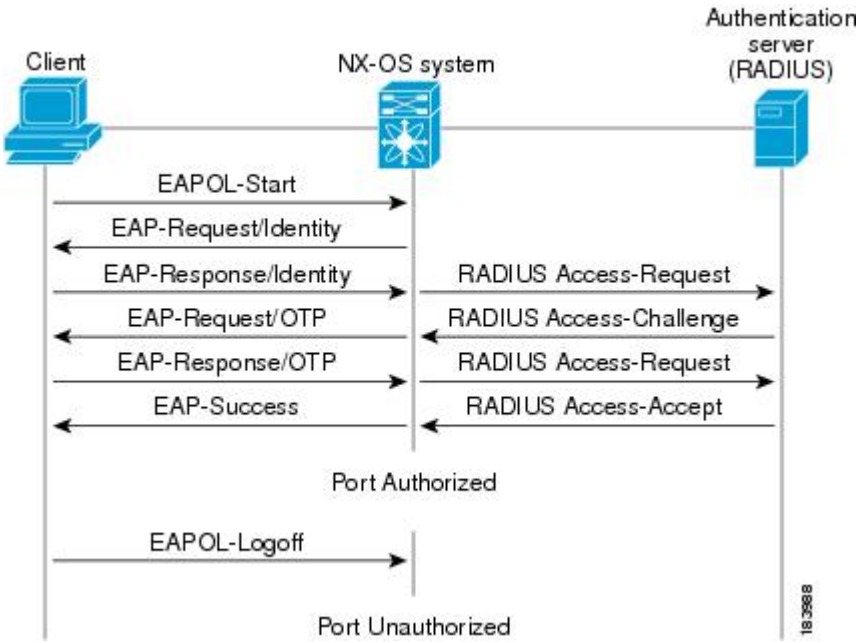
（注） ネットワーク アクセス デバイスで 802.1X がイネーブルになっていない場合、またはサポートされていない場合、Cisco NX-OS デバイスはサプリカントからの EAPOL フレームをすべてドロップします。サプリカントが、認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、サプリカントはポートが許可ステートにあるものとしてデータを送信します。ポートが許可ステートになっている場合は、サプリカントの認証が成功したことを意味します。

サプリカントが自己の識別情報を提示すると、オーセンティケータは仲介装置としてのロールを開始し、認証が成功または失敗するまで、サプリカ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、オーセンティケータのポートは許可ステートになります。

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。

次の図に、サプリカントが RADIUS サーバにワンタイム パスワード（OTP）認証方式を使用して開始するメッセージ交換を示します。OTP 認証デバイスは、シークレット パスフレーズを使用して、一連のワンタイム（使い捨て）パスワードを生成します。

図 *2*：メッセージ交換



ユーザのシークレット パスフレーズは、認証時やパスフレーズの変更時などにネットワークを通過することはありません。

インターフェイスのオーセンティケータ PAE ステータス

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity（PAE）インスタンスが作成されます。オーセンティケータ PAE は、

インターフェイスでの認証をサポートするプロトコル エンティティです。インターフェイスで802.1Xをディセーブルにしても、オーセンティケータ PAEインスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

許可ステートおよび無許可ステートのポート

サプリカントのネットワークへのアクセスが許可されるかどうかは、オーセンティケータのポート ステートで決まります。ポートは、無許可ステートで開始します。このステートにあるポートは、802.1Xプロトコルパケットを除いたすべての入トラフィックおよび出トラフィックを禁止します。サプリカントの認証に成功すると、ポートは許可ステートに移行し、サプリカントのすべて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 ポートに接続した場合、オーセンティケータはクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x対応のクライアントが、802.1x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。

ポートには次の許可ステートがあります。

Force authorized

802.1X ポートベースの認証をディセーブルにし、認証情報の交換を必要としないで許可ステートに移行します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。この許可ステートはデフォルトです。

Force unauthorized

ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。オーセンティケータは、インターフェイスを経由してクライアントに認証サービスを提供することができません。

自動

802.1Xポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのはEAPOLフレームだけです。ポートのリンク ステートがダウンからアップに移行したとき、またはサプリカントから EAPOL 開始フレームを受信したときに、認証プロセスが開始します。オーセンティケータは、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。オーセンティケータはサプリカントのMACアドレスを使用して、ネットワークアクセスを試みる各サプリカントを一意に識別します。

サプリカントの認証に成功すると（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、認証されたサプリカントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することは

できます。認証サーバに到達できない場合、オーセンティケータ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、サプリカントのネットワーク アクセスは認可されません。

サプリカントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、オーセンティケータの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。

MAC 認証バイパス

MAC 認証バイパス機能を使用して、サプリカントの MAC アドレスに基づいてサプリカントを認証するように、Cisco NX-OS デバイスを設定できます。たとえば、プリンタなどのデバイスに接続されている 802.1X 機能を設定したインターフェイスで、この機能をイネーブルにすることができます。

サプリカントからの EAPOL 応答を待機している間に 802.1X 認証がタイムアウトした場合は、MAC 認証バイパスを使用して Cisco NX-OS デバイスはクライアントの許可を試みます。

インターフェイスで MAC 認証バイパス機能をイネーブルにすると、Cisco NX-OS デバイスは MAC アドレスをサプリカント ID として使用します。認証サーバには、ネットワーク アクセスが許可されたサプリカントの MAC アドレスのデータベースがあります。Cisco NX-OS デバイスは、インターフェイスでクライアントを検出した後、クライアントからのイーサネット パケットを待ちます。Cisco NX-OS デバイスは、MAC アドレスに基づいてユーザ名とパスワードを含んだ RADIUS アクセス/要求フレームを認証サーバに送信します。許可に成功した場合、Cisco NX-OS デバイス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。

リンクのライフタイム中に EAPOL パケットがインターフェイスで検出される場合、こ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 Cisco NX-OS デバイスが判別し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを許可します。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。

Cisco NX-OS デバイスがすでに MAC 認証バイパスを使用してインターフェイスを許可していて、802.1X サプリカントを検出した場合、Cisco NX-OS デバイスはインターフェイスに接続されているクライアントを無許可にしません。再認証を実行する際に、Termination-Auction RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、Cisco NX-OS デバイスは 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（Attribute [27]）と Termination-Action RADIUS 属性（Attribute [29]）に基づいていて、Termination-Action RADIUS 属性（Attribute [29]）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、再認証中に接続が失われます。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。
- ポート セキュリティ：同じレイヤ 2 ポート上で 802.1X 認証とポート セキュリティを設定できます。
- 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。

802.1X とポート セキュリティ

ポート セキュリティと 802.1X は同じインターフェイス上に設定できます。ポート セキュリティによって、802.1X 認証の MAC アドレスを保護できます。802.1X はポート セキュリティよりも前にパケットを処理するので、1 つのインターフェイスで両方をイネーブルにすると、802.1X が、そのインターフェイスで、未知の MAC アドレスからのインバウンド トラフィックを妨げます。

同じインターフェイス上で 802.1X とポート セキュリティをイネーブルにしても、ポート セキュリティは設定どおりにスティッキ方式またはダイナミック方式で MAC アドレスの学習を続行します。また、シングル ホスト モードとマルチ ホスト モードのどちらで 802.1X をイネーブルにするかによって、次のいずれかが発生します。

シングル ホスト モード

ポート セキュリティは認証済みのホストの MAC アドレスを学習します。

マルチ ホスト モード

ポートセキュリティは、このインターフェイスでダイナミックに学習された MAC アドレスをドロップし、802.1X で認証された最初のホストの MAC アドレスを学習します。

802.1X がポート セキュリティに渡した MAC アドレスによってセキュア MAC アドレスの適用可能な最大数を違反することになる場合、デバイスはホストに認証エラー メッセージを送信します。

802.1X によって認証された MAC アドレスは、たとえそのアドレスがポート セキュリティによってスティッキ方式またはスタティック方式で学習されていたとしても、ダイナミック方式で学習されたアドレスと同様に扱われます。802.1X で認証されたセキュア MAC アドレスを削除しようとしても、そのアドレスはセキュア アドレスのまま保持されます。

認証済みのホストの MAC アドレスがスティッキ方式またはスタティック方式でセキュア アドレスになった場合、デバイスはそのアドレスをダイナミック方式で学習されたものとして扱うので、その MAC アドレスを手動で削除することはできません。

認証済みのホストのセキュアMACアドレスがポートセキュリティのエージング期限に達すると、ポート セキュリティは 802.1X と連動して、そのホストを再認証します。デバイスは、エージングのタイプに応じて、次のように異なる動作をします。

Absolute

ポート セキュリティは 802.1X に通知し、デバイスはホストの再認証を試行します。そのアドレスが引き続きセキュアアドレスになるかどうかは、再認証の結果によって決まります。再認証が成功すれば、デバイスはそのセキュア アドレスのエージング タイマーを再起動します。再認証に失敗した場合、デバイスはそのインターフェイスのセキュア アドレス リストからそのアドレスをドロップします。

Inactivity

ポート セキュリティは、そのインターフェイスのセキュア アドレス リストからそのセキュアアドレスをドロップし、802.1X に通知します。デバイスはホストの再認証を試行します。再認証が成功すれば、ポート セキュリティは再度そのアドレスをセキュア アドレスにします。

シングル ホストおよびマルチ ホストのサポート

802.1X機能では、1つのポートのトラフィックを1台のエンドポイント装置に限定することも（シングル ホスト モード）、1 つのポートのトラフィックを複数のエンドポイント装置に許可することも（マルチ ホスト モード）できます。

シングル ホスト モードでは、802.1X ポートで 1 台のエンドポイント装置のみからのトラフィックが許可されます。エンドポイント装置が認証されると、Cisco NX-OS デバイスはポートを許可ステートにします。エンドポイント装置がログオフすると、Cisco NX-OS デバイスはポートを無許可ステートに戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション（SA）違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングル ホスト モードは、ホストツースイッチ型トポロジで1台のホストがCisco NX-OSデバイスのレイヤ2ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。

マルチ ホスト モードに設定されている 802.1X ポートで、認証が必要になるのは最初のホストだけです。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワーク アクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワーク アクセスを拒否されます。マルチ ホスト モードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。マルチ ホスト モードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます。

サポートされるトポロジ

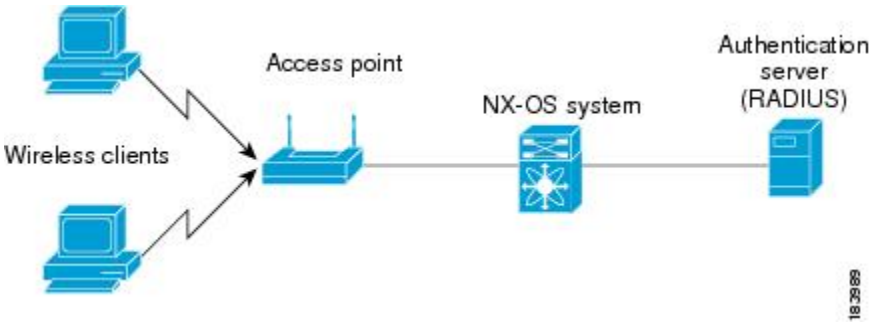
802.1X ポートベースの認証は、次の 2 つのトポロジでサポートされます。

- ポイントツーポイント
- Wireless LAN（ワイヤレス LAN）

ポイントツーポイント構成では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサプリカント（クライアント）を 1 台だけ接続することができます。オーセンティケータは、ポートのリンク ステートがアップ ステートに移行したときにサプリカントを検出します。サプリカントがログオフしたとき、または別のサプリカントに代わったときには、オーセンティケータはポートのリンク 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。

次の図に、ワイヤレス LAN 上での 802.1X ポートベースの認証を示します。802.1X ポートはマルチ ホスト ポートとして設定され、1 台のサプリカントが認証されるとすぐにポートが許可されます。

図 *3*：ワイヤレス *LAN* の例



ポートが許可されると、ポートに間接的に接続された他のすべてのホストに対して、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）、Cisco NX-OS デバイスは接続しているすべてのサプリカントのネットワーク アクセスを禁止します。

802.1X のバーチャライゼーション サポート

802.1X の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

802.1X のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	802.1Xにライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

802.1X の前提条件

802.1X には次の前提条件があります。

- ネットワーク内の 1 つまたは複数の RADIUS サーバがアクセス可能であること。
- MACアドレス認証バイパス機能をイネーブルにする場合を除き、802.1Xサプリカントがポートに接続されていること。

802.1X の注意事項と制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、物理ポート上だけです。
- Cisco NX-OS ソフトウェアは、ポート チャネルまたはサブインターフェイスでは 802.1X 認証をサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネルのメンバ ポートでは 802.1X 認証をサポートしますが、ポート チャネル自体ではサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネル メンバが 802.1X 用に設定されている場合、そのメンバでは次の 802.1X 設定をサポートしません。
  - シングル ホスト モードではホスト モードを設定できません。メンバ ポートではマルチホスト モードだけがサポートされます。
  - メンバ ポートでは MAC 認証バイパスをイネーブルにできません。
  - ポート チャネルではポート セキュリティを設定できません。
- 802.1X設定を含むメンバポートと含まないメンバポートはポートチャネルで共存できます。ただし、チャネリングと 802.1X が連携して動作するためには、すべてのメンバ ポートで 802.1X 設定を同一にする必要があります。

- 802.1X 認証をイネーブルにした場合、サプリカントが認証されてから、イーサネット インターフェイス上のレイヤ 2 またはレイヤ 3 のすべての機能がイネーブルになります。
- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、ポート チャネル、トランク、またはアクセス ポート内のイーサネット インターフェイス上だけです。
- Cisco NX-OS ソフトウェアは、ポート チャネル内のトランク インターフェイスまたはメンバ インターフェイス上ではシングル ホスト モードをサポートしません。
- Cisco NX-OS ソフトウェアは、トランク インターフェイス上では MAC アドレス認証バイパス機能をサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネル上では MAC アドレス認証バイパス機能をサポートしません。
- Cisco NX-OS ソフトウェアは、vPC ポートでの Dot1X および MCT をサポートしません。
- Cisco NX-OS ソフトウェアは、次の 802.1X プロトコル拡張機能をサポートしません。
  - 論理 VLAN 名から ID への 1 対多のマッピング
  - Web 許可
  - ダイナミック ドメイン ブリッジ割り当て
  - IP テレフォニー
- 次に、ダイナミック VLAN 割り当ての制約事項を示します。
  - ダイナミック VLAN 割り当ては、ストレート スルー接続でのみ、HIF ポート（FEX ポート）でサポートされます。
  - この機能は、Switchport アクセス ポート上でのみサポートされます。
  - RADIUS により割り当てられる VLAN は、スイッチですでに設定されている必要があります。
  - この機能は、VPC ポート、ポート チャネル、トランク ポート、および L3 ポートではサポートされません。
  - RADIUS により VLAN が割り当てられた後、別のアクセス VLAN でそれを上書きすることはできません。

802.1X のデフォルト設定

次の表に、802.1X パラメータのデフォルト設定を示します。

表 *1* : *802.1X* のデフォルト パラメータ

パラメータ	デフォルト
802.1X 機能	ディセーブル
AAA 802.1X 認証方式	未設定
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル（**force-authorized**） （注） ポートはサプリカントとの 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。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
待機タイムアウト時間	60 秒（Cisco NX-OS デバイスがサプリカ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）
再送信タイムアウト時間	30 秒（Cisco NX-OS デバイスが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（Cisco NX-OS デバイスが認証プロセスを再開するまでに、EAP-Request/Identity フレームを送信する回数）
ホスト モード	シングル ホスト
サプリカント タイムアウト時間	30秒（認証サーバからの要求をサプリカントにリレーするとき、Cisco NX-OS デバイスがサプリカントに要求を再送信するまでに、サプリカントの応答を待つ時間）
認証サーバ タイムアウト時間	30秒（サプリカントからの応答を認証サーバにリレーするとき、Cisco NX-OS デバイスがサーバに応答を再送信するまでに、サーバからの応答を待つ時間）

802.1X の設定

ここでは、802.1X 機能の設定方法について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

802.1X の設定プロセス

ここでは、802.1X を設定するプロセスについて説明します。

手順の概要

1. 802.1X 機能をイネーブルにします。
2. リモート RADIUS サーバへの接続を設定します。
3. イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

手順の詳細

ステップ 1 802.1X 機能をイネーブルにします。

ステップ 2 リモート RADIUS サーバへの接続を設定します。

ステップ 3 イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

802.1X 機能のイネーブル化

サプリカント デバイスを認証する前に、Cisco NX-OS デバイス上で 802.1X 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature dot1x**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X機能をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X 機能のステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA 認証方式の設定

802.1X 認証にリモート RADIUS サーバを使用できます。RADIUS サーバおよび RADIUS サーバ グループを設定し、デフォルト AAA 認証方式を指定したあとに、Cisco NX-OS デバイスは 802.1X 認証を実行します。

はじめる前に

リモート RADIUS サーバ グループの名前またはアドレスを取得します。

手順の概要

1. **configure terminal**
2. **aaa authentication dot1x default group***group-list*
3. **exit**
4. （任意） **show radius-server**
5. （任意） **show radius-server group** [*group-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authentication dot1x default group***group-list* 例： `switch(config)# aaa authentication dot1x default group rad2`	802.1X 認証に使用する RADIUS サーバ グループを指定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：認証に RADIUS サーバのグローバル プールを使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 5	**show radius-server group** [*group-name*] 例： `switch# show radius-server group rad2`	（任意） RADIUS サーバ グループの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの 802.1X 認証の制御

インターフェイス上で実行される 802.1X 認証を制御できます。インターフェイスの 802.1X 認証ステートは、次のとおりです。

自動

インターフェイス上で、802.1X 認証をイネーブルにします。

強制認証

インターフェイス上の 802.1X 認証をディセーブルにし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。このステートがデフォルトです。

Force-unauthorized

インターフェイス上のすべてのトラフィックを禁止します。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot* / *port*
3. **dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**}
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **show dot1x interface ethernet***slot*/*port*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot* / *port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**} 例： `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。デフォルトの設定は force-authorized です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**show dot1x interface ethernet***slot*/*port* 例： `switch# show dot1x interface ethernet 2/1`	（任意） インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

メンバ ポートでの 802.1X 認証の設定

ポート チャネルのメンバで 802.1X 認証を設定できます。

（注） ポート チャネル自体では 802.1X 認証を設定できません。

メンバ ポートで 802.1X 認証を設定する方法は 2 つあります。メンバ ポートで 802.1X を設定してからそのポートをポート チャネルに追加する方法と、ポート チャネルを作成し、そのポート チャネルにポートを追加してからそのポートで 802.1X を設定する方法です。ここで示す手順は、1 つめの方法の手順です。2 つめの方法で 802.1X を設定するには、次のコマンドを使用します。

- **interface port-channel** *channel-number*
- **interface ethernet** *slot*/*port*
- **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
- **dot1x port-control auto**

（注） 上記のコマンドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS Interfaces Command Reference*』を参照してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x port-control auto**
4. [**no**] **switchport**
5. **dot1x host-mode multi-host**
6. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **exit**
8. **exit**
9. （任意） **show dot1x all**
10. （任意） **show dot1x interface ethernet***slot*/*port*
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x port-control auto** 例： `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。
ステップ 4	[**no**] **switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 ポートとして設定します。**no** キーワードを使用する場合は、レイヤ 3 ポートとして設定します。
ステップ 5	**dot1x host-mode multi-host** 例： `switch(config-if)# dot1x host-mode multi-host`	インターフェイスのマルチ ホスト モードをイネーブルにします。このコマンドはポート チャネルにポートを追加する際に必要です。
ステップ 6	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。チャネル番号の有効範囲は 1 ～ 4096 です。ポート チャネルがない場合は、Cisco NX-OS ソフトウェアによって、このチャネル グループに関連付けられたポート チャネルが作成されます。 オプションの **force** キーワードを使用すると、互換性のない設定を持つインターフェイスを強制的にチャネルに追加できます。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。 （注） ポート チャネルから 802.1X 対応ポートを削除するには、**no channel-group** *channel-number* コマンドを使用します。

ステップ 7	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 10	**show dot1x interface ethernet***slot*/*port* 例： `switch# show dot1x interface ethernet 7/1`	（任意） インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータ PAE の作成または削除

インターフェイスで 802.1X オーセンティケータ Port Access Entity（PAE）インスタンスを作成または削除できます。

（注） デフォルトでは、インターフェイスで 802.1X をイネーブルにしたときに、Cisco NX-OS ソフトウェアによってインターフェイスでオーセンティケータ PAE インスタンスが作成されます。

はじめる前に

802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show dot1x interface ethernet***slot*/*port*
3. **interface ethernet***slot*/*port*
4. [**no**] **dot1x pae authenticator**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**show dot1x interface ethernet***slot*/*port* 例： `switch# show do1x interface ethernet 2/1`	（任意） インターフェイス上の 802.1X の設定を表示します。

ステップ 3	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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	[**no**] **dot1x pae authenticator** 例： `switch(config-if)# dot1x pae authenticator`	インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、**no** 形式を使用します。 （注） オーセンティケータ PAE がインターフェイスにすでに存在している場合は、**dot1x pae authentication** コマンドを実行してもインターフェイス上の設定は変更されません。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

グローバル定期再認証のイネーブル化

802.1X グローバル定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔は 3600 秒（1 時間）です。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x re-authentication**
3. **dot1x timeout re-authperiod** *seconds*
4. （任意） **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x re-authentication** 例： `switch(config)# dot1x re-authentication`	Cisco NX-OS デバイス上ですべてのサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。
ステップ 3	**dot1x timeout re-authperiod** *seconds* 例： `switch(config)# dot1x timeout re-authperiod 3000`	再認証の間隔（秒）を設定します。 デフォルトは 3600 秒です。有効な範囲は 1 ～ 65535 です。 （注） 定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		（任意）
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの定期再認証のイネーブル化

インターフェイスの802.1X定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔はグローバル値にデフォルト設定されます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x re-authentication**
4. （任意） **dot1x timeout re-authperiod***seconds*
5. **exit**
6. （任意） **show dot1x all**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x re-authentication** 例： `switch(config-if)# dot1x re-authentication`	インターフェイスに接続されているサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。

	コマンドまたはアクション	目的
ステップ 4	**dot1x timeout re-authperiod***seconds* 例： `switch(config-if)# dot1x timeout re-authperiod 3300`	（任意） 再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。有効な範囲は 1 ～ 65535 です。 （注） インターフェイス上の定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 6	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

手動によるサプリカントの再認証

Cisco NX-OS デバイス全体のサプリカントまたはインターフェイスのサプリカントを手動で再認証できます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **dot1x re-authenticate** [**interface***slot*/*port*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot1x re-authenticate** [**interface***slot*/*port*] 例： `switch# dot1x re-authenticate interface 2/1`	Cisco NX-OS デバイスまたはインターフェイス上のサプリカントを再認証します。

手動による 802.1X 認証の初期化

Cisco NX-OS デバイスまたは特定のインターフェイスですべてのサプリカントの認証を、手動で初期化することができます。

（注） 認証を初期化すると、クライアントの認証プロセスを開始する前に既存のすべての認証ステータスがクリアされます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **dot1x initialize** [**interface ethernet** *slot*/*port*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot1x initialize** [**interface ethernet** *slot*/*port*] 例： `switch# dot1x initialize interface ethernet 2/1`	Cisco NX-OS デバイスまたは指定のインターフェイス上の 802.1X 認証を初期化します。

802.1X グローバル認証タイマーの変更

Cisco NX-OS デバイスでは、次の 802.1X グローバル認証タイマーをサポートしています。

待機時間タイマー

デバイスがサプリカントを認証できない場合、デバイスは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。デフォルトは 60 秒です。有効な範囲は 1 ～ 65535 です。

スイッチとサプリカント間の再送信時間タイマー

クライアントは、デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。デバイスがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機した後、フレームを再送信します。デフォルトは 30 です。範囲は 1 ～ 65535 秒です。

（注） また、待機時間タイマーおよびスイッチとサプリカント間の送信時間タイマーをインターフェイス レベルでも設定できます。

（注） このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカ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場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **dot1x timeout quiet-period** *seconds*
3. （任意） **dot1x timeout tx-period** *seconds*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的
ステップ 2	**dot1x timeout quiet-period** *seconds* 例： `switch(config)# dot1x timeout quiet-period 30`	（任意） Cisco NX-OS デバイスがサプリカントとの認証情報の交換に失敗した後、待機状態を続ける時間を秒数で設定します。デフォルトは 60 秒です。範囲は 1 ～ 65535 秒です。
ステップ 3	**dot1x timeout tx-period** *seconds* 例： `switch(config)# dot1x timeout tx-period 20`	（任意） Cisco NX-OS デバイスが、EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの 802.1X 認証タイマーの変更

Cisco NX-OS デバイスのインターフェイス上で変更できる 802.1X 認証タイマーは、次のとおりです。

待機時間タイマー

Cisco NX-OS デバイスがサプリカントを認証できない場合、スイッチは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。デフォルトは、グローバル待機時間タイマーの値です。範囲は 1 ～ 65535 秒です。

レート制限タイマー

レート制限時間中、サプリカントから過剰に送信されている EAPOL-Start パケットを抑制します。オーセンティケータはレート制限時間中、認証に成功したサプリカントからの EAPOL-Start パケットを無視します。デフォルト値は 0 秒で、オーセンティケータはすべての EAPOL-Start パケットを処理します。範囲は 1 ～ 65535 秒です。

レイヤ 4 パケットに対するスイッチと認証サーバ間の再送信タイマー

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、Cisco NX-OS デバイスは所定の時間だけ待機した後、パケットを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 応答フレームに対するスイッチとサプリカント間の再送信タイマー

サプリカントは、Cisco NX-OS デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。Cisco NX-OS デバイスがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機した後、フレームを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 要求フレームに対するスイッチとサプリカント間の再送信タイマー

サプリカントは、EAP 要求フレームを受信したことを Cisco NX-OS デバイスに通知します。オーセンティケータがこの通知を受信できなかった場合、オーセンティケータは所定の時間だけ待機した後、フレームを再送信します。デフォルトは、グローバル再送信時間タイマーの値です。範囲は 1 ～ 65535 秒です。

（注） このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカ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場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. （任意） **dot1x timeout quiet-period***seconds*
4. （任意） **dot1x timeout ratelimit-period***seconds*
5. （任意） **dot1x timeout server-timeout***seconds*
6. （任意） **dot1x timeout supp-timeout***seconds*
7. （任意） **dot1x timeout tx-period***seconds*
8. **exit**
9. （任意） **show dot1x all**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x timeout quiet-period***seconds* 例： `switch(config-if)# dot1x timeout quiet-period 25`	（任意） オーセンティケータが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの時間を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 4	**dot1x timeout ratelimit-period***seconds* 例： `switch(config-if)# dot1x timeout ratelimit-period 10`	（任意） 認証に成功したサプリカントからの EAPOL-Start パケットを無視する時間を秒数で設定します。デフォルト値は 0 秒です。範囲は 1 ～ 65535 秒です。
ステップ 5	**dot1x timeout server-timeout***seconds* 例： `switch(config-if)# dot1x timeout server-timeout 60`	（任意） Cisco NX-OS デバイスが認証サーバにパケットを送信する前に待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

	コマンドまたはアクション	目的
ステップ 6	**dot1x timeout supp-timeout***seconds* 例： `switch(config-if)# dot1x timeout supp-timeout 20`	（任意） Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サプリカントが EAP 要求フレームに応答してくるのを待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 7	**dot1x timeout tx-period***seconds* 例： `switch(config-if)# dot1x timeout tx-period 40`	（任意） サプリカントから EAP 要求フレームを受信した通知が送信されない場合に、EAP 要求フレームを再送信する間隔を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 9	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

シングル ホスト モードまたはマルチ ホスト モードのイネーブル化

インターフェイス上でシングル ホスト モードまたはマルチ ホスト モードをイネーブルにすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x host-mode** {**multi-host** | **single-host**}
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x host-mode** {**multi-host**	**single-host**} 例： `switch(config-if)# dot1x host-mode multi-host`	ホスト モードを設定します。デフォルトは、single-host です。 （注） 指定したインターフェイスで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC 認証バイパスのイネーブル化

サプリカントの接続されていないインターフェイス上で、MAC認証バイパスをイネーブルにすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x mac-auth-bypass** [**eap**]
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x mac-auth-bypass** [**eap**] 例： `switch(config-if)# dot1x mac-auth-bypass`	MAC認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。**eap** キーワードを使用して、許可に EAP を使用するように Cisco NX-OS デバイスを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスでの 802.1X 認証のディセーブル化

Cisco NX-OS デバイス上の 802.1X 認証をディセーブルにできます。デフォルトでは、802.1X 機能をイネーブルにすると、Cisco NX-OS ソフトウェアが 802.1X 認証をイネーブルにします。ただし、802.1X 機能をディセーブルにした場合、設定は Cisco NX-OS デバイスから削除されます。Cisco NX-OS ソフトウェアでは、802.1X の設定を失わずに 802.1X 認証をディセーブルにできます。

（注） 802.1X 認証をディセーブルにすると、設定されているポート モードに関係なく、すべてのインターフェイスのポート モードがデフォルトの force-authorized になります。802.1X 認証を再びイネーブルにすると、Cisco NX-OS ソフトウェアはインターフェイス上に設定したポート モードを復元します。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no dot1x system-auth-control**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的
ステップ 2	**no dot1x system-auth-control** 例： `switch(config)# no dot1x system-auth-control`	Cisco NX-OS デバイス上の 802.1X 認証をディセーブルにします。デフォルトではイネーブルになっています。 （注） Cisco NX-OS デバイス上の 802.1X 認証をイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X 機能のステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 機能のディセーブル化

Cisco NX-OS デバイス上の 802.1X 機能をディセーブルにできます。

802.1X をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。Cisco NX-OS ソフトウェアは、802.1X を再度イネーブルにして設定を回復する場合に使用できる自動チェックポイントを作成します。詳細については、ご使用のプラットフォームの『*Cisco NX-OS System Management Configuration Guide*』を参照してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no feature dot1x**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**no feature dot1x** 例： `switch(config)# no feature dot1x`	802.1X 機能をディセーブルにします。 **注意** 802.1X機能をディセーブルにすると、802.1X のすべての設定が削除されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X グローバル設定のデフォルト値へのリセット

802.1X グローバル設定をデフォルト値に設定できます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x default**
3. **exit**
4. （任意） **show dot1x all**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x default** 例： `switch(config)# dot1x default`	802.1X グローバル設定をデフォルト値に戻します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X インターフェイス設定のデフォルト値へのリセット

インターフェイスの 802.1X 設定をデフォルト値にリセットすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x default**
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x default** 例： `switch(config-if)# dot1x default`	インターフェイスの 802.1X 設定をデフォルト値に戻します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オーセンティケータとサプリカント間のフレーム再送信最大リトライ回数のグローバル設定

オーセンティケータとサプリカント間の再送信時間を変更できるだけでなく、（サプリカントから応答がなかった場合に）Cisco NX-OS デバイスが認証プロセスを再開するまでに、サプリカントに EAP-Request/Identity フレームを送信する回数を設定することができます。

（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、特定のサプリカ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場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x max-req***retry-count*
3. **exit**
4. （任意） **show dot1x all**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x max-req***retry-count* 例： `switch(config)# dot1x max-req 3`	802.1X認証プロセスを再開するまでの、最大要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータとサプリカント間のフレーム再送信最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに認証要求を再送信する最大回数を設定できます。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x max-req** *count*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-req** *count* 例： `switch(config-if)# dot1x max-req 3`	最大認証要求リトライ回数を変更します。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。 （注） 指定したインターフェイスで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 認証の RADIUS アカウンティングのイネーブル化

802.1X 認証のアクティビティに対する RADIUS アカウンティングをイネーブルにできます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x radius-accounting**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的
ステップ 2	**dot1x radius-accounting** 例： `switch(config)# dot1x radius-accounting`	802.1X に対する RADIUS アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA アカウンティング方式の設定

802.1X 機能に対する AAA アカウンティング方式をイネーブルにできます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa accounting dot1x default group***group-list*
3. **exit**
4. （任意） **show aaa accounting**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**aaa accounting dot1x default group***group-list*	802.1X に対する AAA アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**：設定済みのすべての RADIUS サーバ • *named-group*：設定済みの任意の RADIUS サーバ グループ名
ステップ 3	**exit**	設定モードを終了します。
ステップ 4	**show aaa accounting**	（任意） AAA アカウンティングの設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、802.1X 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
switch# show aaa accounting
switch# copy running-config startup-config
```

インターフェイスでの再認証最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに再認証要求を再送信する最大回数を設定できます。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x max-reauth-req***retry-count*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-reauth-req***retry-count* 例： `switch(config-if)# dot1x max-reauth-req 3`	最大再認証要求リトライ回数を変更します。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 設定の確認

802.1X 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show dot1x	802.1X 機能のステータスを表示します。
show dot1x all [**details** | **statistics** | **summary**]	802.1X機能のすべてのステータスおよび設定情報を表示します。

コマンド	目的
show dot1x interface ethernet*slot*/*port* [**details** | **statistics** | **summary**]	イーサネット インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
show running-config dot1x [**all**]	実行コンフィギュレーション内の 802.1X 機能の設定を表示します。
show startup-config dot1x	スタートアップ コンフィギュレーション内の 802.1X 機能の設定を表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS Security Command Reference*』を参照してください。

802.1X のモニタリング

Cisco NX-OS デバイスが保持している 802.1X のアクティビティに関する統計情報を表示できます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **show dot1x** {**all** | **interface ethernet***slot*/*port*} **statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show dot1x** {**all** | **interface ethernet***slot*/*port*} **statistics** 例： `switch# show dot1x all statistics`	802.1X 統計情報を表示します。

802.1X の設定例

次に、アクセス ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
```

```
dot1x port-control auto
```

次に、トランク ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
dot1x host-mode multi-host
```

（注） 802.1X 認証が必要なすべてのインターフェイスに対して、**dot1x pae authenticator** コマンドおよび **dot1x port-control auto** コマンドを繰り返してください。

802.1X に関する追加情報

ここでは、802.1X の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
IEEE Std 802.1X- 2004（IEEE Std 802.1X-2001 の改訂版）	『*802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*』
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 3580	『*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』

MIB

MIB	MIB のリンク
• IEEE8021-PAE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

802.1X の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2* : *802.1X* の機能の履歴

機能名	リリース	機能情報
802.1X	6.0(1)	Release 5.2 以降、変更はありません。
802.1X	5.2(1)	Release 5.1 以降、変更はありません。
802.1X	5.1(1)	Release 5.0 以降、変更はありません。