domain（AAA）～ dot1x timeout（EtherSwitch）

domain（AAA）

RADIUS アプリケーションのユーザ名のドメイン オプションを設定するには、動的許可ローカル サーバ コンフィギュレーション モードで **domain** コマンドを使用します。 設定されたユーザ名のドメイン オプションをディセーブルにするには、このコマンドの **no** 形式を使用します。

domain {**delimiter** *character*| **stripping [right-to-left]**}

no domain {**delimiter** *character*| **stripping [right-to-left]**}

構文の説明

delimiter *character*	ドメイン デリミタを指定します。 **@**、**/**、**$**、**%**、****、**#**、または **-** のいずれかのオプションを指定できます。
stripping	**@** ドメイン デリミタの左側にある名前と着信ユーザ名を比較します。
right-to-left	右から左方向に見て最初のデリミタで文字列を終了します。

コマンド デフォルト

ユーザ名のドメイン オプションは設定されていません。

コマンド モード

動的許可ローカル サーバ コンフィギュレーション（config-locsvr-da-radius）

コマンド履歴

リリース	変更内容
12.2(31)SB14	このコマンドが導入されました。
12.2(33)SRC5	このコマンドが、Cisco IOS Release 12.2(33)SRC5 に統合されました。
Cisco IOS XE Release 2.3	このコマンドが変更されました。 このコマンドが ASR 1000 シリーズ ルータに実装されました。
15.1(2)T	このコマンドが Cisco IOS Release 15.1(2)T に統合されました。 このコマンドも変更されました。 **right-to-left** キーワードが追加されました。

使用上のガイドライン

ドメイン ストリッピングが設定されていない場合は、パケット オブ ディスコネクト（POD）のメッセージの認証、許可、およびアカウンティング（AAA）で提供される完全なユーザ名がオンライン加入者と比較されます。 ドメイン ストリッピングを設定すると、**@** ドメイン デリミタの前にあるユーザ名のみを使用した接続解除メッセージを送信できます。 ネットワーク アクセス サーバ（NAS）は、このユーザ名を潜在的なドメインを持つ任意のオンライン加入者と比較および照合します。

たとえば、ドメイン ストリッピングが設定されている場合に、ユーザ名「test」を使用した POD メッセージを送信すると、POD メッセージとオンライン加入者間の比較が実行され、ユーザ名「test@cisco.com」または「test」を使用した加入者が、指定されたユーザ名「test」と照合されます。

例

次の設定例を使用して、ユーザ名を右から左に向かって照合します。 ユーザ名が user1@cisco.com の場合、POD メッセージにより照合されるユーザ名は user1@cisco.com になります。

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

次の設定例を使用して、ユーザ名を左から右に向かって照合します。 ユーザ名が user1@cisco.com の場合、POD メッセージにより照合されるユーザ名は user1 になります。

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

関連コマンド

コマンド	説明
aaa server radius dynamic-author	AAA サーバとしてデバイスを設定して、外部ポリシー サーバとの相互作用を実行します。

dot1x control-direction

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x control-direction** コマンドは、**authentication control-direction** コマンドに置き換えられています。 詳細については、**authentication control-direction** コマンドを参照してください。

IEEE 802.1X が制御するポートを単方向または双方向に変更するには、インターフェイス コンフィギュレーション モードで **dot1x control-direction** コマンドを使用します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x control-direction {**both**| **in**}

no dot1x control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが導入されました。
12.4(6)T	このコマンドが、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SXI	このコマンドは、**authentication control-direction** コマンドに置き換えられました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、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が定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する 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はポートを通過できるようになります。

単方向ステート

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに移行します。

単方向制御ポートをイネーブルにすると、接続ホストはスリープ モードまたは電源切断状態になります。 ホストはそのネットワークの他の装置とトラフィックを交換しません。 単方向ポートに接続されているホストはトラフィックをネットワークに送信できず、ホストはネットワークの他の装置からのトラフィックだけを受信します。

双方向ステート

dot1x control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、ポートは両方向のアクセスを制御します。 この状態では、スイッチ ポートは EAPOL パケットだけを受信または送信し、他のパケットはすべてドロップされます。

both キーワードを使用するか、またはこのコマンドの **no** 形式を使用すると、ポートはデフォルト設定の双方向モードに変更されます。

Catalyst 6500 シリーズ スイッチ

ポートを双方向に設定すると、Wake-on-LAN（WoL）による 802.1X 認証がイネーブルになります。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチ ポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次の例では、単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
```

次に、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction both
```

または

```
Switch(config-if)# no dot1x control-direction
```

設定を確認するには、show dot1x all 特権 EXEC コマンドを入力します。 show dot1x all コマンド出力は、ポート名とポートのステートを除き、すべてのデバイスで同一です。 ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

dot1x control-direction in コマンドを入力して単方向制御をイネーブルにする場合、show dot1x all コマンド出力では次のように表示されます。

```
ControlDirection = In
```

dot1x control-direction in コマンドを入力しても、設定の競合によりポートでこのモードをサポートできない場合、show dot1x all コマンド出力では次のように表示されます。

```
ControlDirection = In (Disabled due to port settings):
```

次に、グローバル 802.1X パラメータをリセットする例を示します。

```
Switch(config)# dot1x default
```

例

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

```
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x control-direction in
```

関連コマンド

コマンド	説明
show dot1x	アイデンティティ プロファイルの詳細を表示します。

dot1x credentials

サプリカント設定時の 802.1X クレデンシャル プロファイルを指定する、またはクレデンシャル構造をインターフェイスに適用し、dot1x クレデンシャルのコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x credentials** コマンドを使用します。 クレデンシャル プロファイルを削除するには、このコマンドの **no** 形式を使用します。

dot1x credentials *name*

no dot1x credentials

構文の説明

name	クレデンシャル プロファイルの名前。

コマンド デフォルト

クレデンシャル プロファイルは指定されません。

コマンド モード

グローバル コンフィギュレーションまたはインターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.4(6)T	このコマンドが導入されました。

使用上のガイドライン

802.1Xクレデンシャル構造は、サプリカントを設定する場合に必要です。 このクレデンシャル構造は、ユーザ名、パスワード、および説明を含む場合があります。

例

次に、サプリカントの設定時に使用する必要があるクレデンシャル プロファイルの例を示します。

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

dot1x pae supplicant キーワードおよびキーワードとともにクレデンシャル構造をインターフェイスに適用して、そのインターフェイス上でのサプリカント機能をイネーブルにできます。

```
interface fastethernet 0/1
```

```
dot1x credentials basic-user
dot1x pae supplicant
```

関連コマンド

コマンド	説明
anonymous-id (dot1x credential)	クレデンシャルプロファイルに関連付けられた匿名アイデンティティを指定します。
description (dot1x credential)	802.1X クレデンシャル プロファイルの説明を指定します。
password (dot1x credential)	802.1X クレデンシャルプロファイルのパスワードを指定します。
username (dot1x credential)	802.1X クレデンシャル プロファイルのユーザ名を指定します。

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証のパラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical {**eapol**| **recovery delay** *milliseconds*}

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL-Success メッセージを送信するように指定します。
recovery delay *milliseconds*	使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカル ポートを再初期化するためにスイッチが待機するリカバリ遅延時間を指定します。有効な値は 1 ～ 10000 ミリ秒です。

コマンド デフォルト

デフォルト設定は、次のとおりです。

- **eapol**：ディセーブル
- *milliseconds*：1000 ミリ秒

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。
12.2(33)SXI	**recovery delay** キーワードは、**authentication critical recovery delay** コマンドに置き換えられました。

例

次に、スイッチが正常にクリティカル ポートを認証した場合にスイッチが EAPOL-Success メッセージを送信するよう指定する例を示します。

```
Switch(config)# dot1x critical eapol
```

次の例では、使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカルなポートの再初期化をスイッチが待機するリカバリ遅延期間を設定する方法を示します。

```
Switch(config)# dot1x critical recovery delay 1500
```

関連コマンド

コマンド	説明
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x critical（インターフェイス コンフィギュレーション）

802.1X クリティカル認証、および任意で 802.1X クリティカル認証リカバリと 802.1X クリティカル認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x critical** コマンドを使用します。 802.1X クリティカル認証、および任意で 802.1X クリティカル認証リカバリと 802.1X クリティカル認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x critical [**recovery action reinitialize**]

no dot1x critical [**recovery action reinitialize**]

構文の説明

recovery action reinitialize	（任意）802.1X クリティカル認証リカバリをイネーブルにし、認証サーバが使用可能なときにポートが認証されるように指定します。

コマンド デフォルト

802.1X クリティカル認証はインターフェイス上でイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。

例

次に、IEEE 802.1X クリティカル認証をインターフェイス上でイネーブルにする例を示します。

```
Router(config-if)# dot1x critical
```

次に、認証サーバが使用可能な場合に 802.1X クリティカル認証リカバリをイネーブルにして、ポートを認証する例を示します。

```
Router(config-if)# dot1x critical recovery action reinitialize
```

次に、IEEE 802.1X クリティカル認証をインターフェイス上でディセーブルにする例を示します。

```
Router(config-if)# no
 dot1x critical
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1Xクリティカル認証パラメータを設定します。

dot1x default

最新の IEEE 802.1x 標準で指定されたデフォルト値にグローバル 802.1X 認証パラメータをリセットするには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x default** コマンドを使用します。

dot1x default

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト値は次のとおりです。

- インターフェイス単位の 802.1X プロトコル イネーブル ステートは、ディセーブルです（強制的に許可）。
- 再認証試行間隔の秒数は、3600 秒です。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- 複数ホストのサポートは、ディセーブルです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

コマンド モード

グローバル コンフィギュレーション（config）インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.2(14)SX	このコマンドが Cisco IOS Release 12.2(14) SX の Supervisor Engine 720 に実装されました。

リリース	変更内容
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(6)T	インターフェイス コンフィギュレーションが、このコマンドのコンフィギュレーション モードとして追加されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、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が定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセスポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザデバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol（EAP）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はポートを通過できるようになります。

現在の 802.1X 設定を確認するには、**show dot1x** コマンドを使用します。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、グローバル 802.1X パラメータをリセットする例を示します。

```
Router(config)# dot1x default
```

次に、FastEthernet インターフェイス 0 のグローバル 802.1X パラメータをリセットする例を示します。

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。
dot1x max-req	認証プロセスを再開する前に、デバイスが EAP 要求/アイデンティティ フレームを送信する最大回数を設定します（応答を受信しないと仮定）。
dot1x re-authentication（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにします。
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	802.1X 情報を表示します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x guest-vlan

アクティブ VLAN を IEEE 802.1x のゲスト VLAN として指定するには、インターフェイス コンフィギュレーション モードで **dot1x guest-vlan** コマンドを使用します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x guest-vlan vlan-id

no dot1x guest-vlan

構文の説明

vlan-id	アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。 指定できる範囲は1～4094です。

コマンド デフォルト

ゲスト VLAN は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	このコマンドは、デフォルトのゲスト VLAN の動作を変えるように変更されました。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.3(1)S	このコマンドが、Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

スタティック アクセス ポートにゲスト VLAN を設定できます。

IEEE 802.1x ポートごとにゲスト VLAN を設定して、現在 IEEE 802.1x 認証を実行していないクライアント（スイッチに接続されているデバイスまたはワークステーション）へのサービスを制限できます。 こうしたユーザは IEEE 802.1x 認証のためにシステムをアップグレードできますが、Windows 98 システムなどのホストでは IEEE 802.1x に対応できません。

IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しない、あるいは EAPOL パケットがクライアントから送信されないと、ソフトウェアではクライアントをゲスト VLAN に割り当てます。

Cisco IOS Release 12.4(11)T 以降では、スイッチは EAPOL パケット履歴を保持します。 リンクの存続時間内に別の EAPOL パケットがインターフェイス上で検出された場合、ゲスト VLAN 機能はディセーブルになります。 ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。 EAPOL 履歴はリンクの損失でリセットされます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1x 非対応クライアントはいくつでもアクセスが許可されます。 IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードまたはマルチホスト モードの IEEE 802.1x スイッチ ポートでサポートされます。

リモート スイッチド ポート アナライザ（RSPAN）VLAN、音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。 ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。 クライアント上の DHCP プロセスが時間切れとなり、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。 **dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドおよび **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用して、IEEE 802.1x 認証プロセスの設定を減らす必要があります。減らす量は、接続される IEEE 802.1x クライアントの種類によって変わります。

例

次の例では、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config-if)# dot1x guest-vlan 5
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# dot1x timeout max-reauth-req 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

show dot1x interface*interface-id* 特権 EXEC コマンドを入力して、デバイスまたは指定したインターフェイスに関する IEEE 802.1x の管理ステータスおよび動作ステータスを表示できます。

関連コマンド

コマンド	説明
dot1x max-reauth-req	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを再送信する回数を指定します。
dot1x timeout	認証の再試行タイムアウトを設定します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。

dot1x guest-vlan supplicant

802.1x 対応サプリカントがゲスト VLAN に移行できるようにするには、グローバル コンフィギュレーション モードで **dot1x guest-vlan supplicant** コマンドを使用します。 802.1x 対応サプリカントがゲスト VLAN に移行できないようにするには、このコマンドの **no** 形式を使用します。

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

802.1x 対応サプリカントはゲスト VLAN に移行できなくなります。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。

例

次に、802.1x 対応サプリカントがゲスト VLAN に移行できるようにする例を示します。

```
Router(config)# dot1x guest-vlan supplicant
```

次に、802.1x 対応サプリカントがゲスト VLAN に移行できないようにする例を示します。

```
Router(config)# no dot1x guest-vlan supplicant
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x initialize

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x initialize** コマンドは、**clear authentication session** コマンドに置き換えられています。 詳細については、**clear authentication session** コマンドを参照してください。

すべての 802.1X 対応インターフェイスの 802.1X クライアントを初期化するには、特権 EXEC モードで **dot1x initialize** コマンドを使用します。 このコマンドには、**no** 形式はありません。

dot1x initialize [**interface** *interface-name*]

構文の説明

interface *interface-name*	（任意）初期化するインターフェイスを指定します。このキーワードを入力しない場合、すべてのインターフェイスが初期化されます。

コマンド デフォルト

ステート マシンはイネーブルになりません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

このコマンドは、802.1X ステート マシンを初期化し、新たな認証環境を設定します。 このコマンドを入力した後、ポートの状態は無許可になります。

例

次に、手動でポートを初期化する例を示します。

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

show dot1x [**interface** *interface-name*] コマンドを入力して、無許可ポートのステータスを確認できます。

関連コマンド

コマンド	説明
show dot1x	アイデンティティ プロファイルの詳細を表示します。

dot1x mac-auth-bypass

クライアント MAC アドレスに基づいてスイッチがクライアントを許可できるようにするには、インターフェイス コンフィギュレーション モードで **dot1x mac-auth-bypass** コマンドを使用します。 MAC 認証バイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

構文の説明

eap	（任意）許可に拡張認証プロトコル（EAP）を使用するようにスイッチを設定します。

コマンド デフォルト

MAC 認証バイパスはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。
15.1(4)M	このコマンドが、Cisco IOS Release 15.1(4)M に統合されました。

使用上のガイドライン

（注） MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。 認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。 許可が失敗した場合、VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

例

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

次に、認証に EAP を使用するようにスイッチを設定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

次に、MAC 認証バイパスをディセーブルにする例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x max-reauth-req

オーセンティケータがクライアントに拡張認証プロトコル（EAP）要求/アイデンティティ フレーム送信する最大回数を設定するには（応答が受信されないと仮定）、インターフェイス コンフィギュレーション モードで **dot1x max-reauth-req** コマンドを使用します。 デフォルト設定の 2 に最大回数を設定するには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *number*

no dot1x max-reauth-req

構文の説明

number	最大回数。 範囲は 1 ～ 10 です。 デフォルトは 2 です。

コマンド デフォルト

コマンドのデフォルトは 2 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(18)SE	このコマンドが導入されました。
12.2(25)SEC	*number* 引数が追加されました。
12.4(6)T	このコマンドが、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。

使用上のガイドライン

このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

設定の確認

show dot1x [interface interface-id] コマンドを入力して、設定を確認できます。

例

次に、無許可ステートに変わる前に認証プロセスが再開される回数を4に設定する例を示します。

```
Router(config-if)# dot1x max-reauth-req 4
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、デバイスがEAP要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x timeout tx-period	スイッチが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x	指定されたポートの IEEE 802.1X の状態を表示します。

dot1x max-req

認証プロセスを再開する前に、ネットワーキング デバイスまたはイーサネット スイッチ ネットワーク モジュールが拡張認証プロトコル（EAP）要求/アイデンティティ フレームを送信できる最大回数を設定するには（応答を受信しないと仮定）、インターフェイス コンフィギュレーション モードまたはグローバル コンフィギュレーション モードで **dot1x max-req** コマンドを使用します。 デフォルト設定の 2 に回数を設定するには、このコマンドの **no** 形式を使用します。

dot1x max-req *retry-number*

no dot1x max-req

構文の説明

retry-number	再試行の最大数。 値は 1 ～ 10 です。 デフォルト値は 2 です。 値は要求 ID を除くすべての EAP パケットに適用できます。

コマンド デフォルト

デフォルトの再試行回数は 2 回です。

コマンド モード

インターフェイス コンフィギュレーション（config）グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが Cisco イーサネット スイッチ ネットワーク モジュールに導入されました。
12.2(14)SX	このコマンドが Cisco IOS Release 12.2(14) SX の Supervisor Engine 720 に実装されました。
12.2(15)ZJ	このコマンドが、シスコ イーサネット スイッチ ネットワーク モジュールの Cisco IOS Release 12.2(15) ZJ のプラットフォーム Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズに実装されました。
12.1(11)AX	このコマンドが、Cisco IOS Release 12.1(11)AX に統合されました。
12.1(14)EA1	このコマンドが Cisco IOS Release 12.1(14) EA1 に統合され、コンフィギュレーション モードは EtherSwitch ネットワーク モジュールを除き、インターフェイス コンフィギュレーション モードに変更されました。

リリース	変更内容
12.3(2)XA	このコマンドが Cisco IOS Release 12.3(2) XA に統合され、Cisco 806、Cisco 831、Cisco 836、Cisco 837、Cisco 1701、Cisco 1710、Cisco 1721、Cisco 1751-V、Cisco 1760 のルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合され、Cisco 1751、Cisco 2610XM、Cisco 2611XM、Cisco 2620XM、Cisco 2621XM、Cisco 2650XM、Cisco 2651XM、Cisco 2691、Cisco 3640、Cisco 3640A、Cisco 3660 のルータ プラットフォームに実装されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、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が定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。 単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol（EAP）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はポートを通過できるようになります。

（注） このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、ネットワーキング デバイスが EAP 要求/アイデンティティ メッセージをクライアント PC に送信する最大回数が 6 である例を示します。

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

次に、認証プロセスを再開するまでに、スイッチが EAP 要求/アイデンティティ フレームを送信する回数を 5 に設定する例を示します。

```
Router(config-if)# dot1x max-req 5
```

関連コマンド

コマンド	説明
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x reauthentication（EtherSwitch）	802.1Xインターフェイスのイーサネット スイッチ ネットワーク モジュール クライアントの定期的な再認証をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x multiple-hosts

（注） このコマンドは、Cisco IOS Release 12.1(14)EA1 および Release 12.4(6)T で有効な **dot1x host-mode** コマンドに置き換えられました。

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 802.1X 許可ポートに、複数のホスト（クライアント）が接続できるようにするには、インターフェイス コンフィギュレーション モードで **dot1x multiple-hosts** コマンドを使用します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x multiple-hosts

no dot1x multiple-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

複数ホストはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.1(14)EA1	このコマンドが Cisco IOS Release 12.1(14) EA1 で **dot1x host-mode** コマンドに置き換えられました。
12.4(6)T	このコマンドが T トレインで **dot1x host-mode** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、スイッチ ポートに限りサポートされます。

このコマンドにより、1 つの 802.1X 対応ポートに複数のクライアントを接続することができます。 このモードでは、接続されたホストのうち 1 つが認証に成功すれば、すべてのホストがネットワーク 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 Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

interface キーワードと **show dot1x**（EtherSwitch） 特権 EXEC コマンドを使用して、現在の 802.1X の複数ホスト設定を確認します。

例

次に、FastEthernet インターフェイス 0/1 上で 802.1X をイネーブルにし、マルチ ホストを許容する例を示します。

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

関連コマンド

コマンド	説明
dot1x default	ポートの認証ステートの手動制御をイネーブルにします。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x pae

ポート アクセス エンティティ（PAE）タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。 設定された PAE タイプをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x pae [**supplicant**| **authenticator**| **both**]

no dot1x pae [**supplicant**| **authenticator**| **both**]

構文の説明

supplicant	（任意）インターフェイスは、サプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	（任意）インターフェイスは、オーセンティケータとしてだけ機能し、サプリカント向けのメッセージに応答しません。
both	（任意）インターフェイスは、サプリカントおよびオーセンティケータとして動作するため、すべての dot1x メッセージに応答します。

コマンド デフォルト

PAE タイプは設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.3(11)T	このコマンドが導入されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

dot1x system-auth-control コマンドが設定されていない場合、**supplicant** キーワードがこのコマンドで使用できる唯一のキーワードとなります。（つまり、**dot1x system-auth-control** コマンドが設定されていない場合、インターフェイスをオーセンティケータとして設定できません）。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x system-auth-control	802.1X SystemAuthControl（ポートベース認証）をイネーブルにします。
interface	インターフェイス タイプを設定します。

dot1x port-control

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x port-control** コマンドは、**authentication port-control** コマンドに置き換えられています。 詳細については、**authentication port-control** コマンドを参照してください。

制御ポートの許可ステートの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x port-control** コマンドを使用します。 ポート制御値をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

no dot1x port-control

構文の説明

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 Extensible Authentication Protocol over LAN（EAPOL）フレームだけです。
force-authorized	インターフェイスの 802.1X をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。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。 **force-authorized** キーワードはデフォルトです。
force-unauthorized	クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

デフォルトの設定は force-authorized です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが Cisco イーサネット スイッチ ネットワーク モジュールに追加されました。
12.1(11)AX	このコマンドが、Cisco IOS Release 12.1(11)AX に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(15)ZJ	このコマンドが、Cisco イーサネット スイッチ ネットワーク モジュールのプラットフォーム Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズに実装されました。
12.3(2)XA	このコマンドが、Cisco 806、Cisco 831、Cisco 836、Cisco 837、Cisco 1701、Cisco 1710、Cisco 1721、Cisco 1751-V、および Cisco 1760 の Cisco スイッチに導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。 Cisco 1751、Cisco 2610XM、Cisco 2611XM、Cisco 2620XM、Cisco 2621XM、Cisco 2650XM、Cisco 2651XM、Cisco 2691、Cisco 3640、Cisco 3640A、および Cisco 3660 のプラットフォームにスイッチのサポートが追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2（17d）SXB に追加されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXI	このコマンドが、**authentication port-control** コマンドに置き換えられました。

使用上のガイドライン

イーサネット スイッチ ネットワーク モジュールの場合

イーサネット スイッチ ネットワーク モジュールには、次の注意事項が適用されます。

- 802.1X プロトコルは、レイヤ 2 スタティック アクセス ポートでサポートされます。
- ポートが次のタイプのいずれかとして設定されていない場合に限り、**auto** キーワードを使用できます。

- トランク ポート：トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- EtherChannel ポート：ポート上で 802.1X をイネーブルにする前に、EtherChannel から 802.1X を削除する必要があります。 EtherChannel または EtherChannel 内のアクティブなポート上で 802.1x をイネーブルにしようとすると、エラーが表示され、802.1x はイネーブルになりません。 まだアクティブになっていない EtherChannel のポートで 802.1X をイネーブルにしても、そのポートが EtherChannel に加入することはありません。
- スイッチ ポート アナライザ（SPAN）宛先ポート：SPAN 宛先ポートで 802.1X をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、802.1X はディセーブルに設定されます。 SPAN 送信元ポートでは 802.1x をイネーブルにすることができます。

デバイスで 802.1X をグローバルにディセーブルにするには、各ポートで 802.1X をディセーブルにする必要があります。 このタスクのグローバル コンフィギュレーション コマンドはありません。

Cisco IOS Release 12.4(4)XC の場合

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチ ポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

設定の確認

show dot1x コマンドを入力し、表示の 802.1x Port Summary セクションの Status カラムを確認することにより、設定を確認できます。 enabled ステータスとは、ポート制御値が auto または force-unauthorized に設定されていることです。

例

次の例では、クライアント PC の認証ステータスが認証プロセスによって決定されることを示します。

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
```

```
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、スイッチまたはイーサネット スイッチ ネットワーク モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x re-authentication	802.1Xインターフェイスのクライアントの定期的な再認証をグローバルでイネーブルにします。
dot1x reauthentication（**EtherSwitch**）	802.1Xインターフェイスのクライアントの定期的な再認証をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
dot1x timeout（**EtherSwitch**）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
show dot1x（**EtherSwitch**）	スイッチまたは指定されたインターフェイスのIEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x re-authenticate（特権 EXEC）

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x re-authenticate** コマンドは、**clear authentication session** コマンドに置き換えられています。 詳細については、**clear authentication session** コマンドを参照してください。

指定した 802.1X 対応ポートの再認証を手動で開始するには、特権 EXEC モードで **dot1x re-authenticate** コマンドを使用します。

dot1x re-authenticate [**interface** *interface-name interface-number*]

構文の説明

interface *interface-name interface-number*	（任意）再認証を開始するインターフェイス。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。

使用上のガイドライン

このコマンドを使用すると、再認証試行（re-authperiod）と自動再認証の間に設定された期間（秒）を待機する必要なく、クライアントを再認証できます。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマン

ドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、ポートに接続されているデバイスを手動で再認証する例を示します。

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x reauthentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。

dot1x reauthentication

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x reauthentication** コマンドは、**authentication periodic** コマンドに置き換えられています。 詳細については、**authentication periodic** コマンドを参照してください。

802.1X インターフェイス上でのクライアント PC の定期的な再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x reauthentication** コマンドを使用します。定期的な再認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x reauthentication

no dot1x reauthentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

定期的な再認証は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXI	このコマンドが、**authentication periodic** コマンドに置き換えられました。

使用上のガイドライン

再認証の間隔は、**dot1x timeout** コマンドを使用して設定できます。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、再認証がイネーブルであり、再認証の間隔が1800秒として設定されている例を示します。

```
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
```

例

次に、Cisco 870 ISR を使用したスイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

例

次に、クライアントの定期的な再認証をイネーブルにする例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

関連コマンド

コマンド	説明
dot1x max-req	クライアントPCが802.1Xをサポートしないと結論する前に、ルータがEAP要求/アイデンティティ フレームをクライアントPCに送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x port-control	802.1X ポート制御値を設定します。
dot1x timeout	再試行タイムアウトを設定します。
show dot1x	802.1X 情報を表示します。

dot1x re-authentication（EtherSwitch）

イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x re-authentication** コマンドを使用します。 定期的な再認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x re-authentication

no dot1x re-authentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

定期的な再認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

定期的な再認証試行が行われる時間間隔を設定するには、**dot1x timeout re-authperiod** グローバル コンフィギュレーション コマンドを使用します。

例

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

```
Router(config)# no dot1x re-authentication
```

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

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

関連コマンド

コマンド	説明
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x system-auth-control

802.1X SystemAuthControl（ポートベース認証）をグローバルでイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x system-auth-control** コマンドを使用します。SystemAuthControl をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x system-auth-control

no dot1x system-auth-control

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システム認証はデフォルトでディセーブルです。 このコマンドがディセーブルの場合、すべてのポートが強制的に許可されているように動作します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.2(14)SX	このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、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が定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制

御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセスポイントを利用できます。802.1xは、スイッチまたはLANが提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザデバイスを認証し、そのポートをVLAN（仮想LAN）に割り当てます。802.1xアクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過するExtensible Authentication Protocol（EAP）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はポートを通過できるようになります。

このコマンドの **no** 形式を使用すると、802.1X 関連の設定がすべて削除されます。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ

802.1Xをイネーブルにする前に、認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。

例

次に、SystemAuthControl をイネーブルにする例を示します。

```
Router(config)# dot1x system-auth-control
```

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1X を実行するインターフェイスで使用する 1 つまたは複数の AAA 方式を指定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
debug dot1x	802.1X デバッグ情報を表示します。
description	802.1X プロファイルの説明を指定します。
device	静的に個々のデバイスを許可または拒否します。
dot1x initialize	すべての802.1X対応インターフェイスで802.1Xステート マシンを初期化します。
dot1x max-req	認証プロセスを再開する前に、ルータまたはイーサネット スイッチ ネットワーク モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。

コマンド	説明
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authenticate	指定した 802.1X 対応ポートの再認証を手動で開始します。
dot1x reauthentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
identity profile	アイデンティティプロファイルを作成し、アイデンティティ プロファイル コンフィギュレーション モードを開始します。
show dot1x	アイデンティティプロファイルの詳細および統計情報を表示します。
template	コマンドをクローニングできる仮想テンプレートを指定します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバルコンフィギュレーションモードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。 再試行タイムアウトのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

All Platforms Except the Cisco 7600 Series Switch

dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

Cisco 7600 Series Switch

dot1x timeout {**reauth-period** *seconds*| **quiet-period** *seconds*| **tx-period** *seconds*| **supp-timeout** *seconds*| **server-timeout** *seconds*}

no dot1x timeout {**reauth-period**| **quiet-period**| **tx-period**| **supp-timeout**| **server-timeout**}

構文の説明

auth-period *seconds*	サプリカント（クライアント）がオーセンティケータからの応答（Extensible Authentication Protocol over LAN（EAPOL）-Start 以外のパケット）を何秒待機するとタイムアウトとなるかを設定します。 • 指定できる範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 • 指定できる範囲は 1 ～ 65535 です。デフォルトは 60 です。

quiet-period *seconds*	認証情報の交換に失敗した後、クライアントの再認証を試行する前に、オーセンティケータ（サーバ）が（保留ステートで）待機し続ける時間（秒単位）を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 120 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 0 ～ 65535 です。 デフォルトは 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、スイッチの処理能力を浪費する EAP-START パケットを送信する PC）から送信される EAP-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、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 指定できる範囲は 1 ～ 65535 です。 デフォルトでは、レート制限はディセーブルになっています。

reauth-period {*seconds* | **server**}	自動再認証が開始されるまでの時間（秒単位）を設定します。 • **server** キーワードは、クライアントの再認証時間値を認証、許可、アカウンティング（AAA）サーバから Session-Timeout（RADIUS 属性 27）値として取得する必要があることを示します。**server** キーワードを使用すると、再認証時のアクションもサーバによって決定され、Termination-Action（RADIUS 属性 29）値として送信されます。終了処理は「終了」または「再認証」のいずれかになる場合があります。**server** キーワードを使用しない場合、終了処理は常に「再認証」になります。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルト値は 3600 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 1 ～ 4294967295 です。 デフォルト値は 3600 です。 詳細については、「使用上のガイドライン」の項を参照してください。 （注） Cisco IOS Release 12.2(33) SXI では有効なこのフレーズは、**authentication timer reauthenticate** コマンドに置き換えられています。 詳細については、**authentication timer reauthenticate** コマンドを参照してください。
server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。 サーバが指定された時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。

start-period *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 値は 1 ～ 65535 です。 デフォルトは 30 です。
supp-timeout *seconds*	EAP 要求 ID 以外のすべての EAP メッセージのオーセンティケータからホストへの再送信時間を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。
tx-period *seconds*	クライアントへの EAP 要求 ID パケットの再送信間隔（応答が受信されると仮定）の秒数を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、サプリカントが再試行時間後に応答を送信しない場合、パケットは再度送信されます。

コマンド デフォルト

定期的な再認証および定期的なレート制限は行われません。

コマンド モード

グローバル コンフィギュレーションまたはインターフェイス コンフィギュレーション

Cisco 7600 スイッチ

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(18)SE	**server-timeout**、**supp-timeout**、および **tx-period** キーワードの範囲が変更されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2（17d）SXB に追加されました。
12.3(11)T	**auth-period**、**held-period**、および **start-period** キーワードが追加されました。
12.2(25)SEC	**tx-period** キーワードの範囲が変更され、**reauth-period** および **server-timeout** キーワードが追加されました。
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	**supp-timeout** キーワードおよび **server-timeout** キーワードが追加されました。このコマンドのコンフィギュレーションモードが、インターフェイス コンフィギュレーション モードに変更されました。
12.4(6)T	**supp-timeout** キーワードが追加され、このコマンドは、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXI	**reauth-period** キーワードは、**authentication timer reauthenticate** コマンドに置き換えられました。

使用上のガイドライン

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

Cisco 7600 スイッチ

dot1x timeout reauth-period コマンドを入力する前に、定期的な再認証をイネーブルにしておく必要があります。 定期的な再認証をイネーブルにするには、**dot1x reauthentication** コマンドを入力します。 定期的な再認証がイネーブルに設定されている場合にだけ、**dot1x timeout reauth-period** コマンドはシステムの動作を有効にします。

例

次に、さまざまな 802.1X 再送信時間およびタイムアウト時間が設定されている例を示します。

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

次に、デフォルトの再認証時間に戻す例を示します。

```
Switch(config-if)# no dot1x timeout reauth-period
```

例

次に、Cisco 7600 スイッチの 802.1X 再送信時間およびタイムアウト時間を設定する例を示します。

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、スイッチまたはイーサネット スイッチ モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x port-control	802.1X ポート制御値を設定します。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
show dot1x	802.1X 情報を表示します。

dot1x timeout（EtherSwitch）

イーサネット スイッチ ネットワーク モジュールがルータに搭載されている場合に、802.1X 認証情報交換の間の再試行秒数を設定するには、グローバル コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

構文の説明

quiet-period *seconds*	イーサネット スイッチ ネットワーク モジュールがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を指定します。範囲は 0 ～ 65535 秒です。 デフォルトは 60 秒です。
re-authperiod *seconds*	再認証の間隔（秒）を指定します。指定できる範囲は 1 ～ 4294967295 です。 デフォルトは 3660 秒です。
tx-period *seconds*	要求を再送信するまでに、スイッチがクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する時間（秒単位）。範囲は 1 ～ 65535 秒です。 デフォルトは 30 秒です。

コマンド デフォルト

quiet-period：60 秒 **re-authperiod**：3660 秒 **tx-period**：30 秒

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。

リリース	変更内容
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

quiet-period キーワード

待機時間中は、イーサネット スイッチ ネットワーク モジュールは認証要求を受け入れまたは開始しなくなります。 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。

re-authperiod キーワード

re-authperiod キーワードは、**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしている場合にのみ、イーサネット スイッチ ネットワーク モジュールの動作に影響します。

例

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Router(config)# dot1x timeout quiet-period 30
```

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

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

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

```
Router(config)# dot1x timeout tx-period 60
```

関連コマンド

コマンド	説明
dot1x max-req	デバイスが、認証プロセスを再始動する前に、EAP 要求/アイデンティティ フレームを送信する最大回数を設定します。
dot1x re-authentication（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにします。

コマンド	説明
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。