CHAPTER 2

Cisco IE 2000 スイッチ Cisco IOS コマンド

aaa accounting dot1x

認証、許可、アカウンティング（AAA）のアカウンティングをイネーブルにし、回線単位またはインターフェイス単位で IEEE 802.1x セッションに対する特定のアカウンティング方式を定義する方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa accounting dot1x** コマンドを使用します。IEEE 802.1x アカウン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

name	サーバ グループに名前を付けます。これは、**broadcast group** および **group** 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。
default	デフォルト リストとして続くアカウンティング方式を、アカウンティング サービス用に指定します。
start-stop	プロセスの開始時に start アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start アカウンティ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。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング 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。
group	アカウンティング 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。 • *name*：サーバ グループ名 • **radius**：全 RADIUS ホストのリスト • tacacs+：全 TACACS+ ホストのリスト **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くのキーワードを入力できます。

radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウン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
15.0(1)EY	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。

例

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。

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

（注） RADIUS 認証サーバは、AAA クライアントから更新パケットやウォッチドッグ パケットを受け入れて記録するよう、適切に設定する必要があります。

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1x が動作しているインターフェイスで使用する 1 つ以上の AAA メソッドを指定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
dot1x reauthentication	定期的な再認証をイネーブルまたはディセーブルにします。
dot1x timeout reauth-period	再認証の間隔（秒）を設定します。

aaa authentication dot1x

認証、許可、アカウンティング（AAA）の方式を IEEE 802.1x 認証に準拠するポートで使用するように指定するには、グローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。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 authentication dot1x {**default**} *word*

no aaa authentication dot1x {**default**}

構文の説明

default	この引数の後に続く、リストされた認証方式をログイン時のデフォルトの方式として指定します。
word	認証用のすべての RADIUS サーバの認証リスト名。有効な名前の長さは 1 ～ 31 文字です。

（注）　他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

word 引数には、クライアントからのパスワードを認証アルゴリズムが確認するために一定の順序で試みる方式を指定します。実際に 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 コマンドを使用して 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。

例

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。

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

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
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

aaa authorization network

ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、IEEE 802.1x AAA ユーザ アクセス コントロール リスト（ACL）または VLAN 割り当てなど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 ホストのリストを指定します。

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
15.0(1)EY	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、ユーザごとの ACL または 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。

例

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。

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

action

VLAN アクセスマップ エントリのアクションを設定するには、アクセスマップ コンフィギュレーション モードで **action** 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。

action {**drop** | **forward**}

no action

構文の説明

drop	指定した条件に一致する場合に、パケットをドロップします。
forward	指定した条件に一致する場合に、パケットを転送します。

コマンド デフォルト

デフォルトのアクションは、パケットの転送です。

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
15.0(1)EY	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。

アクションが **drop** の場合は、一致条件にアクセス コントロール リスト（ACL）名を設定後、そのマップを VLAN に適用してアクセス マップを定義する必要があります。定義しない場合、すべてのパケットがドロップされることがあります。

アクセス マップ コンフィギュレーション モードでは、**match** アクセス マップ コンフィギュレーション コマンドを使用して、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。

drop パラメータおよび **forward** パラメータは、このコマンドの **no** 形式では使用しません。

例

次の例では、VLAN アクセス マップ vmap4 を指定し 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場合に、VLAN がその IP パケットを転送するように指定します。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(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。

関連コマンド

コマンド	説明
access-list {**deny** | **permit**}	番号付き標準 ACL を設定します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
ip access-list	名前付きアクセス リストを作成します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
match（クラスマップ コンフィギュレーション）	VLAN マップの一致条件を定義します。
show vlan access-map	スイッチで作成された VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

alarm contact

システム アラーム接点を設定するには、グローバル コンフィギュレーション モードで **alarm contact** のコマンドを使用します。

alarm contact *contact* {**description** {*line*} | **severity** {**major** | **minor** | **none**} | **trigger**{**closed** | **open**}| **all**}

no alarm contact *contact* {**description** {*line*} | **severity** {**major** | **minor** | **none**} | **trigger**{**closed** | **open**}| **all**}

構文の説明

contact	アラーム接点番号を指定します。範囲番号は 1 ～ 2 です。
description *line*	アラームを説明する文字列を設定します。
severity	レポートされる重大度を設定します。
major	アラームをメジャーな重大度に設定します。
minor	アラームをマイナーな重大度に設定します。
none	重大度を設定しません。
trigger	アラーム トリガーを設定します。
closed	アラーム接点を閉じます。
open	アラーム接点を開きます。
all	すべてのアラーム接点を設定します。

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
15.0(1)EY	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、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

例

次に、アラーム接点を 1 に設定し、重大度をメジャーに設定する例を示します。

```
Switch(config)# alarm contact 1 severity major
```

次に、アラーム接点 1 の重大度を解除する例を示します。

```
Switch(config)# no alarm contact 1 severity major
```

次に、アラーム 1 のトリガーを closed に設定する例を示します。

```
Switch(config)# alarm contact 1 trigger closed
```

次に、アラーム 1 のトリガーの closed を解除する例を示します。

```
Switch(config)# no alarm contact 1 trigger closed
```

関連コマンド

コマンド	説明
show alarm settings	すべてのスイッチのアラーム設定を表示します。

alarm facility fcs-hysteresis

フレーム チェック シーケンス（FCS）エラー ヒステリシスしきい値を FCS ビットエラー レートから変動率として設定するには、FCS ビット エラー レートの変動は、グローバル コンフィギュレーション モードで、**alarm facility fcs-hysteresis** コマンドを使用します。FCS エラー ヒステリシスしきい値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。

alarm facility fcs-hysteresis *percentage*

構文の説明

percentage	ヒステリシスしきい値の変動率です。指定できる範囲は 1 ～ 10% です。

コマンド デフォルト

デフォルトのしきい値は 10% です。入力アラームは両方とも、notifies と Syslog に関連付けられます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ヒステリシスしきい値を設定すると、設定されたレートの近くまで FCS ビットエラー レートが変動した場合にアラームがトリガーされます。

FCS ヒステリシスしきい値はスイッチすべてのポートで設定します。FCS エラー レートは **fcs-threshold** 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単位で設定します。

しきい値がデフォルト値ではない場合、**show running-config** 特権 EXEC コマンドの出力に表示されます。

例

次の例では、FCS エラー ヒステリシスを 5% に設定する方法を示します。ビット エラー レートが設定した FCS ビットエラー レートを 5% 超過するとアラームがトリガーされます。

```
Switch(config)# alarm facility fcs-hysteresis 5
```

関連コマンド

コマンド	説明
fcs-threshold	インターフェイスの FCS エラー レートを設定します。

alarm facility input-alarm

外部の接点アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility input-alarm** コマンドを使用します。外部の接点アラーム設定をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

alarm facility input-alarm *number* {**notifies** | **relay major** | **syslog**}

no alarm facility input-alarm *number* {**notifies** | **relay major** | **syslog**}

構文の説明

number	アラーム接点番号。有効な値は 1 または 2 です。
notifies	システムがサーバに通知を送信できるようにします。
relay major	メジャー リレー設定をイネーブルにします。
syslog	システム ロガーをイネーブルにします。

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
15.0(1)EY	このコマンドが導入されました。

例

次に、サーバに送信された通知で入力アラームを 2 に設定する例を示します。

```
Switch(config)# alarm facility 2 notifies
```

関連コマンド

コマンド	説明
show alarm settings	環境アラーム設定およびオプションが表示されます。

alarm facility power-supply

システムがデュアル電源モードで稼働している場合に、電源の欠落または障害を検出するアラーム オプションを設定するには、グローバル コンフィギュレーション モードで **alarm facility power-supply** コマンドを使用します。指定した設定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。

alarm facility power-supply {**disable** | **notifies** | **relay** {**major** | **minor**} | **syslog**}

no alarm facility power-supply {**disable** | **notifies** | **relay** {**major** | **minor**} | **syslog**}

構文の説明

disable	電源アラームをディセーブルにします。
notifies	電源アラーム トラップを SNMP サーバに送信します。
relay major	アラームをメジャー リレー回路に送信します。
relay minor	アラームをマイナー リレー回路に送信します。
syslog	電源アラーム トラップを syslog サーバに送信します。

コマンド デフォルト

電源アラーム メッセージは保存されますが、SNMP サーバ、リレー、または syslog サーバに送信されません。デフォルトでは、両方の入力アラームは出力アラーム「Major」にマッピングされます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

電源アラームは、システムがデュアル電源モードの場合にのみ生成されます。2 つめの電源が接続された場合、**power-supply dual** 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デュアル電源モードの動作を設定します。

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** 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 SNMP サーバを設定してください。

例

次に、電源モニタリング アラームをディセーブルにする例を示します。

```
Switch(config)# alarm facility power-supply relay disable
Switch(config)#
```

次に、SNMP サーバに通知を送信するように電源モニタリング アラームを設定する例を示します。

```
Switch(config)# alarm facility power-supply relay notifies
Switch(config)#
```

次の例では、電源モニタリング アラームをメジャー リレー回路に送信する設定方法を示します。

```
Switch(config)# alarm facility power-supply relay major
Switch(config)#
```

次の例では、電源モニタリング アラームをマイナー リレー回路に送信する設定方法を示します。

```
Switch(config)# alarm facility power-supply relay minor
Switch(config)#
```

次に、syslog サーバに送信するように電源モニタリング アラームを設定する例を示します。

```
Switch(config)# alarm facility power-supply relay syslog
Switch(config)#
```

関連コマンド

コマンド	説明
ptp（インターフェイス コンフィギュレーション）	スイッチをデュアル電源モードで動作するように設定します。
show alarm settings	環境アラーム設定およびオプションが表示されます。
snmp-server enable traps	スイッチでさまざまなトラップ タイプ SNMP 通知をネットワーク管理システム（NMS）に送信します。

alarm facility sd-card

SD カードを設定するには、グローバル コンフィギュレーション モードで **alarm facility sd-card** コマンドを使用します。SD カードをデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

alarm facility sd-card {**notifies** | **relay major** | **syslog**}

no alarm facility sd-card {**notifies** | **relay major** | **syslog**}

構文の説明

notifies	システムがサーバに通知を送信できるようにします。
relay major	メジャー リレー設定をイネーブルにします。
syslog	システム ロガーをイネーブルにします。

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、SD カードが取り付けられた場合に、サーバに通知するように入力アラームを設定する方法を示します。

```
Switch(config)# alarm facility sd-card notifies
```

関連コマンド

コマンド	説明
show alarm settings	環境アラーム設定およびオプションが表示されます。

alarm facility temperature

プライマリ温度モニタリング アラームの設定、または上限値が低いセカンダリ温度アラームしきい値を設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** コマンドを使用します。温度モニタリング アラームの設定を削除またはセカンダリ温度アラーム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。

alarm facility temperature {**primary** {**high** | **low** | **notifies** | **relay** {**major**} | **syslog**} | **secondary** {**high** | **low** | **notifies** | **relay** {**major** | **minor**}| **syslog**}}

no alarm facility temperature {**primary** {**high** | **low** | **notifies** | **relay** {**major**} | **syslog**} | **secondary** {**high** | **low** | **notifies** | **relay** {**major** | **minor**}| **syslog**}}

構文の説明

primary	プライマリ モニタのアラームの温度を設定します。
high	プライマリ温度アラームまたはセカンダリ温度アラームの高温しきい値を設定します。指定できる範囲は、–238 ～ 572 °F（–150 ～ 300 °C）です。
low	プライマリ温度アラームまたはセカンダリ温度アラームの低温しきい値を設定します。指定できる範囲は、–328 ～ 482 °F（-200 ～ 250 °C）です。
notifies	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを SNMP サーバに送信します。
relay major	プライマリ温度アラームまたはセカンダリ温度アラームをメジャー リレー回路に送信します。
syslog	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを syslog サーバに送信します。
secondary	セカンダリ モニタのアラームの温度を設定します。

コマンド デフォルト

プライマリ温度アラームは –4 ～ 203 °F（–20 ～ 95 ºC）の範囲でイネーブルになっており、ディセーブルにできません。アラームはメジャー リレーに関連付けられています。セカンダリ温度アラームはデフォルトでディセーブルになっています。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

プライマリ温度アラームは自動的にイネーブルになります。アラームはディセーブルにできませんが、アラーム オプションを設定できます。

プライマリ温度アラームの範囲は、**high** および **low** キーワードを使用して設定できます。

セカンダリ温度アラームを使用してプライマリ温度の高温しきい値（203 ºF（95 ºC））より低い高温アラームをトリガーできます。温度しきい値とアラーム オプションを設定できます。

notifies キーワードを使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** 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 SNMP サーバを設定してください。

例

次の例では、セカンダリ温度の高温しきい値に 113 °F（45 °C）とアラームを設定し、トラップをマイナー リレー回路、syslog、および SNMP サーバに送信する方法を示します。

```
Switch(config)# alarm facility temperature secondary high 45
Switch(config)# alarm facility temperature secondary relay minor
Switch(config)# alarm facility temperature secondary syslog
Switch(config)# alarm facility temperature secondary notifies
```

次の例では、セカンダリ温度アラームをディセーブルにする方法を示します。

```
Switch(config)# no alarm facility temperature secondary 45
```

次の例では、プライマリ温度アラームを設定し、syslog とメジャー リレー回路にアラームとトラップを送信する方法を示します。

```
Switch(config)# alarm facility temperature primary syslog
Switch(config)# alarm facility temperature primary relay major
```

関連コマンド

コマンド	説明
show alarm settings	環境アラーム設定およびオプションが表示されます。
snmp-server enable traps	スイッチでさまざまなトラップ タイプ SNMP 通知をネットワーク管理システム（NMS）に送信します。

alarm profile（グローバル コンフィギュレーション）

アラーム プロファイルを作成し、アラーム プロファイル 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 **alarm profile** コマンドを使用します。アラーム プロファイルを削除するには、このコマンドの **no** 形式を使用します。

alarm profile *name*

no alarm profile *name*

構文の説明

name	アラームのプロファイル名です。

コマンド デフォルト

アラーム プロファイルは作成されません。

プロファイルを作成しても、アラームは 1 つもイネーブルになりません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

アラームプロファイル コンフィギュレーション モードでは、次のコマンドが使用できます。

- **alarm** *alarm-id*：指定したアラームをイネーブルにします。
- **exit**：アラーム プロファイル コンフィギュレーション モードを終了します。
- **help**：インタラクティブ ヘルプ システムの説明が表示されます。
- **no**：コマンドを無効にするか、コマンドのデフォルト値を設定します。
- **notifies** *alarm-id*：アラームの通知がイネーブルになり、簡易ネットワーク管理プロトコル（SNMP）トラップが SNMP サーバに送信されます。
- **relay-major** *alarm-id*：アラームがメジャー リレー回路に送信されます。
- **relay-minor** *alarm-id*：アラームがマイナー リレー回路に送信されます。
- **syslog** *alarm-id*：アラームが syslog ファイルに送信されます。

alarm-id には、アラーム ID を 1 つまたはスペースで区切って複数入力します。

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** 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 SNMP サーバを設定してください。

インターフェイスにはすべて、デフォルト プロファイルが存在します。**show alarm profile** ユーザ EXEC コマンドを入力して defaultPort の出力を表示します。

表 2-1 では、アラーム ID と対応するアラームの説明を示します。

表 2-1　AlarmList ID 番号とアラームの説明

AlarmList ID	アラームの説明
1	リンク障害です。
2	ポートでフォワーディングされません。
3	ポートが動作していません。
4	FCS エラー レートがしきい値を超過しています。

アラーム プロファイルを作成すると、**alarm-profile** 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、プロファイルをインターフェイスに関連付けられます。

デフォルトでは、*defaultPort* プロファイルはすべてのインターフェイスに適用されます。このプロファイルによって、ポートが動作していない（3）アラームのみがイネーブルになります。このプロファイルは、**alarm profile defaultPort** グローバル コンフィギュレーション コマンドを使用し、アラーム プロファイル コンフィギュレーション モードを開始して変更できます。

例

次の例では、ポートのリンク障害（アラーム 1）とポートでフォワーディングされない（アラーム 2）アラームがイネーブルのアラーム プロファイル fastE を作成する方法を示します。リンク障害アラームはマイナー リレー回路に関連付けられており、ポートでフォワーディングされないアラームはメジャーリレー回路に関連付けられています。このアラームは SNMP サーバに送信され、システム ログ ファイル（syslog）に書き込まれます。

```
Switch(config)# alarm profile fastE
Switch(config-alarm-prof)# alarm 1 2
Switch(config-alarm-prof)# relay major 2
Switch(config-alarm-prof)# relay minor 1
Switch(config-alarm-prof)# notifies 1 2
Switch(config-alarm-prof)# syslog 1 2
```

次の例では、my-profile という名前のアラーム リレー プロファイルを削除する方法を示します。

```
Switch(config)# no alarm profile my-profile
```

関連コマンド

コマンド	説明
alarm profile（インターフェイス コンフィギュレーション）	インターフェイスにアラーム プロファイルを関連付けます。
show alarm settings	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。
snmp-server enable traps	スイッチでさまざまなトラップ タイプ SNMP 通知をネットワーク管理システム（NMS）に送信します。

alarm profile（インターフェイス コンフィギュレーション）

アラーム プロファイルをポートに接続するには、インターフェイス コンフィギュレーション モードで **alarm profile** コマンドを使用します。ポートからプロファイルの関連付けを解除するには、このコマンドの **no** 形式を使用します。

alarm profile *name*

no alarm profile

構文の説明

name	アラームのプロファイル名です。

コマンド デフォルト

アラーム プロファイル *defaultPort* がすべてのインターフェイスに適用されています。このプロファイルでは、ポートが動作していないアラームのみがイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

アラーム プロファイルを作成して、アラームを 1 つ以上イネーブルにし、アラーム オプションを指定するには、**alarm profile** 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。

インターフェイスに関連付けられるアラーム プロファイルは 1 つのみです。

アラーム プロファイルをインターフェイスに関連付けると、すでに関連付けられていたアラーム プロファイルは上書きされます（*defaultPort* プロファイルを含む）。

例

次の例では、ポートにアラーム プロファイル fastE を関連付ける方法を示します。

```
Switch(config)# interface fastethernet1/2
Switch(config-if)# alarm profile fastE
```

次の例では、ポートからアラーム プロファイルの関連付けを解除して、*defaultPort* プロファイルに戻す方法を示します。

```
Switch(config)# interface fastethernet1/2
Switch(config-if)# no alarm profile
```

関連コマンド

コマンド	説明
alarm profile（グローバル コンフィギュレーション）	アラーム プロファイルを作成および指定して、アラームプロファイル コンフィギュレーション モードが開始されます。
show alarm settings	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。

alarm relay-mode

スイッチのアラーム リレー モードを設定するには、グローバル コンフィギュレーション モードで **alarm relay-mode** コマンドを使用します。アラーム リレー モードをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

alarm relay-mode energized

no alarm relay-mode energized

構文の説明

energized	アラーム リレー モードを通電に設定します。

コマンド デフォルト

アラーム リレーを通電解除します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

アラーム リレーがにオープンされると、ポジティブ モードに設定されます。スイッチの電源がオフの場合、アラーム リレーはすべてオープンです。アラーム イベントが 1 つ以上検出されると、アラーム リレーはクローズされます。

例

次の例では、アラーム リレーをネガティブ モードに設定する方法を示します。

```
Switch(config)# alarm relay-mode energized
Switch(config)#
```

関連コマンド

コマンド	説明
alarm profile（グローバル コンフィギュレーション）	アラーム プロファイルを作成および指定して、アラームプロファイル コンフィギュレーション モードが開始されます。
show alarm profile	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。
show alarm settings	環境アラーム設定およびオプションが表示されます。

archive download-sw

TFTP サーバから新しいイメージをスイッチにダウンロードし、既存のイメージを上書きまたは保持するには、特権 EXEC モードで **archive download-sw** コマンドを使用します。

archive download-sw {**/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **no-version-check** | **/overwrite** | **/reload** | **/safe**} *source-url*

構文の説明

/directory	イメージのディレクトリを指定します。
/force-reload	ソフトウェア イメージのダウンロードが成功した後で無条件にシステムのリロードを強制します。
/imageonly	ソフトウェア イメージだけをダウンロードし、組み込みデバイス マネージャに関連する HTML ファイルはダウンロードしません。既存のバージョンの HTML ファイルは、既存のバージョンが上書きまたは削除されている場合にだけ削除されます。
/leave-old-sw	ダウンロードに成功した後で古いソフトウェア バージョンを保存します。
/no-set-boot	新しいソフトウェア イメージのダウンロードに成功した後、BOOT 環境変数の設定は新しいソフトウェア イメージを指定するように変更されません。
/no-version-check	スイッチ上で動作中のイメージとそのバージョンの互換性を確認せずに、ソフトウェア イメージをダウンロードします。
/overwrite	ダウンロードされたイメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	設定が変更されて保存されていない場合を除き、イメージのダウンロードに成功した後でシステムをリロードします。
/safe	現在のソフトウェア イメージを保存します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。
source-url	ローカルまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文： **ftp:**[[*//username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTPS サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[*//username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文： **tftp:**[[*//location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、スイッチにダウンロードし、インストールするソフトウェア イメージです。

コマンド デフォルト

現行のソフトウェア イメージは、ダウンロードされたイメージで上書きされません。

ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。

新しいイメージは flash: ファイル システムにダウンロードされます。

BOOT 環境変数は、flash: ファイル システムの新しいソフトウェア イメージを示すよう変更されます。

イメージ名では大文字と小文字が区別されます。イメージ ファイルは tar フォーマットで提供されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

一度に 1 つずつのディレクトリを指定するには、**archive download-sw /directory** コマンドを使用します。

/imageonly オプションは、既存のイメージが削除または置き換えられている場合に、既存のイメージの HTML ファイルを削除します。（HTML ファイルのない）Cisco IOS イメージだけがダウンロードされます。

/safe または **/leave-old-sw** オプションを指定すると、十分なフラッシュ メモリがない場合には新しいイメージのダウンロードが行われないようにすることができます。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合に、エラーが発生します。

/leave-old-sw オプションを使用し、新しいイメージをダウンロードしたときに古いイメージが上書きされなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。詳細については、「delete」（P.2-124）を参照してください。

フラッシュ デバイスのイメージをダウンロードされたイメージで上書きする場合は、**/overwrite** オプションを使用します。

/overwrite オプションなしでこのコマンドを指定する場合、ダウンロード アルゴリズムは、新しいイメージが、スイッチ フラッシュ デバイスのイメージと同じではないことを確認します。イメージが同じである場合は、ダウンロードは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがダウンロードされます。

新しいイメージをダウンロードした後で、**reload** 特権 EXEC コマンドを入力して新しいイメージの使用を開始するか、または **archive download-sw** コマンドの **/reload** オプションか **/force-reload** オプションを指定してください。

/directory オプションを使用して、イメージのディレクトリを指定します。

例

次の例では、172.20.129.10 の TFTP サーバから新しいイメージをダウンロードし、スイッチでイメージを上書きする方法を示します。

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

次の例では、172.20.129.10 の TFTP サーバからソフトウェア イメージだけをスイッチにダウンロードする方法を示します。

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

次の例では、ダウンロードに成功した後で古いソフトウェア バージョンを保存する方法を示します。

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

関連コマンド

コマンド	説明
archive tar	tar ファイルを作成し、tar ファイルのファイルを一覧表示し、tar ファイルからファイルを抽出します。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。
delete	フラッシュ メモリ デバイスのファイルまたはディレクトリを削除します。

archive tar

tar ファイルの作成、tar ファイル内のファイルの一覧表示、または tar ファイルからのファイルの抽出を行うには、特権 EXEC モードで **archive tar** コマンドを使用します。

archive tar {**/create** *destination-url* **flash:**/*file-url*} | {**/table** *source-url*} | {**/xtract** *source-url* **flash:**/*file-url* [*dir/file...*]}

構文の説明

/create *destination-url* **flash:**/*file-url*	ローカルまたはネットワーク ファイル システムに新しい tar ファイルを作成します。 *destination-url* には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTPS サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、作成する tar ファイルです。 **flash:**/*file-url* には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の場所を指定します。 送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

/table *source-url*	既存の tar ファイルの内容を画面に表示します。 *source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文： **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • セキュア HTTPS サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • RCP の構文： **rcp:**[[*//username***@***location*]*/directory*]*/tar-filename***.tar** • TFTP の構文：**tftp:**[[*//location*]*/directory*]*/tar-filename***.tar** *tar-filename***.tar** は、表示する tar ファイルです。
/xtract *source-url* **flash:***/file-url* [*dir/file...*]	tar ファイルからローカル ファイル システムにファイルを抽出します。 *source-url* には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文： **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • セキュア HTTPS サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • RCP の構文： **rcp:**[[*//username***@***location*]*/directory*]*/tar-filename***.tar** • TFTP の構文：**tftp:**[[*//location*]*/directory*]*/tar-filename***.tar** *tar-filename***.tar** は、抽出される tar ファイルです。 **flash:***/file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

イメージ名では、大文字と小文字が区別されます。

例

次の例では、tar ファイルを作成する方法を示します。このコマンドはローカル フラッシュ デバイスの new-configs ディレクトリの内容を、172.20.10.30 の TFTP サーバの saved.tar という名前のファイルに書き込みます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

次の例では、フラッシュ メモリに含まれるファイルの内容を表示する方法を示します。tar ファイルの内容が画面に表示されます。

```
Switch# archive tar /table flash:cies-lanbase-tar.12-44.EX.tar
info (219 bytes)

cies-lanbase-mz.12-44.EX/ (directory)
cies-lanbase-mz.12-44.EX (610856 bytes)
cies-lanbase-mz.12-44.EX/info (219 bytes)
info.ver (219 bytes)
```

次の例では、*/html* ディレクトリおよびその内容だけを表示する方法を示します。

```
flash:cies-lanbase-tar.12-44.EX.tar cies-lanbase-12-44.EX/html
cies-lanbase-mz.12-44.EX/html/ (directory)
cies-lanbase-mz.12-44.EX/html/const.htm (556 bytes)
cies-lanbase-mz.12-44.EX/html/xhome.htm (9373 bytes)
cies-lanbase-mz.12-44.EX/html/menu.css (1654 bytes)
<output truncated>
```

次の例では、172.20.10.30 のサーバにある tar ファイルの内容を抽出する方法を示します。ここでは、ローカル フラッシュ ファイル システムのルート ディレクトリに単に new-configs ディレクトリを抽出しています。saved.tar ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

関連コマンド

コマンド	説明
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。

archive upload-sw

スイッチの既存のイメージをサーバにアップロードするには、特権 EXEC モードで **archive upload-sw** コマンドを使用します。

archive upload-sw [**/version** *version_string*] *destination-url*

構文の説明

/version *version_string*	（任意）アップロードするイメージの特定バージョン文字列を指定します。
destination-url	ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスです。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTPS サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Secure Copy Protocol（SCP）の構文： **scp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、サーバに保存するソフトウェア イメージの名前です。

コマンド デフォルト

フラッシュ ファイル システムから現在稼働中のイメージをアップロードします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

組み込みデバイス マネージャに関連付けられている HTML ファイルが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

ファイルは、Cisco IOS イメージ、HTML ファイル、info の順序でアップロードされます。これらのファイルがアップロードされると、ソフトウェアは tar ファイルを作成します。

イメージ名では、大文字と小文字が区別されます。

例

次の例では、現在実行中のイメージを、172.20.140.2 の TFTP サーバへアップロードする方法を示します。

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

関連コマンド

コマンド	説明
archive download-sw	新しいイメージをスイッチにダウンロードします。
archive tar	tar ファイルを作成し、tar ファイルのファイルを一覧表示し、tar ファイルからファイルを抽出します。

arp access-list

アドレス解決プロトコル（ARP）アクセス コントロール リスト（ACL）を定義する場合、または定義済みリストの末尾に句を追加する場合は、グローバル コンフィギュレーション モードで **arp access-list** コマンドを使用します。指定された ARP アクセス 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。

arp access-list *acl-name*

no arp access-list *acl-name*

構文の説明

acl-name	ACL の名前

コマンド デフォルト

ARP アクセス リスト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

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

arp access-list コマンドを入力すると、ARP アクセス リスト コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **default**：コマンドをデフォルト設定に戻します。
- **deny**：拒否するパケットを指定します。詳細については、「deny（ARP アクセス リスト コンフィギュレーション）」（P.2-125）を参照してください。
- **exit**：ARP アクセス リスト コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。
- **permit**：転送するパケットを指定します 詳細については、「permit（ARP アクセス リスト コンフィギュレーション）」（P.-393）を参照してください。

指定された一致条件に基づいて ARP パケットを転送またはドロップするには、**permit** または **deny** 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。

ARP ACL が定義されると、**ip arp inspection filter vlan** 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 VLAN に ARP ACL を適用できます。IP/MAC アドレス バインディングだけを含む ARP パケットが ACL と比較されます。それ以外のすべてのパケット タイプは、検証されずに、入力 VLAN 内でブリッジングされます。ACL がパケットを許可すると、スイッチがパケットを転送します。明示的拒否ステートメントによって ACL がパケットを拒否すると、スイッチがパケットをドロップします。暗黙拒否ステートメントによって ACL がパケットを拒否すると、スイッチはパケットを DHCP バインディングのリストと比較します。ただし、ACL がスタティック（パケットがバインディングと比較されない）である場合を除きます。

例

次の例では、ARP アクセス リストを定義し、IP アドレスが 1.1.1.1 で MAC アドレスが 0000.0000.abcd のホストからの ARP 要求と ARP 応答の両方を許可する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 00001.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 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
deny（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの比較による一致に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
permit（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの比較による一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

authentication command bounce-port ignore

スイッチ スタックまたはスタンドアロン スイッチ上で、ポートを一時的にディセーブルにするコマンドをスイッチが無視できるようにするには、グローバル コンフィギュレーション モードで **authentication command bounce-port ignore** コマンドを使用します。デフォルトのステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command bounce-port ignore

no authentication command bounce-port ignore

（注）　このコマンドを使用するには、スイッチが LAN Base イメージまたは IP Base イメージを実行している必要があります。

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

このスイッチは、RADIUS 認可変更（CoA）**bounce port** コマンドを受け入れます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

CoA **bounce port** コマンドによってリンク フラップが発生し、ホストからの DHCP 再ネゴシエーションが作動します。これは VLAN 変更が発生した場合に有益であり、エンドポイントは、変更を検出するサプリカントを持たないプリンタなどのデバイスです。スイッチが **bounce port** コマンドを無視するように設定するには、このコマンドを使用します。

例

次の例では、スイッチが CoA **bounce port** コマンドを無視するように設定する方法を示します。

```
Switch(config)# authentication command bounce-port ignore
```

関連コマンド

コマンド	説明
authentication command disable-port ignore	スイッチが CoA **disable port** コマンドを無視するように設定します。

authentication command disable-port ignore

スイッチ スタックまたはスタンドアロン スイッチ上で、ポートをディセーブルにするコマンドをスイッチが無視できるようにするには、グローバル コンフィギュレーション モードで **authentication command disable-port ignore** コマンドを使用します。デフォルトのステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command disable-port ignore

no authentication command disable-port ignore

（注）　このコマンドを使用するには、スイッチが LAN Base イメージまたは IP Base イメージを実行している必要があります。

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

このスイッチは、RADIUS 認可変更（CoA）**disable port** コマンドを受け入れます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

CoA **disable port** コマンドはセッションをホスティングするポートを管理上シャットダウンし、セッションを終了させます。スイッチがこのコマンドを無視するように設定するには、このコマンドを使用します。

例

次の例では、スイッチが CoA **disable port** コマンドを無視するように設定する方法を示します。

```
Switch(config)# authentication command disable-port ignore
```

関連コマンド

コマンド	説明
authentication command bounce-port ignore	スイッチが CoA **bounce port** コマンドを無視するように設定します。

authentication control-direction

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

authentication control-direction {both | in}

no authentication control-direction

構文の説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デフォルト設定の双方向モードに戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

例

次の例では、双方向モードをイネーブルにする方法を示します。

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

次の例では、単一方向モードをイネーブルにする方法を示します。

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

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
authentication violation	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。
show authentication	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。

authentication event

ポートの特定の認証イベントの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 **authentication event** コマンドを使用します。指定した設定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 event {**fail** [**action** [**authorize vlan** *vlan-id* | **next-method**] {| **retry** {*retry count*}]} { **no-response action authorize vlan** *vlan-id*} {**server** {**alive action reinitialize**} | {**dead action** [**authorize** | **reinitialize vlan** *vlan-id*]}}

no authentication event {**fail** [**action** [**authorize vlan** *vlan-id* | **next-method**] {| **retry** {*retry count*}]} { **no-response action authorize vlan** *vlan-id*} {**server** {**alive action reinitialize**} | {**dead action** [**authorize** | **reinitialize vlan** *vlan-id*]}}

構文の説明

fail	失敗認証のパラメータを設定します。
action	（任意）認証イベントの必須アクションを設定します。
authorize	（任意）ポートを認証します。
vlan	（任意）1 ～ 4094 の認証失敗 VLAN を指定します。
vlan-id	1 ～ 4094 の VLAN ID 番号です。
next-method	（任意）次の認証方式に移動します。
retry	（任意）認証失敗後の再試行をイネーブルにします。
retry count	0 ～ 5 の再試行の回数です。
no-response	非応答ホスト アクションを設定します。
server	AAA サーバ イベントのアクションを設定します。
alive action	認証、許可、アカウンティング（AAA）サーバ稼働アクションを設定します。
reinitialize	すべての認証済みクライアントを再初期化します。
dead action	AAA サーバ停止アクションを設定します。

コマンド デフォルト

イベント応答はポートに設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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 **fail**、**no-response**、または **event** キーワードを付けて使用して、特定のアクションのスイッチ応答を設定します。

server-dead イベントの場合：

- スイッチが critical-authentication ステートに移ると、認証を試行している新しいホストが critical-authentication VLAN（または*クリティカル VLAN*）に移動されます。ポートがシングルホスト モード、マルチホスト モード、マルチ認証モード、または MDA モードの場合、これが適用されます。認証済みホストは認証済み VLAN に残り、再認証タイマーはディセーブルになります。
- クライアントで Windows XP を稼働し、クライアントが接続されているクリティカル ポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないことを報告します。

  Windows XP クライアントに DHCP が設定されており、DHCP サーバからの IP アドレスが設定されている場合に、クリティカル ポートで EAP-Success メッセージを受信しても、DHCP 設定プロセスが再開しない場合があります。

no-response イベントの場合：

- IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しないか、EAPOL パケットがクライアントから送信されないと、スイッチではクライアントをゲスト VLAN に割り当てます。
- スイッチは EAPOL パケット履歴を保持します。リンクの存続時間内に別の EAPOL パケットがポート上で検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴はクリアされます。
- スイッチ ポートがゲスト VLAN（マルチホスト モード）に移動されると、IEEE 802.1x 対応でないクライアントに、アクセスが許可されます。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加わると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN の無許可ステートに移行し、認証が再開されます。

  リモート スイッチド ポート アナライザ（RSPAN）VLAN、音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN 機能は、アクセス ポートでだけサポートされます。内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされません。
- MAC 認証バイパスが IEEE 802.1x ポートでイネーブルの場合に、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、スイッチでは、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。
  - 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。
  - 認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

  詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass」の項を参照してください。

authentication-fail イベントの場合：

- サプリカントが認証に失敗すると、ポートは制限 VLAN に移動され、EAP 成功メッセージがサプリカントに送信されます。これは、サプリカントには実際の認証の失敗が通知されないためです。
  - EAP の成功メッセージが送信されない場合、サプリカントは 60 秒ごと（デフォルト）に EAP 開始メッセージを送信して認証を行おうとします。

  - 一部のホスト（たとえば、Windows XP を実行中のデバイス）は、EAP の成功メッセージを受け取るまで DHCP を実装できません。

  制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でだけサポートされます。ポートが制限 VLAN に配置されると、サプリカントの MAC アドレスが MAC アドレス テーブルに追加されます。ポート上の他の MAC アドレスはすべてセキュリティ違反として扱われます。

- レイヤ 3 ポートの内部 VLAN を制限 VLAN として設定することはできません。同じ VLAN を制限 VLAN としておよび音声 VLAN として指定することはできません。

  制限付き VLAN による再認証。再認証がディセーブルにされていると、制限 VLAN 内のポートは、ディセーブルにされている場合に再認証要求を受け取りません。

  再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol（EAP）ログオフ イベントを受け取る必要があります。ホストがハブ経由で接続されている場合：

  - ホストが切断された場合にポートではリンクダウン イベントを受け取らないことがあります。
  - ポートでは、次の再認証試行が行われるまで、新しいホストを検出しないことがあります。

  制限 VLAN を異なるタイプの VLAN として再設定すると、制限 VLAN のポートも移行され、それらは現在認証されたステートのままになります。

例

次の例では、**authentication event fail** コマンドの設定方法を示します。

```
Switch(config-if)# authentication event fail action authorize vlan 20
```

次の例では、応答なしアクションの設定方法を示します。

```
Switch(config-if)# authentication event no-response action authorize vlan 10
```

次の例では、サーバ応答アクションの設定方法を示します。

```
Switch(config-if)# authentication event server alive action reinitialize
```

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。マルチ認証（multiauth）モードのポートの場合、またはポートの音声ドメインが MDA モードである場合、このコマンドを使用します。

```
Switch(config-if)# authentication event server dead action authorize vlan 10
```

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。ホストが複数のモード、またはマルチ認証（multiauth）モードのポートの場合、このコマンドを使用します。

```
Switch(config-if)# authentication event server dead action reinitialize vlan 10
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication fallback

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にポートを設定するには、インターフェイス コンフィギュレーション モードで **authentication fallback** 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 fallback *name*

no authentication fallback *name*

構文の説明

name	Web 認証のフォールバック プロファイル。

コマンド デフォルト

フォールバックはイネーブルではありません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

フォールバック方式を設定する前に **authentication port-control auto** 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必要があります。

Web 認証をフォールバック方式として設定できるのは、802.1x または MAB に対してだけです。したがってフォールバックできるようにするには、この認証方式の 1 つまたは両方を設定する必要があります。

例

次の例では、ポートのフォールバック プロファイルを指定する方法を示します。

```
Switch(config-if)# authentication fallback profile1
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

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。指定した設定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 host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

no authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

構文の説明

multi-auth	（任意）ポートのマルチ認証モード（multiauth モード）をイネーブルにします。
multi-domain	（任意）ポートのマルチドメイン モードをイネーブルにします。
multi-host	（任意）ポートのマルチホスト モードをイネーブルにします。
single-host	（任意）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
15.0(1)EY	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 Phone 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。

例

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。

```
Switch(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。

```
Switch(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。

```
Switch(config)# 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。

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

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication mac-move permit

スイッチで 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。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 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 移動はイネーブルです。

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
15.0(1)EY	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、スイッチの 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。

例

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
authentication violation	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。
show authentication	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。

authentication open

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 open** コマンドを使用します。オープン アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication open

no authentication open

コマンド デフォルト

オープン アクセスはディセ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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

認証の前にネットワーク アクセスを必要とするデバイスでは、オープン認証がイネーブルにされている必要があります。

オープン認証をイネーブルにしてあるときは、ポート ACL を使用してホスト アクセスを制限する必要があります。

例

次の例では、ポートのオープン アクセスをイネーブルにする方法を示します。

```
Switch(config-if)# authentication open
```

次の例では、ポートのオープン アクセスをディセーブルにするようポートを設定する方法を示します。

```
Switch(config-if)# no authentication open
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。

コマンド	説明
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication order

ポートで使用する認証方式の順序を設定するには、インターフェイス コンフィギュレーション モードで **authentication order** コマンドを使用します。指定した設定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 order [**dot1x** | **mab**] {**webauth**}

no authentication order

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

デフォルトの認証順序は **dot1x**、**mab**、および **webauth** 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
15.0(1)EY	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。リスト内の方式の 1 つで成功しないと、次の方式が試行されます。

各方式は一度だけ試行できます。弾力的順序付けは、802.1x と MAB の間でだけ可能です。

Web 認証は、スタンドアロン方式として設定するか、順序において 802.1x または MAB のいずれかの後で最後の方式として設定することができます。Web 認証は **dot1x** または **mab** に対するフォールバックとしてだけ設定する必要があります。

例

次の例では、最初の認証方式として 802.1x を、2 番めの方式として MAB を、3 番めの方式として Web 認証を追加する方法を示します。

```
Switch(config-if)# authentication order dotx mab webauth
```

次の例では、最初の認証方式として MAC 認証バイパス（MAB）を、2 番めの認証方式として Web 認証を追加する方法を示します。

```
Switch(config-if)# authentication order mab webauth
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。

コマンド	説明
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	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。

authentication periodic

ポートで再認証をイネーブルまたはディセーブルにするには、インターフェイス コンフィギュレーション モードで **authentication periodic** コマンドを使用します。再認証をディセーブルにする場合は、このコマンドの **no** 形式を入力します。

authentication periodic

no authentication periodic

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

再認証はディセ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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

authentication timer 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、定期的に再認証を行う間隔の時間量を設定します。

例

次の例では、ポートの定期的再認証をイネーブルにする方法を示します。

```
Switch(config-if)# authentication periodic
```

次の例では、ポートの定期的再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no authentication periodic
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication port-control

ポートの認証ステートの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication port-control** 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 port-control {**auto** | **force-authorized** | **force-un authorized**}

no authentication port-control {**auto** | **force-authorized** | **force-un authorized**}

構文の説明

auto	ポートの IEEE 802.1x 認証をイネーブルにします。ポートは、IEEE 802.1x 認証情報のスイッチとクライアントの間での交換に基づいて、許可ステートまたは無許可ステートに変わります。
force-authorized	ポートの IEEE 802.1x 認証をディセーブルにします。ポートは、認証情報を交換することなく、許可ステートに変わります。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
force-un authorized	ポートへのアクセスをすべて拒否します。ポートは、クライアントによる認証の試行をすべて無視して、無許可ステートに変わります。スイッチはポートを介してクライアントに認証サービスを提供できません。

コマンド デフォルト

デフォルトの設定は force-authorized です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

auto キーワードは、次のいずれかのポート タイプでだけ使用してください。

- トランク ポート：トランク ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック ポート：ダイナミック ポートは、ネイバーとネゴシエートして、トランク ポートになることができます。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとすると、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミック VLAN に変更しようとすると、エラー メッセージが表示され、VLAN 設定は変更されません。

- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。
- スイッチド ポート アナライザ（SPAN）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

スイッチで IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** 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。特定のポートで IEEE 802.1x 認証をディセーブルにするか、デフォルト設定に戻すには、**no authentication port-control** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポート ステートを自動に設定する方法を示します。

```
Switch(config-if)# authentication port-control auto
```

次の例では、ポート ステートを force- authorized ステートに設定する方法を示します。

```
Switch(config-if)# authentication port-control force-authorized
```

次の例では、ポート ステートを force-unauthorized ステートに設定する方法を示します。

```
Switch(config-if)# authentication port-control force-unauthorized
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication priority

ポート 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。指定した設定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。

auth priority [**dot1x** | **mab**] {**webauth**}

no auth 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
15.0(1)EY	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、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。

例

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

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

次の例では、MAC 認証バイパス（MAB）を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

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

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication timer	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。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	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。

authentication timer

802.1x 対応ポートのタイム アウトと再認証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 **authentication timer** コマンドを使用します。指定した設定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 timer {{[**inactivity** | **reauthenticate**] [**server** | *am*]} {**restart** *value*}}

no authentication timer {{[**inactivity** | **reauthenticate**] [**server** | *am*]} {**restart** *value*}}

構文の説明

inactivity	（任意）この時間間隔を過ぎてもアクティビティがない場合に、クライアントが無許可にされる秒数を指定します。
reauthenticate	（任意）自動再認証の試行を開始するまでの時間を秒単位で指定します。
server	（任意）無許可ポートの認証の試行が行われるまでの間隔を秒単位で指定します。
restart	（任意）無許可ポートの認証の試行が行われるまでの間隔を秒単位で指定します。
value	（任意）1 から 65535 までの値（秒）を入力します。

コマンド デフォルト

inactivity、**server**、および **restart** キーワードは 60 秒に設定されます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

タイムアウト値を設定しないと、802.1x セッションは、無期限で認証されたままになります。他のホストではそのポートを使用できず、接続されているホストは、同じスイッチの別のポートに移動できません。

例

次の例では、認証非アクティビティ タイマーを 60 秒に設定する方法を示します。

```
Switch(config-if)# authentication timer inactivity 60
```

次の例では、再認証タイマーを 120 秒に設定する方法を示します。

```
Switch(config-if)# authentication timer restart 120
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。

コマンド	説明
authentication fallback	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。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。
show authentication	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。

authentication violation

新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、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。指定した設定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 violation {**protect** | **restrict** | **shutdown**}

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

構文の説明

protect	予期しない着信 MAC アドレスはドロップされます。syslog エラーは生成されません。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	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

デフォルトでは、**authentication violation shutdown** モードはイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

例

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。

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

次の例では、新しいデバイスがポートに接続された場合にシステム エラー メッセージを生成し、制限モードに切り替わるように IEEE 802.1x 対応ポートを設定する方法を示します。

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

次の例では、新しいデバイスがポートに接続された場合にそのデバイスを無視するように IEEE 802.1x 対応ポートを設定する方法を示します。

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

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	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。

コマンド	説明
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	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。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	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。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	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。
show authentication	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。

auto qos voip

QoS ドメイン内の Voice over IP（VoIP）の Quality of Service（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos voip** 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。

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

no auto qos voip [**cisco-phone** | **cisco-softphone** | **trust**]

（注） このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

構文の説明

cisco-phone	このポートが Cisco IP Phone に接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。
cisco-softphone	このポートが Cisco SoftPhone が動作している装置に接続されていると判断し、VoIP の QoS を自動設定します。
trust	このポートが信頼できるスイッチまたはルータに接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッド ポートでは、着信パケットの DSCP 値が信頼されます。

コマンド デフォルト

auto-QoS は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、表 2-2 に示すように、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 2-2　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VoIP Control トラフィック	ルーティング プロトコル トラフィック	STP[1] BPDU[2] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[3]	46	24、26	48	56	34	–	
CoS[4]	5	3	6	7	3	–	
CoS から入力キューへのマッピング	2、3、4、5、6、7（キュー 2）					0、1（キュー 1）	
CoS から出力キューへのマッピング	5（キュー 1）	3、6、7（キュー 2）			4（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. STP = スパニングツリー プロトコル
2. BPDU = ブリッジ プロトコル データ ユニット
3. DSCP = Diffserv コード ポイント
4. CoS = Class of Service（サービス クラス）

表 2-3 に、入力キューに対して生成された Auto-QoS の設定を示します。

表 2-3　入力キューに対する Auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	キュー（バッファ）サイズ
SRR [1] 共有	1	0、1	81 %	67 %
Priority	2	2、3、4、5、6、7	19 %	33 %

1. SRR = Shaped Round Robin（シェイプド ラウンド ロビン）。入力キューは共有モードだけをサポートします。

表 2-4 に、出力キューに対して生成される auto-QoS の設定を示します。

表 2-4　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	5	最大 100%	16 %	10%
SRR 共有	2	3、6、7	10%	6 %	10%
SRR 共有	3	2、4	60%	17 %	26 %
SRR 共有	4	0、1	20%	61 %	54 %

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

LAN Base イメージは、2 つの入力キューと 4 つの出力キューをサポートします。

LAN Lite イメージは、入力キューも出力キューもサポートしません。

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ装置などが含まれます。

Auto-QoS は、スイッチとルーテッド ポート上の Cisco IP Phone を使用した VoIP と、Cisco SoftPhone アプリケーションが稼働する装置を使用した VoIP に対してスイッチを設定します。これらのリリースは Cisco IP SoftPhone バージョン 1.3(3) 以降だけをサポートします。接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

show auto qos コマンド出力は Cisco IP Phone のサービス ポリシー情報を表示します。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした *後* で、auto-QoS を調整できます。

（注）　スイッチは、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

最初のポートで auto-QoS 機能をイネーブルにすると、次の自動アクションが実行されます。

- QoS がグローバルにイネーブルになり（**mls qos** グローバル コンフィギュレーション コマンド）、そのあと、他のグローバル コンフィギュレーション コマンドが追加されます。

  スイッチ ポートが Cisco IOS Release 15.0(1) EY で **auto qos voip cisco-phone** 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設定された場合、このリリースでは新しい auto-QoS によって生成されたコマンドは、ポートに適用されません。このようなコマンドを自動的に適用するには、設定を削除してからポートに再度適用する必要があります。

- Cisco SoftPhone が動作する装置に接続されたネットワーク エッジにあるポートに **auto qos voip cisco-softphone** 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、スイッチはポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。スイッチは、表 2-3 および表 2-4 の設定に従ってポート上の入力および出力キューを設定します。

- ネットワーク内部に接続されたポート上で、**auto qos voip trust** 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、スイッチは、入力パケットでルーティングされないポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。スイッチは、表 2-3 および表 2-4 の設定値に従ってポートの入力キューと出力キューを設定します。

スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで auto-QoS をイネーブルにすることができます。ルーテッド ポートにある Cisco IP Phone で auto-QoS をイネーブルにする場合、スタティック IP アドレスを IP Phone に割り当てる必要があります。

（注）　Cisco SoftPhone が稼働する装置がスイッチまたはルーテッド ポートに接続されている場合、スイッチはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。詳細については、**debug auto qos** コマンドを参照してください。

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** 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。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。**no mls qos** 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、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合は、パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念はありません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

例

次の例では、ポートに接続されているスイッチまたはルータが信頼できる装置である場合に、auto-QoS をイネーブルにし、着信パケットで受信した QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

設定を確認するには、**show auto qos interface** *interface-id* 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
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。
mls qos cos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos map {**cos-dscp** *dscp1 ... dscp8* | **dscp-cos** *dscp-list* to *cos*}	CoS/DSCP マップまたは DSCP/CoS マップを定義します。
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue input bandwidth	シェイプド ラウンドロビン（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos trust	ポートの信頼状態を設定します。
queue-set	ポートをキューセットにマッピングします。

コマンド	説明
show auto qos	auto-QoS 情報を表示します。
show mls qos interface	ポート レベルで QoS 情報を表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

boot buffersize

ファイル システムでシミュレートした NVRAM のバッファ サイズを指定するには、グローバル コンフィギュレーション モードで **boot buffersize** 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。

boot buffersize *size*

no boot buffersize *size*

構文の説明

size	NVRAM のシミュレーション バッファ サイズ。有効な値は 4096 ～ 1048576 です。

コマンド デフォルト

デフォルトのファイル システムでシミュレートした NVRAM のブートのバッファ サイズは 65536 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
15.0(1)EY	このコマンドが導入されました。

例

次に、ファイル システムでシミュレートした NVRAM のブートのバッファ サイズを 15000 に変更する例を示します。

```
Switch(config)# boot buffersize 15000
Switch(config)#
```

関連コマンド

コマンド	説明
show boot buffersize	ファイル システムでシミュレートした NVRAM バッファ サイズを表示します。

boot config-file

システム コンフィギュレーションの不揮発性コピーの読み込みおよび書き込みに Cisco IOS が使用するファイル名を指定するには、グローバル コンフィギュレーション モードで **boot config-file** 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。

boot config-file flash:*/file-url*

no boot config-file

構文の説明

flash:*/file-url*	コンフィギュレーション ファイルのパス（ディレクトリ）および名前です。

コマンド デフォルト

デフォルトのコンフィギュレーション ファイルは、flash:config.text 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot enable-break

自動起動プロセスの中断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 **boot enable-break** 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。

boot enable-break

no boot enable-break

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

ディセーブル コンソール上で Break キーを押しても自動ブート プロセスを中断することはできません。

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
15.0(1)EY	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と、フラッシュ ファイル システムが初期化された後で Break キーを押して、自動ブート プロセスを中断できます。

（注）　このコマンドの設定に関係なく、スイッチ前面パネルの MODE ボタンを押すと、いつでも自動ブート プロセスを中断することができます。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot fast

システム障害発生後のスイッチの起動時間を最適化するには、グローバル コンフィギュレーション モードで **boot fast** 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。

boot fast

no boot fast

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

イネーブル

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

このコマンドはデフォルトでイネーブルになっていますが、システム障害発生後はこの機能は自動的にディセーブルになります。

スイッチの起動時間を最適化し、メモリ テスト、ファイル システム チェック（FSCK）、POST プロセスをディセーブルにするには、このコマンドを使用してブート ファスト機能を再びイネーブルにします。

BOOT 環境変数内の情報を使用して自動的にシステムを起動するようスイッチが設定されている場合、次のリロード シーケンスがすぐに発生します。それ以外は、これらのリロード シーケンスはブート ローダ コンフィギュレーション モードで手動 **boot** コマンドを発行した後に発生します。

最初のリロード

このスイッチは boot fast 機能をディセーブルにし、次の警告メッセージを表示します。

```
"Reloading with boot fast feature disabled"
```

システム メッセージが表示された後、システムは crashinfo を保存し、次のリロードのサイクルのために自動的にリセットされます。

2 回めのリロード

ブートローダはフルメモリ テストと LED ステータスの進行状況の FSCK チェックを実行します。メモリ テストと FSCK テストが成功した場合、システムは追加の POST テストを実行し、その結果がコンソールに表示されます。

boot fast 機能は、システムが正常に起動した後に再びイネーブルになります。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper

ブートローダ初期化中にダイナミックにファイルをロードして、ブートローダの機能を拡張またはパッチを当てるには、グローバル コンフィギュレーション モードで **boot helper** コマンドを使用します。このコマンドを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。

boot helper *filesystem*:*/file-url ...*

no boot helper

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	ローダー初期化中に動的にロードするためのパス（ディレクトリ）およびロード可能なファイルのリストです。イメージ名はセミコロンで区切ります。

コマンド デフォルト

ヘルパー ファイルはロードされません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper-config-file

Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前を指定します。これがセットされていない場合は、CONFIG_FILE 環境変数によって指定されたファイルがロードされたすべてのバージョンの Cisco IOS によって使用されます。グローバル コンフィギュレーション モードで **boot helper-config-file** 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。

boot helper-config-file *filesystem*:*/file-url*

no boot helper-config file

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	ロードするパス（ディレクトリ）およびヘルパー コンフィギュレーション ファイル

コマンド デフォルト

ヘルパー コンフィギュレーション ファイルは指定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER_CONFIG_FILE 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot host

ルータ固有のコンフィギュレーション ファイルを最適化するには、グローバル コンフィギュレーション モードで **boot host** 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。

boot host {**dhcp** | **retry timeout** *seconds*}

no boot host {**dhcp** | **retry timeout** *seconds*}

構文の説明

dhcp	DHCP を使用してコンフィギュレーション ファイルをダウンロードします。
retry	コンフィギュレーションのダウンロードを再試行します。
timeout *seconds*	タイムアウトを秒単位でセットします。有効な値は 60 ～ 65535 秒です。

コマンド デフォルト

リトライ タイムアウト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
15.0(1)EY	このコマンドが導入されました。

例

次に、DHCP を使用してルータ固有のコンフィギュレーション ファイルを最適化する例を示します。

```
Switch(config)# boot host dhcp
Switch(config)#
```

次に、リトライ タイムアウトを 120 秒に再設定する例を示します。

```
Switch(config)# boot host retry timeout 120
Switch(config)#
```

次に、リトライ タイムアウトをディセーブルにする例を示します。

```
Switch(config)# no boot host retry timeout 120
Switch(config)#
```

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot manual

次の起動サイクル時にスイッチの手動による起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 **boot manual** 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。

boot manual

no boot manual

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

手動による起動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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

システムを次回再起動すると、スイッチはブートローダ モードで起動します。これは *switch:* プロンプトによってわかります。システムを起動するには、**boot** ブートローダ コマンドを使用して起動可能なイメージの名前を指定します。

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot private-config-file

プライベート コンフィギュレーションの不揮発性コピーの読み込みおよび書き込みに Cisco IOS が使用するファイル名を指定するには、グローバル コンフィギュレーション モードで **boot private-config-file** 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。

boot private-config-file *filename*

no boot private-config-file

構文の説明

filename	プライベート コンフィギュレーション ファイルの名前

コマンド デフォルト

デフォルトのコンフィギュレーション ファイルは、*private-config* 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ファイル名は、大文字と小文字を区別します。

例

次の例では、プライベート コンフィギュレーション ファイルの名前を pconfig と指定する方法を示します。

```
Switch(config)# boot private-config-file pconfig
```

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot system

Cisco IOS イメージを次回の起動サイクル中にロードするように指定するには、グローバル コンフィギュレーション モードで **boot system** 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。

boot system *filesystem*:*/file-url ...*

no boot system

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	ブート可能なイメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。

コマンド デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムを起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

archive download-sw 特権 EXEC コマンドを使用してシステム イメージを保存している場合、**boot system** コマンドを使用する必要はありません。**boot system** コマンドは自動的に処理され、ダウンロードされたイメージがロードされます。

このコマンドは、BOOT 環境変数の設定を変更します。詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

channel-group

イーサネット ポートを EtherChannel グループに割り当て、EtherChannel モードをイネーブルにするか、または両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。イーサネット ポートを EtherChannel グループから削除する場合は、このコマンドの **no** 形式を使用します。

channel-group *channel-group-number* **mode** {**active** | {**auto** [**non-silent**]} | {**desirable** [**non-silent**]} | **on** | **passive**}

no channel-group

PAgP モード:
channel-group *channel-group-number* **mode** {{auto [**non-silent**]} | {**desirable** [**non-silent}}**

LACP モード:
channel-group *channel-group-number* **mode** {**active** | **passive**}

on モード:
channel-group *channel-group-number* **mode on**

構文の説明

channel-group-number	チャネル グループ番号を指定します。指定できる範囲は 1 ～ 6 です。
mode	EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol（LACP）をイネーブルにします。 active モードは、ポートをネゴシエーション ステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポート グループで形成されます。
auto	ポート集約プロトコル（PAgP）デバイスが検出された場合に限り、PAgP をイネーブルにします。 auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。チャネルは、desirable モードの別のポート グループでだけ形成されます。**auto** がイネーブルの場合、サイレント動作がデフォルトになります。
desirable	PAgP を無条件にイネーブルにします。 desirable モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、desirable モードまたは auto モードの別のポート グループで形成されます。**desirable** がイネーブルの場合は、デフォルトでサイレント動作となります。
non-silent	（任意）他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。

on	on モードをイネーブルにします。 on モードでは、使用可能な EtherChannel が存在するのは、両方の接続ポート グループが on モードになっている場合だけです。
passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。 passive モードは、ポートをネゴシエーション ステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。チャネルは、active モードの別のポート グループでだけ形成されます。

コマンド デフォルト

チャネル グループは割り当てることができません。

モード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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 EtherChannel の場合、物理ポートをチャネル グループに割り当てる前に、先に **interface port-channel** 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ポートチャネル インターフェイスを作成しておく必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。論理インターフェイスがまだ作成されていない場合は、チャネル グループが最初の物理ポートを取得した時点で、自動的にポートチャネル インターフェイスが作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

チャネル グループの一部である物理ポートに割り当てられた IP アドレスをディセーブルにする必要はありませんが、これをディセーブルにすることを強く推奨します。

interface port-channel コマンドの次に **no switchport** 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、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポート チャネルの論理インターフェイスを手動で設定してください。

EtherChannel を設定した後、ポートチャネル インターフェイスに加えられた設定の変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

auto モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント モードを設定するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、物理ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネル グループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

on モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。

注意　**on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP が稼働している複数の EtherChannel グループは、同じスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol 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プロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては上書きされません。

アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。

セキュア ポートを EtherChannel の一部として、または EtherChannel ポートをセキュア ポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

注意　物理 EtherChannel ポート上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジ グループを割り当てることは、ループが発生する原因になるため、行わないでください。

例

次に、EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを PAgP モード **desirable** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

次に、EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを LACP モード **active** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

関連コマンド

コマンド	説明
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。
show pagp	PAgP チャネル グループ情報を表示します。

channel-protocol

チャネリングを管理するため、ポート上で使用されるプロトコルを制限するには、インターフェイス コンフィギュレーション モードで **channel-protocol** 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。

channel-protocol {**lacp** | **pagp**}

no channel-protocol

構文の説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	ポート集約プロトコル（PAgP）で EtherChannel を設定します。

コマンド デフォルト

EtherChannel に割り当てられているプロトコルはありません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定は **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

channel-group インターフェイス コンフィギュレーション コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

例

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
Switch(config-if)# channel-protocol lacp
```

設定を確認するには、**show etherchannel** [*channel-group-number*] **protocol** 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
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel protocol	EtherChannel のプロトコル情報を表示します。

cip enable

VLAN の Common Industrial Protocol（CIP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **cip enable** コマンドを使用します。CIP 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。

cip enable

no cip 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

デフォルトでは、すべての VLAN で CIP 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

インターフェイスには物理インターフェイスではなく、VLAN を使用します。

CIP はスイッチの VLAN で 1 つのみイネーブルにできます。

CIP をイネーブルにする際は、CIP セキュリティ パスワードを設定することを推奨します。

例

次に、VLAN 3 で CIP をイネーブルにする例を示します。

```
Switch(config)# interface vlan 20
Switch(config-if)# cip enable
```

次の例では、2 つめの VLAN で CIP をイネーブルにしようとすると表示されるメッセージを示します。

```
Switch(config)# interface vlan 3
Switch(config-if)# cip enable
CIP is already enabled on Vlan 20
```

関連コマンド

コマンド	説明
cip security	CIP セキュリティ オプションを設定します。
show cip	CIP サブシステムに関する情報を表示します。

cip security

スイッチに Common Industrial Protocol（CIP）セキュリティ オプションを設定するには、グローバル コンフィギュレーション モードで **cip security** コマンドを使用します。パスワードの中止またはタイムアウト値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

cip security {**password** *password* | **window timeout** *value*}

no cip security {**password** *password* | **window timeout**}

構文の説明

password *password*	CIP セキュリティの ASCII パスワードを設定します。
window timeout	CIP セキュリティ ウィンドウのタイムアウトを設定します。
value	CIP セキュリティ ウィンドウのタイムアウト値を設定します。指定できる範囲は 1 ～ 3600 秒です。デフォルトは 600 秒です。

コマンド デフォルト

パスワード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
15.0(1)EY	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 で CIP をイネーブルにする際は、CIP セキュリティ パスワードを設定することを推奨します。設定しないと、すべての CIP ユーザがスイッチを設定できます。

例

次の例では、CIP セキュリティ ウィンドウのタイムアウト値を 1 時間に設定する方法を示します。

```
Switch(config)# cip security window timeout 3600
```

次の例では、CIP セキュリティ パスワードを 123 に設定する方法を示します。

```
Switch(config)# cip security password abc123
```

関連コマンド

コマンド	説明
cip enable	VLAN 上で CIP をイネーブルにします。
show cip	CIP サブシステムに関する情報を表示します。

cisp enable

スイッチがサプリカント 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スイッチの Client Information Signalling Protocol（CISP）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 **cisp enable** コマンドを使用します。

cisp enable

no cisp enable

構文の説明

cisp enable	CISP をイネーブルにします。

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
15.0(1)EY	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プリカント 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 モードがサーバである必要があります。

VTP モードを設定する場合は、MD5 チェックサムの不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。

例

次の例では、CISP をイネーブルにする方法を示します。

```
switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials（グローバル コンフィギュレーション）*profile*	プロファイルをサプリカント スイッチに設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

class

指定のクラスマップ名のトラフィック分類の一致基準を（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用して）定義するには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

class *class-map-name*

no class *class-map-name*

構文の説明

class-map-name	クラス マップ名です。

コマンド デフォルト

ポリシー マップ クラス マップは定義されていません。

コマンド モード

ポリシー 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用する前に、**policy-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ポリシー マップを識別し、ポリシー マップ コンフィギュレーション モードを開始する必要があります。ポリシー マップを指定すると、ポリシー マップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** 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、ポリシー マップをポートへ添付することができます。

class コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **exit**：ポリシーマップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをそのデフォルト設定に戻します。
- **police**：分類したトラフィックのポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** および **police aggregate** ポリシーマップ クラス コマンドを参照してください。
- **set**：分類したトラフィックに割り当てる値を指定します。詳細については、**set** コマンドを参照してください。
- **trust**：**class** コマンドまたは **class-map** コマンドで分類したトラフィックの信頼状態を定義します。詳細については、**trust** コマンドを参照してください。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

例

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。このコマンドが入力方向に添付された場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP Diffserv コードポイント（DSCP）を 10 に設定し、平均レート 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超過するトラフィックは、ポリシング設定 DSCP マップから受信した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

設定を確認するには、**show policy-map** 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
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。
trust	**class** ポリシー マップ コンフィギュレーション コマンドまたは **class-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分類されたトラフィックの信頼状態を定義します。

class-map

指定したクラス名とパケットとの照合に使用するクラス マップを作成して、クラスマップ 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 **class-map** コマンドを使用します。既存のクラス マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*

構文の説明

match-all	（任意）このクラス マップ内のすべての一致ステートメントの論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
match-any	（任意）このクラス マップ内の一致ステートメントの論理和をとります。1 つ以上の条件が一致していなければなりません。
class-map-name	クラス マップ名です。

コマンド デフォルト

クラス マップは定義されていません。

match-all または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

クラス マップ一致基準を作成または変更するクラスの名前を指定し、クラス マップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。

グローバルに名前が付けられたポートごとに適用されるサービス ポリシーの一部としてパケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

Quality of Service（QoS）クラスマップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドを利用することができます。

- **description**：クラス マップを説明します（最大 200 文字）。s**how class-map** 特権 EXEC コマンドは、クラスマップの説明と名前を表示します。
- **exit**：QoS クラスマップ コンフィギュレーション モードを終了します。
- **match**：分類基準を設定します。詳細については、**match（クラスマップ コンフィギュレーション）**コマンドを参照してください。
- **no**：クラス マップから一致ステートメントを削除します。
- **rename**：現在のクラス マップの名前を変更します。クラス マップ名をすでに使用されている名前に変更すると、「`A class-map with this name already exists`」というメッセージが表示されます。

物理ポート単位でパケット分類を定義するため、クラス マップごとに 1 つずつに限り **match** コマンドがサポートされています。この状況では、**match-all** キーワードと **match-any** キーワードは同じです。

1 つのクラス マップで設定できるアクセス コントロール リスト（ACL）は 1 つだけです。ACL には複数のアクセス コントロール エントリ（ACE）を含めることができます。

例

次の例では、クラス マップ class1 に 1 つの一致基準（アクセス リスト 103）を設定する方法を示します。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次の例では、クラス マップ class1 を削除する方法を示します。

```
Switch(config)# no class-map class1
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる）を定義します。
match（クラスマップ コンフィギュレーション）	トラフィックを分類するための一致条件を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show class-map	QoS クラス マップを表示します。

clear dot1x

スイッチまたは指定したポートの IEEE 802.1x 情報をクリアするには、特権 EXEC モードで **clear dot1x** コマンドを使用します。

clear dot1x {**all** | **interface** *interface-id*}

構文の説明

all	スイッチのすべての IEEE 802.1x 情報をクリアします。
interface *interface-id*	指定したインターフェイスの IEEE 802.1x 情報をクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

clear dot1x all コマンドを使用して、すべての情報をクリアできます。また、**clear dot1x interface** *interface-id* コマンドを使用して、指定されたインターフェイスの情報だけをクリアできます。

例

次の例では、すべての IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x all
```

次の例では、指定されたインターフェイスの IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x interface gigabithethernet1/1
```

情報が削除されたかどうかを確認するには、**show dot1x** 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
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します。

clear eap sessions

スイッチまたは指定したポートの Extensible Authentication Protocol（EAP）セッション情報をクリアするには、特権 EXEC モードで **clear eap sessions** コマンドを使用します。

clear eap sessions [**credentials** *name* [**interface** *interface-id*] | **interface** *interface-id* | **method** *name* | **transport** *name*] [**credentials** *name* | **interface** *interface-id* | **transport** *name*] ...

構文の説明

credentials *name*	（任意）指定したプロファイルの EAP クレデンシャル情報をクリアします。
interface *interface-id*	（任意）指定したインターフェイスの EAP 情報をクリアします。
method *name*	（任意）指定した方式の EAP 情報をクリアします。
transport *name*	（任意）指定した下位レベルの EAP トランスポート情報をクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

clear eap sessions コマンドを使用して、すべてのカウンタをクリアできます。キーワードを使用して、特定の情報だけをクリアできます。

例

次の例では、すべての EAP 情報をクリアする方法を示します。

```
Switch# clear eap
```

次の例では、指定されたプロファイルの EAP セッション クレデンシャル情報をクリアする方法を示します。

```
Switch# clear eap sessions credential type1
```

情報が削除されたかどうかを確認するには、**show dot1x** 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
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

clear errdisable interface

errdisable になっている 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

vlan list	（任意）再びイネーブルにする VLAN のリスト。VLAN リストを指定しない場合、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

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
15.0(1)EY	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 interface** コマンドを使用して VLAN の errdisable をクリアできます。

例

次に、ポート 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例を示します。

```
Switch# clear errdisable interface GigabitEthernet1/2 vlan
```

関連コマンド

コマンド	説明
errdisable detect cause	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。
errdisable recovery	回復メカニズム変数を設定します。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	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 arp inspection log

ダイナミックな Address Resolution Protocol（ARP）インスペクション ログ バッファをクリアするには、特権 EXEC モードで **clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

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

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
Switch# clear ip arp inspection log
```

ログがクリアされたかどうかを確認するには、**show ip arp inspection log** 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
arp access-list	ARP アクセス コントロール リスト（ACL）を定義します。
ip arp inspection log-buffer	ダイナミック ARP インスペクション ロギング バッファを設定します。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show inventory log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

clear ip arp inspection statistics

ダイナミックな Address Resolution Protocol（ARP）インスペクション統計情報をクリアするには、特権 EXEC モードで **clear ip arp inspection statistics** コマンドを使用します。

clear ip arp inspection statistics [**vlan** *vlan-range*]

構文の説明

vlan *vlan-range*	（任意）指定した 1 つ以上の VLAN の統計情報をクリアします。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、VLAN 1 の統計情報をクリアする方法を示します。

```
Switch# clear ip arp inspection statistics vlan 1
```

統計情報が削除されたかどうかを確認するには、**show ip arp inspection statistics vlan 1** 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
show inventory statistics	すべての VLAN または指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、および IP 検証に失敗したパケットの統計情報を表示します。

clear ip dhcp snooping

DHCP スヌーピング バインディング データベース、DHCP スヌーピング バインディング データベース エージェント統計情報、または DHCP スヌーピング統計カウンタをクリアするには、特権 EXEC モードで **clear ip dhcp snooping** コマンドを使用します。

clear ip dhcp snooping {**binding** {***** | *ip-address* | **interface** *interface-id* | **vlan** *vlan-id*} | **database statistics** | **statistics**}

構文の説明

binding	DHCP スヌーピング バインディング データベースを消去します。
*****	すべての自動バインディングをクリアします。
ip-address	バインディング エントリ IP アドレスをクリアします。
interface *interface-id*	バインディング入力インターフェイスをクリアします。
vlan *vlan-id*	バインディング エントリ VLAN をクリアします。
database statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。
statistics	DHCP スヌーピング統計カウンタをクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

clear ip dhcp snooping database statistics コマンドを入力すると、スイッチは統計情報をクリアする前にバインディング データベースおよびバインディング ファイル内のエントリを更新しません。

例

次の例では、DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアする方法を示します。

```
Switch# clear ip dhcp snooping database statistics
```

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

次の例では、DHCP スヌーピング統計カウンタをクリアする方法を示します。

```
Switch# clear ip dhcp snooping statistics
```

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントまたはバインディング ファイルを設定します。
show ip dhcp snooping binding	DHCP スヌーピング データベース エージェントのステータスを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントの統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を表示します。

clear ipc

プロセス間通信（IPC）プロトコルの統計情報をクリアするには、特権 EXEC モードで **clear ipc** コマンドを使用します。

clear ipc {**queue-statistics** | **statistics**}

（注）　このコマンドは、スイッチで IP サービス イメージが稼働されている場合にのみ表示されます。

構文の説明

queue-statistics	すべてのキュー統計情報をクリアします。
statistics	統計情報をクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

clear ipc statistics コマンドを使用してすべての統計情報をクリアできますが、**clear ipc queue-statistics** コマンドを使用してキューの統計情報だけをクリアすることもできます。

例

次の例では、すべての統計情報をクリアする方法を示します。

```
Switch# clear ipc statistics
```

次の例では、キューの統計情報だけをクリアする方法を示します。

```
Switch# clear ipc queue-statistics
```

統計情報が削除されたかどうかを確認するには、**show ipc rpc** または **show ipc session** 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
show ipc {**rpc** | **session**}	IPC マルチキャスト ルーティングの統計情報を表示します。

clear ipv6 dhcp conflict

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバ データベースからアドレス競合をクリアするには、特権 EXEC モードで **clear ipv6 dhcp conflict** コマンドを使用します。

clear ipv6 dhcp conflict {***** | *IPv6-address*}

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

構文の説明

*****	すべてのアドレス競合。
IPv6-address	競合するアドレスを含むホスト IPv6 アドレスをクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**} グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

アドレス パラメータとしてアスタリスク（*****）文字を使用すると、DHCP はすべての競合をクリアします。

例

次の例では、DHCPv6 サーバ データベースからすべてのアドレス競合をクリアする方法を示します。

```
Switch# clear ipv6 dhcp conflict *
```

関連コマンド

コマンド	説明
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

clear lacp

Link Aggregation Control Protocol（LACP）のチャネル グループのカウンタをクリアするには、特権 EXEC モードで **clear lacp** コマンドを使用します。

clear lacp {*channel-group-number* **counters** | **counters**}

構文の説明

channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 48 です。
counters	トラフィック カウンタをクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

clear lacp counters コマンドを使用することで、カウンタをすべてクリアできます。また、指定のチャネル グループのカウンタだけをクリアする場合には、**clear lacp** *channel-group-number* **counters** コマンドを使用します。

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear lacp 4 counters
```

情報が削除されたかどうかを確認するには、**show lacp counters** または **show lacp 4 counters** 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
show lacp	LACP チャネル グループ情報を表示します。

clear mac address-table

MAC アドレス テーブルから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、または特定の VLAN 上のすべてのダイナミック アドレスを削除するには、特権 EXEC モードで **clear mac address-table** コマンドを使用します。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*] | **notification**}

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address *mac-addr*	（任意）指定したダイナミック MAC アドレスを削除します。
interface *interface-id*	（任意）指定し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。
vlan *vlan-id*	（任意）指定した 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。
notification	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

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
15.0(1)EY	このコマンドが導入されました。

例

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。

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

show mac address-table 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
show mac access-group	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。
show mac address-table notification	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。
snmp trap mac-notification change	特定のインターフェイス上の簡易ネットワーク管理プロトコル（SNMP）MAC アドレス通知トラップをイネーブルにします。

clear mac address-table move update

MAC アドレス テーブル移行更新関連カウンタをクリアするには、特権 EXEC モードで **clear mac address-table move update** コマンドを使用します。

clear mac address-table move update

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

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、MAC アドレス テーブル移行更新関連カウンタをクリアする方法を示します。

```
Switch# clear mac address-table move update
```

show mac address-table move update 特権 EXEC コマンドを入力することにより、情報がクリアされたかどうかを確認できます。

関連コマンド

コマンド	説明
mac address-table move update {**receive** | **transmit**}	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。
show mac address-table move update	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。

clear nmsp statistics

ネットワーク モビリティ サービス プロトコル（NMSP）の統計情報をクリアするには、特権 EXEC モードで **clear nmsp statistics** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

clear nmsp statistics

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

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、NMSP の統計情報をクリアする方法を示します。

```
Switch# clear nmsp statistics
```

show nmsp statistics 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
show nmsp	NMSP 情報を表示します。

clear pagp

ポート集約プロトコル（PAgP）のチャネル グループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

clear pagp {*channel-group-number* **counters** | **counters**}

構文の説明

channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 6 です。
counters	トラフィック カウンタをクリアします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、**clear pagp** *channel-group-number* **counters** コマンドを使用すると、指定のチャネル グループのカウンタだけをクリアできます。

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear pagp 10 counters
```

情報が削除されたかどうかを確認するには、**show pagp** 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
show pagp	PAgP チャネル グループ情報を表示します。

clear port-security

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定のタイプ（configured、dynamic、または sticky）のすべてのセキュア アドレスを削除するには、特権 EXEC モードで **clear port-security** コマンドを使用します。

clear port-security {**all** | **configured** | **dynamic** | **sticky**} [[**address** *mac-addr* | **interface** *interface-id*] [**vlan** {*vlan-id* | {**access** | **voice**}}]]

構文の説明

all	すべてのセキュア MAC アドレスを削除します。
configured	設定済みセキュア MAC アドレスを削除します。
dynamic	ハードウェアによって自動学習されたセキュア MAC アドレスを削除します。
sticky	自動学習または設定済みのいずれかのセキュア MAC アドレスを削除します。
address *mac-addr*	（任意）指定したダイナミック セキュア MAC アドレスを削除します。
interface *interface-id*	（任意）指定した物理ポートまたは VLAN 上のすべてのダイナミック セキュア MAC アドレスを削除します。
vlan	（任意）指定した VLAN から指定したセキュア MAC アドレスを削除します。**vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポート上で、クリアする必要のあるアドレスの VLAN の VLAN ID を指定します。 • **access**：アクセス ポートで、アクセス VLAN 上の指定したセキュア MAC アドレスをクリアします。 • **voice**：アクセス ポートで、音声 VLAN 上の指定したセキュア MAC アドレスをクリアします。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、MAC アドレス テーブルからすべてのセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security all
```

次の例では、MAC アドレス テーブルから特定の設定済みセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security configured address 0008.0070.0007
```

次の例では、特定のインターフェイスで学習されたすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic interface gigabitethernet1/1
```

次の例では、アドレス テーブルからすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic
```

show port-security 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
switchport port-security	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します。
switchport port-security mac-address *mac-address*	セキュア MAC アドレスを設定します。
switchport port-security maximum *value*	セキュア インターフェイスにセキュア MAC アドレスの最大数を設定します。
show port-security	インターフェイスまたはスイッチに定義されたポート セキュリティ設定を表示します。

clear psp counter

すべてのプロトコルについてドロップされたパケットのプロトコル ストーム プロテクション カウンタをクリアするには、特権 EXEC モードで **clear psp counter** コマンドを使用します。

clear psp counter [**arp** | **igmp** | **dhcp**]

構文の説明

arp	（任意）ARP および ARP スヌーピングのドロップされたパケットのカウンタをクリアします。
dhcp	（任意）DHCP および DHCP スヌーピングのドロップされたパケットのカウンタをクリアします。
igmp	（任意）IGMP および IGMP スヌーピングのドロップされたパケットのカウンタをクリアします。

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
15.0(58)SE	このコマンドが導入されました。

例

この例では、DHCP のプロトコル ストーム プロテクション カウンタがクリアされます。

```
Switch# clear psp counter dhcp
Switch#
```

関連コマンド

コマンド	説明
psp	ARP、DHCP、または IGMP のプロトコル ストーム プロテクションを設定します。
show psp config	プロトコル ストーム プロテクションの設定を表示します。
show psp statistics	ドロップされたパケットの数を表示します。

clear rep counters

指定したインターフェイスまたはすべてのインターフェイスの Resilient Ethernet Protocol（REP）カウンタをクリアするには、特権 EXEC モードで **clear rep counters** コマンドを使用します。

clear rep counters [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）カウンタをクリアする REP インターフェイスを指定します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

すべての REP カウンタをクリアするには、**clear rep counters** コマンドを使用します。また、**clear rep counters interface** *interface-id* コマンドを使用すると、そのインターフェイスのカウンタだけをクリアできます。

clear rep counters コマンドを入力すると、**show interface rep detail** コマンドの出力に表示されるカウンタだけをクリアできます。SNMP に表示されるカウンタは読み取り専用であるため、クリアできません。

例

次の例では、すべての REP インターフェイスのすべての REP カウンタをクリアする方法を示します。

```
Switch# clear rep counters
```

REP 情報が削除されたかどうかを確認するには、**show interfaces rep detail** 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
show interfaces rep detail	REP の設定およびステータス情報の詳細を表示します。

clear spanning-tree counters

スパニングツリーのカウンタをクリアするには、特権 EXEC モードで **clear spanning-tree counters** コマンドを使用します。

clear spanning-tree counters [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニングツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネルの範囲は 1 ～ 6 です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

interface-id 値が指定されていない場合は、すべてのインターフェイスのスパニングツリー カウンタがクリアされます。

例

次の例では、すべてのインターフェイスのスパニングツリー カウンタをクリアする方法を示します。

```
Switch# clear spanning-tree counters
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステート情報を表示します。

clear spanning-tree detected-protocols

すべてのインターフェイスまたは指定したインターフェイスでプロトコル移行プロセスを再開（強制的に近接スイッチと再びネゴシエートさせる）するには、特権 EXEC モードで **clear spanning-tree detected-protocols** コマンドを使用します。

clear spanning-tree detected-protocols [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）指定したインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 6 です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus（RPVST+）プロトコルまたは Multiple Spanning Tree Protocol（MSTP）が稼働するスイッチは、組み込み済みのプロトコル移行メカニズムをサポートしています。それによって、スイッチはレガシー IEEE 802.1D スイッチと相互に動作できるようになります。RPVST+ スイッチまたは MSTP スイッチが、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーション ブリッジ プロトコル データ ユニット（BPDU）を受信した場合は、そのポートで IEEE 802.1D BPDU だけを送信します。マルチ スパニングツリー（MST）スイッチが、レガシー BPDU、別のリージョンに関連付けられた MST BPDU（バージョン 3）、または高速スパニングツリー（RST）BPDU（バージョン 2）を受信したときは、そのポートがリージョンの境界にあることも検出できます。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなった場合は、自動的に RPVST+ モードまたは MSTP モードには戻りません。これは、レガシー スイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

例

次に、ギガビット イーサネット ポート上でプロトコル移行プロセスを再開する例を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet1/1
```

次に、ファスト イーサネット ポートでプロトコル移行プロセスを再開する例を示します。

```
Switch# clear spanning-tree detected-protocols interface fastethernet1/1
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステート情報を表示します。
spanning-tree link-type	デフォルト リンクタイプ設定を上書きし、スパニングツリーがフォワーディング ステートに高速移行できるようにします。

clear vmps statistics

VLAN Query Protocol（VQP）クライアントが保持する統計情報をクリアするには、特権 EXEC モードで **clear vmps statistics** コマンドを使用します。

clear vmps statistics

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

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、VLAN メンバーシップ ポリシー サーバ（VMPS）統計情報をクリアする方法を示します。

```
Switch# clear vmps statistics
```

情報が削除されたかどうかを確認するには、**show vmps statistics** 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
show vmps	VQP バージョン、再確認間隔、再試行回数、VMPS IP アドレス、および現在のサーバとプライマリ サーバを表示します。

clear vtp counters

VLAN トランキング プロトコル（VTP）とプルーニング カウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

clear vtp counters

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

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

情報が削除されたかどうかを確認するには、**show vtp counters** 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
show vtp	VTP 管理ドメイン、ステータス、カウンタの一般情報を表示します。

cluster commander-address

クラスタ メンバ スイッチがクラスタに加入した場合に、MAC アドレスをそのクラスタ メンバ スイッチに自動的に提供するには、グローバル コンフィギュレーション モードの cluster commander-address コマンドを使用します。デバッグまたはリカバリ手順の間だけスイッチをクラスタから削除する場合は、クラスタ メンバ スイッチ コンソール ポートから、このコマンドの **no** 形式を使用します。

cluster commander-address *mac-address* [**member** *number* **name** *name*]

no cluster commander-address

構文の説明

mac-address	クラスタ コマンド スイッチの MAC アドレス
member *number*	（任意）設定されたクラスタ メンバ スイッチの番号を指定します。指定できる範囲は 0 ～ 15 です。
name *name*	（任意）設定されたクラスタの名前を指定します（最大 31 文字）。

コマンド デフォルト

このスイッチはどのクラスタのメンバでもありません。

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
15.0(1)EY	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、スタンドアロン クラスタ メンバ スイッチから 入力する必要はありません。クラスタ コマンド スイッチは、メンバ スイッチがクラスタに加入した場合に、MAC アドレスをそのメンバ スイッチに自動的に提供します。クラスタ メンバ スイッチは、この情報および他のクラスタ情報をその実行コンフィギュレーション ファイルに追加します。

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。

各クラスタ メンバは、クラスタ コマンド スイッチを 1 つしか持てません。

クラスタ メンバ スイッチは、*mac-address* パラメータによりシステム リロード中にクラスタ コマンド スイッチの ID を保持します。

特定のクラスタ メンバ スイッチで **no** 形式を入力すると、デバッグまたはリカバリ手順の間そのクラスタ メンバ スイッチをクラスタから削除できます。通常は、メンバがクラスタ コマンド スイッチと通信ができなくなった場合にだけ、クラスタ メンバ スイッチ コンソール ポートからこのコマンドを使用することになります。通常のスイッチ構成では、クラスタ コマンド スイッチで **no cluster member** *n* グローバル コンフィギュレーション コマンドを入力することによってだけ、クラスタ メンバ スイッチを削除することを推奨します。

スタンバイ クラスタ コマンド スイッチがアクティブになった場合（クラスタ コマンド スイッチになった場合）、このスイッチは cluster commander-address 行をその設定から削除します。

例

次の例では、実行中のクラスタ メンバの設定から、その出力を一部示します。

```
Switch(config)# show running-configuration

<output truncated>

cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster

<output truncated>
```

次の例では、クラスタ メンバ コンソールでクラスタからメンバを削除する方法を示します。

```
Switch # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no cluster commander-address
```

設定を確認するには、**show cluster** 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
debug cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster discovery hop-count

候補スイッチの拡張検出を行うためのホップカウント制限を設定するには、クラスタ コマンド 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 **cluster discovery hop-count** 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。

cluster discovery hop-count *number*

no cluster discovery hop-count

構文の説明

number	クラスタ コマンド スイッチが候補の検出を制限するクラスタ エッジからのホップの数。指定できる範囲は 1 ～ 7 です。

コマンド デフォルト

ホップ カウントは 3 に設定されています。

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
15.0(1)EY	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、クラスタ コマンド スイッチ上でだけ使用できます。このコマンドは、クラスタ メンバ スイッチでは機能しません。

ホップ カウントが 1 に設定された場合、拡張検出はディセーブルになります。クラスタ コマンド スイッチは、クラスタのエッジから 1 ホップの候補だけを検出します。クラスタのエッジとは、最後に検出されたクラスタのメンバ スイッチと最初に検出された候補スイッチの間の点です。

例

次の例では、ホップ カウント制限を 4 に設定する方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster discovery hop-count 4
```

設定を確認するには、**show cluster** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。

cluster enable

スイッチをクラスタ コマンド スイッチとしてイネーブルにするにはクラスタ名を割り当て、任意でメンバ番号を割り当てるには、コマンド対応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 **cluster enable** コマンドを使用します。すべてのメンバを削除して、このクラスタ コマンド スイッチを候補スイッチにするには、このコマンドの **no** 形式を使用します。

cluster enable *name* [*command-switch-member-number*]

no cluster enable

構文の説明

name	クラスタ名（最大 31 文字）。指定できる文字は、英数字、ダッシュ、および下線だけです。
command-switch-member-number	（任意）クラスタのクラスタ コマンド スイッチにメンバ番号を割り当てます。指定できる範囲は 0 ～ 15 です。

コマンド デフォルト

このスイッチはクラスタ コマンド スイッチではありません。

クラスタ名は定義されません。

スイッチがクラスタ コマンド スイッチである場合、メンバ番号は 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
15.0(1)EY	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、どのクラスタにも属していない任意のコマンド対応スイッチ上で入力します。装置がすでにクラスタのメンバとして設定されている場合、コマンドはエラーとなります。

クラスタ コマンド スイッチをイネーブルにするときには、クラスタに名前を付けてください。スイッチがすでにクラスタ コマンド スイッチとして設定されており、クラスタ名が以前の名前と異なっている場合、コマンドはクラスタ名を変更します。

例

次の例では、クラスタ コマンド スイッチをイネーブルにし、クラスタに名前を付け、クラスタ コマンド スイッチ メンバ番号を 4 に設定する方法を示します。

```
Switch(config)# cluster enable Engineering-IDF4 4
```

設定を確認するには、クラスタ コマンド スイッチで **show cluster** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster holdtime

ハートビート メッセージを受信しなくなってから、スイッチ（コマンドまたはクラスタ メンバ スイッチ）が他のスイッチのダウンを宣言するまでの期間を秒単位で設定するには、グローバル コンフィギュレーション モードで **cluster holdtime** コマンドを使用します。期間をデフォルト値に設定する場合は、このコマンドの **no** 形式を使用します。

cluster holdtime *holdtime-in-secs*

no cluster holdtime

構文の説明

holdtime-in-secs	スイッチ（コマンドまたはクラスタ メンバ スイッチ）が、他のスイッチのダウンを宣言するまでの期間（秒）。指定できる範囲は 1 ～ 300 秒です。

コマンド デフォルト

デフォルトのホールド時間は 80 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

クラスタ コマンド スイッチ上でだけ、このコマンドと **cluster timer** 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ください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。

ホールドタイムは通常インターバル タイマー（**cluster timer**）の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールド タイムをインターバル タイムで割った秒数」回のハートビート メッセージが連続して受信されなかったことになります。

例

次の例では、クラスタ コマンド スイッチでインターバル タイマーおよびホールド タイム時間を変更する方法を示します。

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster member

候補をクラスタに追加するには、クラスタ コマンド スイッチでグローバル コンフィギュレーション モードで **cluster member** コマンドを使用します。メンバをクラスタから削除するには、このコマンドの **no** 形式を使用します。

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]

no cluster member *n*

構文の説明

n	（任意）クラスタ メンバを識別する番号。指定できる範囲は 0 ～ 15 です。
mac-address *H.H.H*	クラスタ メンバ スイッチの MAC アドレス（16 進数）を指定します。
password *enable-password*	（任意）候補スイッチのパスワードをイネーブルにします。候補スイッチにパスワードがない場合、パスワードは必要ありません。
vlan *vlan-id*	（任意）クラスタ コマンド スイッチが候補をクラスタに追加するときに使用される VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

新しくイネーブルになったクラスタ コマンド スイッチには、関連するクラスタ メンバはありません。

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
15.0(1)EY	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、候補をクラスタに追加したり、メンバをクラスタから削除したりする場合にクラスタ コマンド スイッチでだけ入力できます。このコマンドをクラスタ コマンド スイッチ以外のスイッチで入力すると、スイッチはコマンドを拒否し、エラー メッセージを表示します。

スイッチをクラスタから削除する場合はメンバ番号を入力してください。ただし、スイッチをクラスタに追加する場合には、メンバ番号を入力する必要はありません。クラスタ コマンド スイッチは、次に利用可能なメンバ番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

候補スイッチがクラスタに加入した場合には、認証を行うためにそのスイッチのイネーブル パスワードを入力してください。パスワードは、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションには保存されません。候補スイッチがクラスタのメンバになった後、そのパスワードはクラスタ コマンド スイッチ パスワードと同じになります。

スイッチが、設定されたホスト名を持たない場合、クラスタ コマンド スイッチは、メンバ番号をクラスタ コマンド スイッチ ホスト名に追加し、これをクラスタ メンバ スイッチに割り当てます。

VLAN ID を指定していない場合、クラスタ コマンド スイッチは自動的に VLAN を選択し、候補をクラスタに追加します。

例

次の例では、スイッチをメンバ 2、MAC アドレス 00E0.1E00.2222、パスワード *key* としてクラスタに追加する方法を示しています。クラスタ コマンド スイッチは、VLAN 3 を経由して候補をクラスタに追加します。

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

次の例では、MAC アドレス 00E0.1E00.3333 のスイッチをクラスタに追加する方法を示します。このスイッチにはパスワードはありません。クラスタ コマンド スイッチは、次に利用可能なメンバ番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

設定を確認するには、クラスタ コマンド スイッチで **show cluster members** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。
show cluster members	クラスタ メンバに関する情報を表示します。

cluster outside-interface

クラスタのネットワーク アドレス変換（NAT）の外部インターフェイスを設定し、IP アドレスのないメンバがクラスタの外部にある装置と通信できるようにするには、グローバル コンフィギュレーション モードで **cluster outside-interface** 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。

cluster outside-interface *interface-id*

no cluster outside-interface

構文の説明

interface-id	外部インターフェイスとして機能するインターフェイス。有効なインターフェイスとしては、物理インターフェイス、ポート チャネル、または VLAN があります。ポート チャネル範囲は 1 ～ 6 です。指定できる VLAN 範囲は 1 ～ 4094 です。

コマンド デフォルト

デフォルトの外部インターフェイスは、クラスタ コマンド スイッチによって自動的に選択されます。

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
15.0(1)EY	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、クラスタ コマンド スイッチ上でだけ入力できます。クラスタ メンバ スイッチでコマンドを入力すると、エラー メッセージが表示されます。

例

次の例では、VLAN 1 に外部インターフェイスを設定する方法を示します。

```
Switch(config)# cluster outside-interface vlan 1
```

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
show running-config	現在の動作設定を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

cluster run

スイッチでクラスタリング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 **cluster run** コマンドを使用します。スイッチでクラスタリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

cluster run

no cluster run

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

すべてのスイッチでクラスタリングがイネーブルです。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

クラスタ コマンド スイッチ上で **no cluster run** コマンドを入力すると、クラスタ コマンド スイッチはディセーブルになります。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタ メンバ スイッチで **no cluster run** コマンドを入力すると、このメンバ スイッチはクラスタから削除されます。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタに属していないスイッチで **no cluster run** コマンドを入力すると、クラスタリングはそのスイッチ上でディセーブルになります。このスイッチは候補スイッチになることができません。

例

次の例では、クラスタ コマンド スイッチでクラスタリングをディセーブルにする方法を示します。

```
Switch(config)# no cluster run
```

設定を確認するには、**show cluster** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster standby-group

既存の Hot Standby Router Protocol（HSRP）にクラスタをバインドして、クラスタ コマンド スイッチの冗長性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 **cluster standby-group** コマンドを使用します。routing-redundancy キーワードを入力することで、同一の HSRP グループが、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用できるようになります。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。

cluster standby-group *HSRP-group-name* [**routing-redundancy**]

no cluster standby-group

構文の説明

HSRP-group-name	クラスタにバインドされる HSRP グループの名前。設定できるグループ名は 32 文字までです。
routing-redundancy	（任意）同一の HSRP スタンバイ グループをイネーブルにし、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用します。

コマンド デフォルト

クラスタは、どの HSRP グループにもバインドされません。

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
15.0(1)EY	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、クラスタ コマンド スイッチ上でだけ入力できます。クラスタ メンバ スイッチでこれを入力すると、エラー メッセージが表示されます。

クラスタ コマンド スイッチは、クラスタ HSRP バインディング情報をすべてのクラスタ HSRP 対応メンバに伝播します。各クラスタ メンバ スイッチはバインディング情報を NVRAM に保存します。HSRP グループ名は、有効なスタンバイ グループである必要があります。そうでない場合、エラーが発生してコマンドが終了します。

クラスタにバインドする HSRP スタンバイ グループのすべてのメンバに同じグループ名を使用する必要があります。バインドされる HSRP グループのすべてのクラスタ HSRP 対応メンバに同じ HSRP グループ名を使用してください （クラスタを HSRP グループにバインドしない場合には、クラスタ コマンダおよびメンバに異なる名前を使用できます）。

例

次の例では、my_hsrp という名前の HSRP グループをクラスタにバインドする方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster standby-group my_hsrp
```

次の例では、同じ HSRP グループ名 my_hsrp を使用して、ルーティング冗長とクラスタ冗長を確立する方法を示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

次の例では、このコマンドがクラスタ コマンド スイッチから実行され、指定された HSRP スタンバイ グループが存在しない場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

次の例では、このコマンドがクラスタ メンバ スイッチで実行された場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。出力は、クラスタ内の冗長性がイネーブルになったかどうかを示します。

関連コマンド

コマンド	説明
standby ip	インターフェイスで HSRP をイネーブルにします。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show standby	スタンバイ グループ情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

cluster timer

ハート ビート メッセージの間隔を秒単位で設定するには、グローバル コンフィギュレーション モードで **cluster timer** コマンドを使用します。デフォルト値の間隔を設定する場合は、このコマンドの **no** 形式を使用します。

cluster timer *interval-in-secs*

no cluster timer

構文の説明

interval-in-secs	ハートビート メッセージ間の間隔（秒）。指定できる範囲は 1 ～ 300 秒です。

コマンド デフォルト

8 秒間隔です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

このコマンドと **cluster holdtime** グローバル コンフィギュレーション コマンドは、クラスタ コマンド スイッチ上に限り入力してください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。

ホールドタイムは通常ハートビート インターバル タイマー（**cluster timer**）の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールド タイムをインターバル タイムで割った秒数」回のハートビート メッセージが連続して受信されなかったことになります。

例

次の例では、クラスタ コマンド スイッチでハートビート間隔のタイマーおよび期間を変更する方法を示します。

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 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
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

define interface-range

インターフェイス レンジ マクロを作成するには、グローバル コンフィギュレーション モードで **define interface-range** コマンドを使用します。定義されたマクロを削除するには、このコマンドの **no** 形式を使用します。

define interface-range *macro-name interface-range*

no define interface-range *macro-name interface-range*

構文の説明

macro-name	インターフェイス範囲マクロの名前（最大 32 文字）
interface-range	インターフェイス範囲。インターフェイス範囲の有効値については、「Usage Guidelines（使用上のガイドライン）」を参照してください。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

マクロ名は、最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。

ある範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、マクロ内では複数のインターフェイス タイプを組み合わせることができます。

interface-range を入力する場合は、次のフォーマットを使用します。

- *type* {*first-interface*} - {*last-interface*}
- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gigabitethernet1/1 - 2** は有効な範囲ですが、**gigabitethernet 1/1-2** は無効な範囲です。

type および *interface* の有効値は次のとおりです。

- **vlan** *vlan-id* - *vlan-ID*（VLAN ID は 1 ～ 4094）

  VLAN インターフェイスは、**interface vlan** コマンドで設定する必要があります（**show running-config** 特権 EXEC コマンドは、設定された VLAN インターフェイスを表示します）。**show running-config** コマンドで表示されない VLAN インターフェイスは、*interface-range* では使用できません。
- **port-channel** *port-channel-number*。ここで、*port-channel-number* は 1 ～ 6 です。
- **fastethernet** module/{*first port*} - {*last port*}
- **gigabitethernet** module/{*first port*} - {*last port*}

物理インターフェイス

- モジュールは常に 0 です。
- 範囲は、*type number/number - number* です（例：**gigabitethernet1/1 - 2**）。

範囲を定義するときは、ハイフン（-）の前にスペースが必要です。次に例を示します。

gigabitethernet1/1 - 2

複数の範囲を入力することもできます。複数の範囲を定義するときは、カンマ（,）の前の最初のエントリの後にスペースを入力する必要があります。カンマの後のスペースは任意になります。次に例を示します。

fastethernet1/3, gigabitethernet1/1 - 2

fastethernet1/3 -4, gigabitethernet1/1 - 2

例

次の例では、複数インターフェイスのマクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show running-config	定義されたマクロを含む現在の動作設定を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

delete

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/force**] [**/recursive**] *filesystem***:***/file-url*

構文の説明

/force	（任意）削除を確認するプロンプトを抑制します。
/recursive	（任意）指定されたディレクトリおよびそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除します。
*filesystem***:**	フラッシュ ファイル システムのエイリアスです。 ローカル フラッシュ ファイル システムの構文 **flash:**
/file-url	削除するパス（ディレクトリ）およびファイル名

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

/force キーワードを使用すると、削除プロセスにおいて削除の確認を要求するプロンプトが、最初の 1 回だけとなります。

/force キーワードを指定せずに **/recursive** キーワードを使用すると、ファイルごとに削除の確認を要求するプロンプトが表示されます。

プロンプト動作は、**file prompt** グローバル コンフィギュレーション コマンドの設定によって異なります。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。このコマンドの詳細については、『*Cisco IOS Command Reference for Release 12.1*』を参照してください。

例

次の例では、新しいイメージのダウンロードが正常に終了した後で、古いソフトウェア イメージを含むディレクトリを削除する方法を示します。

```
Switch# delete /force /recursive flash:/old-image
```

dir *filesystem***:** 特権 EXEC コマンドを入力することにより、ディレクトリが削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
archive download-sw	新しいイメージをスイッチにダウンロードし、既存のイメージを上書きまたは保存します。

deny（ARP アクセス リスト コンフィギュレーション）

DHCP バインディングとの一致に基づいて ARP パケットを拒否するには、アドレス解決プロトコル（ARP）のアクセスリスト コンフィギュレーション モードで **deny** コマンドを使用します。アクセス リストから指定されたアクセス コントロール エントリ（ACE）を削除するには、このコマンドの **no** 形式を使用します。

deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

no deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

構文の説明

request	（任意）ARP 要求との一致を定義します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信元 IP アドレスを指定します。
any	IP アドレスまたは MAC アドレスを拒否します。
host *sender-ip*	指定された送信側 IP アドレスを拒否します。
sender-ip sender-ip-mask	指定された範囲の送信側 IP アドレスを許可します。
mac	送信側 MAC アドレスを拒否します。
host *sender-mac*	特定の送信側 MAC アドレスを拒否します。
sender-mac sender-mac-mask	指定された範囲の送信側 MAC アドレスを拒否します。
response ip	ARP 応答の IP アドレス値を定義します。
host *target-ip*	指定されたターゲット IP アドレスを拒否します。
target-ip target-ip-mask	指定された範囲のターゲット IP アドレスを拒否します。
mac	ARP 応答の MAC アドレス値を拒否します。
host *target-mac*	指定されたターゲット MAC アドレスを拒否します。
target-mac target-mac-mask	指定された範囲のターゲット MAC アドレスを拒否します。
log	（任意）ACE と一致するパケットを記録します。

コマンド デフォルト

ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。

コマンド モード

ARP 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

deny 句を追加すると、一致条件に基づいて ARP パケットをドロップできます。

例

次の例では、ARP アクセス リストを定義し、IP アドレスが 1.1.1.1 で MAC アドレスが 0000.0000.abcd のホストからの ARP 要求と ARP 応答の両方を拒否する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 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
arp access-list	ARP アクセス コントロール リスト（ACL）を定義します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
permit（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

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 トラフィックの転送を回避するには、MAC アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。拒否条件を名前付き MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

{**deny** | **permit**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

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

構文の説明

any	送信元または宛先 MAC アドレスを拒否します。
host *src MAC-addr* | *src-MAC-addr mask*	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。
host *dst-MAC-addr* | *dst-MAC-addr mask*	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。
type mask	（任意）Ethernet II または SNAP カプセル化によるパケットの Ethertype 番号を使用して、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。
aarp	（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 を選択します。
amber	（任意）EtherType DEC-Amber を選択します。
cos *cos*	（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）値を選択します。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。**cos** 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。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニング ツリーを選択します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	（任意）EtherType DEC-Diagnostic を選択します。
dsm	（任意）EtherType DEC-DSM を選択します。
etype-6000	（任意）EtherType 0x6000 を選択します。
etype-8042	（任意）EtherType 0x8042 を選択します。
lat	（任意）EtherType DEC-LAT を選択します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を選択します。
lsap *lsap-number mask*	（任意）802.2 カプセル化によるパケットの LSAP 番号（0 ～ 65535）を指定して、パケットのプロトコルを識別します。 *mask* 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。

mop-console	（任意）EtherType DEC-MOP Remote Console を選択します。
mop-dump	（任意）EtherType DEC-MOP Dump を選択します。
msdos	（任意）EtherType DEC-MSDOS を選択します。
mumps	（任意）EtherType DEC-MUMPS を選択します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を選択します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（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）を選択します。

（注）　**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。

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。表 2-5 に、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一覧表示します。

表 2-5　IPX フィルタ基準

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

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
15.0(1)EY	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。

名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

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。

```
Switch(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。

```
Switch(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。

```
Switch(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
mac access-list extended	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。
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 トラフィックが転送されるのを許可します。
show access-lists	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

IEEE 802.1x 認証をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x** 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 {**critical** {**eapol** | **recovery delay** *milliseconds*} | {**guest-vlan supplicant**} | **system-auth-control**}

no dot1x {**critical** {**eapol** | **recovery delay**} | {**guest-vlan supplicant**} | **system-auth-control**}

（注）　**credentials** *name* キーワードは、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、サポートされていません。

構文の説明

critical {**eapol** | **recovery delay** ***milliseconds***}	アクセス不能認証バイパス パラメータを設定します。詳細については、**dot1x critical**（グローバル コンフィギュレーション）コマンドを参照してください。
guest-vlan supplicant	スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにします。
system-auth-control	スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。

コマンド デフォルト

IEEE 802.1x 認証はディセーブルで、オプションのゲスト VLAN の動作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
15.0(1)EY	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 認証をグローバルにイネーブルにする前に、認証、許可、アカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。

スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 802.1x 認証および EtherChannel が設定されているインターフェイスから EtherChannel の設定を削除します。

EAP-Transparent LAN Service（TLS）および EAP-MD5 で IEEE 802.1x を認証する Cisco Access Control Server（ACS）アプリケーションが稼働する装置を使用している場合、装置が ACS バージョン 3.2.1 以上で稼働していることを確認します。

guest-vlan supplicant キーワードを使用して、スイッチでオプションの IEEE 802.1x ゲスト VLAN の動作をグローバルにイネーブルにできます。詳細については、**dot1x guest-vlan** コマンドを参照してください。

例

次の例では、スイッチで IEEE 802.1x 認証をグローバルにイネーブルにする方法を示します。

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

次の例では、スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにする方法を示します。

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

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x critical（グローバルコンフィギュレーション）	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x guest-vlan	アクティブ VLAN をイネーブルにし、IEEE 802.1x ゲスト VLAN として指定します。
dot1x port-control	ポートの認証ステートの手動制御をイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail max-attempts

ポートが制限 VLAN に移行するまでに許容できる最大認証試行回数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x auth-fail max-attempts** 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 auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts

構文の説明

max-attempts	ポートが制限 VLAN に移行するまでに許容される最大認証試行回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルト値は 3 です。

コマンド デフォルト

デフォルト値は 3 回です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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 で許容される最大の認証試行回数を再設定する場合、変更内容は再認証タイマーが期限切れになった後で反映されます。

例

次の例では、ポート 3 の制限 VLAN にポートが移行する前に許容される最大の認証試行回数を *2* に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x auth-fail vlan [*vlan id*]	オプションの制限 VLAN の機能をイネーブルにします。
dot1x max-reauth-req [*count*]	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する最大回数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail vlan

ポートで制限 VLAN をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x auth-fail vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

構文の説明

vlan-id	VLAN を 1 ～ 4094 の範囲で指定します。

コマンド デフォルト

制限 VLAN 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

次のように設定されたポートで制限 VLAN を設定できます。

- シングルホスト（デフォルト）モード
- 認証用 auto モード

再認証をイネーブルにする必要があります。ディセーブルになっていると、制限 VLAN のポートは再認証要求を受け取りません。再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol（EAP）ログオフ イベントを受け取る必要があります。ホストがハブを介して接続されている場合、ホストが切断されているとポートがリンクダウン イベントを受け取ることができず、次の再認証試行が行われるまで新しいホストが検出されないことがあります。

サプリカントが認証に失敗すると、ポートは制限 VLAN に移行し、EAP *認証成功*メッセージがサプリカントに送信されます。サプリカントには実際の認証失敗が通知されないため、この制限ネットワーク アクセスに混乱が生じることがあります。EAP の成功メッセージは、次の理由で送信されます。

- EAP の成功メッセージが送信されない場合、サプリカントは 60 秒ごと（デフォルト）に EAP 開始メッセージを送信して認証を行おうとします。
- 一部のホスト（たとえば、Windows XP を実行中のデバイス）は、EAP の成功メッセージを受け取るまで DHCP を実装できません。

サプリカントは、認証から EAP 成功メッセージを受け取った後で不正なユーザ名とパスワードの組み合わせをキャッシュし、再認証のたびにその情報を使用する可能性があります。サプリカントが正しいユーザ名とパスワードの組み合わせを送信するまで、ポートは制限 VLAN のままになります。

レイヤ 3 ポートに使用する内部 VLAN は、制限 VLAN として設定することはできません。

VLAN を制限 VLAN と音声 VLAN の両方に設定することはできません。そのように設定すると、syslog メッセージが生成されます。

制限 VLAN ポートが無許可ステートに移行すると、認証プロセスが再起動されます。サプリカントが再度認証プロセスに失敗すると、認証は保持ステートで待機します。サプリカントが正常に再認証された後、すべての IEEE 802.1x ポートが再初期化され、通常の IEEE 802.1x ポートとして扱われます。

制限 VLAN を異なる VLAN として再設定すると、制限 VLAN のポートも移行し、そのポートは現在認証されたステートのままになります。

制限 VLAN をシャットダウンするか VLAN データベースから削除すると、制限 VLAN のポートはただちに無許可ステートに移行し、認証プロセスが再起動します。制限 VLAN 設定がまだ存在するため、認証は保持ステートで待機しません。制限 VLAN が非アクティブである間も、制限 VLAN がアクティブになったときにポートがただちに制限 VLAN になるように、すべての認証試行がカウントされます。

制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でだけサポートされます。そのため、ポートが制限 VLAN に配置されると、サプリカントの MAC アドレスが MAC アドレス テーブルに追加され、ポートに表示される他の MAC アドレスは、すべてセキュリティ違反として扱われます。

例

次の例では、ポート 1 で制限 VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x auth-fail max-attempts [***max-attempts***]	サプリカントを制限 VLAN に割り当てる前に、試行可能な認証回数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x control-direction

wake-on-LAN（WoL）機能を搭載した IEEE 802.1x 認証をイネーブルにし、ポート制御を単一方向モードまたは双方向モードに設定するには、インターフェイス コンフィギュレーション モードで **dot1x control-direction** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no dot1x control-direction

構文の説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デフォルト設定の双方向モードに戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

WoL の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication（IEEE 802.1x ポートベース認証の設定）」の章の「Using IEEE 802.1x Authentication with Wake-on-LAN（Wake-on-LAN を使った IEEE 802.1x 認証の使用）」の項を参照してください。

例

次の例では、単一方向制御をイネーブルにする方法を示します。

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

次の例では、双方向制御をイネーブルにする方法を示します。

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

設定を確認するには、**show dot1x all** 特権 EXEC コマンドを入力します。

show dot1x all 特権 EXEC コマンド出力は、ポート名とポートのステートを除き、すべてのスイッチで同一です。ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

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

dot1x control-direction in 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単一方向制御をイネーブルにする場合、これが **show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection  = In
```

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを入力しても、設定の競合によりポートでこのモードをサポートできない場合、**show dot1x all** コマンド出力で次のように表示されます。

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

関連コマンド

コマンド	説明
show dot1x [**all** | **interface** *interface-id*]	指定したインターフェイスに対する制御方向のポート設定ステータスを表示します。

dot1x credentials（グローバル コンフィギュレーション）

サプリカント スイッチでプロファイルを設定するには、グローバル コンフィギュレーション モードで **dot1x credentials** コマンドを使用します。

dot1x credentials *profile*

no dot1x credentials *profile*

構文の説明

profile	サプリカント スイッチのプロファイルを指定します。

コマンド デフォルト

スイッチにプロファイルは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

このスイッチをサプリカントにするには、オーセンティケータとして別のスイッチをセットアップしてある必要があります。

例

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch(config)# dot1x credentials profile
```

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
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

dot1x critical（グローバル コンフィギュレーション）

クリティカル認証または認証、許可、アカウンティング（AAA）失敗ポリシーとも呼ばれているアクセス不能な認証バイパス機能のパラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。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 critical {**eapol** | **recovery delay** *milliseconds*}

no dot1x critical {**eapol | recovery delay**}

構文の説明

eapol	スイッチによりクリティカルなポートが critical-authentication ステートに置かれた場合、EAPOL-Success メッセージを送信するようスイッチを指定します。
recovery delay *milliseconds*	ミリ秒のリカバリ遅延のピリオドを設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。

コマンド デフォルト

クリティカルなポートを critical-authentication ステートに置くことによってそのクリティカルなポートの認証に成功した場合に、スイッチは EAPOL-Success メッセージをホストに送信しません。

リカバリ遅延期間は、1000 ミリ秒（1 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

クリティカルなポートが critical-authentication ステートに置かれた場合、スイッチが EAPOL-Success メッセージを送信するよう指定するには、**eapol** キーワードを使用します。

使用不能な RADIUS サーバが使用可能になった場合にスイッチがクリティカルなポートを再初期化するために待機するリカバリ遅延期間を設定するには、**recovery delay** *milliseconds* キーワードを使用します。デフォルトのリカバリ遅延期間は 1000 ミリ秒です。ポートは、秒単位で再初期化できます。

アクセス不能な認証バイパスをポート上でイネーブルにするには、**dot1x critical** 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。スイッチがクリティカルなポートに割り当てるアクセス VLAN を設定するには、**dot1x critical vlan** *vlan-id* 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、リカバリ遅延期間として 200 をスイッチに設定する方法を示します。

```
Switch# dot1x critical recovery delay 200
```

設定を確認するには、**show dot1x** 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
dot1x critical（インターフェイス コンフィギュレーション）	アクセス不能な認証バイパス機能をイネーブルにし、この機能にアクセス VLAN を設定します。
show dot1x	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x critical（インターフェイス コンフィギュレーション）

クリティカル認証または認証、許可、アカウンティング（AAA）失敗ポリシーとも呼ばれているアクセス不能な認証バイパス機能のパラメータをイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x critical** コマンドを使用します。ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定することもできます。この機能をディセーブルにするか、またはデフォルトに戻すには、このコマンドの **no** 形式を使用します。

dot1x critical [**recovery action reinitialize** | **vlan** *vlan-id*]

no dot1x critical [**recovery** | **vlan**]

構文の説明

recovery action reinitialize	（任意）アクセス不能な認証バイパスのリカバリ機能をイネーブルにし、認証サーバが使用可能になった場合にリカバリ アクションによりポートを認証するよう指定します。
vlan *vlan-id*	（任意）スイッチがクリティカルなポートに割り当てることのできるアクセス VLAN を指定します。有効な範囲は 1 ～ 4094 です。

コマンド デフォルト

アクセス不能認証バイパス機能はディセーブルです。

リカバリ アクションは設定されていません。

アクセス VLAN 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を指定するには、**vlan** *vlan-id* キーワードを使用します。指定された VLAN タイプは、次のようにポート タイプに適合している必要があります。

- クリティカルなポートがアクセス ポートの場合、VLAN はアクセス VLAN でなければなりません。
- クリティカルなポートがルーテッド ポートの場合、VLAN を指定できます（指定は任意）。

クライアントで Windows XP を稼働し、クライアントが接続されているクリティカル ポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないことを報告します。

Widows XP クライアントが DHCP 用に設定されていて、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP-Success メッセージを受信しても DHCP 設定プロセスが再開されない場合があります。

アクセス不能認証バイパス機能および制限 VLAN を IEEE802.1x ポート上に設定できます。スイッチが制限 VLAN でクリティカル ポートの再認証を試行し、RADIUS サーバがすべて使用できない場合、スイッチはポートの状態をクリティカル認証ステートに移行し、ポートは制限 VLAN のままとなります。

アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。

例

次の例では、アクセス不能認証バイパス機能をポート上でイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x critical（グローバル コンフィギュレーション）	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x default

デフォルト値に IEEE 802.1x パラメータをリセットするには、インターフェイス コンフィギュレーション モードで **dot1x default** コマンドを使用します。

dot1x default

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト値は次のとおりです。

- ポート単位の IEEE 802.1x プロトコルのイネーブル ステートはディセーブルです（force-authorized）。
- 再認証試行間隔の秒数は、3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- ホスト モードはシングル ホストです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

コマンド モード

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、ポート上の IEEE 802.1x パラメータをリセットする方法を示します。

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

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x fallback

ポートを 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に設定するには、インターフェイス コンフィギュレーション モードで **dot1xfallback** 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 fallback *profile*

no dot1x fallback

構文の説明

profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイル。

コマンド デフォルト

フォールバックはイネーブルではありません。

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
15.0(1)EY	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、スイッチ ポートで **dot1x port-control** auto 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必要があります。

例

次の例では、IEEE 802.1x 認証用に設定されているスイッチ ポートにフォールバック プロファイルを指定する方法を示します。

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートの Web 認証をイネーブルにします。
ip admission name proxy http	スイッチの Web 認証をグローバルにイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x guest-vlan

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

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

構文の説明

vlan-id	IEEE 802.1x ゲスト VLAN であるアクティブ VLAN。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

ゲスト VLAN は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

非プライベート VLAN に属するスタティック アクセス ポートにゲスト VLAN を設定できます。

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

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

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

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

ゲスト VLAN は、シングルホスト モードおよびマルチホスト モードの IEEE 802.1x ポート上でサポートされます。

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

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。IEEE 802.1x 認証プロセスの設定を減らします（**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された IEEE 802.1x クライアントのタイプによって異なります。

スイッチは *MAC 認証バイパス*をサポートします。MAC 認証バイパスは IEEE 802.1x ポートでイネーブルの場合、スイッチは、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication（IEEE 802.1x ポートベース認証の設定）」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass（MAC 認証バイパスを使った IEEE 802.1x 認証の使用）」の項を参照してください。

例

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

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

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

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

次の例では、オプションのゲスト VLAN の動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x guest-vlan 5
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x	オプションのゲスト VLAN のサプリカント機能をイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x host-mode

IEEE 802.1x 許可ポートで単一のホスト（クライアント）または複数のホストを許可するには、インターフェイス コンフィギュレーション モードで **dot1x host-mode** コマンドを使用します。IEEE 802.1x 許可ポートでマルチドメイン認証（MDA）をイネーブルにするには、**multi-domain** キーワードを使用します。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 host-mode {**multi-host** | **single-host** | **multi-domain**}

no dot1x host-mode [**multi-host** | **single-host** | **multi-domain**}

構文の説明

multi-host	スイッチ上で複数のホストをイネーブルにします。
single-host	スイッチ上で単一のホストをイネーブルにします。
multi-domain	スイッチ ポート上で MDA をイネーブルにします。

コマンド デフォルト

デフォルト設定は、シングルホスト モードです。

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
15.0(1)EY	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、IEEE 802.1x 対応ポートを単一のクライアントに限定したり、複数のクライアントを IEEE 802.1x 対応ポートに接続したりすることができます。マルチホスト モードでは、接続されたホストのうち 1 つだけが許可されれば、すべてのホストのネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

ポートで MDA をイネーブルにするには、**multi-domain** キーワードを使用します。MDA はポートをデータ ドメインと音声ドメインの両方に分割します。MDA により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が同じ IEEE 802.1x 対応ポート上で許可されます。

このコマンドを入力する前に、指定のポートで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。

例

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにして、ポートの IEEE 802.1x 認証をイネーブルにし、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。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにし、IEEE 802.1x 認証をイネーブルにし、指定されたポートで MDA をイネーブルにする方法を示します。

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

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x initialize

ポート上で新しく認証セッションを初期化する前に、指定の IEEE 802.1x 対応ポートを手動で無許可ステートに戻すには、特権 EXEC モードで **dot1x initialize** コマンドを使用します。

dot1x initialize [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）初期化するポートを指定します。

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
15.0(1)EY	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、IEEE 802.1x ステート マシンを初期化し、新たな認証環境を設定します。このコマンドを入力した後、ポートの状態は無許可になります。

例

次の例では、ポートを手動で初期化する方法を示します。

```
Switch# dot1x initialize interface gigabitethernet1/2
```

show dot1x [**interface** *interface-id*] 特権 EXEC コマンドを入力することにより、ポート ステータスが無許可になっていることを確認できます。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x mac-auth-bypass

MAC 認証バイパス機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x mac-auth-bypass** コマンドを使用します。MAC 認証バイパス機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x mac-auth-bypass [**eap** | **timeout inactivity** *value*]

no dot1x mac-auth-bypass

構文の説明

eap	（任意）認証に Extensible Authentication Protocol（EAP）を使用するようスイッチを設定します。
timeout inactivity *value*	（任意）接続されたホストが無許可ステートになる前に非アクティブである秒数を設定します。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

MAC 認証バイパスはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

特に言及されない限り、MAC 認証バイパス機能の使用上のガイドラインは IEEE802.1x 認証の使用上のガイドラインと同じです。

ポートが MAC アドレスで認証された後で、ポートから MAC 認証バイパス機能をディセーブルにした場合、ポート ステートには影響ありません。

ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再許可できます。

ポートが許可ステートの場合、再許可が発生するまでポートはこのステートのままになります。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが IEEE 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）IEEE 802.1x 認証を使用してインターフェイスを認証します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。

MAC 認証バイパスおよび IEEE 802.lx 認証の相互作用の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication（IEEE 802.1x ポートベース認証の設定）」の章の「Understanding IEEE 802.1x Authentication with MAC Authentication Bypass（MAC 認証バイパスを使った IEEE 802.1x 認証について）」の項および「IEEE 802.1x Authentication Configuration Guidelines（IEEE 802.1x 認証設定ガイドライン）」の項を参照してください。

例

次の例では、MAC 認証バイパスをイネーブルにし、認証に EAP を使用するようスイッチを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass eap
```

次の例では、MAC 認証バイパスをイネーブルにし、接続されたホストが 30 秒間非アクティブである場合にタイムアウトを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass timeout inactivity 30
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-reauth-req

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再起動する回数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 **dot1x max-reauth-req** 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 max-reauth-req *count*

no dot1x max-reauth-req

構文の説明

count	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数です。指定できる範囲は 0 ～ 10 です。

コマンド デフォルト

デフォルトは 2 回です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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。

例

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

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

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x max-req	スイッチが認証プロセスを再起動する前に、EAP フレームを認証サーバに送信する最高回数を設定します（応答を受信しないと仮定）。
dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-req

認証プロセスを再開する前に、スイッチが Extensible Authentication Protocol（EAP）フレーム（応答が受信されないと見なされます）を認証サーバからクライアントに送信する最大回数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-req** 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 max-req *count*

no dot1x max-req

構文の説明

count	スイッチが、認証プロセスを再起動する前に、認証サーバから EAP フレームを再送信する回数です。範囲は 1 ～ 10 です。

コマンド デフォルト

デフォルトは 2 回です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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。

例

次の例では、認証プロセスを再起動する前に、スイッチが EAP フレームを認証サーバからクライアントに送信する回数を 5 回に設定する方法を示します。

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

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x pae

IEEE 802.1x Port Access Entity（PAE）オーセンティケータとしてポートを設定するには、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。IEEE 802.1x 認証をポート上でディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x pae authenticator

no dot1x pae

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

ポートは IEEE 802.1x PAE オーセンティケータではありません。IEEE 802.1x 認証はポート上でディセーブルです。

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
15.0(1)EY	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。

例

次の例では、ポートの IEEE 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x pae
```

設定を確認するには、**show dot1x** または **show eap** 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
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します。
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

dot1x port-control

ポートの認証ステートの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x port-control** コマンドを使用します。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 port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

構文の説明

auto	ポートで IEEE 802.1x 認証をイネーブルにし、スイッチおよびクライアント間の IEEE 802.1x 認証交換に基づきポートを許可または無許可ステートに変更します。
force-authorized	ポートで IEEE 802.1x 認証をディセーブルにし、認証情報の交換をせずにポートを許可ステートに移行します。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
force-unauthorized	クライアントからの認証の試みをすべて無視し、ポートを強制的に無許可ステートに変更することにより、このポート経由のすべてのアクセスを拒否します。スイッチはポートを介してクライアントに認証サービスを提供できません。

コマンド デフォルト

デフォルトの設定は force-authorized です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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 IEEE 802.1x 認証をイネーブルにする前に、**dot1x system-auth-control** 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、スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする必要があります。

IEEE 802.1x 標準は、レイヤ 2 のスタティック アクセス ポート、音声 VLAN のポート、およびレイヤ 3 のルーテッド ポート上でサポートされます。

ポートが、次の項目の 1 つとして設定されていない場合に限り **auto** キーワードを使用できます。

- トランク ポート：トランク ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。

- ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。
- スイッチド ポート アナライザ（SPAN）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

スイッチで IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** 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。特定のポートの IEEE 802.1x 認証をディセーブルにするか、デフォルトの設定に戻すには、**no dot1x port-control** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポートの IEEE 802.1x 認証をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x re-authenticate

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

dot1x re-authenticate [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）再認証するインターフェイスのモジュールおよびポート番号。

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
15.0(1)EY	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、再認証試行（re-authperiod）と自動再認証の間に設定された期間（秒）を待機することなく、クライアントを再認証できます。

例

次に、ポートに接続されたデバイスを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet1/2
```

関連コマンド

コマンド	説明
dot1x reauthentication	クライアントの定期的な再認証を有効にします。
dot1x timeout reauth-period	再認証の間隔（秒）を設定します。

dot1x reauthentication

クライアントの定期的な再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x reauthentication** コマンドを使用します。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 reauthentication

no dot1x reauthentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

定期的な再認証はディセーブルです。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

dot1x timeout reauth-period インターフェイス コンフィギュレーション コマンドを使用して、定期的に再認証を行う間隔の時間量を設定します。

例

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

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

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

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
dot1x re-authenticate	すべての IEEE 802.1x 対応ポートの再認証を手動で初期化します。
dot1x timeout reauth-period	再認証の間隔（秒）を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

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、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

interface *interface-id*	（任意）照会されるポートを指定します。

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
15.0(1)EY	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。

例

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。

```
Switch# dot1x test eapol-capable interface gigabitethernet1/2
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL
capable
```

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	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 の準備が整っているかどうかを確認するためにクエリーが実行されるポートからの EAPOL 応答の待機に使用するタイムアウトを設定するには、グローバル コンフィギュレーション モードで **dot1x test timeout** コマンドを使用します。

dot1x test timeout *timeout*

構文の説明

timeout	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
15.0(1)EY	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。

例

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。

```
Switch# 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
dot1x test eapol-capable [**interface** *interface-id*]	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

IEEE 802.1x タイマーを設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

quiet-period *seconds*	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を指定します。指定できる範囲は 1 ～ 65535 です。
ratelimit-period *seconds*	この期間中に認証に成功したクライアントからの Extensible Authentication Protocol over LAN（EAPOL）パケットをスイッチが無視した秒数を指定します。指定できる範囲は 1 ～ 65535 です。
reauth-period {*seconds* | **server**}	再認証の間隔（秒）を設定します。 キーワードの意味は次のとおりです。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : セッションタイムアウト RADIUS 属性（属性 [27]）の値として秒数を設定します。
server-timeout *seconds*	認証サーバに対して、スイッチのパケット再送信を待機する秒数を指定します。指定できる範囲は 30 ～ 65535 です
supp-timeout *seconds*	スイッチが IEEE 802.1x クライアントへパケットを再送信する前に待機する秒数を指定します。指定できる範囲は 30 ～ 65535 です
tx-period *seconds*	要求を再送信するまでに、スイッチがクライアントからの EAP-Request/Identity フレームに対する応答を待機する秒数を指定します。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

reauth-period は 3600 秒です。

quiet-period は 60 秒です。

tx-period は 5 秒です。

supp-timeout は 30 秒です。

server-timeout は 30 秒です。

rate-limit は 1 秒です。

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
15.0(1)EY	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しただけの場合、**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 サーバに転送します。

例

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

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

次に、定期的な再認証をイネーブルにし、再認証の間隔（秒）としてセッション タイムアウト RADIUS 属性の値を指定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

次の例では、スイッチから認証サーバへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config)# dot1x timeout server-timeout 45
```

次の例では、EAP request フレームに対するスイッチからクライアントへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

次に、要求を再送信するまでに、クライアントからの EAP 要求/ID フレームに対する応答を待機する秒数を 60 に設定する例を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

次の例では、認証に成功したクライアントからの EAPOL パケットをスイッチが無視する秒数を 30 と設定する方法を示します。

```
Switch(config-if)# dot1x timeout ratelimit-period 30
```

設定を確認するには、**show dot1x** 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
dot1x max-req	スイッチが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最高回数を設定します。
dot1x reauthentication	クライアントの定期的な再認証を有効にします。
show dot1x	すべてのポートの IEEE 802.1x ステータスを表示します。

dot1x violation-mode

新しいデバイスをポートに接続するか、最大数のデバイスをポートに接続した後で新しいデバイスをポートに接続する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 **dot1x violation-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。

dot1x violation-mode {**shutdown** | **restrict** | **protect**}

no dot1x violation-mode

構文の説明

shutdown	エラーによって、予期しない新たな 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。
restrict	違反エラーの発生時に Syslog エラーを生成します。
protect	新しい MAC アドレスからパケットをそのままドロップします。これがデフォルト設定です。

コマンド デフォルト

デフォルトでは、**dot1x violation-mode protect** がイネーブルになっています。

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
15.0(1)EY	このコマンドが導入されました。

例

次の例では、新しいデバイスをポートに接続するときに、IEEE 802.1x 対応ポートを errdisable に設定して、シャットダウンする方法を示します。

```
Switch(config-if)# dot1x violation-mode shutdown
```

次の例では、新しいデバイスをポートに接続するときに、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 IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode restrict
```

次の例では、新しいデバイスをポートに接続するときに、新たに接続されたデバイスを無視するように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode protect
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

duplex

ポートのデュプレックス モードで動作するように指定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。ポー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。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	自動によるデュプレックス設定をイネーブルにします（接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードで動作すべきかを判断します）。
full	全二重モードをイネーブルにします。
half	半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

コマンド デフォルト

ファスト イーサネット ポートおよびギガビット イーサネット ポートに対するデフォルトは **auto** です。

100BASE-*x*（-*x* は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **full** です。

二重オプションは、1000BASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、または -ZX）SFP モジュールではサポートされていません。

ご使用のスイッチでサポートされている SFP モジュールについては、製品のリリース ノートを参照してください。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ファスト イーサネット ポートでは、接続された装置がデュプレックス パラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**half** を指定するのと同じ効果があります。

ギガビット イーサネット ポートでは、接続装置がデュプレックス パラメータを自動ネゴシエートしないときにポートを **auto** に設定すると、**full** を指定する場合と同じ効果があります。

（注） デュプレックス モードが **auto** で接続されている装置が半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはリンクの反対側のデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

注意　インターフェイス速度およびデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# duplex full
```

設定を確認するには、**show interfaces** 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
show interfaces	スイッチのインターフェイスの設定を表示します。
speed	10/100 または 10/100/1000 Mb/s インターフェイスの速度を設定します。

errdisable detect cause

特定の原因またはすべての原因に対して error-disable 検出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 **errdisable detect cause** コマンドを使用します。errdisable 検出機能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。

errdisable detect cause {**all** | **arp-inspection** | **bpduguard** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **link-flap** | **loopback** | **pagp-flap** | **psp** | **security-violation shutdown vlan** | **sfp-config-mismatch**}

no errdisable detect cause {**all** | **arp-inspection** | **bpduguard** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **link-flap** | **loopback** | **pagp-flap** | **psp** | **security-violation shutdown vlan** | **sfp-config-mismatch**}

errdisable detect cause bpduguard shutdown vlan

no errdisable detect cause bpduguard shutdown vlan

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック アドレス解決プロトコル（ARP）インスペクションのエラー検出をイネーブルにします。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに error-disable を指定します。
dhcp-rate-limit	DHCP スヌーピングのエラー検出をイネーブルにします。
dtp-flap	ダイナミック トランキング プロトコル（DTP）フラップのエラー検出をイネーブルにします。
gbic-invalid	無効なギガビット インターフェイス コンバータ（GBIC）モジュール用のエラー検出をイネーブルにします。 **（注）** このエラーは、スイッチでの無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。
inline-power	インライン パワーに対し、エラー検出をイネーブルにします。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。
pagp-flap	ポート集約プロトコル（PAgP）フラップの errdisable 原因のエラー検出をイネーブルにします。
psp	プロトコル ストーム プロテクションのエラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ブリッジ プロトコル データ ユニット（BPDU）ガードとポート セキュリティについては、このコマンドを使用して、ポート全体をディセーブルにするのではなく、ポートの特定の VLAN のみをディセーブルにするようにスイッチを設定できます。

VLAN ごとに errdisable 機能をオフにしていて BPDU ガード違反が発生した場合は、ポート全体がディセーブルになります。VLAN ごとに errdisable 機能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。

原因（**link-flap**、**dhcp-rate-limit** など）は、errdisable ステートが発生した理由です。原因がポートで検出された場合、ポートは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU、音声認識 802.1x セキュリティ、ガードおよびポート セキュリティ機能のため、違反の発生時に、ポート全体でなく、ポート上の障害のある VLAN だけをシャットダウンするようスイッチを設定することができます。

原因に対して **errdisable recovery** 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、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、ポートは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、ポートを手動で errdisable ステートから回復させる必要があります。

プロトコル ストーム プロテクションでは、最大 2 個の仮想ポートについて過剰なパケットがドロップされます。**psp** キーワードを使用した仮想ポート エラーのディセーブル化は、EtherChannel インターフェイスおよび Flexlink インターフェイスでサポートされません。

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

例

次の例では、リンクフラップ errdisable 原因の errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable で BPDU ガードをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable で音声認識 802.1x セキュリティをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
clear errdisable interface	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。

errdisable detect cause small-frame

着信 VLAN タグ付きパケットのフレームが小さく（67 バイト以下）、設定された最低速度（しきい値）で到着する場合に、任意のスイッチ ポートを errdisable にすることを許可するには、グローバル コンフィギュレーション モードで **errdisable detect cause small-frame** 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。

errdisable detect cause small-frame

no errdisable detect cause small-frame

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

この機能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
15.0(1)EY	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、小さいフレームの着信機能をグローバルにイネーブルにします。各ポートのしきい値を設定するには、**small violation-rate** 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。

ポートが自動的に再びイネーブルになるように設定するには、**errdisable recovery cause small-frame** 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。回復時間を設定するには、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、小さい着信フレームが設定されたしきい値で到着すると errdisable モードになるスイッチ ポートをイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause small-frame
```

設定を確認するには、**show interfaces** 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
errdisable recovery cause small-frame	回復タイマーをイネーブルにします。
errdisable recovery	指定された errdisable ステートから回復する時間を指定します。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small-frame violation rate	ポートが errdisable ステートとなる、小さい着信フレームの伝送速度（しきい値）を設定します。

errdisable recovery cause small-frame

スイッチに小さいフレームが着信してポートが errdisable になった後でポートを自動的に再有効化する回復タイマー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 **errdisable recovery cause small-frame** 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。

errdisable recovery cause small-frame

no errdisable recovery cause small-frame

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

この機能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
15.0(1)EY	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、errdisable ポートの回復タイマーをイネーブルにします。回復時間を設定するには、errdisable **recovery interval** *interval* 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、回復タイマーを設定する方法を示します。

```
Switch(config)# errdisable recovery cause small-frame
```

設定を確認するには、**show interfaces** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが指定した最小サイズより小さく、指定した伝送速度（しきい値）で到着する場合に、スイッチ ポートを errdisable 状態にします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small-frame violation rate	ポートが errdisable ステートとなる、（小さい）着信フレームのサイズを設定します。

errdisable recovery

回復メカニズム変数を設定するには、グローバル コンフィギュレーション モードで **errdisable recovery** 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。

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** |**link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **psp** | **security-violation** | **sfp-config-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **psp** | **security-violation** | **sfp-config-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

構文の説明

cause	特定の原因から回復するように errdisable メカニズムをイネーブルにします。
all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
bpduguard	ブリッジ プロトコル データ ユニット（BPDU）ガード errdisable ステートから回復するタイマーをイネーブルにします。
channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
dtp-flap	ダイナミック トランキング プロトコル（DTP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	ギガビット インターフェイス コンバータ（GBIC）モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 **（注）** このエラーは無効な Small Form-Factor Pluggable（SFP）の errdisable ステートを意味します。
inline-power	インライン パワーに対し、エラー検出をイネーブルにします。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル（PAgP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。
psp	プロトコル ストーム プロテクションの errdisable ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1x 違反ディセーブル ステートから回復するタイマーをイネーブルにします。
udld	単方向リンク検出（UDLD）errdisable ステートから回復するタイマーをイネーブルにします。

vmps	VLAN メンバーシップ ポリシー サーバ（VMPS）errdisable ステートから回復するタイマーをイネーブルにします。
interval *interval*	指定された errdisable ステートから回復する時間を指定します。指定できる範囲は 30 ～ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルト間隔は 300 秒です。 **（注）** errdisable recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

コマンド デフォルト

すべての原因に対して回復はディセーブルです。

デフォルトの回復間隔は 300 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

原因（**link-flap**、**bpduguard** など）は、errdisable ステートが発生した理由として定義されます。原因がポートで検出された場合、ポートは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

その原因に対して errdisable の回復をイネーブルにしない場合、ポートは、**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 コマンドが入力されるまで errdisable ステートのままです。原因の回復をイネーブルにした場合、ポートは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でポートを errdisable ステートから回復させる必要があります。

例

次の例では、BPDU ガード errdisable 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
```

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

設定を確認するには、**show errdisable recovery** 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
clear errdisable interface	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

exception crashinfo

Cisco IOS イメージでエラーが発生した場合は、スイッチが拡張 crashinfo ファイルを作成するように設定するには、グローバル コンフィギュレーション モードで **exception crashinfo** コマンドを使用します。この機能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。

exception crashinfo

no exception crashinfo

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

スイッチが拡張 crashinfo ファイルを作成します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

基本 crashinfo ファイルには、失敗した Cisco IOS のイメージ名とバージョン、およびプロセッサ レジスタのリストが含まれます。拡張 crashinfo ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。

スイッチが拡張 crashinfo ファイルを作成しないように設定するには、**no exception crashinfo** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スイッチが拡張 crashinfo ファイルを作成しないように設定する方法を示します。

```
Switch(config)# no exception crashinfo
```

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
show running-config	定義されたマクロを含む動作設定を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

fallback profile

Web 認証用にフォールバック プロファイルを作成するには、グローバル コンフィギュレーション モードで **fallback profile** 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。

fallback profile *profile*

no fallback profile

構文の説明

profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。

コマンド デフォルト

フォールバック プロファイル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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

フォールバック プロファイルは、サプリカントを持たない IEEE 802.1x ポートの IEEE 802.1x フォールバック動作を定義するために使用されます。サポートされる動作は、Web 認証へのフォールバックだけです。

fallback profile コマンドを入力すると、プロファイル コンフィギュレーション モードが開始され、次のコンフィギュレーション コマンドが使用可能になります。

- **ip**：IP コンフィギュレーションを作成します。
- **access-group**：まだ認証されていないホストによって送信されるパケットのアクセス コントロールを指定します。
- **admission**：IP アドミッション ルールを適用します。

例

次の例では、Web 認証で使用されるフォールバック プロファイルの作成方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

show running-configuration [**interface** *interface-id*] 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
dot1x fallback	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。
ip admission	スイッチ ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。
show fallback profile	スイッチの設定済みプロファイルを表示します。

fcs-threshold

フレーム チェック シーケンス（FCS）のビット エラー レートを設定するには、インターフェイス コンフィギュレーション モードで **fcs-threshold** コマンドを使用します。デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

fcs-threshold *value*

no fcs-threshold *value*

構文の説明

value	値範囲は 6 ～ 11 で、10^{-6} ～ 10^{-11} ビットエラー レートを示します。

コマンド デフォルト

デフォルトは 8 です。これは、イーサネット標準の 10^{-8} ビット エラー レートを示します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

イーサネット標準の上限ビット エラー レートは 10^{-8} です。スイッチで設定可能なビット エラー レートの範囲は 10^{-6} ～ 10^{-11} です。スイッチのビット エラー レートは自然数です。ビット エラー レートに 10^{-9} を設定する場合は、係数に 9 を入力します。

スイッチに FCS エラー ヒステリシスしきい値を設定して、実際のビット エラー レートの変動が設定したビット エラー レートに接近すると切り替わるアラームを防止するには、**alarm facility fcs hysteresis** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、ポートの FCS ビット エラー レートを 10^{-10} に設定する方法を示します。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# fcs-threshold 10
```

関連コマンド

コマンド	説明
alarm facility fcs-hysteresis	スイッチの FCS ヒステリシスしきい値をポートに設定された FCS ビット エラー レートの許容変動率で設定します。
show fcs-threshold	インターフェイスそれぞれの FCS エラー ビット レート設定を正数の係数として表示します。

fixup

一部のプロトコルは、レイヤ 2 で NAT 間で透過的に動作しません。これらのプロトコルは、Application Layer Gateway（ALG）を使用して「修正」する必要があります。ARP と ICMP の修正はデフォルトでイネーブルです。レイヤ 2 NAT インスタンスに対するこれらの設定を変更するには、config l2nat モードで **fixup** コマンドを使用します。

指定したプロトコルのフィックスアップをディセーブルにするには、このコマンドの **no** 形式を入力します。

fixup { arp | icmp | all }

no fixup { arp | icmp | all }

構文の説明

arp	ARP を修正します
icmp	ICMP を修正します
all	ARP と ICMP を両方とも修正します

コマンド デフォルト

イネーブル

コマンド モード

Config-l2nat

コマンド履歴

リリース	変更内容
15.0(2)EB	このコマンドが導入されました。

使用上のガイドライン

各レイヤ 2 NAT インスタンスに対するこれらの設定を行います。

例

次に、レイヤ 2 NAT インスタンスの ARP をイネーブルにする例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# fixup arp
```

関連コマンド

コマンド	説明
l2nat instance	レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。
show l2nat instance	指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat interface	1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat statistics	すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。
show l2nat statistics interface	指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。

flowcontrol

インターフェイスの受信フロー制御ステートを設定するには、インターフェイス コンフィギュレーション モードで、**flowcontrol** コマンドを使用します。

flowcontrol receive {**desired** | **off** | **on**}

構文の説明

receive	インターフェイスがリモート デバイスからフロー制御パケットを受信できるかどうかを設定します。
desired	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼働させることができます。
off	接続装置がフロー制御パケットをインターフェイスへ送信する機能をオフにします。
on	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼働させることができます。

コマンド デフォルト

デフォルトは、**flowcontrol receive off** に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ある装置に対してフロー制御 **send** が動作可能でオンになっていて、接続のもう一方の側で輻輳が少しでも検出された場合は、休止フレームを送信することによって、リンクの相手側またはリモート装置に輻輳を通知します。ある装置に対してフロー制御 **receive** がオンで、休止フレームを受信した場合、データ パケットの送信は停止します。こうすることにより、輻輳期間中にデータ パケットの損失を防ぎます。

（注） スイッチは、ポーズ フレームを受信できますが、送信はできません。

このスイッチでは、送信フロー制御の休止フレームはサポートされません。

on および **desired** キーワードは同一の結果になることに注意してください。

flowcontrol コマンドを使用してポートが輻輳中にトラフィック レートを制御するよう設定する場合、フロー制御はポート上で次の条件のうちの 1 つに設定されます。

- **receive on** または **desired**：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要がある装置、または送信可能な接続装置と連動できます。ポートはポーズ フレームを受信できます。
- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

表 2-6 は、各設定の組み合わせによるローカル ポートおよびリモート ポート上のフロー制御の結果を示したものです。表は **receive desired** キーワードの使用時と **receive on** キーワードの使用時の結果が同一になることを前提としています。

表 2-6　フロー制御設定およびローカル/リモート ポート フロー制御解決

フロー制御設定		フロー制御解決	
ローカル デバイス	**リモート デバイス**	**ローカル デバイス**	**リモート デバイス**
send off/receive on	**send on/receive on**	受信だけ行います。	送受信を行います。
	send on/receive off	受信だけ行います。	送信だけ行います。
	send desired/receive on	受信だけ行います。	送受信を行います。
	send desired/receive off	受信だけ行います。	送信だけ行います。
	send off/receive on	受信だけ行います。	受信だけ行います。
	send off/receive off	送受信を行いません。	送受信を行いません。
send off/receive off	**send on/receive on**	送受信を行いません。	送受信を行いません。
	send on/receive off	送受信を行いません。	送受信を行いません。
	send desired/receive on	送受信を行いません。	送受信を行いません。
	send desired/receive off	送受信を行いません。	送受信を行いません。
	send off/receive on	送受信を行いません。	送受信を行いません。
	send off/receive off	送受信を行いません。	送受信を行いません。

例

次の例では、リモート ポートによってフロー制御がサポートされないようにローカル ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# flowcontrol receive off
```

設定を確認するには、**show interfaces** 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
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

inside from

外部アドレスに内部アドレスを変換するには、config-l2nat モードで **inside from** コマンドを入力します。変換を削除するには、このコマンドの **no** 形式を使用します。

inside from {**host** | **range** | **network**} *original ip* **to** *translated ip* [**mask**] *number* | *mask*

no inside from {**host** | **range** | **network}** *original ip* **to** *translated ip* [**mask**] *number* | *mask*

構文の説明

host	単一のホスト アドレスを変換します。
range	ホスト アドレス範囲を変換します。*number* を入力して範囲のサイズを指定します。
network	サブネット内のすべてのホスト アドレスを変換します。ホストのオクテットは 1.1.0.0 のように 0 にする必要があります。別の値を入力した場合、無視されます。*translated ip* を入力する場合、**mask** *mask* を含めます。
original ip **to** *translated ip*	ホストのプライベート IP アドレス、範囲、またはネットワークおよび対応するパブリック IP アドレス。
mask *mask*	**network** オプションを使用する場合以外は任意です。サブネット マスク。有効なサブネットは 255.255.0.0、255.255.255.0、255.255.255.128、255.255.255.192、255.255.255.224、および 255.255.255.240 です。
number	**range** オプションを使用する場合以外は任意です。範囲のサイズ。

コマンド デフォルト

なし

コマンド モード

Config-l2nat モード

コマンド履歴

リリース	変更内容
15.0(2)EB	このコマンドが導入されました。

使用上のガイドライン

- 各レイヤ 2 NAT インスタンスの変換を設定します。
- 指定されたレイヤ 2 NAT インスタンスがすでにある場合、新しい変換値は前述のリストに追加されます。
- 内部ネットワークのデバイスから外部ネットワーク デバイスに ping を実行するには、外部デバイスの変換済みアドレスを使用します。たとえば、外部ホスト 10.10.10.100 が内部ホスト 192.168.1.100 に変換される場合は、ping 192.168.1.100 です。
- 範囲：
  - 範囲は互いに重複させないでください。
  - 範囲は /24 のネットワーク設定と重複させないでください。
  - オリジナルと変換された IP アドレスは 1 対 1 に対応させる*必要があります*（x.x.x.1 ～ y.y.y.1、x.x.x.2 ～ x.x.x.2 など）。元のアドレスおよび変換されたアドレスがこのように対応していない場合は、**host** コマンドを使用して各アドレスを個別に設定できます。
- 各変換の個別の統計情報は **host** および **range** オプションを使用して変換されるアドレスには利用できますが、**network** オプションによって変換されるアドレスには利用 *できません*。

例

次に、内部アドレス 192.168.0.100 を外部アドレス 10.1.0.100 に変換するように、Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from host 192.168.0.100 to 10.1.0.100
```

次に、5 つの内部アドレスの範囲を対応する外部アドレスに変換するように、Instance1 という名前のインスタンスを設定する例を示します。192.168.142.1 は 10.10.10.1、192.168.142.2 は 10.10.10.2 などに変換されます。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from range 192.168.142.1 to 10.10.10.1 5
```

次に、内部サブネット上のすべてのアドレスを外部サブネット上の対応するアドレスに変換するように、Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from network 192.168.142.0 to 20.20.30.0 mask 255.255.255.0
```

関連コマンド

コマンド	説明
l2nat instance	レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。
outside from	レイヤ 2 NAT を使用して、外部アドレスを内部アドレスに変換します。
show l2nat instance	指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat interface	1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat statistics	すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。
show l2nat statistics interface	指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。

interface port-channel

ポート チャネル論理インターフェイスのアクセスまたは作成を行うには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。ポート チャネルを削除する場合は、このコマンドの **no** 形式を使用します。

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

構文の説明

port-channel-number	ポート チャネル番号。範囲は 1 ～ 6 です。

コマンド デフォルト

ポート チャネル論理インターフェイスは定義されません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを獲得すると、ポートチャネル インターフェイスは自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

interface port-channel コマンドの次に **no switchport** 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、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポート チャネルの論理インターフェイスを手動で設定してください。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

注意　ポート チャネル インターフェイスをルーテッド ポートとして使用する場合、チャネル グループに割り当てられた物理ポート上のレイヤ 3 に、アドレスを割り当てないようにしてください。

注意　レイヤ 3 のポート チャネル インターフェイスとして使用されているチャネル グループの物理ポート上で、ブリッジ グループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol（CDP）を使用する場合には、これを物理ポートでだけ設定してください。ポート チャネル インターフェイスでは設定できません。
- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、そのポートは EtherChannel に加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、ポート チャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
Switch(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** 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
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

interface range

インターフェイスの範囲を入力し、複数のポートでコマンドを同時に実行するには、グローバル コンフィギュレーション モードで **interface range** コマンドを使用します。インターフェイス範囲を削除する場合は、このコマンドの **no** 形式を使用します。

interface range {*type* | *id*} {*port-range* | **macro** *name*}

no interface range {*port-range* | **macro** *name*}

構文の説明

port-range	ポート範囲。*port-range* の有効値のリストについては、「Usage Guidelines（使用上のガイドライン）」を参照してください。
macro *name*	マクロ名を指定します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

インターフェイス範囲コンフィギュレーション モードを開始して入力した、すべてのインターフェイスのパラメータは、その範囲内のすべてのインターフェイスに対する属性になります。

VLAN については、既存の VLAN スイッチ仮想インターフェイス（SVI）でだけ **interface range** コマンドを使用することができます。VLAN の SVI を表示する場合は、**show running-config** 特権 EXEC コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用することはできません。**interface range** コマンドのもとで入力したコマンドは、この範囲のすべての既存の VLAN SVI に適用されます。

あるインターフェイス範囲に対して行われた設定変更は、すべて NVRAM に保存されますが、インターフェイス範囲自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力できます。

- 最大 5 つまでのインターフェイス範囲を指定。
- 定義済みのインターフェイス範囲マクロ設定を指定。

範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、各範囲をカンマ（,）で区切ることにより、1 つのコマンドで最大 5 つのインターフェイス範囲を定義できます。

port-range タイプおよびインターフェイスの有効値は次のとおりです。

- **fastethernet** *module*/{*first port*} - {*last port*},
  - 使用可能範囲は、*type number/number - number* です（例：**gigabitethernet1/1 - 2**）。
- **loopback** *loopback-number - loopback number* : *loopback-number* は 1 ～ 2147483647
- **port-channel** *port-channel-number - port-channel-number* : *port-channel-number* は 1 ～ 6 です

（注）　ポート チャネルの **interface range** コマンドを使用した場合、範囲内の最初と最後のポート チャネル番号はアクティブなポート チャネルである必要があります。

- **tunnel** *tunnel-number* - *tunnel-number* : *tunnel-number* は 1 ～ 2147483647
- **vlan** *vlan-ID* - *vlan-ID*（vlan ID の範囲は 1 ～ 4094）

範囲を定義するときは、最初の入力とハイフン（-）の間にスペースが必要です。

```
interface range gigabitethernet1/1 -2
```

範囲を複数定義するときでも、最初のエントリとカンマ（,）の間にスペースを入れる必要があります。

```
interface range fastethernet1/1 - 2, gigabitethernet1/1 - 2
```

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。

また、*port-range* で単一インターフェイスを指定することもできます。つまりこのコマンドは、**interface** *interface-id* グローバル コンフィギュレーション コマンドに類似しています。

インターフェイスの範囲の設定に関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、**interface range** コマンドを使用して、インターフェイス範囲コンフィギュレーション モードを開始し、2 つのポートにコマンドを入力する方法を示します。

```
Switch(config)# interface range gigabitethernet1/1 - 2
```

次の例では、同じ機能に対して 1 つのポート範囲マクロ macro1 を使用する方法を示します。この利点は、macro1 を削除するまで再利用できることです。

```
Switch(config)# define interface-range macro1 gigabitethernet1/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイス範囲のマクロを作成します。
show running-config	スイッチで現在の動作設定情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip access-group

レイヤ 2 またはレイヤ 3interface へのアクセスを制御するには、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。インターフェイスからすべてまたは指定のアクセス 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-number* | *name*} {**in** | **out**}

no ip access-group [*access-list-number* | *name*] {**in** | **out**}

構文の説明

access-list-number	IP アクセス コントロール リスト（ACL）の番号です。指定できる範囲は、1 ～ 199 または 1300 ～ 2699 です。
name	**ip access-list** グローバル コンフィギュレーション コマンドで指定された IP ACL 名です。
in	入力パケットに対するフィルタリングを指定します。
out	発信パケットに対するフィルタリングを指定します。このキーワードは、レイヤ 3 のインターフェイス上に限り有効です。

コマンド デフォルト

アクセス リストは、インターフェイスには適用されません。

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

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

名前付きまたは番号付きの標準/拡張 IP アクセス リストをインターフェイスに適用できます。名前を付けてアクセス リストを定義するには、**ip access-list** 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。番号付きアクセス リストを定義するには、**access list** 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。1 ～ 99 および 1300 ～ 1999 の範囲の番号付き標準アクセス リスト、または 100 ～ 199 および 2000 ～ 2699 の範囲の番号付き拡張アクセス リストを使用できます。

このコマンドを使用して、アクセス リストをレイヤ 2 またはレイヤ 3 のインターフェイスに適用できます。ただし、レイヤ 2 のインターフェイス（ポート ACL）には、次のような制限があることに注意してください。

- ACL は受信方向のレイヤ 2 ポートにだけ適用できます。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC ACL だけを適用できます。
- レイヤ 2 のインターフェイスはロギングをサポートしていません。**log** キーワードが IP ACL で指定された場合、無視されます。
- レイヤ 2 のインターフェイスに適用された IP ACL は、IP パケットだけをフィルタにかけます。非 IP パケットをフィルタリングするには、MAC 拡張 ACL とともに **mac access-group** 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。

（注）　ユーザは同一のスイッチ上で、ルータ ACL、入力ポート ACL、VLAN マップを使用できます。ただし、ポート ACL はルータ ACL または VLAN マップよりも優先されます。ルータの ACL は IP サービス イメージが実行されているスイッチでのみサポートされます。

- 入力ポートの ACL がインターフェイスに適用され、さらにインターフェイスがメンバとなっている VLAN に VLAN マップが適用された場合、ACL のポート上で受信した着信パケットは、そのポート ACL でフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- 入力ルータの ACL および入力ポートの ACL が SVI に存在している場合､ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合､ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- VLAN マップ、出力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

IP の ACL は、送信側または受信側のレイヤ 3 インターフェイス両方に適用できます。

レイヤ 3 のインターフェイスでは、IP の ACL を各方向に 1 つ適用できます。

VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。標準入力アクセス リストでは、スイッチは、パケットを受信すると、パケットの送信元アドレスをアクセス リストに比較して検査します。IP 拡張アクセス リストでは、任意で、宛先 IP アドレス、プロトコル タイプ、ポート番号などのパケット内の他のフィールドを検査することができます。アクセス リストがパケットを許可する場合に、スイッチはパケットの処理を続行します。アクセス リストがパケットを拒否する場合は、スイッチはそのパケットをドロップします。アクセス リストがレイヤ 3 のインターフェイスに適用された場合、パケットのドロップにともない（デフォルト設定）、インターネット制御メッセージ プロトコル（ICMP）の Host Unreachable のメッセージが生成されます。ICMP Host Unreachable メッセージは、レイヤ 2 インターフェイスでドロップされたパケットに対しては生成されません。

通常の発信アクセス リストでは、パケットを受信して、それを制御されたインターフェイスへ送信した後、スイッチがアクセス リストと照合することでパケットを確認します。アクセス リストがパケットを許可した場合、スイッチはパケットを送信します。アクセス リストがパケットを拒否した場合、スイッチはパケットをドロップし、デフォルトの設定では、ICMP Host Unreachable メッセージが生成されます。指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

例

次の例では、ポートの入力パケットに IP アクセス リスト 101 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# ip access-group 101 in
```

関連コマンド

コマンド	説明
access list	番号付き ACL を設定します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
ip access-list	名前付き ACL を設定します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show access-lists	スイッチで設定された ACL を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show ip access-lists	スイッチで設定された IP ACL を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show ip interface	インターフェイスのステータスと設定に関する情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip address

レイヤ 2 スイッチの IP アドレスや、各スイッチ仮想インターフェイス（SVI）の IP アドレスまたはレイヤ 3 スイッチのルーテッド ポートを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除したり、IP 処理をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

構文の説明

ip-address	[IP Address]。
subnet-mask	関連する IP サブネットのマスク。
secondary	（任意）設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

コマンド デフォルト

IP アドレスは定義されていません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

Telnet のセッションで、スイッチの IP アドレスを削除した場合、スイッチの接続が切断されます。

ホストは、インターネット制御メッセージ プロトコル（ICMP）Mask Request メッセージを使用して、サブネット マスクを判別できます。ルータは、この要求に対して ICMP Mask Reply メッセージで応答します。

no ip address コマンドを使って IP アドレスを削除することで、特定のインターフェイス上の IP プロセスをディセーブルにできます。スイッチが、その IP アドレスのうちの 1 つを使用している他のホストを検出した場合、コンソールにエラー メッセージを送信します。

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定することができます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストと ARP 要求は、IP ルーティング テーブル内のインターフェイス ルートと同様に、適切に処理されます。

（注） ネットワーク セグメント上のすべてのルータがセカンダリのアドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。

Open Shortest Path First（OSPF）のルーティングの場合、インターフェイスのすべてのセカンダリ アドレスが、プライマリ アドレスと同一の OSPF 領域にあることを確認してください

スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。ソフトウェアに、設定できるルーテッド ポートおよび SVI の個数制限はありません。この個数と設定されている他の機能の数との相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用し、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。詳細については、**sdm prefer** コマンドを参照してください。

例

次の例では、サブネット ネットワークでレイヤ 2 スイッチの IP アドレスを設定する方法を示します。

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

次の例では、レイヤ 3 スイッチ上のポートに IP アドレスを設定する方法を示します。

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip admission

Web 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、fallback-profile 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

構文の説明

rule	IP アドミッション ルールをインターフェイスに適用します。

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
15.0(1)EY	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 コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

例

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。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1/1
Switch(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。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

関連コマンド

コマンド	説明
dot1x fallback	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。
fallback profile	ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show ip admission	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。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip admission name proxy http

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 proxy http** 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 proxy http

no ip admission name proxy http

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

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
15.0(1)EY	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 proxy http コマンドにより、Web 認証がスイッチ上でグローバルにイネーブルになります。

スイッチで Web 認証をグローバルに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。

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

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

関連コマンド

コマンド	説明
dot1x fallback	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。
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。
show ip admission	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。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip arp inspection filter vlan

ダイナミック アドレス解決プロトコル（ARP）インスペクションがイネーブルの場合に、スタティック IP アドレスが設定されたホストからの ARP 要求および応答を許可または拒否するには、グローバル コンフィギュレーション モードで **ip arp inspection filter 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。

ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

構文の説明

arp-acl-name	ARP アクセス コントロール リスト（ACL）の名前
vlan-range	VLAN の番号または範囲。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
static	（任意）ARP ACL の暗黙的な拒否を明示的な拒否として処理し、ACL 内の以前の句と一致しないパケットを廃棄します。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。

コマンド デフォルト

VLAN には、定義された ARP ACL が適用されていません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ARP ACL がダイナミック ARP インスペクションの VLAN に適用されている場合、IP-to-MAC 15.0(1)EY のアドレス バインディングを持つ ARP パケットだけが ACL と比較されます。ACL がパケットを許可すると、スイッチがパケットを転送します。それ以外のすべてのパケット タイプは、検証されずに、入力 VLAN 内でブリッジングされます。

スイッチが ACL 内の明示的な拒否ステートメントによってパケットを拒否すると、パケットがドロップされます。スイッチが暗黙の拒否ステートメントによってパケットを拒否すると、パケットは DHCP バインディングのリストと照合されます。ただし、ACL がスタティック（パケットがバインディングと比較されない）である場合を除きます。

ARP ACL を定義、または定義済みのリストの末尾に句を追加するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、ダイナミック ARP インスペクション用に ARP ACL static-hosts を VLAN 1 に適用する方法を示します。

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

設定を確認するには、**show ip arp inspection vlan 1** 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
arp access-list	ARP ACL を定義します。
deny（**ARP アクセス リスト コンフィギュレーション**）	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
permit（**ARP アクセス リスト コンフィギュレーション**）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。

ip arp inspection limit

インターフェイスのアドレス解決プロトコル（ARP）の入力要求および応答のレートを制限するには、インターフェイス コンフィギュレーション モードで **ip arp inspection limit** コマンドを使用します。DoS 攻撃が発生した場合にダイナミック ARP インスペクションによってスイッチ リソースのすべてが消費されないようにします。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。

ip arp inspection limit {**rate** *pps* [**burst interval** *seconds*] | **none**}

no ip arp inspection limit

構文の説明

rate *pps*	1 秒間に処理される入力パケット数の上限を指定します。範囲は、0 ～ 2048 pps です。
burst interval *seconds*	（任意）インターフェイスで高速 ARP パケットをモニタリングする連続的インターバルを秒単位で指定します。範囲は 1 ～ 15 秒です。
none	処理可能な着信 ARP パケットのレートに上限を指定しません。

コマンド デフォルト

1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチド ネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。

信頼できるすべてのインターフェイスでは、レート制限は行われません。

バースト インターバルは 1 秒です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

レートは、信頼できるインターフェイスおよび信頼できないインターフェイスの両方に適用されます。複数のダイナミック ARP インスペクション対応 VLAN でパケットを処理するようにトランクに適切なレートを設定するか、**none** キーワードを使用してレートを無制限にします。

スイッチが、設定されているレートを超えるレートのパケットを、バーストの秒数を超える連続する秒数受信すると、インターフェイスが errdisable ステートになります。

インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** 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と、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートは、集約が反映されるように、より大きいレートに設定する必要があります。着信パケットのレートが、ユーザが定義したレートを超えると、スイッチはインターフェイスを errdisable ステートにします。errdisable 回復機能は、回復の設定に従ってポートを errdisable ステートから自動的に移行させます。

EtherChannel ポートの着信 ARP パケットのレートは、すべてのチャネル メンバの着信 ARP パケット レートの合計と同じです。EtherChannel ポートのレート制限は、必ずすべてのチャネル メンバの着信 ARP パケットのレートを調べてから設定してください。

例

次の例では、ポート上の着信 ARP 要求のレートを 25 pps に制限し、インターフェイスのモニタリング インターバルを 5 秒間に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 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
show inventory interfaces	指定のインターフェイス、またはすべてのインターフェイスに対して、ARP パケットの信頼状態およびレート制限を表示します。

ip arp inspection log-buffer

ダイナミック アドレス解決プロトコル（ARP）インスペクションのロギング バッファを設定するには、グローバル コンフィギュレーション モードで **ip arp inspection log-buffer** 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。

ip arp inspection log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}

no ip arp inspection log-buffer {**entries** | **logs**}

構文の説明

entries *number*	バッファに記録されるエントリを指定します。指定できる範囲は 0 ～ 1024 です
logs *number* **interval** *seconds*	システム メッセージを生成するために、指定された間隔で必要なエントリを指定します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。

コマンド デフォルト

ダイナミック ARP がイネーブル、拒否またはドロップされると、ARP パケットが記録されます。

ログ エントリ数は、32 です。

システム メッセージ数は、毎秒 5 つに制限されます。

ロギングレート インターバルは、1 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

0 の値は、**logs** および **interval** キーワードの両方で許可されていません。

logs および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、X 割る Y（X/Y）のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y 割る X（Y/X）秒ごとに送信されます。たとえば、**logs** *number* が 20 で、**interval** *seconds* が 4 の場合、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

ログ バッファ エントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同一の VLAN 上のパケットを同一の ARP パラメータで多数受信すると、スイッチは、ログ バッファ内の 1 つのエントリとしてパケットを結合し、1 つのエントリとしてシステム メッセージを生成します。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリに対しては、その他の統計情報は表示されません。出力にこのようなエントリが表示される場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

例

次の例では、最大 45 のエントリを保持できるようにロギング バッファを設定する方法を示します。

```
Switch(config)# ip arp inspection log-buffer entries 45
```

次の例では、ロギング レートを 4 秒あたり 20 のログ エントリに設定する方法を示します。この設定では、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

設定を確認するには、**show ip arp inspection log** 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
arp access-list	ARP アクセス コントロール リスト（ACL）を定義します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show inventory log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

ip arp inspection trust

検査対象の着信アドレス解決プロトコル（ARP）パケットを指定するインターフェイスの信頼状態を設定するには、インターフェイス コンフィギュレーション モードで **ip arp inspection trust** 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。

ip arp inspection trust

no ip arp inspection trust

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

インターフェイスは、信頼できない状態です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

スイッチは、信頼できるインターフェイス上で受信した ARP パケットを確認せず、単純にパケットを転送します。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。

例

次の例では、ポートを信頼できる状態に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 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
ip arp inspection log-buffer	ダイナミック ARP インスペクション ロギング バッファを設定します。
show inventory interfaces	指定のインターフェイス、またはすべてのインターフェイスに対して、ARP パケットの信頼状態およびレート制限を表示します。
show inventory log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

ip arp inspection validate

ダイナミック アドレス解決プロトコル（ARP）インスペクションの特定のチェックを実行するには、グローバル コンフィギュレーション モードで **ip arp inspection validate** 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。

ip arp inspection validate {[**src-mac**] [**dst-mac**] [**ip** [**allow zeros**]]}

no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip** [**allow zeros**]]

構文の説明

src-mac	（任意）イーサネット ヘッダーの送信元 MAC アドレスを ARP 本文の送信側 MAC アドレスと比較します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。
dst-mac	（任意）イーサネット ヘッダーの宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較します。この検査は、ARP 応答に対して実行されます。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。
ip	（任意）ARP 本文を確認して、無効な IP アドレスや予期しない IP アドレスがないかを比較します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信側 IP アドレスは、すべての ARP 要求および応答と比較されます。ターゲット IP アドレスは ARP 応答でだけチェックされます。
allow-zeros	（任意）送信側アドレスが 0.0.0.0（ARP プローブ）である ARP が拒否されないように、IP 検証テストを変更します。

コマンド デフォルト

検査は実行されません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが **src-mac** および **dst-mac** の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって **src-mac** および **dst-mac** の検証がディセーブルになります。

allow-zeros キーワードは、次の方法で ARP アクセス コントロール リスト（ACL）と連動します。

- ARP ACL が ARP プローブを拒否するように設定されている場合は、**allow-zero** キーワードが指定されていても、ARP プローブはドロップされます。
- ARP プローブを明確に許可する ARP ACL を設定し、**ip arp inspection validate ip** コマンドを設定する場合、**allow-zeros** キーワードを入力しない限り、ARP プローブはドロップされます。

このコマンドの **no** 形式を使用すると、指定されたチェックだけがディセーブルになります。どのオプションもイネーブルにしない場合は、すべてのチェックがディセーブルになります。

例

次に、送信元 MAC の検証をイネーブルにする例を示します。

```
Switch(config)# ip arp inspection validate src-mac
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 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
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。

ip arp inspection vlan

VLAN 単位でダイナミック アドレス解決プロトコル（ARP）インスペクション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 arp inspection 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。

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

構文の説明

vlan-range	VLAN の番号または範囲。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

すべての VLAN で ARP インスペクション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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ダイナミック ARP インスペクションをイネーブルにする VLAN を指定する必要があります。

ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、または EtherChannel ポートでサポートされます。

例

次の例では、VLAN 1 でダイナミック ARP インスペクションをイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection vlan 1
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 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
arp access-list	ARP アクセス コントロール リスト（ACL）を定義します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。

ip arp inspection vlan logging

VLAN 単位で記録するパケットのタイプを制御するには、グローバル コンフィギュレーション モードで **ip arp inspection vlan logging** コマンドを使用します。このロギング制御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 arp inspection vlan *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**} | **arp-probe**}

no ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **dhcp-bindings** | **arp-probe**}

構文の説明

vlan-range	ロギング用に設定された VLAN。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
acl-match {**matchlog** | **none**}	アクセス コントロール リスト（ACL）との一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **matchlog**：アクセス コントロール エントリ（ACE）に指定されたロギング設定に基づいてパケットを記録します。このコマンドに **matchlog** キーワード、**permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否されたアドレス解決プロトコル（ARP）パケットが記録されます。 • **none**：ACL に一致するパケットを記録しません。
dhcp-bindings {**permit** | **all** | **none**}	Dynamic Host Configuration Protocol（DHCP）バインディングとの一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **all**：DHCP バインディングと一致するすべてのパケットをロギングします。 • **none**：DHCP バインディングに一致するパケットを記録しません。 • **permit**：DHCP バインディングで許可されたパケットをロギングします。
arp-probe	具体的に許可されたパケットが ARP プローブである場合に、パケットのロギングを指定します。

コマンド デフォルト

拒否またはドロップされたパケットは、すべて記録されます。ARP プローブ パケットは記録されません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

logged の用語は、エントリがログ バッファに置かれ、システム メッセージが生成されることを意味します。

acl-match キーワードと **dhcp-bindings** キーワードは連携しています。ACL の一致を設定すると、DHCP バインディングの設定はディセーブルになりません。ロギング基準をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。いずれのオプションも指定しない場合は、ARP パケットが拒否されたときに、すべてのロギング タイプが記録されるようにリセットされます。使用できるオプションは、次の 2 つです。

- **acl-match**：拒否されたパケットが記録されるように、ACL との一致に関するロギングがリセットされます。
- **dhcp-bindings**：拒否されたパケットが記録されるように、DHCP バインディングとの一致に関するロギングがリセットされます。

acl-match キーワードと **dhcp-bindings** キーワードのどちらも指定されないと、拒否されたすべてのパケットが記録されます。

ACL の末尾にある暗黙の拒否には、**log** キーワードが含まれません。つまり、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドで **static** キーワードを使用した場合、ACL は DHCP バインディングを上書きします。ARP ACL の末尾で明示的に **deny ip any mac any log** ACE を指定しない限り、拒否された一部のパケットが記録されない場合があります。

例

次の例では、ACL 内の **permit** コマンドと一致するパケットを記録するように、VLAN 1 の ARP インスペクションを設定する方法を示します。

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 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
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP インスペクション ロギング バッファを設定します。
show inventory log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。

ip dhcp snooping

DHCP スヌーピングをグローバルに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 dhcp snooping** 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。

ip dhcp snooping

no ip dhcp snooping

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
15.0(1)EY	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、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。

ip dhcp snooping vlan *vlan-id* 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 VLAN 上でスヌーピングをイネーブルにするまで DHCP スヌーピングはアクティブになりません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping vlan	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip igmp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping binding

DHCP スヌーピング バインディング データベースを設定し、バインディング エントリをデータベースに追加するには、特権 EXEC モードで **ip dhcp snooping binding** コマンドを使用します。バインディング データベースから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 dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	MAC アドレス。
vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 4094 です。
ip-address	IP アドレス。
interface *interface-id*	バインディング エントリを追加または削除するインターフェイスを指定します。
expiry *seconds*	バインディング エントリが無効になるまでのインターバル（秒）を指定します。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

デフォルトのデータベースは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
15.0(1)EY	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、スイッチをテストまたはデバッグするときに使用します。

DHCP スヌーピング バインディング データベースでは、各データベース エントリ（別名、バインディング）には、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進数）、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、8192 のバインディングを含めることができます。

設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。動的および静的に設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポートに、有効期限が 1000 秒の DHCP バインディング設定を生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/1 expiry 1000
```

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングおよび設定情報を表示します。
show ip source binding	DHCP スヌーピング バインディング データベース内の動的および静的に設定されたバインディングを表示します。

ip dhcp snooping database

DHCP スヌーピング バインディング データベース エージェ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 **ip dhcp snooping database** コマンドを使用します。エージェントのディセーブル化、タイムアウト値のリセット、または書き込み遅延値のリセットを行うには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {{**flash:**/*filename* | **ftp:**//*user:password@host/filename* | **http:**//[[*username:password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** | **rcp:**//*user@host/filename* | **tftp:**//*host/filename*} | **timeout** *seconds* | **write-delay** *seconds*}

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

構文の説明

flash:/*filename*	データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。
ftp://*user*:*password*@*host*/*filename*	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
http://*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar**	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
rcp://*user@host/filename*	データベース エージェントまたはバインディング ファイルがリモート コピー プロトコル（RCP）サーバにあることを指定します。
tftp://*host/filename*	データベース エージェントまたはバインディング ファイルが TFTP サーバにあることを指定します。
timeout *seconds*	データベース転送プロセスを打ち切るまでの時間（秒）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
write-delay *seconds*	バインディング データベースが変更された後に、転送を遅らせる期間（秒）を指定します。デフォルト値は 300 秒です。指定できる範囲は 15 ～ 86400 です。

コマンド デフォルト

データベース エージェントまたはバインディング ファイルの URL は、定義されていません。

タイムアウト値は、300 秒（5 分）です。

書き込み遅延値は、300 秒（5 分）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
15.0(1)EY	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 バインディング データベースには、8192 のバインディングを含めることができます。

データベース内のリース時間を正確な時間にするには、ネットワーク タイム プロトコル（NTP）をイネーブルにし、次の機能を設定することを強く推奨します。

- NTP 認証
- NTP ピアおよびサーバ アソシエーション
- NTP ブロードキャスト サービス
- NTP アクセス制限
- NTP パケット送信元 IP アドレス

NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。

NVRAM とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを TFTP サーバ上に保存することを推奨します。スイッチがネットワークベースの URL（TFTP や FTP など）の設定済み URL 内のバインディング ファイルにバインディングを書き込む前に、この URL に空のファイルを作成しておく必要があります。

DHCP スヌーピング バインディング データベースを NVRAM に保存するには、**ip dhcp snooping database flash:***filename* コマンドを使用します。**ip dhcp snooping database timeout** コマンドに 0 秒を設定し、データベースを TFTP ファイルに書き込んでいるときに、TFTP サーバがダウンした場合、データベース エージェントは転送を無期限に続けようとします。この転送が進行中の間、他の転送は開始されません。サーバがダウンしている場合、ファイルを書き込むことができないため、これはあまり重要ではありません。

エージェントをディセーブルにするには、**no ip dhcp snooping database** コマンドを使用します。

タイムアウト値をリセットするには、**no ip dhcp snooping database timeout** コマンドを使用します。

書き込み遅延値をリセットするには、**no ip dhcp snooping database write-delay** コマンドを使用します。

例

次の例では、IP アドレス 10.1.1.1 の directory という名前のディレクトリ内にバインディング ファイルを保存する方法を示します。TFTP サーバに file という名前のファイルが存在しなければなりません。

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

次の例では、NVRAM に file01.txt というバインディング ファイルを保存する方法を示します。

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

設定を確認するには、**show ip dhcp snooping database** 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
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping information option

DHCP オプション 82 データ挿入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 dhcp snooping information option** コマンドを使用します。DHCP オプション 82 データ挿入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 dhcp snooping information option

no ip dhcp snooping information option

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 オプション 82 データは挿入されます。

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
15.0(1)EY	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、スイッチがホストからの DHCP 要求を受信すると、オプション 82 情報がパケットに追加されます。オプション 82 情報には、スイッチ MAC アドレス（リモート ID サブオプション）、およびパケットが受信された **vlan-mod-port**（回線 ID サブオプション）のポート ID が含まれます。スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

DHCP サーバがパケットを受信する場合、リモート ID、回線 ID、または両方を使用して IP アドレスを割り当てるとともに、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数の制限などのポリシーを適用することができます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。

スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同じサブネット上にある場合は、サーバはこの応答をブロードキャストします。スイッチは、リモート ID または回線 ID フィールドを検査し、オプション 82 データが最初から挿入されていたかを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP ホストに接続するスイッチ ポートにパケットを転送します。

例

次に、DHCP Option 82 データ挿入をイネーブルにする例を示します。

```
Switch(config)# ip dhcp snooping information option
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping information option allow-untrusted

オプション 82 情報を持つ DHCP パケットを、エッジ スイッチに接続されている信頼できないポートで受信したアグリゲーション スイッチで受信する場合は、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 allow-untrusted** 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。

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

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

スイッチは、エッジ スイッチに接続されている信頼できないポートで受信する、オプション 82 情報を持つ DHCP パケットをドロップします。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

ホストに接続されたエッジ スイッチが、ネットワークのエッジで DHCP オプション 82 情報を挿入するように設定したい場合があります。また集約スイッチでは、DHCP スヌーピング、IP ソース ガード、またはダイナミック アドレス解決プロトコル（ARP）インスペクションなどの DHCP セキュリティ機能をイネーブルにすることもできます。ただし、アグリゲーション スイッチで DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないポートで受信されたオプション 82 情報を持つパケットをドロップし、信頼できるインターフェイスに接続されたデバイスの DHCP スヌーピング バインディングを学習しません。

ホストに接続されたエッジ スイッチがオプション 82 情報を挿入する場合に、アグリゲーション スイッチで DHCP スヌーピングを使用するには、アグリゲーション スイッチで **ip dhcp snooping information option allow-untrusted** コマンドを入力します。アグリゲーション スイッチは信頼できないポートで DHCP スヌーピング パケットを受信しますが、ホストのバインディングを学習できます。アグリゲーション スイッチで DHCP セキュリティ機能をイネーブルにすることも可能です。アグリゲーション スイッチが接続されているエッジ スイッチ上のポートは、信頼できるポートとして設定する必要があります。

（注） 信頼できないデバイスが接続されたアグリゲーション スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

例

次の例では、アクセス スイッチが、エッジ スイッチからの信頼できないパケットのオプション 82 情報を確認せずに、パケットを受け入れるように設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

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、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 [**string** *ASCII-string* | **hostname**]

no ip dhcp snooping information option format remote-id

構文の説明

string *ASCII-string*	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。
hostname	スイッチのホスト名をリモート ID として指定します。

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
15.0(1)EY	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。

例

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。

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

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping limit rate

インターフェイスが秒単位で受信できる DHCP メッセージ数を設定するには、インターフェイス コンフィギュレーション モードで **ip dhcp snooping limit rate** 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。

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

構文の説明

rate	インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数。指定できる範囲は 1 ～ 2048 です。

コマンド デフォルト

DHCP スヌーピング レート制限は、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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

通常、レート制限は信頼できないインターフェイスに適用されます。信頼できるインターフェイスのレート制限を設定する場合、信頼できるインターフェイスはスイッチ内の複数の VLAN 上（一部はスヌーピングされない場合があります）の DHCP トラフィックを集約するので、インターフェイス レート制限を高い値に調整する必要があることに注意してください。

レート制限を超えた場合、インターフェイスが errdisable になります。**errdisable recovery dhcp-rate-limit** 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エラー回復をイネーブルにした場合、インターフェイスはすべての原因が時間切れになった際に動作を再試行します。エラー回復メカニズムがイネーブルでない場合、**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までインターフェイスは errdisable ステートのままです。

例

次の例は、インターフェイス上でメッセージ レート制限を 1 秒あたり 150 メッセージに設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

関連コマンド

コマンド	説明
errdisable recovery	回復メカニズムを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping trust

DHCP スヌーピングでは信頼できるポートとしてポートを設定するには、インターフェイス コンフィギュレーション モードで **ip dhcp snooping trust** 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。

ip dhcp snooping trust

no ip dhcp snooping trust

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 スヌーピング信頼は、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
15.0(1)EY	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 サーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCP クライアントに接続されたポートを信頼できないポートとして設定します。

例

次の例では、ポート上で DHCP スヌーピング信頼をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping verify

DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスに一致するようにスイッチを信頼できないポート上で確認するように設定するには、グローバル コンフィギュレーション モードで **ip dhcpsnooping verify** コマンドを使用します。スイッチが MAC アドレスを確認しないように設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-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

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

サービスプロバイダー ネットワークで、スイッチが信頼できないポートの DHCP クライアントからパケットを受信した場合、スイッチは自動的に送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致するかを確認します。アドレスが一致する場合、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

例

次の例では、MAC アドレス確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

VLAN 上で DHCP スヌーピング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 dhcp snooping 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。

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

構文の説明

vlan-range	DHCP スヌーピングをイネーブルにする VLAN ID または VLAN 範囲を指定します。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。

コマンド デフォルト

すべての VLAN 上で DHCP スヌーピングがディセーブルです。

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
15.0(1)EY	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 上で DHCP スヌーピングをイネーブルにする前に、まず 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。

例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping vlan information option format-type circuit-id string

オプション 82 サーキット ID サブオプ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 **ip dhcp snooping vlan information option format-type circuit-id string** コマンドを使用します。デフォルトのサーキット 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 vlan *vlan-id* **information option format-type circuit-id** [**override**] **string** *ASCII-string*

no ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id** [**override**] **string**

（注）　このコマンドは IP サービス イメージが実行されているスイッチでのみサポートされます。

構文の説明

vlan *vlan-id*	VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
override	（任意）3 ～ 63 の ASCII 文字（スペースなし）を使用して、上書き文字列を指定します。
string *ASCII-string*	3 ～ 63 の ASCII 文字（スペースなし）を使用して、サーキット ID を指定します。

コマンド デフォルト

vlan-mod-port 形式のスイッチ VLAN およびポート ID は、デフォルトのサーキット ID 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
15.0(1)EY	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、デフォルトのサーキット ID サブオプションは、**vlan-mod-port** 形式のスイッチ VLAN およびポート ID です。このコマンドを使用すると、サーキット ID となる ASCII 文字列を設定できます。**vlan-mod-port** フォーマット タイプを無効にし、その代わりにサーキット ID を使用して、加入者情報を定義する場合、**override** キーワードを使用します。

（注）　スイッチ上で文字数の多いサーキット ID を設定する場合、NVRAM またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。

例

次の例では、オプション 82 サーキット ID サブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

次の例では、オプション 82 サーキット ID 上書きサブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

（注） リモート ID 設定を含むグローバル コマンド出力だけを表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。サーキット ID として設定したインターフェイス単位または VLAN 単位の文字列は表示されません。

関連コマンド

コマンド	説明
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します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip igmp filter

レイヤ 2 インターフェイス上のすべてのホストがインターネット グループ管理プロトコル（IGMP）プロファイルをインターフェイスに適用することにより、1 つまたは複数の IP マルチキャスト グループに加入できるかどうかを制御するには、インターフェイス コンフィギュレーション モードで **ip igmp filter** コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*

no ip igmp filter

構文の説明

profile number	適用する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP のフィルタは適用されていません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

IGMP のプロファイルは 1 つまたは複数のポート インターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

例

次の例では、IGMP プロファイル 22 をポートに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp filter 22
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
ip igmp profile	指定された IGMP プロファイル番号を設定します。
show ip dhcp snooping statistics	指定された IGMP プロファイルの特性を表示します。
show running-config interface *interface-id*	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能なインターネット グループ管理プロトコル（IGMP）グループの最大数を設定、または転送テーブル内でエントリが最大数に達する場合の IGMP スロットリング動作を設定するには、インターフェイス コンフィギュレーション モードで **ip igmp max-groups** コマンドを使用します。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリング アクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

構文の説明

number	インターフェイスが参加できる IGMP グループの最大数。指定できる範囲は 0 ～ 4294967294 です デフォルト設定は無制限です。
action deny	最大数のエントリが IGMP スヌーピング転送テーブルにある場合、次の IGMP Join レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループに置き換えます。

コマンド デフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループ エントリの最大数があることをスイッチが学習した後の、デフォルトのスロットリング アクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

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
15.0(1)EY	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、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、または EtherChannel グループに属するポートに対して IGMP 最大グループ数を設定することはできません。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- スロットリング アクションを **deny** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートをスイッチがドロップします。
- スロットリング アクションを **replace** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したマルチキャスト エントリを受信した IGMP レポートと置き換えます。
- 最大グループ制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups** {**deny** | **replace**} コマンドを入力しても無効です。

例

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるように設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
show running-config interface *interface-id*	インターフェイスが参加できる IGMP グループの最大数やスロットリング アクションなど、スイッチのインターフェイス上で実行コンフィギュレーションを表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip igmp profile

インターネット グループ管理プロトコル（IGMP）プロファイルを作成し、IGMP プロファイル 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 **ip igmp profile** コマンドを指定します。このモードで、スイッチポートからの IGMP メンバーシップ レポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*

no ip igmp profile *profile number*

構文の説明

profile number	設定する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否することを指定します。これがデフォルトの状態です。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にする、またはデフォルトにリセットします。
- **permit**：一致するアドレスを許可することを指定します。
- **range**：プロファイルの IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

関連コマンド

コマンド	説明
ip igmp filter	指定のインターフェイスに対し、IGMP を適用します。
show ip dhcp snooping statistics	すべての IGMP プロファイルまたは指定の IGMP プロファイル番号の特性を表示します。

ip igmp snooping

スイッチでインターネット グループ管理プロトコル（IGMP）スヌーピングをグローバルにまたは VLAN 単位でイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping** 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。

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

コマンド デフォルト

スイッチ上で、IGMP スヌーピングはグローバルにイネーブルです。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip dhcp snooping statistics	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping last-member-query-interval

インターネット グループ管理プロトコル（IGMP）の設定可能な Leave タイマーをグローバルに、または VLAN 単位でイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping last-member-query-interval** 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。

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval**

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび Leave タイマーをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
time	秒単位のタイムアウト間隔。指定できる範囲は 100 ～ 32768 ミリ秒です。

コマンド デフォルト

デフォルトのタイムアウト設定は 1000 ミリ秒です。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN 上に Leave タイマーを設定すると、グローバル設定を上書きします。

IGMP 設定可能な Leave タイムは、IGMP バージョン 2 を実行するデバイスでだけサポートされます。

設定は、NVRAM に保存されます。

例

次の例では、IGMP Leave タイマーを 2000 ミリ秒でグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

次の例では、VLAN 1 上で IGMP Leave タイマーを 3000 ミリ秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan immediate-leave	IGMP 即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをグループのメンバとして設定します。
show ip igmp snooping	IGMP スヌーピング設定を表示します。

ip igmp snooping querier

レイヤ 2 ネットワークのインターネット グループ管理プロトコル（IGMP）クエリア機能をグローバルに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 igmp snooping querier** コマンドを使用します。キーワードとともにコマンドを入力すると、VLAN インターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。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。

ip igmp snooping querier [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

no ip igmp snooping querier [**vlan** *vlan-id*] [**address** | **max-response-time** | **query-interval** | **tcn query** { **count** *count* | **interval** *interval*} | **timer expiry** | **version**]

構文の説明

vlan *vlan-id*	（任意）指定した VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
address *ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time *response-time*	（任意）IGMP クエリア レポートを待機する最長時間を設定します。指定できる範囲は 1 ～ 25 秒です。
query-interval *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
tcn query[count *count* | **interval** *interval*]	（任意）トポロジ変更通知（TCN）に関連するパラメータを設定します。キーワードの意味は次のとおりです。 • **count** *count*：TCN 時間間隔に実行される TCN クエリーの数を設定します。指定できる範囲は 1 ～ 10 です。 • **interval** *interval :* TCN クエリー間隔を設定します。指定できる範囲は 1 ～ 255 です。
timer expiry	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
version *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

コマンド デフォルト

IGMP スヌーピング クエリア機能は、スイッチでグローバルにイネーブルです。

イネーブルになっている場合、マルチキャスト対応デバイスから IGMP トラフィックを検出すると、IGMP スヌーピング クエリアはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリー メッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピング クエリアは、IGMP *バージョン 2*（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP *バージョン 1*（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time** 値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、**max-response-time** を設定できません （値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリー メッセージを拒否することがあります。デバイスで IGMP 一般クエリー メッセージを受け入れる場合、IGMP スヌーピング クエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピング クエリア機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピング クエリアの時間間隔を 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピング クエリアの TCN クエリー カウントを 25 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier version 2
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。

ip igmp snooping report-suppression

インターネット グループ管理プロトコル（IGMP）レポート抑制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 igmp snooping report-suppression** コマンドを使用します。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャスト ルータへ転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

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

IGMP レポート抑制はイネーブルです。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャスト ルータに送信されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
Switch(config)# no ip igmp snooping report-suppression
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn

インターネット グループ管理プロトコル（IGMP）トポロジ変更通知 (TCN) の動作を設定するには、グローバル コンフィギュレーション モードで **ip igmp snooping tcn** 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。

ip igmp snooping tcn {**flood query count** *count* | **query solicit**}

no ip igmp snooping tcn {**flood query count** | **query solicit**}

構文の説明

flood query count *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。
query solicit	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。

コマンド デフォルト

TCN フラッド クエリー カウントは 2 です。

TCN クエリー要求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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

TCN イベント後にマルチキャスト トラフィックがフラッディングする時間を制御するには、**ip igmp snooping tcn flood query count** 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。**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッド クエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャスト トラフィックのフラッディングは、7 つの一般的クエリーを受信するまで継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

スパニングツリー ルートかどうかにかかわらず、グローバル Leave メッセージを送信するようにスイッチをイネーブルにするには、**ip igmp snooping tcn query solicit** 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。また、このコマンドは、TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げます。

例

次の例では、マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を 7 に指定する方法を示します。

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn flood	インターフェイスのフラッディングを IGMP スヌーピング スパニングツリー TCN 動作として指定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn flood

マルチキャスト フラッディングをインターネット グループ管理プロトコル（IGMP）スヌーピング スパニングツリー トポロジ変更通知（TCN）の動作として設定するには、インターフェイス コンフィギュレーション モードで **ip igmp snooping tcn flood** コマンドを使用します。マルチキャスト フラッデ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。

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

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

マルチキャスト フラッディングは、スパニングツリー TCN のイベント中、インターフェイス上でイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	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 TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングします。異なるマルチキャスト グループに加入している接続ホストを持つポートがスイッチに多数ある場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。

ip igmp snooping tcn flood query count *count* 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、フラッディング クエリー カウントを変更できます。

例

次の例では、インターフェイス上でマルチキャスト フラッディングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no ip igmp snooping tcn flood
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn	スイッチで IGMP TCN 動作を設定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping vlan immediate-leave

VLAN 単位でインターネット グループ管理プロトコル（IGMP）スヌーピング即時脱退処理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 igmp snooping immediate-leave** 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。

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

構文の説明

vlan-id	IGMP および即時脱退をイネーブルにする特定の VLAN。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

コマンド デフォルト

IGMP の即時脱退処理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
15.0(1)EY	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 ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN の各ポート上で 1 つのレシーバの最大値が設定されている場合に限り、即時脱退処理の機能を設定してください。設定は、NVRAM に保存されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。

例

次の例では、VLAN 1 で IGMP 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan mrouter

マルチキャスト ルータ ポートを追加したり、マルチキャスト学習方式を設定するには、グローバル コンフィギュレーション モードで **ip igmp snooping vlan mrouter** 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。

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**}}

構文の説明

vlan-id	IGMP スヌーピングをイネーブルにして、指定した VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
interface *interface-id*	マルチキャスト ルータへのネクスト ホップ インターフェイスを指定します。キーワードの意味は次のとおりです。 • **fastethernet** *interface number*：ファスト イーサネット IEEE 802.3 インターフェイス。 • **gigabitethernet** *interface number*：ギガビットイーサネット IEEE 802.3z インターフェイス。 • **port-channel** *interface number :* チャネル インターフェイス。指定できる範囲は 0 ～ 6 です。
learn {**cgmp** | **pim-dvmrp**}	マルチキャスト ルータの学習方式を指定します。キーワードの意味は次のとおりです。 • **cgmp**：Cisco Group Management Protocol（CGMP）パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。 • **pim-dvmrp**：IGMP クエリーおよびプロトコル独立型マルチキャスト ディスタンス ベクトル マルチキャスト ルーティング プロトコル（PIM-DVMRP）パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。

コマンド デフォルト

デフォルトでは、マルチキャスト ルータ ポートはありません。

デフォルトの学習方式は **pim-dvmrp** です。IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。

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
15.0(1)EY	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 ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

CGMP の学習方式は制御トラフィックの削減に役立ちます。

設定は、NVRAM に保存されます。

例

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/1
```

次の例では、マルチキャスト ルータの学習方式を CGMP として指定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan static

インターネット グループ管理プロトコル（IGMP）スヌーピングをイネーブルに、マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、グローバル コンフィギュレーション モードで **ip igmp snooping static** コマンドを使用します。スタティックなマルチキャスト グループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	特定の VLAN の IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
ip-address	指定のグループ IP アドレスを持ったマルチキャスト グループのメンバとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバ ポートのインターフェイスを指定します。キーワードの意味は次のとおりです。 • **fastethernet** *interface number*：ファスト イーサネット IEEE 802.3 インターフェイス。 • **gigabitethernet** *interface number*：ギガビットイーサネット IEEE 802.3z インターフェイス。 • **port-channel** *interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 6 です。

コマンド デフォルト

デフォルトでは、マルチキャスト グループのメンバとしてスタティックに設定されたポートはありません。

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
15.0(1)EY	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 ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM に保存されます。

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet1/1
Configuring port gigabitethernet1/1 on group 0100.5e02.0203
```

設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip source binding

スイッチ上のスタティックな IP 送信元バインディングを設定するには、グローバル コンフィギュレーション モードで **ip source binding** コマンドを使用します。スタティック バインディングを削除するには、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 source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。有効な範囲は 1 ～ 4094 です。
ip-address	IP アドレスを指定します。
interface *interface-id*	IP 送信元バインディングを追加または削除するインターフェイスを指定します。

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
15.0(1)EY	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 IP 送信元バインディング エントリには、IP アドレス、関連付けられた MAC アドレス、および関連付けられた VLAN 番号が含まれます。エントリは、MAC アドレスおよび VLAN 番号に基づいています。IP アドレスだけの変更でエントリを変更する場合は、スイッチは新しいエントリを作成せずに、エントリを更新します。

例

次の例では、スタティック IP 送信元バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/1
```

次の例では、スタティック バインディングを追加してから、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet1/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet1/1
```

コマンド設定を確認するには、**show ip source binding** 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
ip verify source	インターフェイス上の IP 送信元ガードをイネーブルにします。
show ip source binding	スイッチ上の IP 送信元バインディングを表示します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ip ssh

セキュア シェル（SSH）Version 1 または SSH Version 2 を実行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 **ip ssh** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。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。

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

構文の説明

1	（任意）スイッチが SSH バージョン 1（SSHv1）を実行するように設定します。
2	（任意）スイッチが SSH バージョン 2（SSHv1）を実行するように設定します。

コマンド デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

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
15.0(1)EY	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しない場合、またはキーワードを指定しないときは、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。また、SSHv1 クライアントもサポートします。SSH サーバおよび SSH クライアントの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

SSHv1 サーバによって生成された Rivest、Shamir、Adelman（RSA）キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。

例

次の例では、スイッチが SSH バージョン 2 を実行するように設定する方法を示します。

```
Switch(config)# ip ssh version 2
```

設定を確認するには、**show ip ssh** または **show ssh** 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
show ip ssh	SSH サーバがイネーブルであるかどうかを表示すると同時に、SSH サーバのバージョンおよび設定情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show ssh	SSH サーバのステータスを表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip sticky-arp（インターフェイス コンフィギュレーション）

スイッチ仮想インターフェイス（SVI）またはレイヤ 3 インターフェイス上で sticky アドレス解決プロトコル（ARP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip sticky-arp** コマンドを使用します。sticky ARP 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 sticky-arp

no ip sticky-arp

（注）　このコマンドは IP サービス イメージが実行されているスイッチでのみサポートされます。

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　sticky ARP は、レイヤ 3 インターフェイスおよび標準 SVI 上でディセーブルになります。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン　sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。

ip sticky-arp インターフェイス コンフィギュレーション コマンドは、次の上でだけサポートされます。

- レイヤ 3 インターフェイス
- 標準 VLAN に属する SVI

レイヤ 3 インターフェイスまたは標準 VLAN に属する SVI 上で

- sticky ARP をイネーブルにするには、**sticky-arp** 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。
- sticky ARP をディセーブルにするには、**no sticky-arp** 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。
- スイッチをデバイスから取り外し、MAC アドレスは異なるが IP アドレスが同じである別のデバイスに接続する場合、ARP エントリは作成されず、次のメッセージが表示されます。

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- スイッチ上で sticky ARP をディセーブルにするには、**no sticky-arp** 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。
- インターフェイス上で sticky ARP をディセーブルにするには、**no sticky-arp** 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

標準 SVI 上で sticky ARP をイネーブルにする方法：

```
Switch(config-if)# ip sticky-arp
```

レイヤ 3 インターフェイスまたは SVI 上で sticky ARP をディセーブルにする方法：

```
Switch(config-if)# no ip sticky-arp
```

設定を確認するには、**show arp** 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
arp	ARP テーブルに永続的エントリを追加します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。
show arp	ARP テーブル内のエントリを表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ip verify source

インターフェイス上で IP ソース ガードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガード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 verify source [**port-security**]

no ip verify source

構文の説明

port-security	（任意）IP および MAC 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します。 **port-security** キーワードを入力しない場合、IP アドレス フィルタリングによる IP ソース ガードがイネーブルになります。

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
15.0(1)EY	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。

送信元 IP および MAC 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 port-security** 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。

送信元 IP および MAC 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、インターフェイスのポート セキュリティをイネーブルにする必要があります。

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 ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source
```

次の例では、送信元 IP および MAC 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方法を示します。

```
Switch(config-if)# ip verify source port-security
```

コマンド設定を確認するには、**show ip source binding** 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
ip source binding	スイッチにスタティック バインディングを設定します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイスの IPv6 アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** コマンドを使用します。インターフェイスから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。

ipv6 address dhcp [**rapid-commit**]

no ipv6 address dhcp [**rapid-commit**]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

構文の説明

rapid-commit	（任意）アドレス割り当てに 2 つのメッセージ交換方式を許可します。

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

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ipv6 address dhcp インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IPv6 アドレスを動的に学習できます。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。これをイネーブルにすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

例

次の例では、IPv6 アドレスを要求して、rapid-commit オプションをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/3
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# ipv6 address dhcp rapid-commit
```

設定を確認するには、**show ipv6 dhcp interface** 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
show ipv6 dhcp interface	DHCPv6 インターフェイスの情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ipv6 dhcp client request vendor

IPv6 クライアントを Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバのオプションを要求するように設定するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client request** コマンドを使用します。要求を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp client request vendor

no ipv6 dhcp client request vendor

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

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

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

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ベンダー固有オプションを要求するには、**ipv6 dhcp client request vendor** 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。イネーブルにすると、IPv6 アドレスを DHCP から取得するときにだけこのコマンドの確認が行われます。インターフェイスが IPv6 アドレスを取得した後でこのコマンドを入力しても、次回クライアントが DHCP から IPv6 アドレスを取得するまでこのコマンドは有効になりません。

例

次の例では、ベンダー固有オプションの要求をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/3
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# ipv6 dhcp client request vendor-specific
```

関連コマンド

コマンド	説明
ipv6 address dhcp	DHCP からインターフェイスの IPv6 アドレスを取得します。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 操作の一部としてプール アドレスに送信するパケットの数を指定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp ping packets** コマンドを使用します。サーバがプール アドレスに ping を送信しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp ping packets *number*

no ipv6 dhcp ping packets

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

構文の説明

number	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。指定できる範囲は 0 ～ 10 です。

コマンド デフォルト

デフォルトは 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
15.0(1)EY	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプール アドレスに ping を送信します。ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 操作がオフになります。

例

次の例では、DHCPv6 サーバによる 2 回の ping 試行を指定する方法を示します（その後、ping 試行を停止します）。

```
Switch(config)# ipv6 dhcp ping packets 2
```

関連コマンド

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6 サーバ データベースからアドレス競合をクリアします。
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol for IPv6（DHCPv6）プール 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 dhcp pool** 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。

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

構文の説明

poolname	DHCPv6 プールのユーザ定義名。プール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

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ipv6 dhcp pool コマンドは、DHCPv6 プール コンフィギュレーション モードをイネーブルにします。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **address prefix** *IPv6-prefix* : アドレス割り当てのアドレス プレフィックスを設定します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **lifetime** *t1 t2* : IPv6 アドレスの*有効*間隔（秒）および*優先*間隔（秒）を設定します。指定できる範囲は 5 ～ 4294967295 秒です。有効なデフォルト値は 2 日です。優先されるデフォルト値は 1 日です。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。間隔を指定しない場合は、**infinite** を指定します。
- **link-address** *IPv6-prefix* : リンクアドレスの IPv6 プレフィックスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィックスと一致する場合、サーバは設定情報プールを使用します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

- **vendor-specific** : DHCPv6 ベンダー固有のコンフィギュレーション モードをイネーブルにします。使用できるコンフィギュレーション コマンドは、次のとおりです。
  - *vendor-id* : ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
  - **suboption** *number* : ベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。

DHCPv6 設定情報プールを作成してから、**ipv6 dhcp server** 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プールとインターフェイス上のサーバを関連付けます。ただし、情報プールを設定しない場合は、**ipv6 dhcp server** 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 DHCPv6 サーバ機能をインターフェイスでイネーブルにする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィックスを使用しないということは、プールは設定されているオプションだけを返すことを指します。

link-address キーワードを使用すると、必ずしもアドレスを割り当てなくてもリンク アドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレス プール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィックスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次の例では、engineering という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次の例では、testgroup という 3 つのリンク アドレス プレフィックスおよび 1 つの IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、350 というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6 dhcp server	インターフェイスで DHCPv6 サービスをイネーブルにします。
show ipv6 dhcp pool	DHCPv6 設定プールの情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ipv6 dhcp server

インターフェイスで Dynamic Host Configuration Protocol for IPv6（DHCPv6）サービスをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp server** コマンドを使用します。インターフェイスで DHCPv6 サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]

no ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

構文の説明

poolname	（任意）IPv6 DHCP プールのユーザ定義名。プール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。
automatic	（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。
rapid-commit	（任意）2 つのメッセージ交換方式を許可します。
preference *value*	（任意）サーバにより送信されるアドバタイズ メッセージのプリファレンス オプションで伝送されるプリファレンス値を指定します。有効な範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。
allow-hint	（任意）サーバが SOLICIT メッセージ内のクライアント提案を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。

コマンド デフォルト

デフォルトでは、DHCPv6 パケットはインターフェイス上で処理されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
15.0(1)EY	このコマンドが追加されました。

使用上のガイドライン

ipv6 dhcp server インターフェイス コンフィギュレーション コマンドは、指定されたインターフェイスで DHCPv6 サービスをイネーブルにします。

automatic キーワードは、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。サーバは、このリンク アドレスと、すべてのアドレス プレフィックスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィックス一致を探します。サーバは最長一致と関連付けられているプールを選択します。

パケットをクライアントから直接受信した場合、サーバは同じ照合を行いますが、照合を行うときに着信インターフェイスに設定されているすべての IPv6 アドレスを使用します。そして再度、サーバは最長のプレフィックス照合を選択します。

rapid-commit キーワードは、2 つのメッセージ交換を使用できるようにします。

preference キーワードを 0 以外の値とともに設定すると、サーバはプリファレンス オプションを追加して、アドバタイズ メッセージのプリファレンス値を伝送します。この動作は、クライアントによるサーバの選択に影響を与えます。プリファレンス オプションを含まないアドバタイズ メッセージのプリファレンス値は 0 であると見なされます。クライアントが、プリファレンス値が 255 であるアドバタイズ メッセージを受信する場合、クライアントはメッセージの送信元であるサーバに要求メッセージを即時に送信します。

allow-hint キーワードを指定する場合、サーバは送信請求メッセージおよび要求メッセージの有効なクライアント提案アドレスを割り当てます。プレフィックス アドレスは、関連付けられているローカル プレフィックス アドレス プール内にあり、デバイスに割り当てられていない場合は有効です。**allow-hint** キーワードを指定しない場合、サーバはクライアント ヒントを無視して、プール内のフリー リストにあるアドレスが割り当てられます。

DHCPv6 クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。これらの機能の 1 つがすでにイネーブルになっているときに同じインターフェイスで別の機能を設定しようとすると、スイッチは次のメッセージのいずれかを返します。

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

例

次の例では、testgroup というプールの DHCPv6 をイネーブルにします。

```
Switch(config-if)# ipv6 dhcp server testgroup
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	DHCPv6 プールを設定して、DHCPv6 プール コンフィギュレーション モードを開始します。
show ipv6 dhcp interface	DHCPv6 インターフェイスの情報を表示します。構文情報については、『*Cisco IOS Software Command Reference, Release 15.0*』を参照してください。

ipv6 mld snooping

IP version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピングをグローバルにイネーブルにするか、または指定した VLAN でイネーブルにするには、キーワードを指定せずにグローバル コンフィギュレーション モードで **ipv6 mld snooping** コマンドを使用します。MLD スヌーピングを、スイッチ、スイッチ スタック、または VLAN 上で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。

ipv6 mld snooping [**vlan** *vlan-id*]

no ipv6 mld snooping [**vlan** *vlan-id*]

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で IPv6 MLD スヌーピングをイネーブルまたはディセーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD 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。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングがグローバルにディセーブルである場合、すべての既存の VLAN インターフェイスで MLD スヌーピングがディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、デフォルトの状態（イネーブル）であるすべての VLAN インターフェイス上で MLD スヌーピングがイネーブルになります。VLAN 設定は、MLD スヌーピングがディセーブルのインターフェイス上のグローバル コンフィギュレーションを上書きします。

MLD スヌーピングがグローバルにディセーブルである場合、VLAN 上で MLD スヌーピングをイネーブルにできません。MLD スヌーピングがグローバルにイネーブルである場合、個々の VLAN 上で MLD スヌーピングをディセーブルにできます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、MLD スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping
```

次の例では、MLD スヌーピングを VLAN でディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 11
```

設定を確認するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントが期限切れになる前に送信される IP version 6（IPv6）マルチキャスト リスナー検出 Mulitcast Address Specific Query（MASQ）またはクエリーを設定するには、グローバル コンフィギュレーション モードで **ipv6 mld snooping last-listener-query-count** コマンドを使用します。クエリー カウントをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー カウントを設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 7 です。

コマンド デフォルト

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です（グローバル カウントを使用します）。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングでは、IPv6 マルチキャスト ルータはマルチキャスト グループに所属するホストにクエリーを定期的に送信します。ホストがマルチキャスト グループを脱退する場合、ホストは静かに脱退する、または Multicast Listener Done メッセージでクエリーに応答できます（IGMP Leave メッセージに相当）。即時脱退が設定されていない場合（1 つのグループに対し複数のクライアントが同じポート上に存在する場合は設定しない）、設定された last-listener クエリー カウントにより、MLD クライアントが期限切れになる前に送信する MASQ の数が決定します。

VLAN に last-listener クエリー カウントを設定した場合、グローバルに設定された値より優先されます。VLAN の数が設定されていない（デフォルトの 0 に設定されている）場合は、グローバルなカウントが使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー カウントをグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

次の例では、last-listener クエリー カウントを VLAN 10 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-interval	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN 上の IP version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピングの last-listener クエリー間隔を設定するには、グローバル コンフィギュレーション モードの **ipv6 mld snooping last-listener-query-interval** コマンドを使用します。この時間間隔は、Multicast Address Specific Query（MASQ）マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する最大時間です。クエリー時間をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval**

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー間隔を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	MASQ を発行した後マルチキャスト グループからポートを削除するまでにマルチキャスト ルータが待機する時間（1000 秒単位）。指定できる範囲は 100 ～ 32,768 です。デフォルト値は 1000（1 秒）です。

コマンド デフォルト

デフォルトのグローバル クエリー間隔（最大応答時間）は 1000（1 秒）です。

デフォルトの VLAN クエリー間隔（最大応答時間）は 0 です（グローバル カウントが使用されます）。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングでは、IPv6 マルチキャスト ルータが MLD Leave メッセージを受信すると、マルチキャスト グループに所属するホストにクエリーを送信します。一定の時間、ポートから MASQ への応答がない場合、ルータはマルチキャスト アドレスのメンバーシップ データベースからそのポートを削除します。last listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除する前にルータが待機する最大時間です。

VLAN クエリー間隔が設定されていると、グローバル クエリー間隔より優先されます。VLAN 間隔が 0 に設定されていると、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー間隔を 2 秒にグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

次の例では、VLAN 1 用の last-listener クエリー間隔を 5.5 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。

ipv6 mld snooping listener-message-suppression

IP version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピング リスナー メッセージ抑制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 **ipv6 mld snooping listener-message-suppression** コマンドを使用します。MLD スヌーピング リスナー メッセージ抑制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。

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

コマンド デフォルト

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピング リスナー メッセージ抑制は、IGMP レポート抑制に相当します。イネーブルの場合、グループに対する受信 MLDv1 レポートはレポート転送時間ごとに 1 回だけ IPv6 マルチキャスト ルータに転送されます。これにより、重複レポートの転送を避けられます。

例

次の例では、MLD スヌーピング リスナー メッセージ抑制をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

次の例では、MLD スヌーピング リスナー メッセージ抑制をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除する前にスイッチが送信する IP version 6（IPv6）マルチキャスト リスナー検出（MLD）クエリーの数を設定するか、または VLAN ID を入力して VLAN 単位でクエリーの数を設定するには、グローバル コンフィギュレーション モードで **ipv6 mld snooping robustness-variable** コマンドを使用します。変数をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable**

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN にロバストネス変数を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 3 です。

コマンド デフォルト

デフォルトのグローバル ロバストネス変数（リスナーを削除する前のクエリー数）は、2 です。

デフォルトの VLAN ロバストネス変数（マルチキャスト アドレスが期限切れになる前のクエリー数）は 0 です。リスナーの期限の判断には、グローバル ロバストネス変数が使用されます。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ロバストネスは、ポートをマルチキャスト グループから削除する前に送信された応答がなかった MLDv1 クエリー数の点から測定されます。設定された回数送信された MLDv1 クエリーに対して受信した MLDv1 レポートがない場合、ポートが削除されます。グローバル値により、スイッチが応答しないリスナーを削除する前に待機するクエリー数が決定し、VLAN 値が設定されていない VLAN すべてに適用します。

VLAN に設定されたロバストネス値はグローバル値より優先されます。VLAN ロバストネス値が 0（デフォルト）の場合、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、スイッチが応答しないリスナー ポートを削除する前に 3 個のクエリーを送信するようグローバル ロバストネス変数を設定する方法を示します。

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

次の例では、VLAN 1 にロバストネス変数を設定する方法を示します。この値は VLAN のグローバル コンフィギュレーションより優先されます。

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping tcn

IP version 6（IPv6）マルチキャスト リスナー検出（MLD）トポロジ変更通知（TCN）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 **ipv6 mld snooping tcn** コマンドを使用します。デフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

flood query count *integer_value*	フラッディング クエリー カウントを設定します。これは、クエリーの受信を要求したポートだけにマルチキャスト データを転送する前に送信されるクエリー数です。指定できる範囲は 1 ～ 10 です。
query solicit	TCN クエリーの送信請求をイネーブルにします。

コマンド デフォルト

TCN クエリー送信請求はディセーブルです。

イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

例

次の例では、TCN クエリー送信請求をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

次の例では、フラッディング クエリー カウントを 5 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping vlan

VLAN インターフェイスで IP version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピング 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 **ipv6 mld snooping vlan** コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

（注） このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
immediate-leave	（任意）VLAN インターフェイス上で MLD の即時脱退処理をイネーブルにします。この機能をインターフェイス上で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。
mrouter interface	（任意）マルチキャスト ルータ ポートを設定します。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。
static *ipv6-multicast-address*	（任意）指定の IPv6 マルチキャスト アドレスでマルチキャスト グループを設定します。
interface *interface-id*	レイヤ 2 ポートをグループに追加します。マルチキャスト ルータまたはスタティック インターフェイスは、物理ポートまたはインターフェイス範囲 1 ～ 48 の**ポートチャネル** インターフェイスになることができます。

コマンド デフォルト

MLD スヌーピング即時脱退処理はディセーブルです。

デフォルトでは、スタティック IPv6 マルチキャスト グループは設定されていません。

デフォルトでは、マルチキャスト ルータ ポートはありません。

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
15.0(1)EY	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

VLAN の各ポート上に 1 つのレシーバだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM に保存されます。

static キーワードは MLD メンバ ポートを静的に設定するために使用されます。

設定およびスタティック ポートとグループは、NVRAM に保存されます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 3750 または Catalyst 3560 スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、VLAN 1 で MLD 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

設定を確認するには、**show ipv6 mld snooping vlan** *vlan-id* ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	IPv6 MLD スヌーピング設定を表示します。