CHAPTER 7

802.1X の設定

この章では、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。

ここでは、次の内容を説明します。

802.1X の概要

802.1X では、クライアント サーバ ベースのアクセス制御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、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 アクセス制御では、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の Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。認証に成功すると、通常のトラフィックをポート経由で送受信することができます。

ここでは、802.1X ポートベースの認証に関する次の内容について説明します。

装置のロール

802.1X ポート ベースの認証では、図 7-1 に示すように、ネットワーク上の装置にはそれぞれ特定のロールがあります。

図 7-1　802.1X 装置のロール

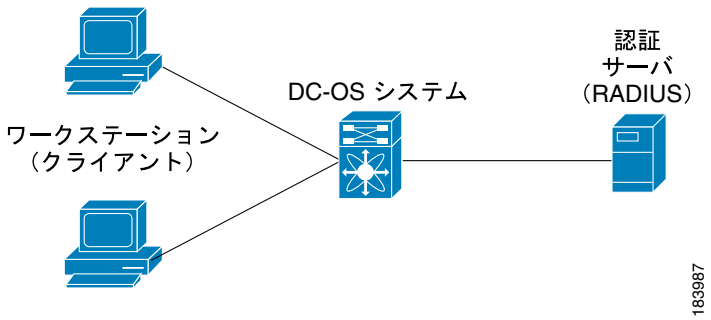


図 7-1 に示す特定のロールは、次のとおりです。

- サプリカント — LAN および NX-OS デバイス サービスへのアクセスを要求し、NX-OS デバイスからの要求に応答するクライアント装置です。ワークステーションでは、Microsoft Windows XP が動作する装置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 802.1X ポートベースの認証の問題に関しては、次の URL にある「Microsoft Knowledge Base」を参照してください。
http://support.microsoft.com/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 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 NX-OS デバイスに通知します 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、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ装置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装置（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）　NX-OS デバイスは、802.1X オーセンティケータにのみなれます。

認証の開始およびメッセージ交換

オーセンティケータ（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。

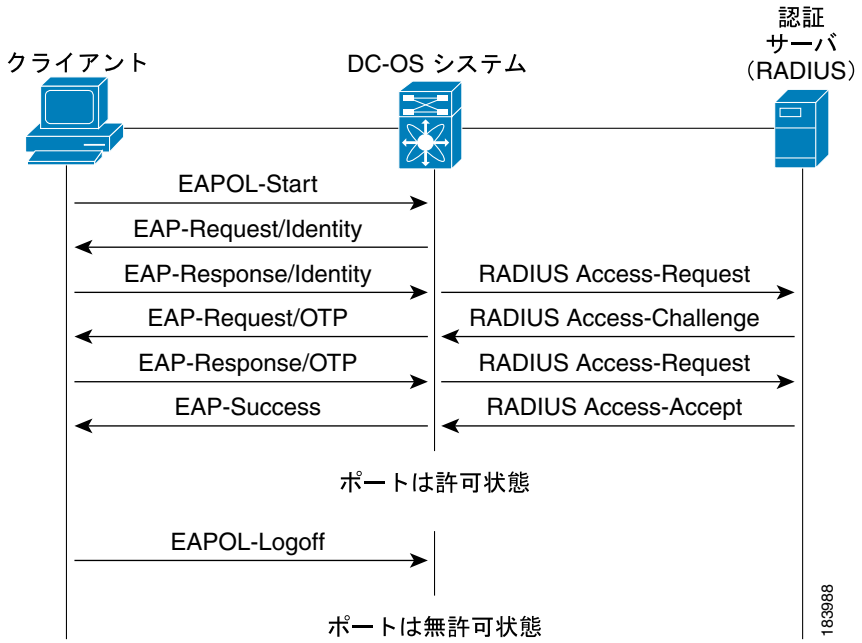
サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

（注）　ネットワーク アクセス装置で 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、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。詳細については、「許可ステートおよび無許可ステートのポート」（p.7-4）を参照してください。

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。詳細については、「許可ステートおよび無許可ステートのポート」（p.7-4）を参照してください。

EAP フレームの特殊な交換は、使用する認証方式によって異なります。図 7-2 に、サプリカントが RADIUS サーバに One-Time-Password（OTP; ワンタイム パスワード）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 認証装置は、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。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。

図 7-2　メッセージ交換



許可ステートおよび無許可ステートのポート

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。ポートは最初、無許可ステートです。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力および出力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。応答がないため、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。

ポートには次の認証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。この認証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（メディア アクセス制御）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に、ポートは無許可ステートに戻ります。

MAC アドレス認証バイパス

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、NX-OS デバイスを設定できます。たとえば、プリンタなどの装置に接続されている 802.1X 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 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、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。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あと、クライアントからのイーサネット パケットを待ちます。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、NX-OS デバイスはネットワークへのクライアント アクセスを許可します。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装置が 802.1X 対応サプリカントであることを 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 リンク ステータスがダウンになると EAPOL 履歴がクリアされます。

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、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 アトリビュート値が DEFAULT であるために前のセッションが終了した場合、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 アトリビュート（Attribute [27]）と Termination-Action RADIUS アトリビュート（Attribute [29]）に基づいていて、Termination-Action RADIUS アトリビュート（Attribute [29]）アクションが初期化の場合、（アトリビュート値は 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のみ、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 — 「ポート セキュリティを使用した 802.1X」（p.7-7）を参照してください。

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。

シングル ホストおよびマルチ ホスト 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（シングルホスト モード）したり、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（マルチホスト モード）することができます。

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だけ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、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、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 Security Association（SA; セキュリティ アソシエーション）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 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のみ適用できます。

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。

ポート セキュリティを使用した 802.1X

NX-OS デバイスでは、同じレイヤ 2 ポート上に 802.1X 認証とポート セキュリティを設定できます。802.1X は、RADIUS サーバを使用して、ポートに接続されるエンドポイント装置を認証します。ポート セキュリティは、MAC アドレスに基づいてポートを保護します（ポートの最大 MAC アドレス数まで）。この違いは、2 つの機能を組み合わせて使用することができます。NX-OS ソフトウェアでは、ホストツースイッチ型トポロジとスイッチツースイッチ型トポロジの両方で、802.1X 認証とレイヤ 2 ポートのポート セキュリティをサポートしています。

802.1X とポート セキュリティを組み合わせる場合は、802.1X とポート セキュリティの両方がサプリカントの MAC アドレスを認証する必要があります。マルチホスト モードでは、ポート セキュリティは最初のサプリカントの MAC アドレスのみ認証します。最初のサプリカントの認証に成功すると、NX-OS デバイスは他のサプリカントからの後続トラフィックをポート セキュリティに送信します。

ポート セキュリティの詳細については、第 13 章「ポート セキュリティの設定」を参照してください。

サポートされるトポロジ

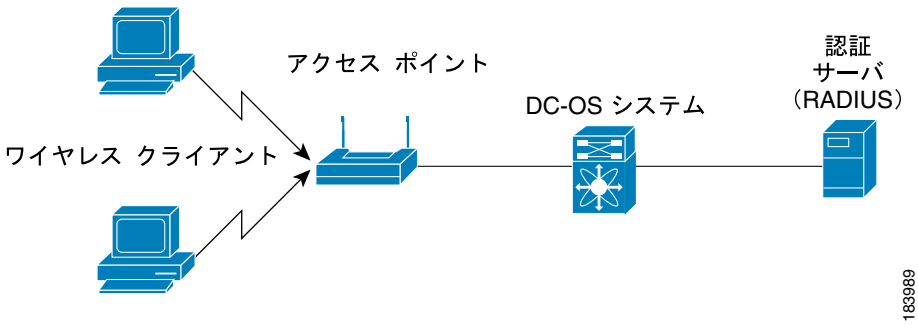
8021X ポートベースの認証は、次の 2 つのトポロジでサポートされます。

- ポイントツーポイント
- ワイヤレス LAN

ポイントツーポイント構成では（図 7-1 [p.7-2] を参照）、802.1X 対応のオーセンティケータ（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。

図 7-3 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。ポートが許可されると、ポートに間接的に接続されている他のすべてのホストは、ネットワークへのアクセスを許可されます。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）、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。

図 7-3　ワイヤレス LAN の例



バーチャライゼーション サポート

802.1X の設定と操作は、Virtual Device Context（VDC）に対してローカルです。VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』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
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、無償で提供されます。NX-OS のライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide, Release 4.0*』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（「MAC アドレス認証バイパスのイネーブル化」[p.7-22] を参照）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 の注意事項と制限事項

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限事項があります。

- NX-OS ソフトウェアは、物理ポートでのみ 802.1X をサポートしています。
- NX-OS ソフトウェアは、サブインターフェイスまたはポートチャネルでは 802.1X をサポートしません。
- 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。
- NX-OS ソフトウェアは、ポート チャネルまたはトランク内のイーサネット インターフェイスでのみ 802.1X 認証をサポートします。
- 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ー 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。
- 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。
- 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
  - ゲスト VLAN

802.1X の設定

ここでは、次の内容について説明します。

（注）　Cisco IOS CLI の知識があるユーザは、この機能に関する Cisco NX-OS のコマンドが Cisco IOS のコマンドで使用されるものと異なる場合があることに注意してください。

802.1X の設定プロセス

802.1X 認証を設定するには、次の作業を行います。

ステップ 1　802.1X 機能をイネーブルにします（「802.1X 機能のイネーブル化」[p.7-10] を参照）。

ステップ 2　リモート RADIUS サーバとの接続を設定します（「802.1X の AAA 認証方式の設定」[p.7-11] を参照）。

ステップ 3　イーサネット インターフェイスで 802.1X 認証をイネーブルにします（「インターフェイスでの 802.1X 認証の制御」[p.7-12] を参照）。

オプションとして、802.1X 認証の次のメンテナンス タスクも実行できます。

- 定期的な自動再認証をイネーブルにします（「グローバル定期再認証のイネーブル化」[p.7-13] を参照）。
- 手動で再認証を実行します（「手動によるサプリカントの再認証」[p.7-16] を参照）。
- 802.1X 機能のステートを初期化します（「手動による 802.1X 認証の初期化」[p.7-17] を参照）。
- 802.1X　グローバル認証タイマーを変更します（「802.1X　グローバル認証タイマーの変更」[p.7-17] を参照）。
- インターフェイスの 802.1X 認証タイマーを変更します（「インターフェイスの 802.1X 認証タイマーの変更」[p.7-19] を参照）。
- インターフェイスで複数ホストをイネーブルにします（「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」[p.7-21] を参照）。
- インターフェイスで MAC アドレス認証バイパス機能をイネーブルにします（「MAC アドレス認証バイパスのイネーブル化」[p.7-22] を参照）。
- 802.1X 認証を禁止します（「NX-OS デバイス上での 802.1X 認証のディセーブル化」[p.7-23] を参照）
- 802.1X 機能をディセーブルにします（「802.1X 機能のディセーブル化」[p.7-24] を参照）。
- 802.1X グローバル設定をデフォルト値にリセットします（「802.1X グローバル設定のデフォルト値へのリセット」[p.7-25] を参照）。
- 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」[p.7-26] を参照）。
- フレーム再送信リトライ回数を変更します（「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」[p.7-27] を参照）。
- 802.1X 認証の RADIUS アカウンティングをイネーブルにします（「8021.X の RADIUS アカウンティングのイネーブル化」[p.7-29] を参照）。
- 802.1X の AAA アカウンティングを設定します（「802.1X の AAA アカウンティング方式の設定」[p.7-30] を参照）。
- 802.1X 認証の最大要求数を変更します（「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」[p.7-28] を参照）。
- 802.1X 再認証の最大要求数を変更します（「インターフェイスでの再認証最大リトライ回数の設定」[p.7-31] を参照）。

802.1X 機能のイネーブル化

サプリカント装置を認証する前に、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **feature dot1x**
3. **exit**
4. **show dot1x**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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。デフォルトはディセーブルです。
ステップ 3	**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 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、NX-OS デバイスは 802.1X 認証を実行します。

RADIUS サーバの設定手順については、第 3 章「RADIUS の設定」を参照してください。RADIUS サーバ グループの設定手順については、第 2 章「AAA の設定」を参照してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

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. **config t**
2. **aaa authentication dot1x default group** *group-list*
3. **exit**
4. **show radius-server**
5. **show radius-server group** [*group-name*]
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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* 引数は、グループ名をスペースで区切ったリストです。グループ名は次のとおりです。 • **radius** — RADIUS サーバのグローバル プールを認証に使用します。 • *named-group* — RADIUS サーバの名前付きサブセットを認証に使用します。

ステップ 3	**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 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。
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。

- auto — インターフェイス上の 802.1X 認証をイネーブルにします。
- force-authorized — 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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。デフォルトは、**force-authorized** です。
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。
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。

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。

手動でサプリカントを再認証する場合は、「手動によるサプリカントの再認証」（p.7-16）を参照してください。

（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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **dot1x re-authentication**
3. **dot1x timeout re-authperiod** *seconds*
4. **exit**
5. **show dot1x all**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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`	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。 デフォルト値は 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にのみ、このコマンドは 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）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`	（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。

手動でサプリカントを再認証する場合は、「手動によるサプリカントの再認証」（p.7-16）を参照してください。

（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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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)#`
		（任意）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`	（任意）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	目的
ステップ 4	**dot1x timeout re-authperiod** *seconds* **例：** `switch(config-if)# dot1x timeout re-authperiod 3300`	（任意）再認証の間隔を秒数で設定します。デフォルト値は 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にのみ、このコマンドは 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)#`
		（任意）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(config)# show dot1x`	（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

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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**dot1x re-authenticate** [**interface** *slot*/*port*] **例：** `switch# dot1x re-authenticate interface 2/1`	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

NX-OS デバイスまたは特定のインターフェイスの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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**dot1x initialize** [**interface ethernet** *slot*/*port*] **例：** `switch# dot1x initialize interface ethernet 2/1`	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

NX-OS デバイスでは、次の 802.1X グローバル認証タイマーがサポートされます。

- 待機時間タイマー — NX-OS デバイスがサプリカントを認証できない場合、所定の時間アイドル状態を続けたあと、再試行します。待機時間タイマーの値でアイドル時間が決まります。認証が失敗する原因には、サプリカントが提供したパスワードが無効な場合があります。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。デフォルト値は 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、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。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）だけ待機したあと、フレームを再送信します。デフォルトは 30 秒です。有効な範囲は 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（「インターフェイスの 802.1X 認証タイマーの変更」[p.7-19] を参照）。

（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必要がある場合にのみ変更してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **dot1x timeout quiet-period** *seconds*
3. **dot1x timeout tx-period** *seconds*
4. **exit**
5. **show dot1x all**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 timeout quiet-period** *seconds* **例：** `switch(config)# dot1x timeout quiet-period 30`	（任意）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あと、待機状態を続ける時間を秒数で設定します。デフォルト値は 60 秒です。有効値の範囲は 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）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。デフォルト値は 30 秒です。有効値の範囲は 1 ～ 65535 秒です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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(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

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 — 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、そのあと再試行します。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。デフォルトより小さい値を入力して、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。有効な範囲は 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。有効な範囲は 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、NX-OS デバイスは所定の時間だけ待機したあと、パケットを再送信します。デフォルト値は 30 秒です。有効な範囲は 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、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。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）だけ待機したあと、フレームを再送信します。デフォルト値は 30 秒です。有効な範囲は 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、NX-OS デバイスに EAP 要求フレームを受信したことを通知します。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あと、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。有効な範囲は 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のみ変更してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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。有効値の範囲は 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。有効値の範囲は 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）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。デフォルト値は 30 秒です。有効値の範囲は 1 ～ 65535 秒です。
ステップ 6	**dot1x timeout supp-timeout** *seconds* **例：** switch(config-if)# dot1x timeout supp-timeout 20	（任意）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。デフォルト値は 30 秒です。有効値の範囲は 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。有効値の範囲は 1 ～ 65535 秒です。
ステップ 8	**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 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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）** 指定のインターフェイスに対し **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)#`
		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。

	コマンド	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。

MAC アドレス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 アドレス認証バイパス機能をイネーブルにすることができます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 アドレス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 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)#`
		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。

	コマンド	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。

NX-OS デバイス上での 802.1X 認証のディセーブル化

NX-OS デバイス上の 802.1X 認証をディセーブルにすることができます。デフォルトでは、802.1X 機能をイネーブルにすると、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 NX-OS デバイスから削除されます。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（「インターフェイスでの 802.1X 認証の制御」[p.7-12] を参照）。802.1X 認証を再びイネーブルにすると、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **no dot1x system-auth-control**
3. **exit**
4. **show dot1x**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 dot1x system-auth-control** **例：** `switch(config)# no dot1x system-auth-control`	NX-OS デバイス上の 802.1X 認証をディセーブルにします。デフォルトはイネーブルです。 **（注）** 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。

	コマンド	目的
ステップ 3	**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 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

NX-OS デバイス上の 802.1X 機能をディセーブルにすることができます。

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 NX-OS デバイスから削除されます。802.1X 認証を停止する場合は、「NX-OS デバイス上での 802.1X 認証のディセーブル化」(p.7-23)を参照してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **no feature dot1x**
3. **exit**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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。

	コマンド	目的

ステップ 3	**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 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **dot1x default**
3. **exit**
4. **show dot1x all**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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#`
		コンフィギュレーション 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **interface ethernet** *slot/port*
3. **dot1x default**
4. **exit**
5. **show dot1x all**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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)#`
		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(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）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のみ変更してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **dot1x max-req** *retry-count*
3. **exit**
4. **show dot1x all**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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。 **（注）** 指定のインターフェイスに対し **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** に設定されているのを確認してください。

ステップ 3	**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。

	コマンド	目的
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、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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。

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。

	コマンド	目的
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。

8021.X 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **dot1x radius-accounting**
3. **exit**
4. **show dot1x**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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 radius-accounting** **例：** switch(config)# dot1x radius-accounting	8021.X に対する RADIUS アカウンティングをイネーブルにします。デフォルトはディセーブルです。
ステップ 3	**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 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

1. **config t**
2. **aaa accounting dot1x default group** *group-list*
3. **exit**
4. **show aaa accounting**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 accounting dot1x default group** *group-list* **例：** `switch(config)# dot1x aaa accounting default group radius`	8021.X に対する AAA アカウンティングをイネーブルにします。デフォルトはディセーブルです。 *group-list* 引数は、グループ名をスペースで区切ったリストです。グループ名は次のとおりです。 • **radius** — RADIUS サーバのグローバル プールを認証に使用します。 • *named-group* — RADIUS サーバの名前付きサブセットを認証に使用します。

ステップ 3	**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 4	**show aaa accounting** **例：** `switch# 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** **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、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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、次の作業のいずれかを行います。

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。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

802.1X 統計情報の表示

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します。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS デバイス上の 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」[p.7-10] を参照）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	`switch# 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。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

802.1X の設定例

次に、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 port-control auto
```

（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 port-control auto** コマンドを繰り返してください。

デフォルト設定

表 7-1 に、802.1X パラメータのデフォルト設定を示します。

表 7-1　802.1X 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（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あと、待機状態を続ける秒数）
再送信タイムアウト時間	30 秒（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（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、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、NX-OS デバイスがサーバに応答を再送信するまでに、サーバのリプライを待つ時間）

その他の参考資料

802.1X の実装に関連する詳細情報については、次を参照してください。

関連資料

関連事項	タイトル
NX-OS ライセンス	『*Cisco NX-OS Licensing Guide, Release 4.0*』
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
VRF の設定	『*Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0*』

規格

規格	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 の確認とダウンロードを行うには、次の URL にアクセスします。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml