



# セキュリティ

---

- [aaa accounting dot1x \(3 ページ\)](#)
- [aaa accounting identity \(5 ページ\)](#)
- [aaa authentication dot1x \(7 ページ\)](#)
- [aaa authorization network \(8 ページ\)](#)
- [aaa new-model \(9 ページ\)](#)
- [authentication host-mode \(11 ページ\)](#)
- [authentication logging verbose \(13 ページ\)](#)
- [authentication mac-move permit \(14 ページ\)](#)
- [authentication priority \(15 ページ\)](#)
- [authentication violation \(18 ページ\)](#)
- [auto security \(20 ページ\)](#)
- [auto security-port \(21 ページ\)](#)
- [cisp enable \(22 ページ\)](#)
- [clear errdisable interface vlan \(24 ページ\)](#)
- [clear mac address-table \(26 ページ\)](#)
- [debug ip rip \(28 ページ\)](#)
- [deny \(MAC アクセス リスト コンフィギュレーション\) \(30 ページ\)](#)
- [dot1x critical \(グローバル コンフィギュレーション\) \(34 ページ\)](#)
- [dot1x logging verbose \(35 ページ\)](#)
- [dot1x pae \(36 ページ\)](#)
- [dot1x supplicant force-multicast \(37 ページ\)](#)
- [dot1x test eapol-capable \(38 ページ\)](#)
- [dot1x test timeout \(39 ページ\)](#)
- [dot1x timeout \(40 ページ\)](#)
- [epm access-control open \(43 ページ\)](#)
- [ip access-group \(44 ページ\)](#)
- [ip admission \(46 ページ\)](#)
- [ip admission name \(47 ページ\)](#)
- [ip device tracking maximum \(50 ページ\)](#)

- ip device tracking probe (51 ページ)
- ip dhcp snooping database (52 ページ)
- ip dhcp snooping information option format remote-id (54 ページ)
- ip dhcp snooping verify no-relay-agent-address (55 ページ)
- ip source binding (56 ページ)
- ip ssh source-interface (58 ページ)
- ip verify source (59 ページ)
- ipv6 snooping policy (60 ページ)
- limit address-count (62 ページ)
- mab request format attribute 32 (63 ページ)
- match (アクセス マップ コンフィギュレーション) (65 ページ)
- mab logging verbose (67 ページ)
- permit (MAC アクセス リスト コンフィギュレーション) (68 ページ)
- radius server (72 ページ)
- router rip (74 ページ)
- show aaa clients (75 ページ)
- show aaa command handler (76 ページ)
- **show aaa local** (77 ページ)
- show aaa servers (78 ページ)
- show aaa sessions (79 ページ)
- show authentication sessions (80 ページ)
- show auto security (83 ページ)
- show cisp (85 ページ)
- show dot1x (87 ページ)
- show eap pac peer (89 ページ)
- show ip dhcp snooping statistics (90 ページ)
- show ip rip database (93 ページ)
- show ip ssh (95 ページ)
- show radius server-group (97 ページ)
- show vlan group (99 ページ)
- switchport port-security aging (100 ページ)
- switchport port-security mac-address (102 ページ)
- switchport port-security maximum (105 ページ)
- switchport port-security violation (107 ページ)
- trusted-port (109 ページ)
- username name masked-secret (110 ページ)
- vlan group (111 ページ)

## aaa accounting dot1x

認証、認可、およびアカウントティング (AAA) アカウントティングをイネーブルにして、IEEE 802.1Xセッションの特定のアカウントティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** 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。IEEE 802.1X アカウントティング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。

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius |
tacacs+} [group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+}
[group {name | radius | tacacs+}... ]}
no aaa accounting dot1x {name | default}
```

### 構文の説明

<b>name</b>	サーバグループ名。これは、 <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合に使用するオプションです。
<b>default</b>	デフォルトリストにあるアカウントティング方式を、アカウントティングサービス用に指定します。
<b>start-stop</b>	プロセスの開始時に <b>start accounting</b> 通知を送信し、プロセスの終了時に <b>stop accounting</b> 通知を送信します。start アカウントティングレコードはバックグラウンドで送信されます。アカウントティングサーバが <b>start accounting</b> 通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
<b>broadcast</b>	複数の AAA サーバに送信されるアカウントティングレコードをイネーブルにして、アカウントティングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
<b>group</b>	アカウントティングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>name</b> : サーバグループの名前。</li> <li>• <b>radius</b> : すべての RADIUS ホストのリスト。</li> <li>• <b>tacacs+</b> : すべての TACACS+ ホストのリスト。</li> </ul> <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合、 <b>group</b> キーワードはオプションです。オプションの <b>group</b> キーワードより多くの値を入力できます。
<b>radius</b>	(任意) RADIUS アカウントティングをイネーブルにします。
<b>tacacs+</b>	(任意) TACACS+ アカウントティングをイネーブルにします。

### コマンドデフォルト

AAA アカウントティング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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

---

**使用上のガイドライン**      このコマンドは、RADIUS サーバへのアクセスが必要です。  
 インターフェイスに IEEE 802.1X RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

次の例では、IEEE 802.1X アカウンティングを設定する方法を示します。

```
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
```

## aaa accounting identity

IEEE 802.1X、MAC 認証バイパス (MAB)、および Web 認証セッションの認証、認可、およびアカウントिंग (AAA) アカウントिंग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、**aaa accounting identity** コマンドを使用します。IEEE 802.1X アカウントिंग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。

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ]}
no aaa accounting identity {name | default}
```

### 構文の説明

<b>name</b>	サーバグループ名。これは、 <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合に使用するオプションです。
<b>default</b>	デフォルトリストにあるアカウントिंग方式を、アカウントिंगサービス用に使用します。
<b>start-stop</b>	プロセスの開始時に <b>start accounting</b> 通知を送信し、プロセスの終了時に <b>stop accounting</b> 通知を送信します。 <b>start</b> アカウントングレコードはバックグラウンドで送信されます。アカウントングサーバが <b>start</b> アカウントング通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
<b>broadcast</b>	複数の AAA サーバに送信されるアカウントングレコードをイネーブルにして、アカウントングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
<b>group</b>	アカウントングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>name</b> : サーバグループの名前。</li> <li>• <b>radius</b> : すべての RADIUS ホストのリスト。</li> <li>• <b>tacacs+</b> : すべての TACACS+ ホストのリスト。</li> </ul> <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合、 <b>group</b> キーワードはオプションです。オプションの <b>group</b> キーワードより多くの値を入力できます。
<b>radius</b>	(任意) RADIUS 認証をイネーブルにします。
<b>tacacs+</b>	(任意) TACACS+ アカウントングをイネーブルにします。

コマンドデフォルト AAA アカウントング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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** AAA アカウンティングアイデンティティをイネーブルにするには、ポリシーモードをイネーブルにする必要があります。ポリシーモードを有効にするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

次の例では、IEEE 802.1X アカウンティングアイデンティティを設定する方法を示します。

```
Device# authentication display new-style
```

```
Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.
```

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```

## aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで使用する認証、認可、およびアカウントリング (AAA) 方式を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上のグローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

### 構文の説明

<b>default</b>	ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。
<b>method1</b>	サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、 <b>group radius</b> キーワードを入力します。  (注) コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは <b>default</b> および <b>group radius</b> キーワードのみです。

### コマンド デフォルト

認証は実行されません。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

**method** 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。IEEE 802.1X に準拠している唯一の方式は、クライアントデータが RADIUS 認証サーバに対して確認される **group radius** 方式です。

**group radius** を指定した場合、**radius-server host** グローバル コンフィギュレーション コマンドを入力して RADIUS サーバを設定する必要があります。

設定された認証方式の一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

次の例では AAA をイネーブルにして IEEE 802.1X 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

## aaa authorization network

IEEE 802.1x VLAN 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、グローバルコンフィギュレーションモードで **aaa authorization network** コマンドを使用します。RADIUS ユーザ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。

**aaa authorization network default group radius**  
**no aaa authorization network default**

### 構文の説明

**default group radius** デフォルトの認証リストとして、サーバグループ内のすべての RADIUS ホストのリストを使用します。

### コマンド デフォルト

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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** 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。認証パラメータは、VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

```
Device(config)# aaa authorization network default group radius
```



## aaa new-model

認証、認可、およびアカウントिंग（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーションモードで **aaa new-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

**aaa new-model**  
**no aaa new-model**

### 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

AAA が有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドにより、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合、**aaa new-model** コマンドを削除するときは、スイッチをリロードしてデフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。



(注) **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

```
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
 login local !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

### 例

次に、AAA を初期化する例を示します。

```
Device(config)# aaa new-model
```

Device (config) #

## 関連コマンド

Command	Description
<b>aaa accounting</b>	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
<b>aaa authentication arap</b>	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
<b>aaa authentication enable default</b>	ユーザが特権コマンドレベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
<b>aaa authentication login</b>	ログイン時の AAA 認証を設定します。
<b>aaa authentication ppp</b>	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
<b>aaa authorization</b>	ネットワークへのユーザアクセスを制限するパラメータを設定します。

## authentication host-mode

ポートで認証マネージャモードを設定するには、インターフェイス コンフィギュレーション モードで **authentication host-mode** 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。

**authentication host-mode** {multi-auth | multi-domain | multi-host | single-host}  
**no authentication host-mode**

構文の説明	multi-auth	multi-domain	multi-host	single-host
	ポートのマルチ認証モード (multi-auth モード) をイネーブルにします。	ポートのマルチドメインモードをイネーブルにします。	ポートのマルチホストモードをイネーブルにします。	ポートのシングルホストモードをイネーブルにします。

**コマンド デフォルト** シングルホストモードがイネーブルにされています。

**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

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** 接続されているデータホストが1つだけの場合は、シングルホストモードを設定する必要があります。シングルホストポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データホストが IP フォン経由でポートに接続されている場合は、マルチドメインモードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメインモードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポートアクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは1つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホストモードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-auth
```

次の例では、ポートのマルチドメインモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-domain
```

次の例では、ポートのマルチホストモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-host
```

次の例では、ポートのシングルホストモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode single-host
```

設定を確認するには、**show authentication sessions interface *interface* details** 特権 EXEC コマンドを入力します。

# authentication logging verbose

認証システムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **authentication logging verbose** コマンドをグローバルコンフィギュレーション モードで使用します。

**authentication logging verbose**  
**no authentication logging verbose**

## 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

システムメッセージの詳細ログは有効になっていません。

## コマンド モード

グローバル コンフィギュレーション (config)

## コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドにより、認証システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システムメッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# authentication logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

## 関連コマンド

コマンド	説明
<b>authentication logging verbose</b>	認証システムメッセージから詳細情報をフィルタリングします。
<b>dot1x logging verbose</b>	802.1X システムメッセージから詳細情報をフィルタリングします。
<b>mab logging verbose</b>	MAC 認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

## authentication mac-move permit

デバイス上でのMAC移動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 **authentication mac-move permit** コマンドを使用します。MAC 移動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。

**authentication mac-move permit**  
**no authentication mac-move permit**

### 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

MAC 移動は無効になっています。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドを使用すると、デバイスの 802.1x 対応ポート間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

MAC 移動は、ポートセキュリティ対応の 802.1x ポートではサポートされません。MAC 移動がスイッチ上でグローバルに設定され、ポートセキュリティ対応ホストが 802.1x 対応ポートに移動した場合、違反エラーが発生します。

次の例では、デバイス上で MAC 移動をイネーブルにする方法を示します。

```
Device(config)# authentication mac-move permit
```

## authentication priority

プライオリティリストに認証方式を追加するには、インターフェイスコンフィギュレーションモードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

構文の説明	dot1x	(任意) 認証方式の順序に 802.1X を追加します。
	mab	(任意) 認証方式の順序に MAC 認証バイパス (MAB) を追加します。
	webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト      デフォルトのプライオリティは、802.1X 認証、MAC 認証バイパス、Web 認証の順です。

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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

使用上のガイドライン      順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証 (webauth) を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。



- (注) クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1X 認証、MAC 認証バイパス (MAB)、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

次の例では、802.1X を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority dotx webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority mab webauth
```

## 関連コマンド

コマンド	説明
<b>authentication control-direction</b>	ポート モードを単一方向または双方向に設定します。
<b>authentication event fail</b>	認証マネージャが認証エラーを認識されないユーザクレデンシャルの結果として処理する方法を指定します。
<b>authentication event no-response action</b>	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
<b>authentication event server alive action reinitialize</b>	以前に到達不能であった認証、許可、アカウントिंगサーバが使用可能になったときに認証マネージャセッションを再初期化します。
<b>authentication event server dead action authorize</b>	認証、許可、アカウントिंगサーバが到達不能になったときに認証マネージャセッションを許可します。
<b>authentication fallback</b>	Web 認証のフォールバック方式をイネーブルにします。
<b>authentication host-mode</b>	ホストの制御ポートへのアクセスを許可します。
<b>authentication open</b>	ポートでオープンアクセスをイネーブルにします。
<b>authentication order</b>	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
<b>authentication periodic</b>	ポートの自動再認証をイネーブルにします。
<b>authentication port-control</b>	制御ポートの許可ステートを設定します。
<b>authentication timer inactivity</b>	機能しない認証マネージャセッションを強制終了するまでの時間を設定します。



コマンド	説明
<b>authentication timer reauthenticate</b>	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
<b>authentication timer restart</b>	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
<b>authentication violation</b>	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
<b>mab</b>	ポートのMAC認証バイパスをイネーブルにします。
<b>show authentication registrations</b>	認証マネージャに登録されている認証方式に関する情報を表示します。
<b>show authentication sessions interface details</b>	指定されたインターフェイスの Authentication Manager に関する詳細情報を表示します。
<b>show authentication sessions</b>	現在の認証マネージャセッションに関する情報を表示します。
<b>show authentication sessions interface</b>	特定のインターフェイスの認証マネージャに関する情報を表示します。

## authentication violation

新しいデバイスがポートに接続されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーションモードで **authentication violation** コマンドを使用します。

**authentication violation** { **protect** | **replace** | **restrict** | **shutdown** }

**no authentication violation** { **protect** | **replace** | **restrict** | **shutdown** }

構文の説明	protect	replace	restrict	shutdown
	予期しない着信 MAC アドレスをドロップします。syslog エラーは生成されません。	現在のセッションを削除し、新しいホストによる認証を開始します。	違反エラーの発生時に Syslog エラーを生成します。	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

コマンド デフォルト Authentication violation shutdown モードがイネーブルにされています。

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

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

使用上のガイドライン ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システムエラーメッセージを生成して、ポートを制限モードに変更するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation replace
```

## auto security

グローバルな自動セキュリティを設定するには、グローバル コンフィギュレーション モードで **auto security** コマンドを使用します。自動セキュリティ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。

**auto security**  
**no auto security**

このコマンドには、引数およびキーワードはありません。

コマンド デフォルト 自動セキュリティがグローバルに有効化されました。

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
	Cisco IOS Release 15.2(7)E1	このコマンドは、Cisco IOS Release 15.2(5)E よりも前のリリースで導入されました。

使用上のガイドライン グローバル コンフィギュレーション モードで自動セキュリティを設定すると、すべてのインターフェイスで自動セキュリティが有効になります。自動セキュリティを無効にすると、すべてのインターフェイスで無効になります。

特定のインターフェイスで自動セキュリティを有効にするには、インターフェイス コンフィギュレーション モードで **auto security-port** コマンドを使用します。



- (注) Cisco IOS リリース 15.2(5)E では、グローバル コンフィギュレーション モードで **auto security** コマンドが設定されると、インターフェイス上で自動セキュリティが有効になります。ただし、**auto security-port {host | uplink}** コマンドはインターフェイスの設定には明示的に保存されません。自動セキュリティがあるインターフェイス上で設定され、**auto security-port {host | uplink}** コマンドがインターフェイスから削除されると、**no auto security-port {host | uplink}** コマンドはインターフェイスの設定に保存されます。

次に、自動セキュリティをグローバルで有効にする例を示します。

```
Device(config)# auto security
```

### 関連コマンド

コマンド	説明
<b>auto security-port</b>	インターフェイス上で自動セキュリティを設定します。
<b>show auto security</b>	自動セキュリティ ステータスを表示します。

## auto security-port

インターフェイスで自動セキュリティを設定するには、インターフェイスコンフィギュレーションモードで **auto security-port** コマンドを使用します。インターフェイスで自動セキュリティを無効にするには、このコマンドの **no** 形式を使用します。

```
auto security {host | uplink}
no auto security
```

### 構文の説明

**host** ホストポートの自動セキュリティを設定します。

**uplink** アップリンクポートの自動セキュリティを設定します。

### コマンドデフォルト

自動セキュリティはすべてのインターフェイス上で無効です。

### 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

グローバルコンフィギュレーションモードで **auto security** コマンドを使用して、自動セキュリティをグローバルに有効にできます。



- (注) Cisco IOS リリース 15.2(5)E では、グローバルコンフィギュレーションモードで **auto security** コマンドが設定されると、インターフェイス上で自動セキュリティが有効になります。ただし、**auto security-port {host | uplink}** コマンドはインターフェイスの設定には明示的に保存されません。自動セキュリティがあるインターフェイス上で設定され、**auto security-port {host | uplink}** コマンドがインターフェイスから削除されると、**no auto security-port {host | uplink}** コマンドはインターフェイスの設定に保存されます。

次に、インターフェイスで自動セキュリティを設定する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# auto security-port host
```

### 関連コマンド

コマンド	説明
<b>auto security</b>	グローバルな自動セキュリティを設定します。
<b>show auto security</b>	自動セキュリティステータスを表示します。

## cisp enable

スイッチ上で Client Information Signalling Protocol (CISP) を有効にして、サブリカントスイッチのオーセンティケータとして機能し、オーセンティケータスイッチのサブリカントとして機能するようにするには、**cisp enable** 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。

**cisp enable**  
**no cisp enable**

### 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

デフォルトの動作や値はありません。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

オーセンティケータとサブリカントスイッチの間のリンクはトランクです。両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバーである必要があります。

VTP モードを設定する場合に MD5 チェックサムの一一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバーが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

次の例では、CISP をイネーブルにする方法を示します。

```
Device(config)# cisp enable
```

### 関連コマンド

コマンド	説明
<b>dot1x credentials</b> プロファイル	プロファイルをサブリカントスイッチに設定します。
<b>dot1x supplicant force-multicast</b>	802.1X サブリカントがマルチキャストパケットを送信するように強制します。

コマンド	説明
<b>dot1x supplicant controlled transient</b>	802.1X サプリカントによる制御アクセスを設定します。
<b>show cisp</b>	指定されたインターフェイスのCISP情報を表示します。

## clear errdisable interface vlan

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]

構文の説明	<i>interface-id</i>	インターフェイスを指定します。
	<i>vlan list</i>	(任意) 再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** **shutdown** および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable** インターフェイスコマンドを使用して VLAN の error-disabled をクリアできます。

次の例では、ギガビットイーサネットポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド	コマンド	説明
	<b>errdisable detect cause</b>	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
	<b>errdisable recovery</b>	回復メカニズム変数を設定します。
	<b>show errdisable detect</b>	errdisable 検出ステータスを表示します。
	<b>show errdisable recovery</b>	errdisable 回復タイマーの情報を表示します。



コマンド	説明
<b>show interfaces status err-disabled</b>	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

## clear mac address-table

特定のダイナミックアドレス、特定のインターフェイス上のすべてのダイナミックアドレス、スタックメンバ上のすべてのダイナミックアドレス、または特定の VLAN 上のすべてのダイナミックアドレスを MAC アドレステーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。このコマンドはまた MAC アドレス通知グローバルカウンタもクリアします。

**clear mac address-table** { **dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification** }

### 構文の説明

<b>dynamic</b>	すべてのダイナミック MAC アドレスを削除します。
<b>address</b> <i>mac-addr</i>	(任意) 指定されたダイナミック MAC アドレスを削除します。
<b>interface</b> <i>interface-id</i>	(任意) 指定された物理ポートまたはポートチャネル上のすべてのダイナミック MAC アドレスを削除します。
<b>vlan</b> <i>vlan-id</i>	(任意) 指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ~ 4094 です。
<b>move update</b>	MAC アドレステーブルの move-update カウンタをクリアします。
<b>notification</b>	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード 特権 EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

情報が削除されたことを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

## 関連コマンド

コマンド	説明
<b>mac address-table notification</b>	MAC アドレス通知機能をイネーブルにします。
<b>mac address-table move update {receive   transmit}</b>	スイッチ上の MAC アドレス テーブル移行更新を設定します。
<b>show mac address-table</b>	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
<b>show mac address-table move update</b>	スイッチに MAC アドレス テーブル移行更新情報を表示します。
<b>show mac address-table notification</b>	<b>interface</b> キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
<b>snmp trap mac-notification change</b>	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

# debug ip rip

Routing Information Protocol (RIP) ルーティング トランザクションに関する情報を表示するには、特権 EXEC モードで **debug ip rip** コマンドを使用します。デバッグ出力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。

```
debug ip rip [{database | events | trigger}]
no debug ip rip [{database | events | trigger}]
```

## 構文の説明

<b>database</b>	(任意) RIP データベースイベントに関する情報を表示します。
<b>events</b>	(任意) RIP プロトコルベースイベントに関する情報を表示します。
<b>trigger</b>	(任意) RIP トリガー拡張機能に関する情報を表示します。

## コマンドモード

特権 EXEC (#)

## コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

## 例

次の例では、デバッグ対象のルータが送信元アドレス 10.89.80.28 のルータから更新を受信しました。このシナリオでは、ルーティングテーブルの更新で約 5 つの宛先に情報が送信されています。更新の 4 番目の宛先アドレスである 172.31.0.0 は、更新が送信されたルータから 15 ホップ以上離れているためアクセスできません。デバッグ対象のルータは、どちらの場合も宛先としてブロードキャストアドレス 255.255.255.255 に更新を送信します。

```
Device# debug ip rip

RIP: received update from 10.89.80.28 on GigabitEthernet0/0/0
  10.89.95.0 in 1 hops
  10.89.81.0 in 1 hops
  10.89.66.0 in 2 hops
  172.31.0.0 in 16 hops (inaccessible)
  0.0.0.0 in 7 hop
RIP: sending update to 255.255.255.255 via GigabitEthernet0/0/0 (10.89.64.31)
  subnet 10.89.94.0, metric 1
  172.31.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Serial1 (10.89.94.31)
  subnet 10.89.64.0, metric 1
  subnet 10.89.66.0, metric 3
  172.31.0.0 in 16 hops (inaccessible)
  default 0.0.0.0, metric 8
```

2 行目は、ルーティングテーブルの更新の例です。特定のインターネットアドレスとデバイス間のホップ数が示されています。

エントリは、デバイスが同様の更新を送信していることを示しています。ただし、カッコ内の数字は IP ヘッダーにカプセル化された送信元アドレスです。

次の例は、起動時、インターフェイス移行イベント中、またはユーザが手動でルーティングテーブルをクリアしたときに表示されるエントリの **debug ip rip** コマンドを示しています。

```
RIP: broadcasting general request on GigabitEthernet0/0/0  
RIP: broadcasting general request on GigabitEthernet1/0/0
```

次のエントリは、送信者からの不正なパケットが原因である可能性が高いです。

```
RIP: bad version 128 from 160.89.80.43
```

#### 関連コマンド

コマンド	説明
<b>show ip rip database</b>	サマリーアドレスに基づいて集約されている関連ルートがある場合に、RIP ルーティング データベース エントリのサマリーアドレスエントリを表示します。

## deny (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックが転送されるのを防止するには、スイッチスタックまたはスタンドアロンスイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。名前付き MAC アクセスリストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [cos cos]
no deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [cos cos]
```

### 構文の説明

<b>any</b>	すべての送信元または宛先 MAC アドレスを拒否します。
<b>host src-MAC-addr   src-MAC-addr mask</b>	ホスト MAC アドレスと任意のサブネットマスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
<b>host dst-MAC-addr   dst-MAC-addr mask</b>	宛先 MAC アドレスと任意のサブネットマスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
<i>type mask</i>	(任意) パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。  type には、0 ~ 65535 の 16 進数を指定できます。  mask は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。
<b>aarp</b>	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。

<b>amber</b>	(任意) EtherType DEC-Amber を指定します。
<b>appletalk</b>	(任意) EtherType AppleTalk/EtherTalk を指定します。
<b>dec-spanning</b>	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
<b>decnet-iv</b>	(任意) EtherType DECnet Phase IV プロトコルを指定します。
<b>diagnostic</b>	(任意) EtherType DEC-Diagnostic を指定します。
<b>dsm</b>	(任意) EtherType DEC-DSM を指定します。
<b>etype-6000</b>	(任意) EtherType 0x6000 を指定します。
<b>etype-8042</b>	(任意) EtherType 0x8042 を指定します。
<b>lat</b>	(任意) EtherType DEC-LAT を指定します。
<b>lavc-sca</b>	(任意) EtherType DEC-LAVC-SCA を指定します。
<b>lsap</b> <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。  <i>mask</i> は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
<b>mop-console</b>	(任意) EtherType DEC-MOP Remote Console を指定します。
<b>mop-dump</b>	(任意) EtherType DEC-MOP Dump を指定します。
<b>msdos</b>	(任意) EtherType DEC-MSDOS を指定します。
<b>mumps</b>	(任意) EtherType DEC-MUMPS を指定します。
<b>netbios</b>	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
<b>vines-echo</b>	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。

<b>vines-ip</b>	(任意) EtherType VINES IP を指定します。
<b>xns-idp</b>	(任意) 10 進数、16 進数、または 8 進数の任意の EtherType である EtherType Xerox Network Systems (XNS) プロトコルスイート (0 ~ 65535) を指定します。
<b>cos cos</b>	(任意) プライオリティを設定するため、0 ~ 7 までのサービスクラス (CoS) 値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。 <b>cos</b> オプションが設定されているかどうかを確認する警告メッセージが表示されます。

**コマンド デフォルト** このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

**コマンド モード** MAC アクセス リスト 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** **mac access-list extended** 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、MAC アクセス リスト コンフィギュレーション モードを開始します。

**host** キーワードを使用した場合、アドレスマスクは入力できません。**host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、**type mask** または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

表 1: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137



IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
Device(config-ext-macl)# deny any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

#### 関連コマンド

コマンド	説明
<b>mac access-list extended</b>	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
<b>permit</b>	MAC アクセスリスト コンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
<b>show access-lists</b>	スイッチに設定されたアクセス コントロール リストを表示します。

## 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

#### 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 成功メッセージを送信するように指定します。

#### コマンド デフォルト

**eapol** 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、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 成功メッセージを送信するよう指定する例を示します。

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

## dot1x logging verbose

802.1xシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **dot1x logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

**dot1x logging verbose**  
**no dot1x logging verbose**

### 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

システムメッセージの詳細ログは有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドにより、802.1Xシステムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# dot1x logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

### 関連コマンド

コマンド	説明
<b>authentication logging verbose</b>	認証システムメッセージから詳細情報をフィルタリングします。
<b>dot1x logging verbose</b>	802.1Xシステムメッセージから詳細情報をフィルタリングします。
<b>mab logging verbose</b>	MAC認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

## dot1x pae

Port Access Entity (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、コマンドの **no** 形式を入力します。

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

### 構文の説明

**supplicant** インターフェイスはサブ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** インターフェイスはオーセンティケータとしてだけ動作し、サブリカント向けのメッセージに応答しません。

### コマンド デフォルト

PAE タイプは設定されていません。

### 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

IEEE 802.1X 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

**dot1x port-control** インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

次に、インターフェイスがサブ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。

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x pae supplicant
```

## dot1x supplicant force-multicast

サブリカントスイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN (EAPOL) パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバルコンフィギュレーションモードで **dot1x supplicant force-multicast** 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 supplicant force-multicast**  
**no dot1x supplicant force-multicast**

### 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

サブリカントスイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

Network Edge Access Topology (NEAT) がすべてのホストモードで機能するようにするには、サブリカントスイッチ上でこのコマンドをイネーブルにします。

次の例では、サブリカントスイッチがオーセンティケータスイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Device(config)# dot1x supplicant force-multicast
```

### 関連コマンド

コマンド	説明
<b>cisp enable</b>	スイッチの Client Information Signalling Protocol (CISP) をイネーブルにすることで、スイッチがサブリカントスイッチに対するオーセンティケータとして動作するようにします。
<b>dot1x credentials</b>	ポートに 802.1x サブリカント資格情報を設定します。
<b>dot1x pae supplicant</b>	インターフェイスがサブリカントとしてだけ機能するように設定します。

## dot1x test eapol-capable

すべてのスイッチポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、スイッチスタックまたはスタンドアロンスイッチ上で特権 EXEC モードで **dot1x test eapol-capable** コマンドを使用します。

**dot1x test eapol-capable** [**interface** *interface-id*]

構文の説明	<b>interface</b> <i>interface-id</i>	(任意) クエリー対象のポートです。
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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1X 機能をテストするには、この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。

次の例では、スイッチ上で IEEE 802.1X の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1X 対応であることを示します。

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

関連コマンド	コマンド	説明
	<b>dot1x test timeout</b> <i>timeout</i>	IEEE 802.1X 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

## dot1x test timeout

IEEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチスタックまたはスタンドアロンスイッチ上でグローバルコンフィギュレーションモードで **dot1x test timeout** コマンドを使用します。

### dot1x test timeout *timeout*

構文の説明	<i>timeout</i>	EAPOL 応答を待機する時間 (秒)。指定できる範囲は 1 ~ 65535 秒です。
-------	----------------	---

コマンド デフォルト      デフォルト設定は 10 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

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

使用上のガイドライン      EAPOL 応答を待機するために使用されるタイムアウトを設定するには、この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。

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Device# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	<b>dot1x test eapol-capable</b> [ interface <i>interface-id</i> ]	すべての、または指定された IEEE 802.1X 対応ポートに接続するデバイスで IEEE 802.1X の準備が整っているかを確認します。

## 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を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。

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

### 構文の説明

<b>auth-period</b> <i>seconds</i>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブ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。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。</p>
<b>held-period</b> <i>seconds</i>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブ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。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
<b>quiet-period</b> <i>seconds</i>	<p>認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
<b>ratelimit-period</b> <i>seconds</i>	<p>動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>有効な範囲は 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。</li> </ul>
<b>server-timeout</b> <i>seconds</i>	<p>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。</p> <ul style="list-style-type: none"> <li>有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。</li> </ul> <p>サーバが指定時間内に 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。</p>



<b>start-period</b> <i>seconds</i>	<p>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。</p> <p>有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。</p> <p>Cisco IOS リリース 15.2(5)E では、サブリカントモードでのみこのコマンドを使用できます。その他のモードでこのコマンドを適用すると、設定からそのコマンドが失われます。</p>
<b>supp-timeout</b> <i>seconds</i>	<p>EAP 要求 ID 以外のすべての EAP メッセージについて、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。</p> <p>有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。</p>
<b>tx-period</b> <i>seconds</i>	<p>クライアントに EAP 要求 ID パケットを再送信する間隔を (応答が受信されないものと仮定して) 秒数で設定します。</p> <ul style="list-style-type: none"> <li>有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。</li> <li>802.1X パケットがサブリカントに送信され、そのサブリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。</li> </ul>

**コマンド デフォルト** 定期的な再認証と定期的なレート制限が行われます。

**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

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**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。

**dot1x reauthentication** 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定期的な再認証をイネーブルにただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザーへの応答時間を短縮できます。

**ratelimit-period** が 0 (デフォルト) に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバーに転送します。

次に、さまざまな 802.1X 再送信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。

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```

## epm access-control open

アクセスコントロールリスト（ACL）が設定されていないポートにオープンディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを使用します。オープンディレクティブ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。

**epm access-control open**  
**no epm access-control open**

**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** デフォルトのディレクティブが適用されます。

**コマンド モード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** スタティック ACL が設定されたアクセスポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープン両方のディレクティブがポートへのアクセスを許可します。

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

次の例では、オープンディレクティブを設定する方法を示します。

```
Device(config)# epm access-control open
```

### 関連コマンド

コマンド	説明
<b>show running-config</b>	現在実行されているコンフィギュレーション ファイルの内容を表示します

## ip access-group

IP アクセスグループを適用するには、インターフェイス コンフィギュレーション モードで **ip access-group** コマンドを使用します。IP アクセスグループを削除するには、このコマンドの **no** 形式を使用します。

**ip access-group** { *access-list-name* | *standard-access-list* | *expanded-access-list* } **in**

**no ip access-group** { *access-list-name* | *standard-access-list* | *expanded-access-list* } **in**

### 構文の説明

*access-list-name* 既存の IP アクセスリスト名。

*standard-access-list* 標準アクセスリスト番号。

- 標準または拡張 IP アクセスリストの有効値は、1～199 です。

*expanded-access-list* 拡張アクセスリスト番号。

- 標準または拡張 IP アクセスリストの有効値は、1300～2699 です。

**in** インバウンドパケットをフィルタリングします。

### コマンド デフォルト

アクセスグループは適用されません。

### 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 (config-if)

### コマンド履歴

リリース	変更内容
Cisco IOS リリース 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

指定したアクセスリストが使用できない場合、すべてのパケットが渡されます（警告メッセージは発行されません）。

#### インターフェイスへのアクセスリストの適用

標準の受信アクセスリストの場合、インターフェイスがパケットを受信すると、Cisco IOS ソフトウェアがこのアクセスリストに照らし合わせてパケットの送信元アドレスをチェックします。拡張アクセスリストの場合、ネットワークデバイスが宛先アクセスリストもチェックします。アクセスリストがアドレスを許可している場合は、パケットの処理を継続します。アクセスリストでアドレスが拒否されている場合、ソフトウェアはパケットを廃棄し、Internet Control Management Protocol (ICMP) ホスト到達不能メッセージを返します。

### 例

次に、ギガビットイーサネット インターフェイス 1/0/1 から受信するパケットにリスト 101 を適用する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# end
```

## ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、フォールバック プロファイル コンフィギュレーション モードでも使用できます。Web 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。

**ip admission rule**  
**no ip admission rule**

### 構文の説明

*rule* IP アドミッション ルール の名前。

### コマンド デフォルト

Web 認証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  
 フォールバック プロファイル 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

**ip admission** コマンドはスイッチポートに web 認証ルールを適用します。

次の例では、スイッチポートに Web 認証ルールを適用する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

次の例では、IEEE 802.1X 対応のスイッチポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

## ip admission name

Web 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 **ip admission name** コマンドを使用します。Web 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。

```
ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
no ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
```

### 構文の説明

<b>name</b>	ネットワークアドミッション制御ルールの名前。
<b>consent</b>	認証プロキシ同意 Web ページを <i>admission-name</i> 引数で指定された IP アドミッションルールに対応させます。
<b>proxy http</b>	Web 認証のカスタムページを設定します。
<b>absolute-timer</b> 分	(任意) 外部サーバがタイムアウトするまでの経過時間 (分)。
<b>inactivity-time</b> 分	(任意) 外部ファイルサーバが到達不能であると見なされるまでの経過時間 (分)。
<b>list</b>	(任意) 指定されたルールをアクセス コントロールリスト (ACL) に関連付けます。
<i>acl</i>	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1~199、または拡張範囲で 1300 から 2699 です。
<i>acl-name</i>	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
<b>service-policy type tag</b>	(任意) コントロールプレーン サービス ポリシーを設定できます。
<i>service-policy-name</i>	<b>policy-map type control tag</b> <i>policyname</i> コマンド、キーワード、および引数を使用して設定されたコントロールプレーンタグのサービスポリシー。このポリシーマップは、タグを受信したときのホストでの処理を適用するために使用されます。

### コマンド デフォルト

Web 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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** **ip admission name** コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証をイネーブルにしてから、**ip access-group in** および **ip admission web-rule** 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、特定のインターフェイス上で Web 認証をイネーブルにします。

**例** 次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

次の例では、スイッチポートでのフォールバックメカニズムとして、Web 認証とともに IEEE 802.1X 認証を設定する方法を示します。

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

関連コマンド	コマンド	説明
	<b>dot1x fallback</b>	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
	<b>fallback profile</b>	Web 認証のフォールバックプロファイルを作成します。



コマンド	説明
<b>ip admission</b>	ポートで Web 認証をイネーブ ルにします。
<b>show authentication sessions interface <i>interface</i> detail</b>	Web 認証セッションのステ ータスに関する情報を表示しま す。
<b>show ip admission</b>	NAC のキャッシュされたエン トリまたは NAC 設定につい ての情報を表示します。

## ip device tracking maximum

レイヤ2アクセスポートでIPデバイストラッキングパラメータを設定するには、インターフェイスコンフィギュレーションモードで **ip device tracking maximum** コマンドを使用します。最大値を削除するには、このコマンドの **no** 形式を使用します。

**ip device tracking maximum** *number*  
**no ip device tracking maximum**

構文の説明	<i>number</i> ポートのIPデバイストラッキングテーブルに作成するバインディングの数。範囲は0 (ディセーブル) ~ 65535 です。	
コマンドデフォルト	なし	
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モード	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** 最大値を削除するには、**no ip device tracking maximum** コマンドを使用します。  
 IPデバイストラッキングを無効にするには、**ip device tracking maximum 0** コマンドを使用します。



(注) このコマンドは、設定されている場合は常にIPDTを有効にします。

### 例

次の例では、レイヤ2アクセスポートでIPデバイストラッキングパラメータを設定する方法を示します。

```
Device# configure terminal
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

## ip device tracking probe

Address Resolution Protocol (ARP) プロブの IP デバイス トラッキング テーブルを設定するには、グローバル コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。ARP インспек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。

**ip device tracking probe** {count number|delay seconds|interval seconds|use-svi address}  
**no ip device tracking probe** {count number|delay seconds|interval seconds|use-svi address}

### 構文の説明

<b>count number</b>	スイッチが ARP プロブを送信する回数を設定します。範囲は 1 ~ 255 です。
<b>delay seconds</b>	スイッチが ARP プロブを送信するまで待機する秒数を設定します。指定できる範囲は 1 ~ 120 です。
<b>interval seconds</b>	スイッチが応答を待ち、ARP プロブを再送信するまでの秒数を設定します。指定できる範囲は 30 ~ 1814400 秒です。
<b>use-svi</b>	スイッチ仮想インターフェイス (SVI) IP アドレスを ARP プロブのソースとして使用します。

### コマンドデフォルト

カウント番号は 3 です。

遅延はありません。

30 秒間隔です。

ARP プロブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

スイッチポートのデフォルトソース IP アドレス 0.0.0.0 が使用され、ARP プロブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プロブに使用するように設定するには、**use-svi** キーワードを使用します。

### 例

次の例では、SVI を ARP プロブのソースとして設定する方法を示します。

```
Device(config)# ip device tracking probe use-svi
```

## ip dhcp snooping database

Dynamic Host Configuration Protocol (DHCP) のスヌーピングデータベースを設定するには、グローバルコンフィギュレーションモードで **ip dhcp snooping database** コマンドを使用します。DHCP スヌーピングサーバ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。

**no ip dhcp snooping database** [ **timeout** | **write-delay** ]

構文の説明	<b>flash:url</b>	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>ftp:url</b>	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>http:url</b>	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>https:url</b>	セキュア HTTP (HTTPS) を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>rnp:url</b>	リモートコピー (RCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>scp:url</b>	セキュアコピー (SCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>tftp:url</b>	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	<b>timeout</b> <i>seconds</i>	タイムアウトインターバルを指定します。有効値は 0 ～ 86,400 秒です。

<b>write-delay</b> <i>seconds</i>	ローカル DHCP スヌーピングデータベースにデータが追加されてから、DHCP スヌーピングエントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ~ 86,400 秒です。
-----------------------------------	--

**コマンド デフォルト** DHCP スヌーピングデータベースは設定されていません。

**コマンド モード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** このコマンドを入力する前に、インターフェイス上でDHCPスヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピングエントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Device(config)# ip dhcp snooping database write-delay 15
```

## ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、スイッチのグローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

### 構文の説明

<b>hostname</b>	スイッチのホスト名をリモート ID として指定します。
<b>string string</b>	1 ~ 63 の ASCII 文字 (スペースなし) を使用して、リモート ID を指定します。

### コマンド デフォルト

スイッチの MAC アドレスは、リモート ID 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** 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 DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列 (スペースなし) のいずれかをリモート ID として設定できます。



(注) ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

## ip dhcp snooping verify no-relay-agent-address

DHCP クライアントメッセージのリレーエージェントアドレス (giaddr) が信頼できないポート上のクライアントハードウェアアドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバルコンフィギュレーションモードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

**ip dhcp snooping verify no-relay-agent-address**  
**no ip dhcp snooping verify no-relay-agent-address**

### 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

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアントメッセージのリレーエージェント IP アドレス (giaddr) フィールドが 0 であることを確認します。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアントメッセージのリレーエージェントの IP アドレス (giaddr) フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

次に、DHCP クライアントメッセージの giaddr 検証をイネーブルにする例を示します。

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

## ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング エントリを削除するには、このコマンドの **no** 形式を使用します。

```
ip source binding mac-address vlan vlan-id ip-address interface interface-id
no ip source binding mac-address vlan vlan-id ip-address interface interface-id
```

構文の説明	<i>mac-address</i>	バインディング対象MACアドレスです。
	<b>vlan</b> <i>vlan-id</i>	レイヤ 2 VLAN ID を指定します。有効な値は 1~4094 です。
	<i>ip-address</i>	バインディング対象 IP アドレスです。
	<b>interface</b> <i>interface-id</i>	物理インターフェイスの ID です。
コマンド デフォルト	IP 送信元バインディングは設定されていません。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

**no** 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディング エントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Device# configure terminal
```



```
Device (config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface  
gigabitethernet1/0/1
```

## ip ssh source-interface

インターフェイスのIPアドレスをセキュアシェル（SSH）クライアントデバイスの送信元アドレスとして指定するには、グローバルコンフィギュレーションモードで **ip ssh source-interface** コマンドを使用します。送信元アドレスとして指定した IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

**ip ssh source-interface** *interface*

**no ip ssh source-interface** *interface*

### 構文の説明

<i>interface</i>	アドレスを SSH クライアントの送信元アドレスとして使用するインターフェイス。
------------------	--

### コマンド デフォルト

宛先に最も近いインターフェイスのアドレスが送信元アドレスとして使用されます（最も近いインターフェイスは SSH パケットが送信される出力インターフェイスです）。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドを指定することにより、SSH クライアントの送信元アドレスとして送信元インターフェイスの IP アドレスを使用するように強制できます。

### 例

次の例では、GigabitEthernet インターフェイス 1/0/1 に割り当てられた IP アドレスが SSH クライアントの送信元アドレスとして使用されます。

```
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
```

## ip verify source

インターフェイス上の IP ソース ガードを有効にするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードを無効にするには、このコマンドの **no** 形式を使用します。

**ip verify source**  
**no ip verify source**

コマンドデフォルト IP 送信元ガード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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

使用上のガイドライン 送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

### 例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをインターフェイス上でイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

設定を確認するには、**show ip verify source** 特権 EXEC コマンドを入力します。

# ipv6 snooping policy



- (注) すべての既存の IPv6 スヌーピング コマンドには、対応する SISF ベースのデバイス トラッキング コマンドが用意され、IPv4 と IPv6 の両方のアドレスファミリに設定を適用できるようになりました。

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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 モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

**ipv6 snooping policy** *snooping-policy*  
**no ipv6 snooping policy** *snooping-policy*

## 構文の説明

*snooping-policy* スヌーピング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。

## コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

## 使用上のガイドライン

IPv6 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。**ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。このモードでは、管理者が次の IPv6 ファーストホップ セキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスを Dynamic Host Configuration Protocol (DHCP) または Neighbor Discovery Protocol (NDP) で収集する必要があることを指定します。
- **security-level** コマンドは、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。

- **trusted-port** コマンドは、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1  
Device(config-ipv6-snooping)#
```

## limit address-count

ポートで使用できる IPv6 アドレスの数を制限するには、Neighbor Discovery Protocol (NDP) インспекション ポリシー コンフィギュレーション モードまたは IPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

**limit address-count maximum**  
**no limit address-count**

### 構文の説明

*maximum* ポートで許可されているアドレスの数。範囲は 1 ~ 10000 です。

### コマンド デフォルト

デフォルト設定は無制限です。

### コマンド モード

ND インспекション ポリシーの設定  
 IPv6 スヌーピング 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

**limit address-count** コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ~ 10000 です。

次に、NDP ポリシー名を **policy1** と定義し、スイッチを NDP インспекション ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を **policy1** と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

## mab request format attribute 32

スイッチ上でVLANIDベースのMAC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 **mab request format attribute 32 vlan access-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。

**mab request format attribute 32 vlan access-vlan**  
**no mab request format attribute 32 vlan access-vlan**

**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** VLAN-ID ベースの MAC 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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

次の例では、スイッチでVLAN-IDベースのMAC認証をイネーブルにする方法を示します。

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

### 関連コマンド

コマンド	説明
<b>authentication event</b>	特定の認証イベントのアクションを設定します。
<b>authentication fallback</b>	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
<b>authentication host-mode</b>	ポートで認証マネージャモードを設定します。
<b>authentication open</b>	ポートでオープンアクセスをイネーブルまたはディセーブルにします。

コマンド	説明
<b>authentication order</b>	ポートで使用する認証方式の順序を設定します。
<b>authentication periodic</b>	ポートで再認証をイネーブルまたはディセーブルにします。
<b>authentication port-control</b>	ポートの認証ステータスの手動制御をイネーブルにします。
<b>authentication priority</b>	ポートプライオリティリストに認証方式を追加します。
<b>authentication timer</b>	802.1X 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。
<b>authentication violation</b>	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
<b>mab</b>	ポートの MAC-based 認証をイネーブルにします。
<b>mab eap</b>	Extensible Authentication Protocol (EAP) を使用するようポートを設定します。
<b>show authentication</b>	スイッチの認証マネージャ イベントに関する情報を表示します。



## match (アクセス マップ コンフィギュレーション)

1つまたは複数のアクセスリストをパケットと照合するようにVLANマップを設定するには、スイッチ スタックまたはスタンドアロン スイッチのアクセスマップ コンフィギュレーション モードで **match** コマンドを使用します。一致パラメータを削除するには、このコマンドの **no** 形式を使用します。

```
match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address
{namenumber} [{namenumber}] [{namenumber}]... | mac address {name} [{name}]
[{name}]...}
no match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address
{namenumber} [{namenumber}] [{namenumber}]... | mac address {name} [{name}]
[{name}]...}
```

### 構文の説明

<b>ip address</b>	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
<b>ipv6 address</b>	パケットを IPv6 アドレス アクセス リストと照合するようにアクセス マップを設定します。
<b>mac address</b>	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
<i>name</i>	パケットを照合するアクセス リストの名前です。
<i>number</i>	パケットを照合するアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

### コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

### コマンド モード

アクセス マップ 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

**vlan access-map** 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、アクセスマップ コンフィギュレーション モードを開始します。

1つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1つまたは複数のアクセス リストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用される VLAN マップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセスリストに対して照合され、IPv6 パケットは IPv6 アクセスリストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレス、IPv6 アドレスおよび MAC アドレスを指定できます。

次の例では、VLAN アクセス マップ `vmap4` を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト `al2` に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Device(config)# vlan access-map vmap4  
Device(config-access-map)# match ip address al2  
Device(config-access-map)# action drop  
Device(config-access-map)# exit  
Device(config)# vlan filter vmap4 vlan-list 5-6
```

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

## mab logging verbose

MAC 認証バイパス (MAB) のシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **mab logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

**mab logging verbose**  
**no mab logging verbose**

### 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

システムメッセージの詳細ログは有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドにより、MAC 認証バイパス (MAB) システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# mab logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

### 関連コマンド

コマンド	説明
<b>authentication logging verbose</b>	認証システムメッセージから詳細情報をフィルタリングします。
<b>dot1x logging verbose</b>	802.1X システムメッセージから詳細情報をフィルタリングします。
<b>mab logging verbose</b>	MAC 認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

## permit (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックの転送を許可するには、スイッチスタックまたはスタンドアロンスイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拡張 MAC アクセスリストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lvc-sca | lsaplsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]  
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lvc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

### 構文の説明

<b>any</b>	すべての送信元または宛先 MAC アドレスを拒否します。
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	ホスト MAC アドレスと任意のサブネットマスクを指定します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	宛先 MAC アドレスと任意のサブネットマスクを指定します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
<i>type mask</i>	(任意) パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。  <ul style="list-style-type: none"> <li>• <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。</li> <li>• <i>mask</i> は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。</li> </ul>

<b>aarp</b>	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
<b>amber</b>	(任意) EtherType DEC-Amber を指定します。
<b>appletalk</b>	(任意) EtherType AppleTalk/EtherTalk を指定します。
<b>dec-spanning</b>	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
<b>decnet-iv</b>	(任意) EtherType DECnet Phase IV プロトコルを指定します。
<b>diagnostic</b>	(任意) EtherType DEC-Diagnostic を指定します。
<b>dsm</b>	(任意) EtherType DEC-DSM を指定します。
<b>etype-6000</b>	(任意) EtherType 0x6000 を指定します。
<b>etype-8042</b>	(任意) EtherType 0x8042 を指定します。
<b>lat</b>	(任意) EtherType DEC-LAT を指定します。
<b>lavc-sca</b>	(任意) EtherType DEC-LAVC-SCA を指定します。
<b>lsap</b> <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。  <i>mask</i> は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
<b>mop-console</b>	(任意) EtherType DEC-MOP Remote Console を指定します。
<b>mop-dump</b>	(任意) EtherType DEC-MOP Dump を指定します。
<b>msdos</b>	(任意) EtherType DEC-MSDOS を指定します。
<b>mumps</b>	(任意) EtherType DEC-MUMPS を指定します。

<b>netbios</b>	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
<b>vines-echo</b>	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。
<b>vines-ip</b>	(任意) EtherType VINES IP を指定します。
<b>xns-idp</b>	(任意) EtherType Xerox Network Systems (XNS) プロトコルスイートを指定します。
<b>cos cos</b>	(任意) プライオリティを設定するため、0～7までの任意の Class of Service (CoS) 値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。 <b>cos</b> オプションが設定されているかどうかを確認する警告メッセージが表示されます。

**コマンド デフォルト** このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

**コマンド モード** MAC アクセス リスト 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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** **appletalk** は、コマンドラインのヘルプストリングには表示されますが、一致条件としてはサポートされていません。

**mac access-list extended** 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、MAC アクセス リスト コンフィギュレーション モードを開始します。

**host** キーワードを使用した場合、アドレスマスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

表 2: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novell 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NetBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
Device(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

## 関連コマンド

コマンド	説明
<b>deny</b>	MAC アクセスリスト コンフィギュレーションを拒否します。条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
<b>mac access-list extended</b>	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
<b>show access-lists</b>	スイッチに設定されたアクセス コントロール リストを表示します。

# radius server



- (注) Cisco IOS 15.2(5)E リリース以降では、Cisco IOS リリース 15.2(5)E より前のリリースで使用されていた **radius-server host** コマンドが **radius server** コマンドに置き換えられました。古いコマンドは廃止されました。

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバーのパラメータを設定するには、スイッチスタックまたはスタンドアロンスイッチで **radius server** コンフィギュレーションサブモード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。

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

## 構文の説明

<b>address {ipv4   ipv6}</b> <i>ip{address / hostname}</i>	RADIUS サーバの IP アドレスを指定します。
<b>auth-port udp-port</b>	(任意) RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。
<b>acct-port udp-port</b>	(任意) RADIUS アカウンティングサーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。
<b>key string</b>	(任意) スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。  (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。必ずこのコマンドの最終項目として <b>key</b> を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 <b>key</b> にスペースが含まれる場合は、引用符が <b>key</b> の一部でない限り、 <b>key</b> を引用符で囲まないでください。
<b>automate tester name</b>	(任意) RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定します。
<b>retransmit value</b>	(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ~ 100 です。この設定は、 <b>radius-server retransmit</b> グローバルコンフィギュレーションコマンドによる設定を上書きします。



---

**timeout seconds** (任意) スイッチが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、`radius-server timeout` グローバル コンフィギュレーション コマンドによる設定を上書きします。

---

**no radius server name** デフォルト設定に戻します。

---



---

#### コマンド デフォルト

- RADIUS アカウンティング サーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバテストはディセーブルです。
- タイムアウトは 60 分 (1 時間) です。
- 自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー (string) は設定されていません。

---

#### コマンド モード

RADIUS サーバ サブモード 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
Cisco IOS Release 15.2(7)E1	<b>radius-server host</b> コマンドを置き換える目的でこのコマンドが追加されました。

---



---

#### 使用上のガイドライン

- RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。
- **key string** サブモード コンフィギュレーション コマンドを使用すると、認証および暗号キーを設定できます。必ずこのコマンドの最終項目として **key** を設定してください。
- RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定するには、**automate-tester name** キーワードを使用します。

次の例では、認証サーバの UDP ポートを 1645、アカウンティング サーバの UDP ポートを 1646 に設定し、文字列を設定する例を示します。

```
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
```

## router rip

RIP ルーティング プロセスを設定するには、グローバル コンフィギュレーション モードで **route r rip** コマンドを使用します。RIP ルーティング プロセスをオフにするには、このコマンドの **no** 形式を使用します。

**router rip**  
**no router rip**

### 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

RIP ルーティング プロセスは定義されていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 例

次に、RIP ルーティング プロセスを開始する例を示します。

```
Device(config)# router rip
```

### 関連コマンド

コマンド	説明
<b>network (RIP)</b>	RIP プロセスのネットワークリストを指定します。

## show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

**show aaa clients [detailed]**

構文の説明	<b>detailed</b> (任意) 詳細なAAAクライアントの統計情報を示します。				
コマンドモード	ユーザ EXEC				
コマンド履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS Release 15.2(7)E1</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。				

次に、**show aaa clients** コマンドの出力例を示します。

```
Device# show aaa clients
Dropped request packets: 0
```

# show aaa command handler

AAA コマンドハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

## show aaa command handler

### 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。

### コマンドモード

ユーザ EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show aaa command handler** コマンドの出力例を示します。

```
Device# show aaa command handler
```

```
AAA Command Handler Statistics:
  account-logon: 0, account-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

# show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

## 構文の説明

**user** AAA ローカルのロックアウトされたユーザを指定します。  
**lockout**

## コマンドモード

ユーザ EXEC

## コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

## show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

**show aaa servers** [ **private** | **public** | [**detailed**] ]

構文の説明	<b>detailed</b>	(任意) AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
	<b>public</b>	(任意) AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
	<b>detailed</b>	(任意) 詳細な AAA サーバの統計情報を表示します。
コマンドモード	ユーザ EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show aaa servers** コマンドの出力例を示します。

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

## show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

### show aaa sessions

#### 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。

#### コマンドモード

ユーザ EXEC

#### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show aaa sessions** コマンドの出力例を示します。

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

## show authentication sessions

現在の認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

**show authentication sessions** [**database**] [**handle** *handle-id* [**details**]] [**interface** *type number* [**details**]] [**mac** *mac-address* [**interface** *type number*]] [**method** *method-name* [**interface** *type number* [**details**]]] [**session-id** *session-id* [**details**]]

### 構文の説明

<b>handle</b> <i>handle-id</i>	(任意) 認証マネージャ情報を表示する特定のハンドルを指定します。
<b>interface</b> <i>type number</i>	(任意) 認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
<b>mac</b> <i>mac-address</i>	(任意) 情報を表示する特定の MAC アドレスを指定します。
<b>method</b> <i>method-name</i>	(任意) 認証マネージャ情報を表示する特定の認証方法を指定します。方式を指定する場合 ( <b>dot1x</b> 、 <b>mab</b> 、または <b>webauth</b> )、インターフェイスも指定できます。
<b>session-id</b> <i>session-id</i>	(任意) 認証マネージャ情報を表示する特定のセッションを指定します。

### コマンドモード

ユーザ EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

現在のすべての認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャセッションに関する情報を表示するには、1つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 3: 認証方式の状態

状態	説明
Not run	このセッションの方式は実行されていません。
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。



状態	説明
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

表 4: 認証方式の状態

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Gi1/0/48   0015.63b0.f676   dot1x   DATA   Authz Success 0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401   mab     DATA   Authz Success 0A3462B10000000D24F80B58
Gi1/0/5    0014.bf5d.d26d   dot1x   DATA   Authz Success 0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions interface gigabitethernet2/0/47
      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A3462C80000000000002763C
      Acct Session ID: 0x00000002
      Handle: 0x25000000

Runnable methods list:
      Method  State
      mab     Failed over
      dot1x   Failed over
-----
      Interface: GigabitEthernet2/0/47
      MAC Address: 0005.5e7c.da05
      IP Address: Unknown
      User-Name: 00055e7cda05
      Status: Authz Success
```

```
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462C8000000010002A238
Acct Session ID: 0x00000003
Handle: 0x91000001
Runnable methods list:
Method State
mab Authc Success
dot1x Not run
```

## show auto security

自動セキュリティステータスを表示するには、特権 EXEC モードで **show auto security** コマンドを使用します。

### show auto-security

このコマンドには引数またはキーワードはありません。

コマンドモード	特権 EXEC (#)
コマンド履歴	リリース Cisco IOS Release 15.2(7)E1 このコマンドが導入されました。

**使用上のガイドライン** グローバル コンフィギュレーション モードで **auto security** コマンドを設定すると、グローバルに自動セキュリティが設定されます（すべてのインターフェイスを含む）。自動セキュリティを無効にすると、すべてのインターフェイスで無効になります。

特定のインターフェイスで自動セキュリティを有効にするには、**auto security-port** コマンドを使用します。

自動セキュリティがグローバルに有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Device# show auto security
Auto Security is Enabled globally
AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/10
GigabitEthernet1/0/12
GigabitEthernet1/0/23
```

自動セキュリティが特定のインターフェイスで有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Device# show auto security
Auto Security is Disabled globally
AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
```

## 関連コマンド

コマンド	説明
<b>auto security</b>	グローバルな自動セキュリティを設定します。
<b>auto security-port</b>	インターフェイス上で自動セキュリティを設定します。

# show cisp

指定されたインターフェイスの CISP 情報を表示するには、特権 EXEC モードで **show cisp** コマンドを使用します。

**show cisp** {[clients | interface *interface-id*] | registrations | summary}

構文の説明		
<b>clients</b>		(任意) CISP クライアントの詳細を表示します。
<b>interface</b> <i>interface-id</i>		(任意) 指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
<b>registrations</b>		CISP の登録情報を表示します。
<b>summary</b>		(任意) CISP のサマリー情報を表示します。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show cisp interface** コマンドの出力例を示します。

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

次に、**show cisp registration** コマンドの出力例を示します。

```
Device# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
```

```
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

## 関連コマンド

コマンド	説明
<b>cisp enable</b>	Client Information Signalling Protocol (CISP) をイネーブルにします。
<b>dot1x credentials profile</b>	サブリカント スイッチでプロファイルを設定します。

# show dot1x

スイッチまたは指定されたポートの 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するには、ユーザー EXEC モードで **show dot1x** コマンドを使用します。

**show dot1x** [**all** [**count** | **details** | **statistics** | **summary**]] [**interface type number** [**details** | **statistics**]] [**statistics**]

構文の説明	<b>all</b>	(任意) すべてのインターフェイスの IEEE 802.1X 情報を表示します。
	<b>count</b>	(任意) 許可されたクライアントと無許可のクライアントの総数を表示します。
	<b>details</b>	(任意) IEEE 802.1X インターフェイスの詳細を表示します。
	<b>statistics</b>	(任意) すべてのインターフェイスの IEEE 802.1X 統計情報を表示します。
	<b>summary</b>	(任意) すべてのインターフェイスの IEEE 802.1X サマリー情報を表示します。
	<b>interface type number</b>	(任意) 指定したポートの IEEE 802.1X ステータスを表示します。
コマンドモード	ユーザ EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show dot1x all** コマンドの出力例を示します。

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

次に、**show dot1x all count** コマンドの出力例を示します。

```
Device# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients       = 0
Unauthorized Clients     = 0
```

```
Total No of Client          = 0
```

次に、**show dot1x all statistics** コマンドの出力例を示します。

```
Device# show dot1x statistics
Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 0

TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0       ReTxReqFail = 0
TxReqID = 0      ReTxReqID = 0    ReTxReqIDFail = 0
TxTotal = 0
```



## show eap pac peer

拡張可能認証プロトコル (EAP) のセキュアトンネリングを介したフレキシブル認証 (FAST) ピアの格納済み Protected Access Credential (PAC) を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

### show eap pac peer

#### 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。

#### コマンドモード

特権 EXEC

#### コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

次に、**show eap pac peers** 特権 EXEC コマンドの出力例を示します。

```
Device > show eap pac peers
No PACs stored
```

#### 関連コマンド

コマンド	説明
<b>clear eap sessions</b>	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

## show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザー EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

**show ip dhcp snooping statistics [ detail ]**

### 構文の説明

**detail** (任意) 詳細な統計情報を表示します。

### コマンドモード

ユーザ EXEC

### コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E1

このコマンドが導入されました。

### 使用上のガイドライン

スイッチスタックでは、すべての統計情報がプライマリスタックで生成されます。新しいアクティブスイッチが選定された場合、統計カウンタはリセットされます。

次に、**show ip dhcp snooping statistics** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics
```

```
Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

次に、**show ip dhcp snooping statistics detail** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics detail
```

```
Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                       = 0
  Interface is in errdisabled      = 0
  Rate limit exceeded              = 0
  Received on untrusted ports      = 0
  Nonzero giaddr                   = 0
  Source mac not equal to chaddr   = 0
  Binding mismatch                 = 0
  Insertion of opt82 fail          = 0
  Interface Down                   = 0
  Unknown output interface         = 0
  Reply output port equal to input port = 0
  Packet denied by platform        = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 5: DHCP スヌーピング統計情報

DHCP スヌーピング統計情報	説明
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートでDHCPパケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバパケット (OFFER、ACK、NAK、LEASEQUERY のいずれか) を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレーエージェントアドレスフィールド (giaddr) がゼロ以外だった回数。または <b>no ip dhcp snooping information option allow-untrusted</b> グローバルコンフィギュレーションコマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレスフィールド (chaddr) がパケットの送信元 MAC アドレスと一致せず、 <b>ip dhcp snooping verify mac-address</b> グローバルコンフィギュレーションコマンドが設定されている回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MACアドレスとVLANのペアのバインディングになっているポートとは異なるポートで、RELEASEパケットまたはDECLINEパケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動してRELEASEまたはDECLINEを実行したことを表すこともあります。MACアドレスは、イーサネットヘッダーの送信元MACアドレスではなく、DHCPパケットのchaddrフィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション82挿入がエラーになった回数。オプション82データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットがDHCPリレーエージェントへの応答であるが、リレーエージェントのSVIインターフェイスがダウンしている回数。DHCPサーバへのクライアント要求の送信と応答の受信の間でSVIがダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション82データまたはMACアドレステーブルのルックアップのいずれかで、DHCP応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション82が使用されておらず、クライアントMACアドレスが期限切れになった場合に発生することがあります。ポートセキュリティオプションでIPSGがイネーブルであり、オプション82がイネーブルでない場合、クライアントのMACアドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

## show ip rip database

関連ルートがサマリーアドレスに基づいて集約されている場合に、RIP (Routing Information Protocol) ルーティングデータベースエントリのサマリーアドレスエントリを表示するには、特権 EXEC モードで **show ip rip database** コマンドを使用します。

**show ip rip database** [*ip-address mask*]

構文の説明	
<i>ip-address</i>	(任意) ルーティング情報が表示されるアドレス。
<i>mask</i>	(任意) サブネットマスクの引数。IP アドレス引数を入力する場合は、サブネットマスクも指定する必要があります。

**コマンドデフォルト** デフォルトの動作や値はありません。

**コマンドモード** 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** サマリーアドレスエントリは、関連する子ルートが要約される場合にのみデータベースに現れます。サマリーアドレスの最後の子ルートが無効になると、そのサマリーアドレスもルーティングテーブルから削除されます。

RIP プライベートデータベースは、RIP のトリガー拡張機能が **ip rip triggered** コマンドでイネーブルになっている場合にのみ入力されます。

### 例

次の出力は、3 つの子ルートがアクティブになっている、ルート 10.11.0.0/16 のサマリーアドレスエントリを示しています。

```
Device# show ip rip database
10.0.0.0/8    auto-summary
10.0.0.0/8
    [1] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
192.168.0.0/8    auto-summary
192.168.0.0/8
    [2] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
172.16.0.0/8    auto-summary
172.16.0.0/24    directly connected, GigabitEthernet7/0/10
```

次の表に、画面に表示されるフィールドについて説明します。

表 6: *show ip rip database* のフィールドの説明

フィールド	説明
10.0.0.0/8 auto-summary	サマリーアドレスエントリ。
172.16.0.0/24 directly connected, GigabitEthernet7/0/10	GigabitEthernet 7/0/10 の直接接続されたエントリ。

## 関連コマンド

コマンド	説明
<b>debug ip rip</b>	RIP ルーティング トランザクションに関する情報を表示します。

# show ip ssh

セキュアシェル（SSH）のバージョンおよび設定データを表示するには、**show ip ssh** 特権 EXEC コマンドを使用します。

## show ip ssh

### 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。

### コマンドモード

特権 EXEC

### コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E1

このコマンドが導入されました。

### 使用上のガイドライン

再試行やタイムアウトなどの設定済みオプションのステータスを表示するには、**show ip ssh** を使用します。このコマンドを使用すると、SSH がイネーブルかディセーブルかを確認できます。

### 例

次に、SSH をイネーブルにした場合の **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

次に、SSH をディセーブルにした場合の **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
%SSH has not been enabled
```

次に、設定された RSA キーサイズを表示する **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
```

```
Minimum expected Diffie Hellman key size : 1024 bits  
IOS Keys in SECSH format(ssh-rsa, base64 encoded): NONE
```



## show radius server-group

RADIUS サーバグループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

**show radius server-group** {*name* | **all**}

### 構文の説明

**name** サーバグループの名前。サーバグループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。

**all** すべてのサーバグループのプロパティを表示します。

### コマンドモード

ユーザ EXEC

特権 EXEC

### コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E1

このコマンドが導入されました。

### 使用上のガイドライン

**aaa group server radius** コマンドで定義したサーバグループを表示するには、**show radius server-group** コマンドを使用します。

次に、**show radius server-group all** コマンドの出力例を示します。

```
Device# show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 7: **show radius server-groups** コマンドのフィールドの説明

フィールド	説明
Server group	サーバグループの名前。
Sharecount	このサーバグループを共有している方式リストの数。たとえば、1つの方式リストが特定のサーバグループを使用する場合、sharecount は 1 です。2つの方式リストが同じサーバグループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバグループが設定解除されました。

フィールド	説明
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバグループ構造の内部参照の数。この数は、このサーバグループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocks はメモリ管理のために内部的に使用されます。

## show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

```
show vlan group [{group-name vlan-group-name [user_count]}]
```

### 構文の説明

**group-name** *vlan-group-name* (任意) 指定した VLAN グループにマッピングされている VLAN を表示します。

**user\_count** (任意) 特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。

### コマンドデフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E1

このコマンドが導入されました。

### 使用上のガイドライン

**show vlan group** コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。**group-name** キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

## switchport port-security aging

セキュアアドレスエントリのエージングタイムおよびタイプを設定する、または特定のポートのセキュアアドレスのエージング動作を変更するには、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポートセキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

### 構文の説明

<b>static</b>	このポートに静的に設定されたセキュアアドレスのエージングをイネーブルにします。
<b>time</b> <i>time</i>	このポートのエージングタイムを指定します。指定できる範囲は0～1440分です。 <i>time</i> が 0 の場合、このポートのエージングはディセーブルです。
<b>type</b>	エージング タイプを設定します。
<b>absolute</b>	<b>absolute</b> エージング タイプを設定します。このポートのすべてのセキュアアドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュアアドレス リストから削除されます。
<b>inactivity</b>	<b>inactivity</b> エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュアアドレスが期限切れになります。

### コマンド デフォルト

ポートセキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。デフォルトのエージング タイプは **absolute** です。デフォルトのスタティック エージング動作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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

特定のポートのセキュアアドレス エージングをイネーブルにするには、ポートエージングタイムを 0 以外の値に設定します。

特定のセキュアアドレスに時間を限定してアクセスできるようにするには、エージングタイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュアアドレスが削除されます。

継続的にアクセスできるセキュアアドレス数を制限するには、エージングタイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュアアドレスが削除され、他のアドレスがセキュアになることができます。

セキュアアドレスへのアクセス制限を解除するには、セキュアアドレスとして設定し、**no switchport port-security aging static** 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、静的に設定されたセキュアアドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュアアドレスに対して、エージングタイプを **absolute**、エージングタイムを2時間に設定します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュアアドレスに対して、エージングタイプを **inactivity**、エージングタイムを2分に設定します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュアアドレスのエージングをディセーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

## switchport port-security mac-address

セキュア MAC アドレスまたはスティッキ MAC アドレスラーニングを設定するには、**switchport port-security mac-address** 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。

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} |
sticky [{mac-address | vlan {vlan-id {access | voice}}]}]
```

### 構文の説明

**mac-address** 48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できません。

**vlan vlan-id** (任意) トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。

**vlan access** (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

**vlan voice** (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

(注) **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

**sticky** スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。

**mac-address** (任意) スティッキ セキュア MAC アドレスを指定する MAC アドレス。

### コマンド デフォルト

セキュア MAC アドレスは設定されていません。

スティッキ ラーニング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

Cisco IOS Release 15.2(7)E1

このコマンドが導入されました。

### 使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。
- 音声 VLAN では、スタティックセキュアまたはスティッキセキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。
- 音声 VLAN はアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

スティッキセキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** 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、インターフェイス上でスティッキラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミックセキュア MAC アドレス (スティッキラーニングがイネーブルになる前に動的に学習されたアドレスを含む) を、スティッキセキュア MAC アドレスに変換し、すべてのスティッキセキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** 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、スティッキラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキセキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレステーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミックアドレスとしてアドレステーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** 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、スティッキセキュア MAC アドレスを設定する場合、これらのアドレスはアドレステーブルおよび実行コンフィギュレーションに追加されます。ポートセキュリティがディセーブルの場合、スティッキセキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキセキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくて済みます。スティッキセキュアアドレスを保存しない場合、アドレスは失われます。スティッキラーニングがディセーブルの場合

合、スティッキセキュア MAC アドレスはダイナミックセキュアアドレスに変換され、実行コンフィギュレーションから削除されます。

- スティックラーニングをディセーブルにして、**switchport port-security mac-address sticky mac-address** インターフェイス コンフィギュレーション コマンドを入力した場合、エラーメッセージが表示され、スティッキセキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキラーニングをイネーブルにして、ポート上で2つのスティッキセキュア MAC アドレスを入力する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```



## switchport port-security maximum

セキュア MAC アドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** 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。

```
switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]
no switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]
```

### 構文の説明

**value** インターフェイスのセキュア MAC アドレスの最大数を設定します。  
デフォルトの設定は 1 秒です。

**vlan** (任意) トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。

**vlan-list** (任意) カンマで区切られた VLAN の範囲またはハイフンで区切られた一連の VLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。

**access** (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

**voice** (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

(注) **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

### コマンド デフォルト

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

スイッチまたはスイッチスタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができます。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

音声 VLAN はアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

- インターフェイスのセキュアアドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュアアドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

## switchport port-security violation

セキュア MAC アドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** 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。

```
switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
no switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
```

### 構文の説明

<b>protect</b>	セキュリティ違反保護モードを設定します。
<b>restrict</b>	セキュリティ違反制限モードを設定します。
<b>shutdown</b>	セキュリティ違反シャットダウン モードを設定します。
<b>shutdown vlan</b>	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

### コマンド デフォルト

デフォルトの違反モードは **shutdown** 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
Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

### 使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。



- (注) トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが **errdisable** になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュアポートが **errdisable** ステートの場合には、**errdisable recovery cause psecure-violation** グローバルコンフィギュレーションコマンドを入力してこのステートを解除するか、**shutdown** および **no shutdown** インターフェイスコンフィギュレーションコマンドを入力して手動で再びイネーブルにできます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが **errdisable** になります。

セキュアポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができます。
- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。

セキュア MAC アドレスの最大値がアドレステーブルに存在し、アドレステーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュアポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

セキュアポートが **errdisable** ステートの場合には、**errdisable recovery cause psecure-violation** グローバルコンフィギュレーションコマンドを入力して、このステートから回復させることができます。**shutdown** および **no shutdown** インターフェイスコンフィギュレーションコマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

## trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND インスペクション ポリシー コンフィギュレーション モードで **trusted-port** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**trusted-port**  
**no trusted-port**

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	どのポートも信頼されていません。	
コマンド モード	ND インスペクション ポリシーの設定 IPv6 スヌーピング 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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** **trusted-port** コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレススプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディングテーブルを維持できるように分析されます。これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

次に、NDP ポリシー名を **policy1** と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーションモードにし、ポートを信頼するように設定する例を示します。

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

次に、IPv6 スヌーピング ポリシー名を **policy1** と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

## username name masked-secret

指定された名前と `masked-secret` を使用してユーザアカウントを設定するには、グローバル コンフィギュレーション モードで `username name masked-secret` コマンドを使用します。

ユーザ名に関連するすべての設定を削除するには、このコマンドの `no` 形式を使用します。

**username** *name* **masked-secret**

**no username** *name* **masked-secret**

### 構文の説明

*name* ユーザ名

**masked-secret** ユーザのシークレットを指定します。シークレットの入力は画面でマスクされ、デフォルトでタイプ 9 に変換されます。

### 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

Cisco IOS リリース 15.2(7)E3 このコマンドが導入されました。

### 使用上のガイドライン

ユーザ名とシークレットを（プレーンテキストで）設定すると、パスワードテキストはそのまま端末に表示され、実行コンフィギュレーションおよびスタートアップコンフィギュレーションにプレーンテキストとして保存されます。`username name masked-secret` コマンドを使用して、画面上のシークレットの入力をマスクできます。

### 例

次に、`username name masked-secret` コマンドの出力例を示します。

```
Device#username cisco masked-secret
Enter secret: *****
Confirm secret: *****
```

# vlan group

VLAN グループを作成または変更するには、グローバルコンフィギュレーションモードで **vlan group** コマンドを使用します。VLAN グループから VLAN リストを削除するには、このコマンドの **no** 形式を使用します。

```

vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list

```

構文の説明	<i>group-name</i>	VLAN グループの名前。名前は最大 32 文字で、文字から始める必要があります。
	<b>vlan-list</b> <i>vlan-list</i>	VLAN グループに追加される 1 つ以上の VLAN を指定します。 <i>vlan-list</i> 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。複数のエントリはハイフン (-) またはカンマ (,) で区切ります。
コマンドデフォルト	なし	
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
	Cisco IOS Release 15.2(7)E1	このコマンドが導入されました。

**使用上のガイドライン** 指定された VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

**vlan group** コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

次に、VLAN 7～9 と 11 を VLAN グループにマッピングする例を示します。

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Device(config)# no vlan group group1 vlan-list 7
```





## 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。