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構成する手順について説明します。また、次のセクションを含みます：

802.1X について

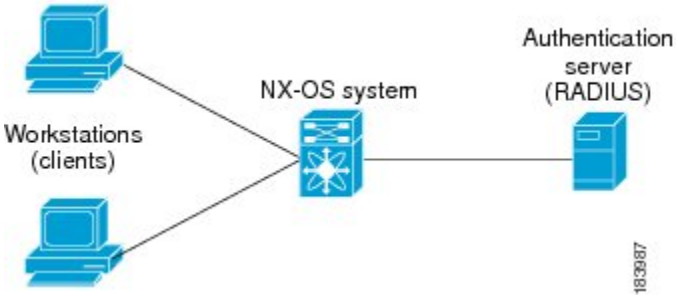
802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

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。

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（Suppliccant）]

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。

[認証サーバ（Authentication server）]

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（Authenticator）]

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。

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。

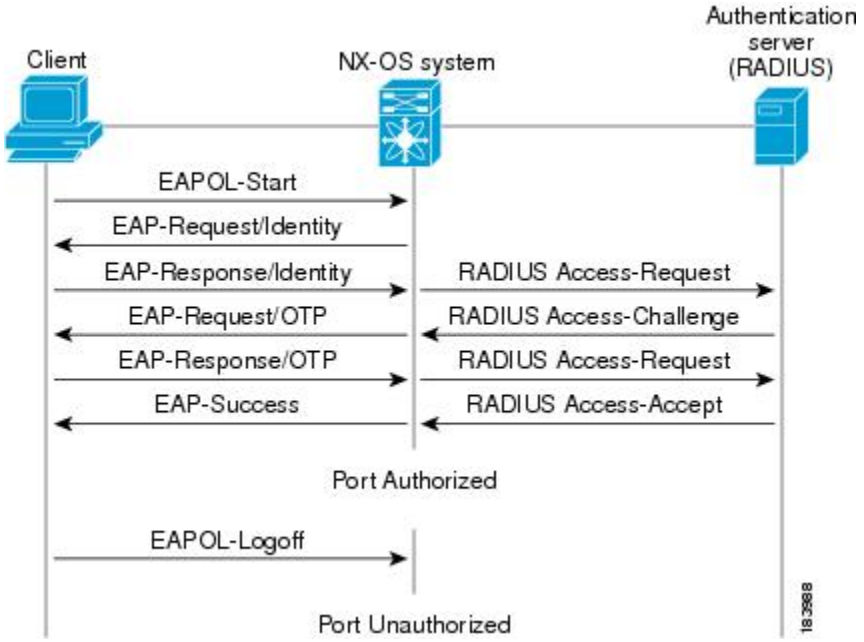
サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

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。

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。

Auto
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。

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、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 リモート認証ダイヤル イン ユーザ サービス（RADIUS）使用ガイドライン」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：この機能は、Nexus 3548 プラットフォーム スイッチではサポートされていません。

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。

MAC-Based Authentication（MAB）に基づくダイナミック VLAN 割り当て

Cisco Nexus 3548 シリーズ スイッチはダイナミック VLAN 割り当てをサポートします。802.1X 認証またはMABが完了した後。ポートを起動する前に、認証の結果としてピア/ホストを特定のVLANに配置できるようにすることができます（許可の一部として）。RADIUS サーバは、一般的に Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。VLAN をポートにバインドするこの手順は、ダイナミック VLAN 割り当てを構成します。

RADIUS からの VLAN 割り当て

dot1x または MAB によって認証が完了すると、RADIUS サーバからの応答にダイナミック VLAN 情報を含むことができるようになり、これをポートに割り当てることができます。この情報は、トンネル属性の形式の受け入れアクセス メッセージの RADIUS サーバからの応答に存在します。VLAN 割り当てのために、次のトンネル属性が送信されます。

Tunnel-type=VLAN(13)

Tunnel-Medium-Type=802

Tunnel-Private-Group-ID=VLANID

アクセス VLAN の設定のために、3 つのパラメータをすべて受け取る必要があります。

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、ポイントツーポイント トポロジをサポートします。

この設定では、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。

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。

表 *1:* ライセンス要件

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。

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。

- 802.1X ポートでマルチ認証モードが有効になります。VLAN の割り当ては、最初の認証済みホストに対し行われます。ユーザ クレデンシャルに基づいてその後に許可されたデータ ホストは、正しく認証されたと見なされます。ただし、まだ VLAN が割り当てられていないか、ポートで最初に正しく認証されたホストと一致する VLAN 割り当てがなされていることを条件とします。これにより、ポートで正常に認証されたすべてのホストは、確実に同じ VLAN メンバになります。VLAN 割り当ての柔軟性は、最初に認証されたホストだけで生じます。
- Cisco Nexus シリーズ スイッチは、以下のものについては、802.1X をサポートしていません。
  - 40G インターフェイス
  - トランジット トポロジの設定
  - VPC ポート
  - PVLAN ポート
  - L3（ルーテッド）ポート
  - ポート セキュリティ
  - CTS および MACsec が有効になっているポート。
  - Dot1x と LACP ポートチャネル
  - VPC ポートおよびサポートされていないすべての機能では、802.1X は無効になります

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、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。
- メンバーが 802.1X 用に設定されている場合、Cisco NX-OS ソフトウェアは、ポート チャネル メンバーでのシングルホスト モードの設定をサポートしません。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。
- 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 認証を有効にした場合、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 のすべての機能が有効になります。
- 802.1X 対応ポートでは、認証が成功した後にのみ STP BPDU が許可されます。STP の競合を回避するために、STP エッジポートでのみ 802.1X 機能をイネーブルにすることを推奨します。
- 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、CTS または MACsec 機能については動作しません。グローバルな「mac-learn disable」と dot1x 機能は相互に排他的であり、同時に設定することはできません。
- Dot1x は IPソースガードおよび URPF 機能とは相互に排他的であり、同時に設定することはできません。Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース9.3（3）にアップグレードする場合は、これらの機能のいずれかを無効にする必要があります。
- 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、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。ポートチャネルでサポートされるモードは、マルチホストモードだけです。
- 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。
- スイッチのリロード中、Dot1x は RADIUS アカウンティングの停止を生成しません。
- 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

- 非アクティブなセッションの再認証を防ぐには、authentication timer inactivity コマンドを使用して、非アクティブタイマーを、authentication timer reauthenticateコマンドで設定された再認証間隔よりも短い間隔に設定します。
- インターフェイスで dot1x が有効になっている異なる VLAN で、同じ MAC が学習されると、セキュリティ違反が発生します。
- DME 対応プラットフォームで dot1x を有効にした状態で MAC の学習を無効に設定しても、エラー メッセージは表示されません。
- VLAN がインターフェイスで設定されていなくても、タグ付き EAPOL フレームは処理され、クライアントのインターフェイスで認証は成功します。
- 孤立ポートで学習されたセキュアな MAC は、vPCピアで同期されません。

802.1x のデフォルト設定

表 *2 : 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	設定なし
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） 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）	3,600 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）

パラメータ	デフォルト
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（認証サーバからサプリカントに要求をリレーする場合、要求をサプリカントに再送信する前に応答のためにCisco NX-OS デバイスが待つ時間）
認証サーバ タイムアウト時間	30 秒（応答をサプリカントから認証サーバにリレーする場合、サーバーに応答を再送信する前にCisco NX-OS デバイスが返信のために待つ時間）

802.1X の設定

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

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 を有効化

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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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
	`switch# configure terminal` `switch(config)#`	
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`	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`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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

	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** 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。

	コマンドまたはアクション	目的
		• radius：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`	RADIUS サーバの設定を表示します。
ステップ 5	**show radius-server group** 例： `switch# show radius-server group rad2`	RADIUS サーバ グループの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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（Auto）
インターフェイス上で、802.1X 認証を有効にします。

強制認証
インターフェイス上の 802.1X 認証を無効にし、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。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	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** | **force-unauthorised**} 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`	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`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

802.1X 機能をイネーブルにします。

手順

	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 dot1x interface ethernet 2/1`	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） 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。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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

手順

	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。
ステップ 4	**dot1x timeout re-authperiod** 例： `switch(config-if)# dot1x timeout re-authperiod 3300`	再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。値の範囲は 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)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 6	**show dot1x all** 例： `switch# show dot1x all`	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 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	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。

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

（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ます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	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	**configure interface ethernet 2/1**
	例：
	`switch# 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`	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`	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。

	コマンドまたはアクション	目的
ステップ 5	**dot1x timeout server-timeout** *seconds* 例： `switch(config-if)# dot1x timeout server-timeout 60`	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。
ステップ 6	**dot1x timeout supp-timeout** *seconds* 例： `switch(config-if)# dot1x timeout supp-timeout 20`	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`	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	**dot1x timeout inactivity-period** *seconds* 例： `switch(config-if)# dot1x timeout inactivity-period 1800`	スイッチが非アクティブ状態を維持できる秒数を設定します。最小推奨値は 1800 秒です。

ステップ 9	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 10	**show dot1x all** 例： `switch# show dot1x all`	802.1X の設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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

手順

	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 デバイスを構成します。

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`	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`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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

手順

	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 構成 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	**dot1x host-mode multi-auth** 例： `switch(config-if)# dot1x host-mode multi-auth`	複数認証モードを設定します。ポートは、EAP または MAB のいずれか、または両方の組み合わせが正常に認証された場合にのみ許可されます。認証に失敗すると、ネットワーク アクセスが制限されます。

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

ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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* システム管理設定ガイド』を参照してください。

始める前に

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

手順

	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： `no feature dot1x`	802.1X 機能をディセーブルにします。 （注） 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`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	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** *slots 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)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

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の最大数の設定

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。

始める前に

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

手順

	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** *slots* | *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。

	コマンドまたはアクション	目的
		（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)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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

手順

	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** *slots* | *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。

	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#`
		設定モードを終了します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

802.1X 構成の確認

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。
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* セキュリティ コマンド リファレンス』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。

始める前に

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

手順

	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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。