CHAPTER 2

Catalyst 3750 スイッチ Cisco IOS コマンド

aaa accounting dot1x

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

シンタックスの説明

name	サーバ グループ名。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 リストにあるアカウンティング方式を、アカウンティング サービス用に使用します。
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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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 Security Command Reference』Release 12.2 > 「Authentication, Authorization, and Accounting」> 「Authentication Commands」**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	再認証の試行の間隔（秒）を設定します。

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで Authentication, Authorization, and Accounting（AAA）メソッドを使用するように指定するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。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**} *method1*

no aaa authentication dot1x {**default**}

シンタックスの説明

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使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。

（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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために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 Security Command Reference**』**Release 12.2 >** 「**Authentication, Authorization, and Accounting**」**>** 「**Authentication Commands**」を参照してください。
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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

aaa authorization network

ユーザごとの Access Control List（ACL; アクセス コントロール リスト）や IEEE 802.1x VLAN 割り当てといったすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、**aaa authorization network** 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。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

シンタックスの説明

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

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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
```

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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

action

VLAN アクセス マップ エントリに対してアクションを設定するには、**action** 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

シンタックスの説明

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

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 Access Control List（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** 形式では使用されません。

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 Access Control List（ACL）を設定します。構文情報については、**『Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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 (class-map configuration)	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。

archive copy-sw

特定のスタック メンバー上のフラッシュ メモリから実行イメージを、1 つ以上の別のスタック メンバー上にあるフラッシュ メモリにコピーするには、スタック マスター上で **archive copy-sw** 特権 EXEC コマンドを使用します。

archive copy-sw [**/destination-system** *destination-stack-member-number*] [**/force-reload**] [**leave-old-sw**] [**/no-set-boot**] [**/overwrite**] [**/reload**] [**/safe**] *source-stack-member-number*

シンタックスの説明

/destination-system *destination-stack-member-number*	（任意）実行イメージのコピー先のメンバー番号。指定できる範囲は 1 ～ 9 です。
/force-reload	（任意）ソフトウェア イメージのダウンロードが成功したあと、無条件にシステムのリロードを強制します。
/leave-old-sw	（任意）ダウンロードが成功したあと、古いソフトウェア バージョンを保存します。
/no-set-boot	（任意）新しいソフトウェア イメージのダウンロードが成功したあと、BOOT 環境変数の設定は新しいソフトウェア イメージを示すように変更されません。
/overwrite	（任意）ダウンロードされたソフトウェア 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	（任意）変更された設定が保存されていない場合を除き、イメージをダウンロードした後でシステムをリロードします。
/safe	（任意）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-stack-member-number	実行イメージのコピー元のメンバー番号。指定できる範囲は 1 ～ 9 です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

現行のソフトウェア イメージは、コピー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 ファイルの両方がコピーされます。

新しいイメージは flash: ファイル システムにコピーされます。

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。

（注）　**archive copy-sw** 特権 EXEC コマンドを正常に使用するには、追加されるスタック メンバー スイッチおよびマスターの両方のイメージを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバからダウンロードしておく必要があります。ダウンロードを実行するには、**archive download-sw** 特権 EXEC コマンドを使用します。

互換性のないソフトウェアが搭載されたスイッチにコピーされるイメージは、少なくとも 1 つのメンバーで実行している必要があります。

アップグレードする各メンバーのコマンドで **/destination-system** *destination-stack-member-number* のオプションを繰り返すことで、複数の具体的なメンバーにイメージをコピーできます。*destination-stack-member-number* を指定しなかった場合は、デフォルト設定で、実行中のイメージ ファイルがすべてのメンバーにコピーされます。

/safe または **/leave-old-sw** オプションを使用した場合に、十分なフラッシュ メモリがないと、新しいイメージのコピーに失敗する場合があります。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たために、新しいイメージをコピーしても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できます。詳細については、「delete」（P.2-111）を参照してください。

フラッシュ デバイスのイメージを、コピー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した場合は、新しいイメージが、スイッチ フラッシュ デバイス上のイメージと同じでないことや、いずれのメンバーでも実行中ではないことが、アルゴリズムによって確認されます。イメージが同じである場合には、コピーは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがコピーされます。

新しいイメージをコピーした後で、**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 copy-sw** コマンドで **/reload** か **/force-reload** オプションを指定してください。

source-stack-member-number オプションを使用する場合、次のオプションを 1 つ以上入力できます。

- **/destination-system** *destination-stack-member-number*
- **/force-reload**
- **/leave-old-sw**
- **/no-set-boot**
- **/overwrite**
- **/reload**
- **/safe**

これよりも前にあるいずれかのオプションの前に *source-stack-member-number* オプションを入力する場合は、**archive copy-sw** *source-stack-member-number* コマンドだけを入力できます。

次の例では、**archive copy-sw** コマンドを入力する方法を示します。

- 実行イメージをメンバーから別のメンバーにコピーして、2 つめのメンバーのフラッシュ メモリのソフトウェア イメージ（すでに存在する場合）をコピーしたイメージで上書きするには、**archive copy-sw /destination** *destination-stack-member-number* **/overwrite** *source-stack-member-number* コマンドを入力します。
- 実行イメージをメンバーから別のメンバーにコピーして、現在のソフトウェア イメージを保持しながらイメージのコピー後にシステムをリロードするには、**archive copy-sw /destination** *destination-stack-member-number* **/safe /reload** *source-stack-member-number* コマンドを入力します。

例

次の例では、スタック メンバー 6 から実行イメージをメンバー 8 にコピーする方法を示します。

```
Switch# archive copy-sw /destination-system 8 6
```

次の例では、メンバー 6 から実行イメージを他のすべてのメンバーにコピーする方法を示します。

```
Switch# archive copy-sw 6
```

次の例では、メンバー 5 から実行イメージをメンバー 7 にコピーする方法を示します。2 つめのメンバーのフラッシュ メモリにイメージがすでに存在する場合は、コピーされたイメージで上書きされます。イメージがコピーされたあと、システムはリロードされます。

```
Switch# archive copy-sw /destination-system 7 /overwrite /force-reload 5
```

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 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 download-sw

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

archive download-sw {**/allow-feature-upgrade** | **/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/destination-system** *stack-member-number* | **/only-system-type** *system-type* | **/overwrite** | **/reload** | **/safe**} *source-url*

シンタックスの説明

/allow-feature-upgrade	異なるフィーチャ セットを持つイメージをインストールできます（たとえば、IP ベース イメージから IP サービス イメージへのアップグレード）。
/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に、BOOT 環境変数の設定が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	イメージ上およびスタック上のスタック プロトコル 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。
/destination-system *stack-member-number*	アップグレードする特定のメンバーを指定します。指定できる範囲は 1 ～ 9 です。
/only-system-type *system-type*	アップグレードする特定のシステム タイプを指定します。指定できる範囲は 0 ～ FFFFFFFF です。
/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	変更された設定が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。 • セカンダリ ブート ローダ（BS1）の構文： **bs1:** • スタンドアロン スイッチまたはマスター上のローカル フラッシュ ファイル システムの構文： **flash:** メンバー上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:** • 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 HTTP 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。

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。

ダウンロードするイメージのスタック プロトコル バージョンの互換性は、スタックのバージョンと検査されます。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	**http** および **https** キーワードが追加されました。
12.2(35)SE	**allow-feature-upgrade** および **directory** キーワードが追加されました。

使用上のガイドライン

/allow-feature-upgrade オプションを使用すると、異なるフィーチャ セットを持つイメージをインストールできます（たとえば、IP ベース イメージから IP サービス イメージへのアップグレード）。

Cisco IOS Release 12.2(35)SE からは、**archive download-sw /directory** コマンドを使用して、一度ディレクトリを指定できます。その後に、ダウンロードする tar ファイルや tar ファイル リストを指定するため、tar ファイルごとに完全なパスを指定することはしません。たとえば、**archive download-sw /directory tftp://10.1.1.10/ c3750-ipservices-tar.122-35.SE.tar c3750-ipbase-tar.122-35.SE.tar** と入力することができます。

/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.2-111）を参照してください。

スタックに存在しているバージョンとは異なるスタック プロトコルのバージョンのイメージをダウンロードする場合は、**/no-version-check** オプションを使用します。このオプションを使用する場合は **/destination-system** オプションを使用し、イメージでアップグレードする具体的なメンバーを指定してください。

（注）　**/no-version-check** オプションの使用には注意が必要です。同一のスタックにするためには、マスターを含め、すべてのメンバーで、スタック プロトコルのバージョンが同一である必要があります。このオプションを指定すると、最初にスタック プロトコルのバージョンと、スタックのバージョンの互換性を確認することなく、イメージをダウンロードできます。

アップグレードするスタック メンバーごとのコマンドで **/destination-system** オプションを繰り返すことで、複数のスタック メンバーを指定し、アップグレードできます。

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、またはスタック メンバーで実行中のもの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
```

次の例では、毎回パスを指定しないで 2 つの tar イメージの場所を指定します。

```
Switch# archive download-sw /directory tftp://10.1.1.10/
c3750-ipservices-tar.122-35.SE.tar c3750-ipbase-tar.122-35.SE.tar.
```

次の例では、スタック メンバー 6 および 8 をアップグレードする方法を示します。

```
Switch# archive download-sw /imageonly /destination-system 6 /destination-system 8
tftp://172.20.129.10/test-image.tar
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバー上のフラッシュ メモリにコピーします。
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。
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

archive tar 特権 EXEC コマンドを使用して、tar ファイルの作成、tar ファイル内のファイルのリスト、または tar ファイルからのファイルの抽出を行います。

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

シンタックスの説明

/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 HTTP 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 ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。 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 HTTP 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 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 HTTP 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。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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:c3750-ipservices-12-25.SEB.tar
info (219 bytes)

c3750-ipservices-mz.12-25.SEB/ (directory)
c3750-ipservices-mz.12-25.SEB (610856 bytes)
c3750-ipservices-mz.12-25.SEB/info (219 bytes)
info.ver (219 bytes)
```

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

```
Switch# archive tar /table flash:c3750-ipservices-12-25.SEB.tar
c3750-ipservices-12-25/html
c3750-ipservices-mz.12-25.SEB/html/ (directory)
c3750-ipservices-mz.12-25.SEB/html/const.htm (556 bytes)
c3750-ipservices-mz.12-25.SEB/html/xhome.htm (9373 bytes)
c3750-ipservices-mz.12-25.SEB/html/menu.css (1654 bytes)
<output truncated>
```

次の例では、172.20.10.30 の TFTP 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 copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバー上のフラッシュ メモリにコピーします。
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

archive upload-sw 特権 EXEC コマンドを使用して、既存のスイッチ イメージをサーバにアップロードします。

archive upload-sw [**/source-system-num** *stack member number* | **/version** *version_string*] **destination-url**

シンタックスの説明

/source-system-num *stack member number*	アップロードするイメージを持った特定のスタック メンバーを指定します。
/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。 • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック メンバー上のローカル フラッシュ ファイル システムの構文： f**lash** *member number***:** • 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 HTTP 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。

デフォルト

フラッシュ ファイル システムから現在稼動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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

/version オプションを使用するためには、**/source-system-num** オプションを指定する必要があります。これらのオプションを同時に使用することで、指定のスタック メンバーの特定のイメージ（実行イメージではない）をアップロードできます。

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、スタック メンバー 6 で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 /source-system-num 6 tftp://172.20.140.2/test-image.tar
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバー上のフラッシュ メモリにコピーします。
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

Address Resolution Protocol（ARP; アドレス解決プロトコル）Access Control List（ACL）を定義する場合、または以前定義したリストの最後にコマンドを追加する場合は、**arp 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。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*

シンタックスの説明

acl-name	ACL の名前

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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**：パケットを拒否するように指定します。詳細については、「deny (ARP access-list configuration)」（P.2-113）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**：パケットを転送するように指定します。詳細については、「permit (ARP access-list configuration)」（P.2-417）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（仮想 LAN）に ARP ACL を適用できます。IP/MAC（メディア アクセス制御）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 access-list configuration)	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 access-list configuration)	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 control-direction

authentication control-direction 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 モードを単一方向または双方向に設定します。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	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)# 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)# 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。

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

authentication event 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、ポートの特定の認証イベントに関するアクションを設定します。

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}}**

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}}**

シンタックスの説明

action	認証イベントの必須アクションを設定します。
alive	Authentication, Authorization, and Accounting（AAA）サーバ稼動アクションを設定します。
authorize	ポートを認証します。
dead	AAA サーバ停止アクションを設定します。
fail	失敗認証のパラメータを設定します。
next-method	次の認証方式に移動します。
no-response	非応答ホスト アクションを設定します。
reinitialize	認証済みクライアントすべてを再初期化します。
retry	失敗認証後の再試行の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。
server	AAA サーバ イベントのアクションを設定します。
vlan	1 ～ 4094 で認証失敗 VLAN を指定します。
vlan-id	1 ～ 4094 の VLAN ID 番号です。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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だけが critical-authentication VLAN に移動されます。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 を稼動し、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 認証成功メッセージを受信しても、DHCP 設定プロセスは再初期化できません。

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。

  Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）VLAN、プライマリ プライベート VLAN、または音声 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 Dynamic Host Configuration Protocol（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 VLAN による再認証をイネーブルにしてください。再認証がディセーブルにされていると、制限 VLAN に含まれているポートでは、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)# 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)# 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)# authentication event server alive action reinitialize
```

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。
authentication order	ポートで使用する認証方式の順序を設定します。

コマンド	説明
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

authentication fallback インターフェイス コンフィギュレーション コマンドを使用して、IEEE 802.1x 認証をサポートしないクライアントに対し、Web 認証をフォールバック方式として使用するようにポートを設定します。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*

シンタックスの説明

name	Web 認証のフォールバック プロファイルを指定します。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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)# 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。

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

authentication host-mode 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、ポートで認証マネージャ モードを設定します。

authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

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

シンタックスの説明

multi-auth	ポートのマルチ許可モード（multiauth モード）をイネーブルにします。
multi-domain	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	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	ポートの単一ホスト モードをイネーブルにします。

デフォルト

単一ホスト 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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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、単一ホスト モードを設定する必要があります。単一ホスト 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。

ハブ越しの 8 台までのデバイスに、個別の認証を通じて保護されたポート アクセスの取得を許可するには、マルチ認証モードを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 **multiauth** 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-auth
```

次の例では、ポートの **multi-domain** 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-domain
```

次の例では、ポートの **multi-host** 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 **single-host** モードをイネーブルにする方法を示します。

```
Switch(config)# 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 open

authentication open 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。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

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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)# 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)# 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。

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 order

authentication order 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、ポートで使用する認証方式の順序を設定します。

authentication order [dot1x | mab] {webauth}

no authentication order

シンタックスの説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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 番目の方式として MAB を、3 番目の方式として Web 認証を追加する方法を示します。

```
Switch(config)# 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 番目の認証方式として Web 認証を追加する方法を示します。

```
Switch(config)# 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。
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

authentication periodic 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、ポートで再認証をイネーブルまたはディセーブルにします。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

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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)# 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)# 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。
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 port-control

authentication port-control インターフェイス コンフィギュレーション コマンドを使用して、ポート許可ステートの手動制御をイネーブルにします。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。

authentication port-control {**auto | force-authorized | force-un authorized**}

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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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 メンバーであるポートを 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。
- Switched Port Analyzer（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)# 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)# 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)# 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

authentication priority 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 プライオリティ リストに認証方式を追加します。

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

no auth priority [**dot1x** | **mab**] {**webauth**}

シンタックスの説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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 番目の認証方式として設定する方法を示します。

```
Switch(config)# 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 番目の認証方式として設定する方法を示します。

```
Switch(config)# 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

authentication timer 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、802.1x 対応ポートのタイムアウトと再認証のパラメータを設定します。

authentication timer {{[**inactivity** | **reauthenticate**] [**server** | *am*]} {**restart** *value*}}

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

シンタックスの説明

inactivity	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です。
reauthenticate	自動再認証の試行が開始されるまで時間（秒）です。
server	無許可ポートの認証の試行が行われるまでの間隔（秒）です。
restart	無許可ポートの認証の試行が行われるまでの間隔（秒）です。
value	1 から 65535 までの値（秒）を入力します。

デフォルト

キーワード **inactivity**、**server**、および **restart** は、オフに設定されます。**reauthenticate** キーワードは 1 時間に設定されます。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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)# 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)# 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

authentication violation 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、新しいデバイスがポートに接続するとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続するときに発生する違反モードを設定します。

authentication violation {protect | restrict | shutdown}

no authentication violation {protect | restrict | shutdown}

シンタックスの説明

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。

デフォルト

デフォルトでは、**authentication violation shutdown** モードはイネーブルにされます。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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する場合に、システム エラー メッセージを生成して、ポートを制限モードに変更するように 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するときに、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。

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 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

auto qos voip インターフェイス コンフィギュレーション コマンドを使用して、Quality of Service（QoS）ドメイン内で Voice over IP（VoIP）の QoS を自動設定します。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**]

シンタックスの説明

cisco-phone	このポートが Cisco IP Phone に接続されていると判断し、VoIP の QoS を自動設定します。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。このキーワードは、10 ギガビット イーサネット インターフェイスではサポートされません。
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。このキーワードは、10 ギガビット イーサネット インターフェイスではサポートされません。
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。

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 2-1 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 2-1　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 コントロール 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 = Spanning-Tree Protocol（スパニング ツリー プロトコル）
2. BPDU = Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）
3. DSCP = Differentiated Service Code Point（Diffserv コード ポイント）
4. CoS = Class of Service（サービス クラス）

表 2-2 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 2-2　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	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR [1] 共有	1	0, 1	81%	67%
プライオリティ	2	2, 3, 4, 5, 6, 7	19%	33%

1. SRR = Shaped Round Robin。入力キューは共有モードだけをサポートします。

表 2-3 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 2-3　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	キューの重み（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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(20)SE	**cisco-softphone** キーワードが追加され、生成される auto-QoS の設定が変更されました。
12.2(40)SE	コマンド出力の情報が変更されました。

使用上のガイドライン

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動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 CallManager 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、CLI（コマンドライン インターフェイス）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 はグローバルにイネーブル化され（**mls qos** グローバル コンフィギュレーション コマンド）、その他のグローバル コンフィギュレーション コマンドが追加されます。
- Cisco IP Phone に接続されたネットワーク エッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチにより信頼境界の機能がイネーブルになります。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、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。Cisco IP Phone がない場合、入力分類は、パケットの QoS ラベルを信頼しないように設定されます。スイッチは、ポートの入力キューと出力キューを、表 2-2 および表 2-3 の設定値に従って設定します。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。

  スイッチ ポートが Cisco IOS Release 12.2(37)SE かそれよりも前のリリースで **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、auto-QoS によって Cisco IOS Release 12.2(40)SE に新しく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、ポートの入力キューと出力キューを、表 2-2 および表 2-3 の設定値に従って設定します。
- 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、ポートの入力キューと出力キューを、表 2-2 および表 2-3 の設定値に従って設定します。

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 が稼動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あと、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、ポリシング無しのベスト 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 gigabitethernet2/0/1
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	Shaped Round Robin（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。

コマンド	説明
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。
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 auto-copy-sw

自動アップグレード プロセスをイネーブルにするには、スタック マスターから **boot auto-copy-sw** 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。このコマンドにより、Version-Mismatch モードのスイッチは、いずれかのスタック メンバー上で実行中のソフトウェア イメージをコピーするか、スイッチ スタックのフラッシュ メモリの tar ファイル イメージをコピーして、自動的にアップグレードされます。自動アップグレード プロ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。

boot auto-copy-sw

no boot auto-copy-sw

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

Version-Mismatch モードのスイッチは、スタック上のバージョンと異なるマイナー バージョン番号を持つスイッチです。Version-Mismatch モードのスイッチは、完全に機能しているメンバーとしてはスタックに加入できません。スタックが Version-Mismatch モードのスイッチにコピーできるイメージを保有している場合、自動アップグレード プロセスを使用することで、スタック メンバーから Version-Mismatch モードのスイッチにイメージを自動でコピーできます。その場合、スイッチは Version-Mismatch モードを終了し、再起動後に完全に機能しているメンバーとしてスタックに加入します。

自動アップグレード プロセスは、Version-Mismatch モードのスイッチだけに影響します。既存のスタック メンバーには影響しません。

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。
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

boot auto-download-sw

boot auto-download-sw 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、ソフトウェアの自動アップグレードのために使用する URL パス名を指定します。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 auto-download-sw *source-url*

no boot auto-download-sw

シンタックスの説明

source-url	自動アップグレードのためのソース URL エイリアス。次のオプションがサポートされています。 • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック メンバー上のローカル フラッシュ ファイル システムの構文： f**lash** *member number***:** • 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 HTTP 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。

デフォルト

ディセーブル。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、ソフトウェアの自動アップグレードのために使用する URL パスを指定します。

このコマンドを使用して、バージョンのミスマッチの場合にアクセスするマスタースイッチの URL を設定できます。

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 config-file

システム設定の不揮発性コピーの読み込みおよび書き込みを行うために、Cisco IOS が使用するファイル名を指定するには、スタンドアロン スイッチ上で **boot config-file** 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

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、CONFIG_FILE 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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

自動ブート プロセスの中断をイネーブルにするには、スタンドアロン スイッチ上で **boot enable-break** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

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。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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

boot helper 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、ブート ローダー初期化中に動的にファイルをロードして、ブート ローダーの機能を拡張したり、パッチを当てたりします。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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

boot helper-config-file 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、Cisco IOS ヘルパー イメージが使用す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。このコマンドが設定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 に使用されます。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

シンタックスの説明

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

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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 manual

次回ブート サイクル中にスイッチの手動起動をイネーブルにするには、スタンドアロン スイッチ上で **boot manual** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

システムを次回再起動すると、スイッチはブート ローダー 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。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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を行うために Cisco IOS が使用するファイル名を指定するには、スタンドアロン スイッチ上で **boot private-config-file** 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。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

シンタックスの説明

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

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

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

boot system 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、次回のブート サイクル中にロードする Cisco IOS イメージを指定します。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* ...| **switch** {*number* | **all**}}

no boot system

no boot system switch {*number* | **all**}

シンタックスの説明

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。
switch	Cisco IOS イメージがロードされるスイッチを指定します。
number	スタック メンバーを指定します。
all	すべてのスタック メンバーを指定します。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEA	**switch** {*number* | **all**} キーワードが追加されました。**boot system** コマンドは現在、スイッチ スタックおよびスタンドアロン スイッチ上で正常に動作します。

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。

スタック マスター上で **boot system** *filesystem:/file-url* コマンドを入力した場合、指定したソフトウェア イメージは、次回のブート サイクルの際に、スタック マスター上でだけロードされます。

スタック マスター上で、次回のブート サイクル中に指定のスタック メンバーでソフトウェア イメージがロードされるように指定するには、**boot system switch** *number* コマンドを使用します。次回のブート サイクル中にすべてのスタック メンバー上でソフトウェア イメージがロードされるように指定するには、**boot system switch all** コマンドを使用します。

boot system switch *number* コマンドまたは **boot system switch all** コマンドをスタック マスター上で入力すると、スタック マスターはスタック メンバー（スタック マスターを除く）上にソフトウェア イメージが存在しているかどうか確認します。スタック メンバー上（スタック メンバー 1 など）にソフトウェア イメージが存在しない場合、次のようなエラー メッセージが表示されます。

```
%Command to set boot system switch all xxx on switch=1 failed
```

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。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー 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

channel-group インターフェイス コンフィギュレーション コマンドを使用して、EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたり、この両方を行ったりします。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 modes:
channel-group *channel-group-number* **mode {**{**auto** [**non-silent**]} | {**desirable** [**non-silent}}**

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

On mode:
channel-group *channel-group-number* **mode on**

シンタックスの説明

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 ～ 48 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	Port Aggregation Protocol（PAgP; ポート集約プロトコル）装置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	無条件に PAgP を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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**active** キーワードおよび **passive** キーワードが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。
12.2(25)SEC	LACP はクロススタック EtherChannel をネゴシエートできるようになりました。

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 を設定したあと、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、物理ポート上で稼動している 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。

クロススタック EtherChannel は、最大 2 つの 10 ギガビット イーサネット インターフェイスをサポートします。

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 を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック構成ではできません）。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 メンバーであるポートを 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

次の例では、スタック内の単一のスイッチ上で、EtherChannel を設定する方法を示します。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 gigabitethernet2/0/1 -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
```

次の例では、スタック内の単一のスイッチ上で、EtherChannel を設定する方法を示します。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 gigabitethernet2/0/1 -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
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバー 2 のポートを 2 つ、スタック メンバー 3 のポートを 1 つチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

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
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。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

channel-protocol

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、チャネリングを管理するために、ポート上で使用されるプロトコルを制限します。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

シンタックスの説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	Port Aggregation Protocol（PAgP）で EtherChannel を設定します。

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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

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。

cisp enable

cisp enable グローバル コンフィギュレーション コマンドを使用して、スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント 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します。

cisp enable

no cisp enable

シンタックスの説明

cisp enable	CISP をイネーブルにします。

デフォルト

デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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 VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）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 (global configuration) *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を分類する一致条件を（**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、**class** ポリシーマップ コンフィギュレーション 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*

シンタックスの説明

class-map-name	クラス マップ名です。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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マッチングを行い、IP Differentiated Service Code Point（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。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した 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

パケットと名前を指定したクラスとの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始するには、**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*

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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、次の設定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）。**show 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。詳細は、**match (class-map configuration)** 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 Access Control List（ACL）は 1 つだけです。ACL には複数の Access Control Entry（ACE; アクセス コントロール エントリ）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 (class-map configuration)	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 情報をでクリアするには、**clear dot1x** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

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*	指定されたインターフェイスの IEEE 802.1x 情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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 gigabithethernet1/0/1
```

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、**clear eap sessions** 特権 EXEC 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*] ...

シンタックスの説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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 energywise neighbors

EnergyWise ネイバー テーブルを削除するには、**clear energywise neighbors** 特権 EXEC コマンドを使用します。

clear energywise neighbors

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、ネイバー テーブルを削除する方法を示します。

```
Switch# clear energywise neighbors
Cleared all non static energywise neighbors
```

show energywise neighbors 特権 EXEC コマンドを入力することによって、テーブルが削除されたことを確認できます。

関連コマンド

コマンド	説明
show energywise neighbors	EnergyWise ネイバー テーブルを表示します。

clear errdisable interface

errdisable になっていた VLAN を再度イネーブルにするには、**clear errdisable interface** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンドのデフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

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

次の例では、ポート Gi4/0/2 で error-disable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface GigabitEthernet4/0/2 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 Address Resolution Protocol（ARP）検査のロギング バッファをクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear ip arp inspection log** 特権 EXEC コマンドを使用します。

clear ip arp inspection log

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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 ACL を定義します。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング 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 検査ログ 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 Address Resolution Protocol（ARP）検査の統計情報をクリアするには、**clear ip arp inspection statistics** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

vlan *vlan-range*	（任意）指定された 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 を指定することができます。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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（メディア アクセス制御）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 エージェントの統計情報または DHCP スヌーピング統計カウンタをクリアするには、**clear ip dhcp snooping** 特権 EXEC 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**}

シンタックスの説明

binding	DHCP スヌーピング バインディング データベースをクリアします。
*****	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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	**statistics** キーワードが導入されました。
12.2(44)SE	*****、*ip-address*、**interface** *interface-id*、および **vlan** *vlan-id* キーワードが追加されました。

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

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

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

シンタックスの説明

queue-statistics	IPC キューの統計情報をクリアします。
statistics	IPC の統計情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。

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、**clear ipv6 dhcp conflict** 特権 EXEC 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 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。

シンタックスの説明

*	すべてのアドレス競合をクリアします。
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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(46)SE	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** {**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。クライアントは近隣探査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 l2protocol-tunnel counters

プロトコル トンネル ポートのプロトコル カウンタをクリアするには、**clear l2protocol-tunnel counters** 特権 EXEC コマンドを使用します。

clear l2protocol-tunnel counters [*interface-id*]

シンタックスの説明

interface-id	（任意）プロトコル カウンタをクリアするインターフェイス（物理インターフェイスまたはポート チャネル）を指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは指定されたインターフェイスのプロトコル トンネル カウンタをクリアするには、このコマンドを使用します。

例

次の例では、インターフェイスのレイヤ 2 プロトコル トンネル カウンタをクリアする方法を示します。

```
Switch# clear l2protocol-tunnel counters gigabitethernet0/3
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報を表示します。

clear lacp

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

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

シンタックスの説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

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

特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバー上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを MAC アドレス テーブルから削除するには、**clear mac-address-table** 特権 EXEC 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**}

シンタックスの説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
dynamic address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
dynamic interface *interface-id*	（任意）指定された物理ポートまたはポート チャネル上のすべてのダイナミック MAC アドレスを削除します。
dynamic vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4094 です。
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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**clear mac-address-table**（ハイフン付き）コマンドは、**clear mac address-table**（ハイフンなし）コマンドに替わりました。

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。

コマンド	説明
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	特定のインターフェイス上の SNMP（簡易ネットワーク管理プロトコル）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 テーブルの移行更新関連カウンタをクリアするには、**clear mac address-table move update** 特権 EXEC コマンドを使用します。

clear mac address-table move update

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

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

Network Mobility Services Protocol（NMSP; ネットワーク モビリティ サービス プロトコル）の統計情報をクリアするには、**clear nmsp statistics** 特権 EXEC 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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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

Port Aggregation Protocol（PAgP）チャネル グループ情報を表示するには、**clear pagp** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

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（設定済み、ダイナミック、またはスティッキ）のすべてのセキュア アドレスを削除するには、**clear port-security** 特権 EXEC 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**}}]]

シンタックスの説明

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セキュア MAC アドレスを削除します。
address *mac-addr*	（任意）指定されたダイナミック セキュア MAC アドレスを削除します。
interface *interface-id*	（任意）指定され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）指定された VLAN から指定されたセキュア 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 上の指定されたセキュア MAC アドレスをクリアします。 • **voice** : アクセス ポートで、音声 VLAN 上の指定されたセキュア 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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。
12.2(25)SEB	**access** および **voice** キーワードが追加されました。

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 gigabitethernet1/0/1
```

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 spanning-tree counters

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

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

シンタックスの説明

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、およびポート チャネルがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

interface-id 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されたインターフェイスで、プロトコル移行プロセスを再開する（近接スイッチと強制的に再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

interface *interface-id*	（任意）指定され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、およびポート チャネルがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルまたは Multiple Spanning-Tree Protocol（MSTP）が稼動するスイッチは、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。Rapid PVST+ 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 Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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。Multiple Spanning-Tree（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 Rapid Spanning-Tree（RST; 高速スパニング ツリー）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を検知します。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的には Rapid PVST+ 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

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

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、**clear vmps statistics** 特権 EXEC コマンドを使用します。

clear vmps statistics

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）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 Trunking Protocol（VTP）およびプルーニング カウンタをクリアするには、**clear vtp counters** 特権 EXEC コマンドを使用します。

clear vtp counters

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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

このコマンドは、スイッチ スタックまたはスタンドアロン クラスタ メンバー 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、メンバー 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ー スイッチに自動的に提供します。クラスタ メンバー 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。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 メンバー スイッチ コンソール ポートから、このグローバル コンフィギュレーション 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

シンタックスの説明

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 メンバー スイッチの番号。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（最大 31 文字）

デフォルト

このスイッチはどのクラスタのメンバーでもありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンドのスイッチ スタックまたはクラスタ コマンド スイッチ上でだけ使用できます。

各クラスタ メンバーは、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 メンバー 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 メンバー 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 メンバー スイッチをクラスタから削除できます。通常は、メンバーがクラスタ 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 メンバー 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 メンバー 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 メンバーの設定から、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 メンバー コンソールでクラスタからメンバー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用にホップカウントの制限を設定するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster discovery hop-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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スタックまたはクラスタ コマンド スイッチに限られます。このコマンドは、クラスタ メンバー 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ー 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

このコマンド対応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し、クラスタ名を割り当て、任意でメンバー番号を割り当てるには、コマンド対応スイッチまたはスイッチ スタック上で **cluster enable** グローバル コンフィギュレーション コマンドを使用します。すべてのメンバーを削除して、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

シンタックスの説明

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 スイッチにメンバー番号を割り当てます。指定できる範囲は 0 ～ 15 です。

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、メンバー番号は 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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ー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 メンバー番号を 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

スイッチ（コマンドまたはクラスタ メンバー スイッチのいずれか）が、他のスイッチのハートビート メッセージを受信しなくなってからそ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、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster holdtime** 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。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

シンタックスの説明

holdtime-in-secs	スイッチ（コマンドまたはクラスタ メンバー 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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 メンバーに伝達します。

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

クラスタに候補を追加するには、クラスタ コマンド スイッチ上で **cluster member** 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。メンバー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*

シンタックスの説明

n	クラスタ メンバーを識別する番号。指定できる範囲は 0 ～ 15 です。
mac-address *H.H.H*	クラスタ メンバー スイッチの MAC（メディア アクセス制御）アドレス（16 進数）
password *enable-password*	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。指定できる範囲は 1 ～ 4094 です。

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 メンバーはありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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、メンバー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ー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、メンバー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ー番号を選択し、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ーになったあと、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、メンバー番号をクラスタ コマンド スイッチ ホスト名に追加し、これをクラスタ メンバー 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、スイッチをメンバー 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ー番号を選択し、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 メンバーに関する情報を表示します。

cluster outside-interface

クラスタの Network Address Translation（NAT; ネットワーク アドレス変換）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ー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、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster outside-interface** 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。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

シンタックスの説明

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 ～ 48 です。指定できる VLAN 範囲は 1 ～ 4094 です。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 メンバー 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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

cluster run

スイッチ上でクラスタリングをイネーブルにするには、**cluster run** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

クラスタ コマンド スイッチまたはクラスタ コマンド スイッチのスタック上で **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 メンバー スイッチで **no cluster run** コマンドを入力すると、このメンバー 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; ホットスタンバイ ルータ プロトコル）にクラスタをバインドして、クラスタ コマンド スイッチ冗長をイネーブルにするには、**cluster standby-group** 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 メンバー 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 対応メンバーに伝播します。各クラスタ メンバー スイッチはバインディング情報を NVRAM（不揮発性 RAM）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ー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 対応メンバーに同じ 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ー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 メンバー 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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。

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、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster timer** 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 メンバーに伝達します。

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

インターフェイス範囲のマクロを作成するには、**define interface-range** 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。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*

シンタックスの説明

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、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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、**gigabitethernet 1/0/1 - 2** は有効な範囲ですが、**gigabitethernet 1/0/1-2** は有効な範囲ではありません。

type および *interface* の有効値は次のとおりです。

- **vlan** *vlan-id* - *vlan-id*（vlan-id の範囲は 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 ～ 48 です。

- **fastethernet** stack member/module/{*first port*} - {*last port*}
- **gigabitethernet** stack member/module/{*first port*} - {*last port*}

物理インターフェイス

- stack member は、スタック内のスイッチ識別に使用する番号です。番号に指定できる範囲は 1 ～ 9 で、スタック メンバーの最初の初期化の際に、スイッチに割り当てられます。
- モジュールは常に 0 です。
- 使用可能範囲は、*type stack member*/**0**/*number* - *number* です（例：**gigabitethernet 1/0/1 - 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。

gigabitethernet1/0/1 - 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。

fastethernet1/0/3, gigabitethernet1/0/1 - 2

fastethernet1/0/3 -4, gigabitethernet1/0/1 - 2

例

次の例では、複数のインターフェイス マクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet1/0/1 - 2, gigabitethernet1/0/1
- 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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

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、**delete** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

/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。 スタック メンバーまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック マスターから、スタック メンバー上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:**
/*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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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*』*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 access-list configuration)

DHCP バインディングとの照合に基づいて Address Resolution Protocol（ARP）パケットを拒否するには、**deny** ARP アクセス リスト コンフィギュレーション コマンドを使用します。アクセス リストから指定された Access Control Entry（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**]

シンタックスの説明

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	送信側 IP アドレスを指定します。
any	すべての IP アドレスまたは MAC（メディア アクセス制御）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 アドレスを拒否します。
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。

デフォルト

デフォルト設定はありません。ただし、ARP アクセス リストの末尾に暗黙の **deny ip any mac any** コマンドがあります。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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 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 access-list configuration)	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 (IPv6 access-list configuration)

IPv6 アクセス リスト コンフィギュレーション モードで、**deny** コマンドを使用して IPv6 アクセス リストの拒否条件を設定します。拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

no deny {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

deny icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

deny tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol（UDP）

deny udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]

（注） このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/*prefix-length*	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および Extended Universal Identifier（EUI）ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/ *prefix-length*	拒否条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Service Code Point（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。

fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。
log	（任意）エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します （コンソールに送信するメッセージ レベルは **logging console** コマンドで制御します）。 メッセージには、アクセス リスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。 **（注）**　ロギングはポート ACL ではサポートされません。
log-input	（任意）**log** キーワードと同じ機能を提供します（ただし、ロギング メッセージには受信インターフェイスも表示されます）。
sequence *value*	（任意）アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）拒否ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。ICMP パケットは ICMP メッセージ タイプによってフィルタリングできます。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージ名、または ICMP メッセージ タイプおよびコードによってフィルタリングできます。使用可能な名前については、「使用上のガイドライン」の項を参照してください。
ack	（任意）TCP プロトコルの場合に限り ACK ビットを設定します。
established	（任意）TCP プロトコルの場合に限り、接続が確立済みであることを意味します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り、PSH ビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCP プロトコルの場合に限り RST ビットを設定します。
syn	（任意）TCP プロトコルの場合に限り SYN ビットを設定します。
urg	（任意）TCP プロトコルの場合に限り URG ビットを設定します。

（注）　**flow-label**, **routing** および **undetermined-transport** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

deny（IPv6 アクセス リスト コンフィギュレーション モード）コマンドは、IPv6 固有である点を除き、**deny**（IPv4 アクセス リスト コンフィギュレーション モード）コマンドと類似しています。

IPv6 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、パケットがアクセス リストを通過する条件を定義するには、**ipv6 access-list** コマンドの後ろに **deny**（IPv6）コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力しないで、**permit**、**deny**、または **remark** ステートメントを既存のアクセス リストに追加できます。リストの最後以外の場所に新しいステートメントを追加するには、挿入する場所を示す、既存の 2 つのエントリ番号の間にある適切なエントリ番号を持った新しいステートメントを作成します。

（注）　すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探査プロセスと同等の Address Resolution Protocol（ARP）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィック フィルタリングに使用します （送信元プレフィクスはトラフィックの送信元に基づいて、宛先プレフィクスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクスと EUI ベースの /128 プレフィクスだけをサポートします。

fragments キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

例

次の例では、CISCO という名の IPv6 アクセス リストを設定し、そのアクセス リストをレイヤ 3 インターフェイス上の発信トラフィックに適用する方法を示します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持ったパケットすべてがインターフェイスで送信されるのを防ぎます。リストの 2 番めの拒否エントリは、5000 未満の送信元 UDP ポート番号を持ったパケットすべてがインターフェイスで送信されるのを防ぎます。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リストの最初の許可エントリは、すべての ICMP パケットのインターフェイスでの送信を許可します。リストの 2 番めの許可エントリは、その他すべてのトラフィックのインターフェイスでの送信を許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるため、この 2 番めの許可エントリが必要となります。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 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。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit (IPv6 access-list configuration)	IPv6 アクセス リストに許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストすべての内容を表示します。

deny (MAC access-list configuration)

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、**deny** MAC アクセス リスト コンフィギュレーション コマンドを使用します。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**]

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
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）パケットの Ethertype 番号と、Ethernet II または Subnetwork Access Protocol（SNAP）カプセル化を使用して、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 Class of Service（CoS; サービス クラス）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）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *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）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 2-4 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 2-4　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

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

MAC アクセス リスト コンフィギュレーション モードを開始するには、**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。

Access Control Entry（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 access-list configuration)	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 ACL を表示します。

diagnostic monitor

diagnostic monitor 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、ヘルス モニタリング診断テストを設定します。テストをディセーブルにし、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。

diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

diagnostic monitor interval switch {*num*} **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*

diagnostic monitor syslog

diagnostic monitor threshold switch {*num*} **test** {*test-id* | *test-id-range* | **all**} **count failure** *count*

no diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor interval switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor syslog

no diagnostic monitor threshold switch {*num*} **test** {*test-id* | *test-id-range* | **all**} **failure count**

シンタックスの説明

switch *num*	モジュール番号を指定します。指定できる範囲は 1 ～ 9 です。
test	実行するテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項を参照してください。
all	すべての診断テストを実行します。
interval	テストを実行する間隔を指定します。
hh:mm:ss	テストの時間間隔を指定します。形式については、「使用上のガイドライン」の項を参照してください。
milliseconds	時間（ミリ秒）を指定します。指定できる値は 0 ～ 999 です。
day	テストの間隔（日数）を指定します。形式については、「使用上のガイドライン」の項を参照してください。
Syslog	ヘルス モニタ診断テストが失敗した場合に Syslog メッセージを生成します。
threshold	障害しきい値を指定します。
failure count *count*	障害しきい値のカウントを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- モニタリングはディセーブルです。
- **syslog** 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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テストをスケジューリングする場合、次の注意事項があります。

- *test-id* : テスト ID のリストを表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
- *test-id-range* : テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。
- *hh* : 時間（0 ～ 23）を入力します。
- *mm* : 分（0 ～ 60）を入力します。
- *ss* : 秒（0 ～ 60）を入力します。
- *milliseconds* : ミリ秒（0 ～ 999）を入力します。
- *day* : 0 ～ 20 の数字として日を入力します。

diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**} コマンドを入力する場合は、次の注意事項に従ってください。

- すべての接続ポートをディセーブルにし、ネットワーク トラフィックを隔離します。テスト中はテスト パケットを送出できません。
- システムまたはテスト済みモジュールをリセットした後で、システムを通常の動作モードに戻します。

（注） スタックのスイッチにリロードされた属性がある診断テストを実行している場合、ケーブル接続の設定に応じてスタックをパーティションで区切ることができます。スタックをパーティションで区切らないようにするには、**show switch detail** 特権 EXEC コマンドを入力して、スタック設定を確認する必要があります。

例

次の例では、2 分ごとに指定したテストを行うように設定する方法を示します。

```
Switch(config)# diagnostic monitor interval switch 1 test 1 00:02:00 0 1
```

次の例では、ヘルス モニタが以前にイネーブルになっていない場合に、指定されたスイッチでテストを実行する方法を示します。

```
Switch(config)# diagnostic monitor switch 1 test 1
```

次の例では、スイッチ上でテスト モニタリング用の障害しきい値を設定する方法を示します。

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
```

次の例では、ヘルス モニタ テストが失敗した場合に Syslog メッセージの生成をイネーブルにする方法を示します。

```
Switch(config)# diagnostic monitor syslog
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

diagnostic schedule

diagnostic schedule 特権 EXEC コマンドを使用して、診断テストのスケジューリングを設定します。スケジューリングを削除し、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。

diagnostic schedule switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

no diagnostic schedule switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

シンタックスの説明

switch *num*	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
test	スケジューリングするテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項を参照してください。
all	すべての診断テストを実行します。
basic	基本的なオンデマンドの診断テストを実行します。
non-disruptive	ノンディスラプティブ ヘルスモニタ テストを実行します。
daily *hh*:*mm*	テストベースの診断タスクのスケジュール（日単位）を指定します。形式については、「使用上のガイドライン」の項を参照してください。
on *mm dd yyyy hh*:*mm*	テストベースの診断タスクのスケジュールを指定します。形式については、「使用上のガイドライン」の項を参照してください。
weekly *day-of-week hh*:*mm*	テストベースの診断タスクのスケジュール（週単位）を指定します。形式については、「使用上のガイドライン」の項を参照してください。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テストをスケジューリングする場合、次の注意事項があります。

- *test-id*：テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。
- *test-id-range*：テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。
- *hh*:*mm*：2 桁の数字（24 時間表記）で時間および分を入力します。コロン（**:**）が必要です。
- *mm*：January、February ～ December のように、月を入力します（大文字または小文字のいずれかを使用）。
- *dd*：2 桁の数字で日を入力します。
- *yyyy*：4 桁の数字で年を入力します。
- *day-of-week*：Monday、Tuesday ～ Sunday のように、曜日を入力します（大文字または小文字のいずれかを使用）。

例

次の例では、特定のスイッチに対して特定の日時に診断テストをスケジューリングする方法を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 on january 3 2006 23:32
```

次の例では、指定されたスイッチで毎週特定の時間に診断テストを行うようスケジューリングする方法を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly friday 09:23
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

diagnostic start

指定した診断テストを実行するには、**diagnostic start** ユーザ コマンドを使用します。

diagnostic start switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}

シンタックスの説明

switch *num*	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
test	実行するテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項を参照してください。
all	すべての診断テストを実行します。
basic	基本的なオンデマンドの診断テストを実行します。
non-disruptive	ノンディスラプティブ ヘルスモニタ テストを実行します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。

test-id-range をカンマおよびハイフンで区切られた整数で入力します（例：1,3-6 はテスト ID 1、3、4、5、および 6）。

例

次の例では、特定のスイッチで診断テストを実行する方法を示します。

```
Switch> diagnostic start switch 1 test 1
Switch>
06:27:50: %DIAG-6-TEST_RUNNING: Switch 1: Running TestPortAsicStackPortLoopback{ID=1} ...
(switch-1)
06:27:51: %DIAG-6-TEST_OK: Switch 1: TestPortAsicStackPortLoopback{ID=1} has completed
successfully (switch-1)
```

次の例では、正常なシステム動作を阻害するスイッチに診断テスト 2 を開始する方法を示します。

```
Switch> diagnostic start switch 1 test 2
Switch 1: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 1: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]: y
Switch>
16:43:29: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state DOWN
16:43:30: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 9 has changed to state DOWN
16:43:30: %STACKMGR-4-SWITCH_REMOVED: Switch 1 has been REMOVED from the stack
Switch#
16:44:35: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state UP
16:44:37: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state UP
16:44:45: %STACKMGR-4-SWITCH_ADDED: Switch 1 has been ADDED to the stack
16:45:00: %STACKMGR-5-SWITCH_READY: Switch 1 is READY
16:45:00: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state UP
16:45:00: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state UP
00:00:20: %STACKMGR-4-SWITCH_ADDED: Switch 1 has been ADDED to the stack (Switch-1)
00:00:20: %STACKMGR-4-SWITCH_ADDED: Switch 2 has been ADDED to the stack (Switch-1)
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan (Switch-1)
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console (Switch-1)
00:00:29: %STACKMGR-5-SWITCH_READY: Switch 2 is READY (Switch-1)
00:00:29: %STACKMGR-5-MASTER_READY: Master Switch 2 is READY (Switch-1)
00:00:30: %STACKMGR-5-SWITCH_READY: Switch 1 is READY (Switch-1)
00:00:30: %DIAG-6-TEST_RUNNING: Switch 1: Running TestPortAsicLoopback{ID=2} ...
(Switch-1)
00:00:30: %DIAG-6-TEST_OK: Switch 1: TestPortAsicLoopback{ID=2} has completed successfully
(Switch-1)
```

次のメッセージは、テストを実行することによりスタック接続性が失われる場合に表示されます。

```
Switch 3: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 3: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]:
```

次のメッセージは、テストを実行することによりスタックの分離が発生する場合に表示されます。

```
Switch 6: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 6: Running test(s) 2 will partition stack
Switch 6: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]:
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

dot1x

IEEE 802.1x 認証をグローバルにイネーブルにするには、**dot1x** グローバル コンフィギュレーション コマンドを使用します。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。

シンタックスの説明

critical {**eapol** | **recovery delay** *milliseconds*}	アクセス不能な認証バイパス パラメータを設定します。詳細は、**dot1x critical (global configuration)** 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。

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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	**guest-vlan supplicant** キーワードが追加されました。
12.2(25)SEE	**critical** {**eapol** | **recovery delay** *milliseconds*} キーワードが追加されました。

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、Authentication, Authorization, and Accounting（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動する装置を使用し、スイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、装置が ACS バージョン 3.2.1 以上で稼動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 (global configuration)	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 に移行されるまでに許容される最大の認証試行回数を設定するには、**dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts

シンタックスの説明

max-attempts	ポートが制限 VLAN に移行するまでに許容される最大の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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

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 gigabitethernet1/0/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

show dot1x [**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 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、**dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

シンタックスの説明

vlan-id	VLAN を 1 ～ 4094 の範囲で指定します。

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

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 Dynamic Host Configuration Protocol（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あと、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 になると、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 gigabitethernet1/0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

show dot1x [**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 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または双方向に設定するには、**dot1x control-direction** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no dot1x control-direction

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEC	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 IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with Wake-on-LAN」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 (global configuration)

dot1x credentials 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、サプリカント スイッチでプロファイルを設定します。

dot1x credentials *profile*

no dot1x credentials *profile*

シンタックスの説明

profile	サプリカント スイッチのプロファイルを指定します。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

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 (global configuration)

dot1x critical 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、アクセス不能な認証バイパス機能のパラメータ（クリティカル認証または Authentication, Authorization, and Accounting [AAA] 失敗ポリシーとも言う）を設定します。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**}

シンタックスの説明

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*	リカバリ遅延期間（ミリ秒）を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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 (interface configuration)	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 (interface configuration)

dot1x critical インターフェイス コンフィギュレーション コマンドを使用して、アクセス不能な認証バイパス機能（クリティカル認証または Authentication, Authorization, and Accounting（AAA）失敗ポリシーとも言う）をイネーブルにします。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**]

シンタックスの説明

recovery action reinitialize	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*	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。指定できる範囲は 1 ～ 4094 です。

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。
12.2(25)SEE	**vlan** *vlan-id* キーワードが追加されました。

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プライベート VLAN のホスト ポートである場合、VLAN はセカンダリ プライベート 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 を稼動し、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 クライアントで DHCP が設定され、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 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。

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、ポートの状態は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 21 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 gigabitethernet1/0/21
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

show dot1x [**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 critical (global configuration)	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

IEEE 802.1x パラメータをデフォルト値にリセットするには、**dot1x default** 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 default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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）。
- 再認証の試行間隔の秒数は 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	このコマンドは、インターフェイス コンフィギュレーション モードに変更されました。

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。

設定を確認するには、`Switch(config-if)#` **`dot1x default`**

`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

IEEE 802.1x 認証をサポートしないクライアントに対し、Web 認証をフォールバック方式として使用するようにポートを設定するには、**dot1xfallback** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x fallback *profile*

no dot1x fallback

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

show dot1x [**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
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。
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。
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。

dot1x guest-vlan

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

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

シンタックスの説明

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

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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	このコマンドは、デフォルトのゲスト VLAN の動作を変えるように変更されました。

使用上のガイドライン

次のいずれかのスイッチ ポートにゲスト VLAN を設定できます。

- 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
- セカンダリ プライベート VLAN に属するプライベート VLAN ポート。スイッチ ポートに接続されるすべてのホストは、端末状態の妥当性の評価に成功したかどうかにかかわらず、プライベート VLAN に割り当てられます。スイッチが、スイッチのプライマリおよびセカンダリ プライベート VLAN の対応付けを使用してプライマリ プライベート VLAN を判別します。

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と、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。

Cisco IOS Release 12.2(25)SE よりも前のスイッチでは、EAPOL パケット履歴を保持していなかったため、インターフェイスで EAPOL パケットが検出されたかどうかに関係なく、ゲスト VLAN への認証アクセスに失敗したクライアントを許可しました。Cisco IOS Release 12.2(25)SE で、このオプションの動作をイネーブルにするには、**dot1x guest-vlan supplicant** 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。

ただし、Cisco IOS Release 12.2(25)SEE では、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドはすでにサポートされていません。**dot1x auth-fail vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力すると、制限 VLAN を使用して、認証に失敗したクライアントにネットワーク アクセスを与えることができます。

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、単一ホスト 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。

Remote Switched Port Analyzer（RSPAN）VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サー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 を設定したあと、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。

Cisco IOS Release 12.2(25)SEE 以上では、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 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。

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 gigabitethernet2/0/1
Switch(config-if)# dot1x guest-vlan 5
```

show dot1x [**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	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

IEEE802.1x 許可ポート上で、単一ホスト（クライアント）または複数のホストを許可するには、**dot1x host-mode** 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。IEEE802.1x 許可ポート上で、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**}

シンタックスの説明

multi-host	スイッチでマルチ ホスト モードをイネーブルにします。
single-host	スイッチで単一ホスト モードをイネーブルにします。
multi-domain	スイッチ ポートで MDA をイネーブルにします。

デフォルト

デフォルト設定は、single-host 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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドに替わるものです。
12.2(35)SE	**multi-domain** キーワードが追加されました。

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 gigabitethernet2/0/1
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 gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

show dot1x [**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
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、**dot1x initialize** 特権 EXEC コマンドを使用します。

dot1x initialize [**interface** *interface-id*]

シンタックスの説明

interface *interface-id*	（任意）ポートを初期化します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

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あと、ポートの状態は無許可になります。

このコマンドには、**no** 形式はありません。

例

次の例では、ポートを手動で初期化する方法を示します。

```
Switch# dot1x initialize interface gigabitethernet2/0/22
```

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、**dot1x mac-auth-bypass** 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。
12.2(35)SE	**timeout inactivity** *value* キーワードが追加されました。

使用上のガイドライン

特に言及されないかぎり、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ると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。

リンクのライフタイム中に EAPOL パケットがインターフェイス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 認証バイパスで認証されたクライアントは再認証できます。

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」の章の「Understanding IEEE 802.1x Authentication with MAC Authentication Bypass」の項および「IEEE 802.1x Authentication Configuration Guidelines」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までに、スイッチが認証プロセスを再始動する上限回数を設定するには、**dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。
12.2(25)SEC	*count* 範囲が変更されました。

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

スイッチが認証プロセスを再始動する前に、Extensible Authentication Protocol（EAP）フレーム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（応答を受信しないことが前提）、**dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req *count*

no dot1x max-req

シンタックスの説明

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。指定できる範囲は 1 ～ 10 です。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	このコマンドは、インターフェイス コンフィギュレーション モードに変更されました。

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 multiple-hosts

このコマンドは、現在は使用されていません。

過去のリリースで、**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドは、IEEE 802.1x 許可ポートで複数のホスト（クライアント）を許可するために使用されました。

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドは、**dot1x host-mode** インターフェイス コンフィギュレーション コマンドに替わりました。

関連コマンド

コマンド	説明
dot1x host-mode	ポートの IEEE 802.1x ホスト モードを設定します。
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

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、**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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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

ポートの許可ステートを手動で制御できるようにするには、**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。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

シンタックスの説明

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すれば、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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 メンバーであるポートを 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。
- Switched Port Analyzer（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 gigabitethernet2/0/21
Switch(config-if)# dot1x port-control auto
```

show dot1x [**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
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

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

dot1x re-authenticate [**interface** *interface-id*]

シンタックスの説明

interface *interface-id*	（任意）再認証するスタック スイッチ番号、モジュール、およびインターフェイスのポート番号

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、再認証試行間隔（re-authperiod）および自動再認証の設定秒数を待たずにクライアントを再認証できます。

例

次の例では、ポートに接続されたデバイスを手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet2/0/21
```

関連コマンド

コマンド	説明
dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
dot1x timeout reauth-period	再認証の試行の間隔（秒）を設定します。

dot1x re-authentication

このコマンドは、現在は使用されていません。

過去のリリースで、**dot1x re-authentication** グローバル コンフィギュレーション コマンドは、定期的な再認証の試行間隔の合計時間を設定するために使用されました。

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドは、**dot1x re-authentication** グローバル コンフィギュレーション コマンドに替わりました。

関連コマンド

コマンド	説明
dot1x reauthentication	再認証の試行の間隔（秒）を設定します。
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x reauthentication

定期的なクライアントの再認証をイネーブルにするには、**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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。**dot1x re-authentication** グローバル コンフィギュレーション コマンド（ハイフン付き）に替わるものです。

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

次の例では、クライアントの定期的な再認証をディセーブルにする方法を示します。

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

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
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	再認証の試行の間隔（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、**dot1x test eapol-capable** 特権 EXEC コマンドを使用します。

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

シンタックスの説明

interface *interface-id*	（任意）クエリー対象のポートです。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

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

関連コマンド

コマンド	説明
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、**dot1x test timeout** 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。

dot1x test timeout *timeout*

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

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 のタイマーを設定するには、**dot1x timeout** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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**}

シンタックスの説明

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あと、待機状態を続ける秒数。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 指定できる範囲は 1 ～ 65535 です。
reauth-period {*seconds* | **server**}	再認証の試行の間隔（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。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。指定できる範囲は 30 ～ 65535 です。
tx-period *seconds*	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。指定できる範囲は 1 ～ 65535 です。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**supp-timeout** および **server-timeout** キーワードが追加され、コマンドはインターフェイス コンフィギュレーション モードに変更されました。
12.2(18)SE	**server-timeout**、**supp-timeout**、および **tx-period** キーワードの範囲が変更されました。
12.2(25)SEC	**tx-period** キーワードの範囲が変更され、**reauth-period server** キーワードが追加されました。
12.2(25)SEE	**ratelimit-period** キーワードが追加されました。
12.2(40)SE	**tx-period** *seconds* の範囲が間違っています。正しい範囲は 1 ～ 65535 です。

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

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

次の例では、定期的な再認証をイネーブルにし、再認証の間隔の秒数としてセッションタイムアウト RADIUS 属性の値を指定する方法を示します。

```
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
```

次の例では、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時間を 60 秒に設定する方法を示します。

```
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再認証をイネーブルにします。
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

dot1x violation-mode 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、新しいデバイスがポートに接続するとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続するときに発生する違反モードを設定します。

dot1x violation-mode {shutdown | restrict | protect}

no dot1x violation-mode

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

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

ポートの動作のデュプレックス モードを指定するには、**duplex** 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

シンタックスの説明

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 10000 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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(20)SE	100 BASE-FX SFP モジュール用に **half** キーワードのサポートが追加されました。

使用上のガイドライン

このコマンドは、10 ギガビット イーサネット インターフェイスでは使用できません。

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とデュプレックス 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、再度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 gigabitethernet1/0/1
Switch(config-if)# duplex full
```

show interfaces 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
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。

energywise (global configuration)

エンティティで EnergyWise をイネーブルにして設定するには **energywise** 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。EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise {**importance** *importance* | **keywords** *word,word,...* | **level** *level* | **management** *udp-port-number* | **name** *name* | **neighbor** [*hostname*| *ip-address*] *udp-port-number* | **role** *role*}

no energywise {**importance** | **keywords** | **management** | **name** | **neighbor** | **role**}

シンタックスの説明

importance *importance*	エンティティの重要度を設定します。 指定できる範囲は 1 ～ 100 です。
keywords *word,word,...*	エンティティのキーワードを 1 つ以上割り当てます。 キーワードを複数割り当てる場合は、キーワードをコンマで区切るようにし、キーワード間にスペースを入れないでください。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
level *level*	エンティティの電力レベルを設定します。 指定できる範囲は 1 ～ 10 です。
management *udp-port-number*	クエリーを送受信する UDP ポートを指定します。 指定できる範囲は 1 ～ 65000 です。
name *name*	EnergyWise 固有のエンティティ名を指定します。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
neighbor [*hostname*| *ip-address*] *udp-port-number*	スタティック ネイバーを割り当てます。 • （任意）ホスト名（*hostname*）または IP アドレス（*ip-address*）。 • クエリーを送受信する UDP ポート（*udp-port-number*）。 指定できる範囲は 1 ～ 65000 です。
role *role*	EnergyWise ドメインにおけるエンティティのロールを指定します。たとえば、lobby.b20。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。

デフォルト

EnergyWise はディセーブルにされています。

重要度は 1 です。

キーワードは定義されていません。

電力レベルは 10 です。

udp-port-number は 43440 です。

name はホスト名です。

ネイバーは割り当てることができません。

role は、モデル番号です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

エンティティをドメインに追加すると、エンティティおよびその PoE ポートで EnergyWise がイネーブルにされます。

例

次の例では、EnergyWise をイネーブルにし、エンティティをドメインに割り当て、パスワード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)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# energywise importance 50
Switch(config)# energywise keywords lab1,devlab
Switch(config)# energywise management 60500
Switch(config)# energywise name Entity01
Switch(config)# energywise neighbor TG3560G-21 43440
Switch(config)# energywise role role.labaccess
Switch(config)# end
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定およびステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。
show energywise recurrence	繰り返し設定およびステータスを表示します。

energywise (interface configuration)

Power over Ethernet（PoE）ポートで EnergyWise を設定するには、**energywise** 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。EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise [**importance** *importance* | **keywords** *word,word,...* | **level** *level* [**recurrence at** *minute hour day_of_month month day_of_week*] | **name** *name* | **role** *role*]

no energywise [**importance** | **keywords** | **level** | **name** | **role**]

シンタックスの説明

importance *importance*	（任意）ポートの重要度を設定します。 指定できる範囲は 1 ～ 100 です。
keywords *word,word,...*	ポートのキーワードを 1 つ以上割り当てます。 キーワードを複数割り当てる場合は、キーワードをコンマで区切るようにし、キーワード間にスペースを入れないでください。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
level *level*	（任意）ポートの電力レベルを設定します。 指定できる範囲は 0 ～ 10 です。 電力レベルが 0 であれば、ポートは電源オフです。 電力レベルが 1 ～ 10 であれば、ポートは電源が入っています。この範囲の任意の値を入力して、PoE ポートに電力を供給できます。
recurrence importance *importance* **at** *minute hour day_of_month month day_of_week*	（任意）電源オンまたは電源オフの繰り返しをスケジューリングします。 • **importance** *importance*：ドメイン内のポートの重要度を設定します。指定できる範囲は 1 ～ 100 です。 • *minute*：指定できる範囲は 0 ～ 59 です。ワイルドカードには * を使用してください。 • *hour*：指定できる範囲は 0 ～ 23 です。ワイルドカードには * を使用してください。 • *day_of_month*：指定できる範囲は 1 ～ 31 です。ワイルドカードには * を使用してください。 • *month*：指定できる範囲は 1（1 月）～ 12（12 月）です。ワイルドカードには * を使用してください。 • *day_of_week*：指定できる範囲は 0（日曜日）～ 6（土曜日）です。ワイルドカードには * を使用してください。 **（注）** 指定する時刻は、PoE エンティティの時間帯に基づく現地時間です。

name *name*	（任意）EnergyWise 固有のポート名を指定します。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
role *role*	（任意）ドメインにおけるポートのロールを指定します。たとえば、lobbyport。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。

デフォルト

重要度は 1 です。

キーワードは定義されていません。

電力レベルは 10 です。

name は、ポート名の短縮版です。たとえば、Gigabit Ethernet 1/0/2 の場合は、Gi1.0.2 です。

role は、モデル番号です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、PoE ポートで EnergyWise をイネーブルにして、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)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
Switch(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
Switch(config-if)# energywise inportance 50
Switch(config-if)# energywise name lobbyInterface.3
Switch(config-if)# energywise role role.lobbyaccess
Switch(config-if)# end
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定およびステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。
show energywise recurrence	繰り返し設定およびステータスを表示します。

energywise domain

エンティティで EnergyWise をイネーブルにし、そのエンティティをドメインに割り当て、ドメインのエンティティ間の通信を保護するパスワードを設定するには **energywise domain** 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。EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise domain *domain-name* **secret** [**0** | **7**] *password* [**protocol udp port** *udp-port-number* [**interface** *interface-id* | **ip** *ip-address*]]

no energywise domain

シンタックスの説明

domain *domain-name*	指定された *domain-name* でドメインにエンティティを割り当てます。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
secret [**0** | **7**] ***password***	ドメイン内のエンティティ間の通信を保護する *password* を設定します。 • （任意）**0**：暗号化されていないパスワードを使用します。 • （任意）**7**：非表示パスワードを使用します。 **0** も **7** も入力しなかった場合、エンティティでは、デフォルト値の 0 を使用します。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
port *udp-port-number*	（任意）クエリーを送受信する UDP ポートを指定します。 指定できる範囲は 1 ～ 65000 です。
interface *interface-id*	（任意）EnergyWise メッセージの送信元のポートを指定します。
ip *ip-address*	（任意）EnergyWise メッセージの送信元の IP アドレスを指定します。

デフォルト

EnergyWise はディセーブルにされており、エンティティはドメインに割り当てられていません。

パスワードは設定されていません。

udp-port-number は 43440 です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

energywise domain *domain-name* **secret** [**0** | **7**] *password* コマンドを入力すると、エンティティでは、ネットワークとの通信および管理アプリケーションとの通信に使用可能な最初のポートを選択します。

例

次の例では、EnergyWise をイネーブルにし、*domain-name* および *password* を設定し、IP アドレスを指定する方法を示します。

```
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定およびステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。

energywise query

energywise query 特権 EXEC コマンドを使用して、電力情報を表示したり、ドメイン内のエンティティまたは PoE ポートに電力を供給したりします。

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **collect** {**delta** | **usage**}

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **set level** *level*

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **sum** {**delta** | **usage**}

シンタックスの説明

importance *importance*	重要度の値に基づき、結果をフィルタリングします。指定した値以下の値のエンティティだけが表示されます。 *importance* の正しい範囲は 1 ～ 100 です。
keywords *word,word,...*	指定した 1 つ以上のキーワードに基づいて結果をフィルタリングします。 キーワードを複数指定する場合は、キーワードをコンマで区切るようにし、キーワード間にスペースを入れないでください。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
name *name*	name に基づいて結果をフィルタリングします。 ワイルドカードの場合は、* を使用するか name フレーズの終わりにアスタリスクを付けて *name** とします。 • 英数字および #、(、%、!、または & などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
collect {**delta** | **usage**}	エンティティまたは PoE ポートの delta 値または usage 値を表示します。 • **delta**：現行の消費電力と使用可能な消費電力の差異だけを表示します。 • **usage**：現行消費電力だけを表示します。
set level *level*	エンティティまたは PoE ポートの電力レベルを設定します。 指定できる範囲は 0 ～ 10 です。 エンティティはレベル 1 からレベル 10 までをサポートします。 PoE ポートは、レベル 0 からレベル 10 までをサポートします。
sum {**delta** | **usage**}	エンティティまたは PoE ポートの delta 値または usage 値の合計を表示します。 • **delta**：現行の消費電力と使用可能な消費電力の差異の合計だけを表示します。 • **usage**：現行消費電力だけを表示します。

デフォルト

重要度値は 1 です。

電力レベルは 10 です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

sum キーワードによる結果では、*応答*合計は正確ではありません。クエリーによる合計は正確であり、クエリーに応答したエンティティの合計数になっています。

ポートを電源オンまたは電源オフにするには、**energywise query** {**keywords** *word,word,...* | **name** *name*} **set level** *level* コマンドを入力します。

注意　このクエリーは、コマンドを入力したエンティティ*および*クエリー基準と一致するその他のドメイン デバイスに影響するため、使用する場合は、注意が必要です。

例

次の複数の例では、エンティティ名をフィルタリングする方法を示します。

```
Switch# energywise query name phone* collect usage
EnergyWise query, timeout is 3 seconds:

Host            Name            Usage
----            ----            -----
2.2.2.21        phone           0.0 (W)
2.2.2.21        phone           15.4 (W)
2.2.2.21        phoneA          0.0 (W)
2.2.2.22        phone           0.0 (W)
2.2.2.21        phoneB          0.0 (W)
2.2.2.22        phoneC          15.4 (W)
2.2.2.21        phone           0.0 (W)
2.2.2.23        phoneD          15.4 (W)
2.2.2.21        phone           0.0 (W)

Queried:  9    Responded:  9      Time:  0.26 seconds

Switch# energywise query name * sum usage
EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
346.3 (W)

Queried:  147    Responded:  147      Time:  0.121 seconds

Switch# energywise query name lobby* collect usage

EnergyWise query, timeout is 3 seconds:

Host            Name              Usage
----            ----              -----
2.2.4.30        lobbyInterface.17 10.0 (W)

Queried:  1    Responded:  1      Time:  0.7 seconds

Switch# energywise query name Fa1.0.4* sum usage

EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
129.0 (W)

Queried:  10    Responded:  10      Time:  0.6 seconds
```

次の例は、デルタ値の合計およびドメインでの潜在的な電力の変化を示します。

```
Switch# energywise query name * sum delta
EnergyWise query, timeout is 3 seconds:

Level   Label       Delta Power (W)
-----   -----       -----------
0       Shut        -12.9
1       Hibernate   +723.8
2       Sleep       +723.8
3       Standby     +723.8
4       Ready       +723.8
5       Low         +723.8
6       Frugal      +723.8
7       Medium      +723.8
8       Reduced     +723.8
9       High        +723.8
10      Full        +723.8

Queried:  48    Responded:  48      Time:  0.15 seconds
```

次の例は、ドメインの消費電力を示します。

```
Switch# show energywise children
Interface   Role               Name                  Usage      Lvl   Imp  Type
---------   ----               ----                  -----      ---   ---  ----
            control            SwitchA               86.0  (W)  10    100  parent
Gi1/0/1     interface          Gi1.0.1               0.0   (W)  10    20   child
.
.
.
Gi1/0/6     interface          Gi1.0.6               0.0   (W)  10    20   child
Gi1/0/7     role.lobbyaccess   lobbyInterface.7      0.0   (W)  10    50   child
Gi1/0/8     interface          Gi1.0.8               0.0   (W)  10    20   child
<output truncated>

Switch# energywise query name * set level 0
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is (48/48) setting entities

Queried:  48   Responded:  48     Time:  0.996 seconds

Switch# energywise query name * set level 10
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is (48/48) setting entities

Queried:  48   Responded:  48     Time:  0.996 seconds
```

次の例では、キーワードによって結果をフィルタリングする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# energywise keywords lobby,sattelite
Switch(config-if)# energywise keywords public
Switch(config-if)# end
Switch# show running-config interface gigabitethernet1/0/2
!
interface GigabitEthernet1/0/2
 energywise level 0 recurrence importance 90 at 0 8 * * *
 energywise level 10 recurrence importance 90 at 0 20 * * *
 energywise importance 50
 energywise role role.lobbyaccess
 energywise keywords lobby,sattelite,public
 energywise name lobbyInterface.2
end

Switch# energywise query keyword lobby collect usage
EnergyWise query, timeout is 3 seconds:

Host            Name              Usage
----            ----              -----
2.2.4.30        lobbyInterface.17 15.4 (W)

Queried:  1    Responded:  1      Time:  0.0 seconds


Switch# energywise query keyword satellite sum usage
EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
15.4 (W)

Queried:  1    Responded:  1      Time:  0.11 seconds
```

errdisable detect cause

特定の原因またはすべての errdisable 検出をイネーブルにするには、**errdisable detect cause** 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。errdisable 検出機能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。

errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power |l2ptguard | link-flap | loopback | pagp-flap | security-violation shutdown vlan | sfp-config-mismatch}

no errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power |l2ptguard | link-flap | loopback | pagp-flap | security-violation shutdown vlan | sfp-config-mismatch}

BPDU ガード機能およびポート セキュリティ機能の場合は、このコマンドを使用し、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グローバルに設定できます。

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。

errdisable detect cause bpduguard shutdown vlan

no errdisable detect cause bpduguard shutdown vlan

シンタックスの説明

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 Address Resolution Protocol（ARP）検査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 errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol（DHCP）スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）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。
l2ptguard	レイヤ 2 プロトコル トンネルの errdisable 原因に対し、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	Port Aggregation Protocol（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。

security-violation shutdown vlan	音声認識 IEEE 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致でエラー検出をイネーブルにします。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**loopback** キーワードが追加されました。
12.1(19)EA1	**dhcp-rate-limit** キーワードが追加されました。
12.2(20)SE	**arp-inspection** キーワードが追加されました。
12.2(25)SE	**l2ptguard** キーワードが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。**inline-power** キーワードおよび **sfp-config-mismatch** キーワードが追加されました。
12.2(46)SE	**security-violation shutdown vlan** キーワードが追加されました。

使用上のガイドライン

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。

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 にできるようにするには、**errdisable detect 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

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 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。

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。
small 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

小さいフレームが着信してポートが errdisable となった後でポートを自動で再度イネーブルにするための回復タイマーをイネーブルにするには、スイッチ上で **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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

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 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

回復メカニズムの変数を設定するには、**errdisable recovery** 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。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** |**l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **sfp-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **sfp-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

シンタックスの説明

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	Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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。
arp-inspection	Address Resolution Protocol（ARP）検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
channel-misconfig	EtherChannel の設定矛盾による 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	Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）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。
l2ptguard	レイヤ 2 プロトコル トンネルによる errdisable ステートから回復するためのタイマー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	Port Aggregation Protocol（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。
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。
sfp-mismatch	SFP 設定の不一致でエラー検出をイネーブルにします。

udld	UniDirectional Link Detection（UDLD; 単方向リンク検出）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 Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**security-violation** キーワードが追加されました。**gbic-invalid** キーワードは、SFP モジュール ポートでサポートされます。
12.1(19)EA1	**dhcp-rate-limit** キーワードが追加されました。
12.2(18)SE	**channel-misconfig** キーワードが追加されました。
12.2(20)SE	**arp-inspection** キーワードが追加されました。
12.2(25)SE	**l2ptguard** キーワードが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。**inline-power** キーワードおよび **sfp-mismatch** キーワードが追加されました。

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
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。
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。

exception crashinfo

Cisco IOS イメージのエラー時にスイッチで拡張 crashinfo ファイルが作成されるよう設定するには、**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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

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 のイメージ名およびバージョン、プロセッサ レジスタのリスト、およびスタック トレースが含まれます。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。

スタック マスター上で **exception crashinfo** 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と、すべてのスタック メンバーは、スタック メンバー上の Cisco IOS イメージが失敗した場合に拡張 crashinfo ファイルを作成するよう設定されます。

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現在の動作設定を表示します。構文情報については、『**Cisco IOS Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

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、**fallback 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

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 1/0/1
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。

flowcontrol

インターフェイスに対する受信フロー制御ステート を設定するには、**flowcontrol** 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。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。

フロー制御をディセーブルにする場合は、**receive off** キーワードを使用します。

flowcontrol receive {**desired** | **off** | **on**}

（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。

シンタックスの説明

receive	インターフェイスがリモート装置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動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動させることができます。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

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 2-5 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 2-5　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 gigabitethernet1/0/21
Switch(config-if)# flowcontrol receive off
```

show interfaces 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
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。

interface port-channel

ポート チャネルの論理インターフェイスにアクセスしたり、作成したりするには、**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*

シンタックスの説明

port-channel-number	ポート チャネル番号。指定できる範囲は 1 ～ 48 です。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	*port-channel-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

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 メンバーであるポートを 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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

interface range

インターフェイス レンジ コンフィギュレーション モードを開始し、複数のポートでコマンドを同時に実行するには、**interface range** 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 {*port-range* | **macro** *name*}

no interface range {*port-range* | **macro** *name*}

シンタックスの説明

port-range	ポート範囲。p*ort-range* の有効値のリストについては、「使用上のガイドライン」の項を参照してください。
macro *name*	マクロ名を指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

インターフェイス範囲を設定する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 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）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（不揮発性 RAM）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。

- **vlan** *vlan-ID* : *vlan-ID*（vlan ID の範囲は 1 ～ 4094）
- **fastethernet** stack member/module/{*first port*} - {*last port*}（module は常に **0**）
- **gigabitethernet** stack member/module/{*first port*} - {*last port*}（module は常に **0**）

  物理インターフェイス

  - stack member は、スタック内のスイッチ識別に使用する番号です。番号に指定できる範囲は 1 ～ 9 で、スタック メンバーの最初の初期化の際に、スイッチに割り当てられます。
  - モジュールは常に 0 です。
  - 使用可能範囲は、*typestack member*/**0**/*number* - *number* です（例：**gigabitethernet1/0/1 - 2**）
- **port-channel** *port-channel-number* - *port-channel-number*、*port-channel-number* は 1 ～ 48 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。

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 gigabitethernet1/0/1 -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 fastethernet1/0/1 - 2, gigabitethernet1/0/1 - 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 gigabitethernet1/0/1 - 2
Switch(config-if-range)#
```

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 gigabitethernet1/0/1 - 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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

interface vlan

動的な Switch Virtual Interface（SVI）を作成、またはこれにアクセスし、インターフェイス コンフィギュレーション モードを開始するには、**interface vlan** グローバル コンフィギュレーション コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*

no interface vlan *vlan-id*

シンタックスの説明

vlan-id	VLAN 番号 指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

SVI は、特定の VLAN に対して、初めて **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、ISL（スイッチ間リンク）または IEEE 802.1Q カプセル化トランクのデータ フレームに関連付けられた VLAN タグ、またはアクセス ポートに設定された VLAN ID に相当します。

（注）物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを入力して SVI を削除すると、削除されたインターフェイスは、それ以降、**show interfaces** 特権 EXEC コマンドの出力には表示されません。

（注）VLAN 1 インターフェイスを削除することはできません。

削除した SVI は、削除したインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力することで、元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチ スタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響がで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。詳細は、**sdm prefer** コマンドを参照してください。

例

次の例では、VLAN ID 23 の新しい SVI を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

show interfaces および **show interfaces vlan** *vlan-id* 特権 EXEC コマンドを入力することによって、設定を確認できます。

関連コマンド

コマンド	説明
show interfaces vlan *vlan-id*	すべてのインターフェイスまたは指定の VLAN の管理ステータスおよび動作ステータスを表示します。

ip access-group

レイヤ 2 またはレイヤ 3 インターフェイスへのアクセスを制御するには、**ip 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。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**}

シンタックスの説明

access-list-number	IP Access Control List（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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	コマンドのサポートがレイヤ 2 インターフェイスまで拡張されました。

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、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 は受信方向に対してだけ適用できます。**out** キーワードはレイヤ 2 のインターフェイスでサポートされていません。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC（メディア アクセス制御）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。

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、ポートの ACL はルータの ACL、または VLAN マップより優先されます。

- 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ーとなっている 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）、Internet Control Message Protocol（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あと、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 gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
```

show ip interface、**show access-lists**、または **show ip access-lists** 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
access list	番号付き ACL を設定します。構文情報については、**『Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
show access-lists	スイッチで設定された ACL を表示します。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。

ip address

レイヤ 2 スイッチの IP アドレスや、各 Switch Virtual Interface（SVI）またはレイヤ 3 スイッチのルーテッド ポートの IP アドレスを設定するには、**ip address** インターフェイス コンフィギュレーション コマンドを使用します。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**]

シンタックスの説明

ip-address	IP アドレス。
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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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、Internet Control Message Protocol（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 Address Resolution Protocol（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。

スイッチが、Bootstrap Protocol（BOOTP）または Dynamic Host Configured Protocol（DHCP）サーバから IP アドレスを受信し、そのスイッチ IP アドレスを **no ip address** コマンドで削除した場合、IP 処理はディセーブルとなり、BOOTP サーバまたは DHCP サーバが再びアドレスを割り当てることはできません。

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。設定できるルーテッド ポートおよび SVI の数はソフトウェアでは制限されていません。ただし、この数と設定された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 使用率に影響がで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 gigabitethernet6/0/1
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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

ip admission

Web 認証をイネーブルにするには、**ip admission** 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

シンタックスの説明

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

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

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 gigabitethernet1/0/1
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	Network Admission Control（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。 詳細については、Cisco.com で『*Network Admission Control Software Configuration Guide*』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、**ip admission name proxy http** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

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

次の例では、スイッチ ポートで Web 認証だけを設定する方法を示します。

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
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 gigabitethernet1/0/1
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	Network Admission Control（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。詳細については、Cisco.com で『*Network Admission Control Software Configuration Guide*』を参照してください。

ip arp inspection filter vlan

ダイナミック Address Resolution Protocol（ARP）検査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、**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**]

シンタックスの説明

arp-acl-name	ARP Access Control List（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 を指定することができます。指定できる範囲は 1 ～ 4094 です。
static	（任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、**static** を指定します。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、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

ARP ACL を VLAN に適用してダイナミック ARP 検査を行う場合は、IP/MAC（メディア アクセス制御）バインディングを含む 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 検査用に 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 access-list configuration)	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 access-list configuration)	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 検査の設定および動作ステートを表示します。

ip arp inspection limit

インターフェイス上の着信 Address Resolution Protocol（ARP）要求および応答のレートを制限するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。DoS 攻撃が発生した場合にダイナミック ARP 検査によってスイッチ 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

シンタックスの説明

rate *pps*	1 秒間に処理される着信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 パケットをモニタする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。

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、レートは無制限です。

バースト インターバルは 1 秒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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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 検査対応 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かぎり、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。

レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

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 メンバーの着信 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 メンバーの着信 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 gigabitethernet1/0/1
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	指定され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 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 Address Resolution Protocol（ARP）検査のロギング バッファを設定するには、**ip arp inspection log-buffer** 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。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**}

シンタックスの説明

entries *number*	バッファに記録されるエントリ数。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、指定されたインターバルで必要なエントリ数 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値 0 は、エントリはログ バッファに配置されるものの、システム メッセージは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。値が 0 の場合、システム メッセージがただちに生成され、ログ バッファは常に空の状態です。

デフォルト

ダイナミック ARP がイネーブル化されると、拒否またはドロップされた 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、1 秒あたり 5 に制限されています。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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。このエントリには、これ以外の統計情報が提供されません。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。

ロギング バッファ コンフィギュレーションは、スイッチ スタックの各スタック メンバーに適用されます。各スタック メンバーでは、**logs** *number* が指定されていて、設定されたレートでシステム メッセージを生成します。たとえば、間隔（レート）が 1 エントリ / 秒の場合、メンバーが 5 つのスタックでは、1 秒当たり最大 5 つのシステム メッセージが生成されます。

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 ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ 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 検査ログ 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 Address Resolution Protocol（ARP）パケットを決定する信頼状態を、インターフェイスに設定するには、**ip arp inspection 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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC（メディア アクセス制御）アドレス バインディングを持つかどうかを検証します。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 gigabitethernet1/0/1
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 検査ロギング バッファを設定します。
show inventory interfaces	指定され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 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 検査ログ 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 Address Resolution Protocol（ARP）検査の特定のチェックを実行するには、**ip arp inspection validate** 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。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]**]

シンタックスの説明

src-mac	イーサネット ヘッダー内の送信元 MAC（メディア アクセス制御）アドレスと、ARP 本体内の送信側 MAC アドレスを比較します。このチェックは、ARP 要求と応答の両方に対して行われます。 このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。
dst-mac	イーサネット ヘッダー内の宛先 MAC アドレスと、ARP 本体内のターゲット MAC アドレスを比較します。このチェックは、ARP 応答に対して行われます。 このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。
ip	ARP 本体内で、無効な予期しない IP アドレスを比較します。このようなアドレスには、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	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。

デフォルト

チェックは行われません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	allow-zero キーワードが追加されました。

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、2 番めのコマンドが 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 Access Control List（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かぎり、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

次の例では、送信元 MAC の検証をイネーブルにする方法を示します。

```
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 検査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 Address Resolution Protocol（ARP）検査をイネーブルにするには、**ip arp inspection 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*

シンタックスの説明

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 を指定することができます。指定できる範囲は 1 ～ 4094 です。

デフォルト

すべての VLAN で ARP 検査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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

ダイナミック ARP 検査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 検査は、アクセス ポート、トランク ポート、EtherChannel ポートおよびプライベート VLAN 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 検査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 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 検査の設定および動作ステートを表示します。

ip arp inspection vlan logging

VLAN 単位でロギングされるパケットのタイプを制御するには、**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**}

シンタックスの説明

vlan-range	ロギングに対して設定された VLAN を指定します。 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 を指定することができます。指定できる範囲は 1 ～ 4094 です。
acl-match {**matchlog** | **none**}	Access Control List（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** : Access Control Entries（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 Address Resolution Protocol（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 バインディングに一致するすべてのパケットを記録します。 • **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 バインディングに許可されたパケットを記録します。
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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	**arp-probe** キーワードが追加されました。

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 を指定しないかぎり、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 検査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 検査ログ バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
show inventory log	ダイナミック ARP 検査ログ 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 検査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、**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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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て、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、**ip dhcp snooping binding** 特権 EXEC 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*

シンタックスの説明

mac-address	MAC（メディア アクセス制御）アドレスを指定します。
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 アドレスを指定します。
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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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
gigabitethernet1/0/1 expiry 1000
```

設定を確認するには、**show ip dhcp snooping binding** または **show ip dhcp 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 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、**ip dhcp snooping database** 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。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**[*number*]**:**/*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**]

シンタックスの説明

flash[*number*]**:**/*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。 （任意）スタック マスターのスタック メンバー番号を指定するには、*number* パラメータを使用します。*number* に指定できる範囲は 1 ～ 9 です。
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 Remote Copy Protocol（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。 デフォルト値は 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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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、Network Time Protocol（NTP; ネットワーク タイム プロトコル）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（不揮発性 RAM）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 データベースをスタック マスター NVRAM に保存するには、**ip dhcp snooping database flash**[*number*]**:**/*filename* コマンドを使用します。データベースは、スタック メンバー NVRAM に保存されません。

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、スタック マスター 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、**ip dhcp snooping information option** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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（メディア アクセス制御）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一サブネットにある場合、サーバは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

次の例では、DHCP オプション 82 データ挿入をイネーブルにする方法を示します。

```
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

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か、オプション 82 情報を持つ DHCP パケットを受け入れるようにアグリゲーション スイッチを設定するには、アグリゲーション スイッチで **ip dhcp snooping information option allow-untrusted** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

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 Address Resolution Protoco（ARP）検査などの 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、**ip dhcp snooping information option format remote-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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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
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します。
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 1 秒あたりに受信することのできる DHCP メッセージの数を設定するには、**ip dhcp snooping limit 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。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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(18)SE	変更された指定範囲は 1 ～ 2048 です。

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
```

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
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

Dynamic Host Configuration Protocol（DHCP）スヌーピングのためにポートを信頼性があるものとして設定するには、**ip dhcp snooping 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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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、ポート上に 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

スイッチが、信頼性のないポート上で Dynamic Host Configuration Protocol（DHCP）パケットの送信元 MAC（メディア アクセス制御）アドレスがクライアントのハードウェア アドレスと一致することを確認するよう設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping verify** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。

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 で Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにするには、**ip dhcp snooping 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*

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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 回線 ID サブオプションを設定するには、**ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトのサーキット 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 information option format-type circuit-id string *ASCII-string*

no ip dhcp snooping vlan vlan information option format-type circuit-id string

シンタックスの説明

vlan *vlan*	VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

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。

（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（不揮発性 RAM）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
```

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

インターフェイスに Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）を適用することで、レイヤ 2 インターフェイス上のすべてのホストが 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、**ip igmp filter** 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

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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、Switch Virtual Interface（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 gigabitethernet1/0/2
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。

コマンド	説明
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 Configuration Fundamentals Command Reference**』**Release 12.2** > 「**File Management Commands**」> 「**Configuration File Management Commands**」を選択してください。

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能な Internet Group Management Protocol（IGMP）グループの最大数を設定したり、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したりするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp max-groups** 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。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**}

シンタックスの説明

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。デフォルトの設定に制限はありません。
action deny	エントリの最大数が IGMP スヌーピング転送テーブルにある場合は、次の IGMP 加入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場合、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。

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あとの、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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**action** {**deny** | **replace**} キーワードが追加されました。

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、Switch Virtual Interface（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あとで、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 gigabitethernet1/0/2
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 gigabitethernet2/0/1
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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

ip igmp profile

Internet Group Management Protocol（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、**ip igmp 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。このモードで、スイッチポートからの IGMP メンバシップ 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*

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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します（デフォルト設定の状態）。
- **[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します。
- **[range]**：プロファイルに対する 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
```

設定を確認するには、**show ip igmp profile** 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 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

Internet Group Management Protocol（IGMP）スヌーピングをスイッチ上でグローバルにイネーブル、または VLAN ごとにイネーブルにするには、**ip igmp 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*]

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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。

コマンド	説明
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

Internet Group Management Protocol（IGMP）の設定可能な Leave タイマーをグローバルにまたは VLAN ベースごとにイネーブルにするには、**ip igmp snooping last-member-query-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。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**

シンタックスの説明t

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。
12.2(46)SE	*time* の範囲が 100 ～ 32768 に変更されました。

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（不揮発性 RAM）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ーとして設定します。
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 Internet Group Management Protocol（IGMP）クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** 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。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**]

シンタックスの説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび 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）Topology Change Notification（TCN; トポロジ変更通知）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 クエリーの時間間隔を設定します。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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

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

Internet Group Management Protocol（IGMP）レポート抑制をイネーブルにするには、**ip igmp snooping report-suppression** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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、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

Internet Group Management Protocol（IGMP）Topology Change Notification（TCN）の動作を設定するには、**ip igmp snooping tcn** 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。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**}

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。

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 ルートかどうかに関わらず、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 Internet Group Management Protocol（IGMP）スヌーピング スパニングツリー Topology Change Notification（TCN）の動作として設定するには、**ip igmp snooping tcn flood** 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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

コマンドの履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。

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 gigabitethernet1/0/2
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 ごとに Internet Group Management Protocol（IGMP）スヌーピング即時脱退処理をイネーブルにするには、**ip igmp snooping immediate-leave** 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。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**

シンタックスの説明

vlan-id	指定された VLAN で IGMP スヌーピングおよび即時脱退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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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 つのレシーバー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（不揮発性 RAM）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 が稼動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したりするには、**ip igmp snooping mrouter** 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。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**}}

シンタックスの説明

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*	ネクストホップ インターフェイスをマルチキャスト ルータに指定します。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 ～ 48 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 Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol（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。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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（不揮発性 RAM）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 gigabitethernet1/0/22
```

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

Internet Group Management Protocol（IGMP）スヌーピングをイネーブルにし、レイヤ 2 ポートをマルチキャストグループ のメンバーとしてスタティックに追加するには、**ip igmp snooping static** 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。スタティックなマルチキャスト グループのメンバー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*

シンタックスの説明

vlan-id	指定した 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。
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 グループのメンバーとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバー 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 ～ 48 です。

デフォルト

デフォルトでは、マルチキャスト グループのメンバー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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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（不揮発性 RAM）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
gigabitethernet1/0/1
Configuring port gigabitethernet1/0/1 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 snap forwarding

Subnetwork Access Protocol（SNAP）カプセル化を使用した IP Version 4（IPv4）および IP Version 6（IPv6）フレームの転送をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip snap forwarding** 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。このフレームの転送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 snap forwarding

no ip snap forwarding

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、SNAP カプセル化を使用した IPv4 および IPv6 フレームを転送しません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をイネーブルにするには、**ip snap forwarding** 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。

スタックに加入しているスイッチが SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をサポートしない場合、スタックのすべてのスイッチは IPv4 および IPv6 フレームを転送せず、転送機能がディセーブルになります。

例

次の例では、SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をイネーブルにする方法を示します。

```
Switch(config)# ip snap forwarding
```

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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

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、**ip source binding** 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。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*

シンタックスの説明

mac-address	MAC（メディア アクセス制御）アドレスを指定します。
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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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
gigabitethernet1/0/1
```

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
gigabitethernet1/0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet1/0/1
```

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

Secure Shell（SSH; セキュア シェル）version 1（SSHv1）または SSH version 2（SSHv2）を実行するようにスイッチを設定するには、**ip ssh** 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。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**]

シンタックスの説明

1	（任意）スイッチが 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（SSHv2）を実行するように設定します。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

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 Release 12.2 Configuration Guides and Command References』> 『Cisco IOS Security Command Reference』Release 12.2 >** 「**Other Security Features**」> 「**Secure Shell Commands**」を選択してください。
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 Release 12.2 Configuration Guides and Command References』> 『Cisco IOS Security Command Reference』Release 12.2 >** 「**Other Security Features**」> 「**Secure Shell Commands**」を選択してください。

ip sticky-arp (global configuration)

プライベート VLAN に属する Switch Virtual Interface（SVI）上で sticky Address Resolution Protoco（ARP）をイネーブルにするには、**ip 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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

sticky ARP はイネーブル化されます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

sticky ARP エントリとは、プライベート VLAN SVI によって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 グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。

- プライベート VLAN を設定する場合、sticky ARP は スイッチでイネーブルです（デフォルト）。

  ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、このコマンドは作用しません。

  no ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、sticky ARP はインターフェイス上でディセーブルになりません。

（注）　プライベート VLAN インターフェイスの ARP エントリを表示し、確認するには、**show arp** 特権 EXEC コマンドを使用するよう推奨します。

- 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
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* 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、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。
- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** 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。

- 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。
- スイッチ上で sticky ARP がディセーブルのときに、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

sticky ARP をディセーブルにするには：

```
Switch(config)# 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 IP Addressing Services Command Reference』 Release 12.4 >** 「**ARP Commands**」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 IP Addressing Services Command Reference』 Release 12.4 >** 「**ARP Commands**」を参照してください。

ip sticky-arp (interface configuration)

Switch Virtual Interface（SVI）またはレイヤ 3 インターフェイス上で sticky Address Resolution Protoco（ARP）をイネーブルにするには、**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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

sticky ARP は、プライベート VLAN SVI 上でイネーブルになります。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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
- プライベート 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。

プライベート VLAN SVI 上で

- プライベート VLAN を設定する場合、sticky ARP は スイッチでイネーブルです（デフォルト）。

  ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、このコマンドは作用しません。

  no ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、sticky ARP はインターフェイス上でディセーブルになりません。

（注）　プライベート VLAN インターフェイスの ARP エントリを表示し、確認するには、**show arp** 特権 EXEC コマンドを使用するよう推奨します。

- 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
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* 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、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。
- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** 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。
- 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には：

```
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には：

```
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 IP Addressing Services Command Reference』 Release 12.4 >「ARP Commands」**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 IP Addressing Services Command Reference』 Release 12.4 >「ARP Commands」**を参照してください。

ip verify source

インターフェイスで 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。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

シンタックスの説明

port-security	（任意）IP および MAC（メディア アクセス制御）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。

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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

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 access-list

IPv6 アクセス リストを定義し、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにするには、**ipv6 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。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。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

access-list-name	IPv6 アクセス リスト名。名前にはスペースまたは引用符を含めることはできません。また、数字で始めることはできません。

デフォルト

IPv6 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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

IPv6 固有である点を除くと、**ipv6 access-list** コマンドは **ip access-list** コマンドと類似しています。

（注）　IPv6 Access Control List（ACL）は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 オプション ヘッダーに基づいた IPv6 トラフィックのフィルタリングに関する情報と任意の上位層プロトコル タイプ情報の詳細については、「**ipv6 access-list**」および「**permit (IPv6 access-list configuration)**」のコマンドを参照してください。変換された IPv6 ACL の設定例については、「例」の項を参照してください。

（注）すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探索プロセスと同等の Address Resolution Protoco（ARP）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6 traffic-filter** 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。着信および発信 IPv6 ACL をレイヤ 3 物理インターフェイス、またはルーテッド ACL の Switch Virtual Interface（SVI）に適用することはできますが、ポート ACL のレイヤ 2 インターフェイスに適用できるのは着信 IPv6 ACL だけです。

（注）**ipv6 traffic-filter** コマンドでインターフェイスに適用された IPv6 ACL は、スイッチによって転送されるトラフィックはフィルタリングしますが、スイッチによって生成されたトラフィックはフィルタリングしません。

例

次の例では、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにし、list2 という名の IPv6 ACL を設定し、その ACL をインターフェイス上の発信トラフィックに適用します。最初の ACL エントリは、ネットワーク FE80:0:0:2::/64 からのすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとして、リンクローカル プレフィクス FE80:0:0:2 のあるパケット）がインターフェイスから送信されるのを防ぎます。ACL の 2 番めのエントリは、その他すべてのトラフィックがインターフェイスから送信されるのを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 ACL の末尾にあるので、この 2 番めのエントリが必要となります。

```
Switch(config)# ipv6 access-list list2
Switch(config-ipv6-acl)# deny FE80:0:0:2::/64 any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter list2 out
```

（注）暗黙の拒否条件に依存するか、または **deny any any** ステートメントを指定してトラフィックをフィルタリングする IPv6 ACL には、プロトコル パケットのフィルタリングを避けるため、リンクローカル アドレスに対する **permit** ステートメントを含める必要があります。また、**deny** ステートメントを使用してトラフィックをフィルタリングする IPv6 ACL では、**permit any any** ステートメントをリストの最後のステートメントとして使用する必要があります。

関連コマンド

コマンド	説明
deny (IPv6 access-list configuration)	IPv6 アクセス リストに拒否条件を設定します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit (IPv6 access-list configuration)	IPv6 アクセス リストに許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストすべての内容を表示します。

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイス上の IPv6 アドレスを取得するには、**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 スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

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。

デフォルト

デフォルト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

コマンドの履歴

リリース	変更内容
12.2(46)SE	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** {**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。

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 gigabitethernet2/0/1
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 インターフェイス情報を表示します。

ipv6 dhcp client request vendor

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバのオプションを要求するように IPv6 クライアントを設定するには、**ipv6 dhcp client request** 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。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 スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト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

コマンドの履歴

リリース	変更内容
12.2(46)SE	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** {**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。

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 gigabitethernet2/0/1
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、**ipv6 dhcp ping packets** 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。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 スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

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。

デフォルト

デフォルト値は 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

コマンドの履歴

リリース	変更内容
12.2(46)SE	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** {**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。

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、**ipv6 dhcp pool** 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。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 スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

poolname	DHCPv6 プールのユーザ定義名。プール名にはシンボリック文字列（Engineering など）または整数（0 など）を使用できます。

デフォルト

デフォル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

コマンドの履歴

リリース	変更内容
12.2(46)SE	**address prefix**、**lifetime**, **link-address**、および **vendor-specific** キーワードがコマンドのサブモードに追加されました。

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** {**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。

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 プレフィクスを設定します。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。
- **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 IPv6 プレフィクスを設定します。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。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。

- **vendor-specific** : DHCPv6 ベンダー固有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 プレフィクスおよび 1 つの IPv6 アドレス プレフィ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 設定プール情報を表示します。

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、**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 スタックでデュアル IPv4/IPv6 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。

シンタックスの説明

poolname	（任意）IPv6 DHCP プールのユーザ定義名。プール名にはシンボリック文字列（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。指定できる範囲は 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。

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

コマンドの履歴

リリース	変更内容
12.2(46)SE	**automatic** キーワードがこのコマンドに追加されました。

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。プレフィクス アドレスは、関連付けられているローカル プレフィクス 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、およびリレー機能は、インターフェイス上で相互に排他的です。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 インターフェイス情報を表示します。

ipv6 mld snooping

IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピングをグローバルまたは指定の VLAN 上でイネーブルにするには、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドをキーワードなしで使用します。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。

シンタックスの説明

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。

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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

クライアントがエージング アウトになる前に送信される IP version 6（IPv6）Multicast Listener Discovery（MLD）Multicast Address Specific Queries（MASQ）を設定するには、**ipv6 mld snooping last-listener-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。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。

シンタックスの説明

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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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。

last-listener クエリー カウントが VLAN 用に設定されている場合、このカウントはグローバルに設定された値より優先されます。VLAN カウント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 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 で IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピングの last-listener クエリー間隔を設定するには、**ipv6 mld snooping last-listener-query-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。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。

シンタックスの説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー時間を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	MASQ を送信したあとマルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する時間（1000 秒単位）を設定します。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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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）Multicast Listener Discovery（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、**ipv6 mld snooping listener-message-suppression** 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。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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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までにスイッチが送信する IP version 6（IPv6）Multicast Listener Discovery（MLD）クエリーの数を設定するには、**ipv6 mld snooping robustness-variable** 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。VLAN ごとに設定するには、VLAN ID を入力します。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。

シンタックスの説明

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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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）Multicast Listener Discovery（MLD）Topology Change Notification（TCN）を設定するには、**ipv6 mld snooping tcn** 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。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。

シンタックスの説明

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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

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）Multicast Listener Discovery（MLD）スヌーピング パラメータを設定するには、**ipv6 mld snooping 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。

シンタックスの説明

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。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	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** {**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。

VLAN の各ポート上に 1 つのレシーバー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（不揮発性 RAM）に保存されます。

static キーワードは MLD メンバー 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。

ipv6 traffic-filter

インターフェイス上で IPv6 トラフィックをフィルタリングするには、**ipv6 traffic-filter** 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。フィルタリングできるトラフィックのタイプと方向は、スイッチ スタックで稼動するイメージによって異なります。インターフェイスでの IPv6 トラフィックのフィルタリ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。

ipv6 traffic-filter *access-list-name* {**in** | **out**}

no ipv6 traffic-filter *access-list-name* {**in** | **out**}

（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。

シンタックスの説明

access-list-name	IPv6 アクセス名を指定します。
in	着信 IPv6 トラフィックを指定します。
out	発信 IPv6 トラフィックを指定します。 （注）　**out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。

デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

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

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。
12.2(35)SE	IP サービスおよび IP ベース イメージの着信レイヤ 3 管理トラフィック（ルータ ACL）のサポートが追加されました。

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** {**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。

物理インターフェイス（レイヤ 2 またはレイヤ 3 ポート）、レイヤ 3 ポート チャネル、または Switch Virtual Interface（SVI）で **ipv6 traffic-filter** コマンドを使用できます。

ACL をレイヤ 3 インターフェイス（ポート ACL）の発信または着信トラフィックに、あるいはレイヤ 2 インターフェイス（ルータ ACL）の着信トラフィックに適用できます。

*いずれか*のポート ACL（IPv4、IPv6、または MAC [メディア アクセス制御]）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

例

次の例では、*cisco* という名のアクセス リストの定義に従って、IPv6 設定のインターフェイスで着信 IPv6 トラフィックをフィルタリングする方法を示します。

```
Switch (config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter cisco in
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、定義されたアクセス リストに拒否または許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストすべての内容を表示します。
show ipv6 interface	IPv6 用に設定されたインターフェイスのユーザビリティ ステータスを表示します。

l2protocol-tunnel

アクセス ポート、IEEE 802.1Q トンネル ポート、またはポート チャネルでレイヤ 2 プロトコルのトンネリングをイネーブルにするには、**l2protocol-tunnel** 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。Cisco Discovery Protocol（CDP）、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、または VLAN Trunking Protocol（VTP）パケットのトンネリングをイネーブルにできます。また、Port Aggregation Protocol（PAgP）、Link Aggregation Control Protocol（LACP）、または UniDirectional Link Detection（UDLD）パケットのポイントツーポイント トンネリングをイネーブルにできます。インターフェイスでトンネ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。

l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] |
[**shutdown-threshold**[**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] *value*] |
[**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] |
[**shutdown-threshold**[**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] |
[**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]]

シンタックスの説明

l2protocol-tunnel	CDP、STP、および VTP パケットのポイントツーマルチポイント トンネリングをイネーブルにします。
cdp	（任意）CDP のトンネリングをイネーブルにします。または、CDP のシャットダウンしきい値またはドロップしきい値を指定します。
stp	（任意）STP のトンネリングをイネーブルにします。または、STP のシャットダウンしきい値またはドロップしきい値を指定します。
vtp	（任意）VTP のトンネリングをイネーブルにします。または、VTP のシャットダウンしきい値またはドロップしきい値を指定します。
point-to-point	（任意）PAgP、LACP、および UDLD パケットのポイントツーポイント トンネリングをイネーブルにします。
pagp	（任意）PAgP のポイントツーポイント トンネリングをイネーブルにします。または、PAgP のシャットダウンしきい値またはドロップしきい値を指定します。
lacp	（任意）LACP のポイントツーポイント トンネリングをイネーブルにします。または、LACP のシャットダウンしきい値またはドロップしきい値を指定します。
udld	（任意）UDLD のポイントツーポイント トンネリングをイネーブルにします。または、UDLD のシャットダウンしきい値またはドロップしきい値を指定します。
shutdown-threshold	（任意）インターフェイスがシャットダウンするまでに受信されるシャットダウンしきい値をレイヤ 2 プロトコル pps（パケット / 秒）の最大レートで設定します。
drop-threshold	（任意）インターフェイスがパケットをドロップするまでに受信されるドロップしきい値をレイヤ 2 プロトコル pps（パケット / 秒）の最大レートで設定します。
value	インターフェイスがシャットダウンするまでにカプセル化に対して受信されるしきい値を pps（パケット / 秒）で指定します。または、インターフェイスがパケットをドロップするまでのしきい値を指定します。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値は設定されていません。

デフォルト

デフォルトでは、レイヤ 2 プロトコルのトンネリングは設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のシャットダウンしきい値は設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のドロップしきい値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

コマンドの履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 パケットをトンネリングするには、このコマンドを入力する必要があります（必要な場合は、プロトコル タイプを指定）。

このコマンドをポート チャネルで入力する場合、チャネル内のすべてのポートが同じ設定になる必要があります。

サービス プロバイダー ネットワーク内のレイヤ 2 プロトコル トンネリングは、レイヤ 2 の情報が確実にネットワーク内のすべてのカスタマー ロケーションに伝播するようにします。プロトコル トンネリングがイネーブルになると、ネットワーク内の伝送用に、プロトコル パケットがシスコの既知のマルチキャスト アドレスでカプセル化されます。パケットが宛先に到着すると、既知の MAC（メディア アクセス制御）アドレスがレイヤ 2 プロトコル MAC アドレスに置き換えられます。

CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。

サービス プロバイダー ネットワークでは、ポイントツーポイント ネットワーク トポロジをエミュレートして EtherChannel の作成を強化するのに、レイヤ 2 プロトコル トンネルを使用できます。PAgP または LACP のプロトコル トンネリングがサービス プロバイダーのスイッチでイネーブルにされている場合、リモート カスタマー スイッチは、Protocol Data Unit（PDU; プロトコル データ ユニット）を受信し、EtherChannel の自動作成をネゴシエートできます。

PAgP、LACP、および UDLD パケットのトンネリングをイネーブルにするには、ポイントツーポイント ネットワーク トポロジが必要になります。リンクダウン検出時間を減らすには、PAgP または LACP パケットのトンネリングをイネーブルにするときにインターフェイスで UDLD もイネーブルにする必要があります。

PAgP、LACP、および UDLD のポイントツーポイント プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。

注意　PAgP、LACP、および UDLD トンネリングは、ポイントツーポイント トポロジをエミュレートすることだけを目的としています。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

shutdown-threshold キーワードを入力して、シャットダウンするまでにインターフェイスで受信されるプロトコルの pps（パケット/秒）数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコル タイプに適用されます。インターフェイスにドロップしきい値も設定する場合は、シャットダウンしきい値がドロップしきい値以上でなければなりません。

シャットダウンしきい値に到達すると、インターフェイスが errdisable になります。**errdisable recovery cause l2ptguard** グローバル コンフィギュレーション コマンドを入力し、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 errdisable ステートから抜け出し、すべての原因がタイムアウトになったときに動作を再開します。**l2ptguard** でエラー回復メカニズムをイネーブルにしない場合、インターフェイスは、**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 ステートのままになります。

drop-threshold キーワードを入力して、インターフェイスがパケットをドロップするまでにインターフェイスで受信されるプロトコルの pps（パケット/秒）数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコル タイプに適用されます。インターフェイスにシャットダウンしきい値も設定する場合は、ドロップしきい値がシャットダウンしきい値以下でなければなりません。

ドロップしきい値に到達すると、受信されるレートがドロップしきい値を下回るまでインターフェイスがレイヤ 2 プロトコル パケットをドロップします。

設定は、NVRAM（不揮発性 RAM）に保存されます。

レイヤ 2 プロトコル トンネリングに関する詳細については、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、CDP パケットのプロトコル トンネリングをイネーブルにし、シャットダウンしきい値を 50 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

次の例では、STP パケットのプロトコル トンネリングをイネーブルにし、ドロップしきい値を 400 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel drop-threshold stp 400
```

次の例では、PAgP および UDLD パケットのポイントツーポイント プロトコル トンネリングをイネーブルにし、PAgP ドロップしきい値を 1000 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

関連コマンド

コマンド	説明
l2protocol-tunnel cos	すべてのトンネリング レイヤ 2 プロトコル パケットに対して Class of Service（CoS）値を設定します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報（ポート、プロトコル、CoS、およびしきい値を含む）を表示します。

l2protocol-tunnel cos

トンネリングされたレイヤ 2 プロトコル パケットすべてに、Class of Service（CoS）値を設定するには、**l2protocol-tunnel cos** 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。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。

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

シンタックスの説明

value	トンネリング レイヤ 2 プロトコル パケットの CoS プライオリティ値を指定します。CoS 値がインターフェイスのデータ パケットに対して設定されている場合、デフォルトでこの CoS 値が使用されます。インターフェイスに CoS 値が設定されていない場合は、デフォルトは 5 です。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティです。

デフォルト

デフォルトでは、インターフェイス上のデータに対して設定された CoS 値が使用されます。CoS 値が設定されていない場合は、すべてのトンネリング レイヤ 2 プロトコル パケットのデフォルトは 5 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

コマンドの履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

イネーブルの場合、トンネリング レイヤ 2 プロトコル パケットがこの CoS 値を使用します。

NVRAM（不揮発性 RAM）に値が保存されます。

例

次の例では、レイヤ 2 プロトコル トンネルの CoS 値を 7 に設定する方法を示します。

```
Switch(config)# l2protocol-tunnel cos 7
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報（CoS を含む）を表示します。

lacp port-priority

Link Aggregation Control Protocol（LACP）のポート プライオリティを設定するには、**lacp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp port-priority *priority*

no lacp port-priority

シンタックスの説明

priority	LACP のポート プライオリティ。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルト値は 32768 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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホット スタンバイ モードに置かれるポートを判別します。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。

ポート プライオリティの比較では、数値が*小さい*ほどプライオリティが*高く*なります。LACP チャネル グループに 9 つ以上のポートがある場合、LACP ポート プライオリティの数値が小さい（つまり、高いプライオリティ値の）9 つのポートがチャネル グループにバンドルされ、それより低いプライオリティのポートはホットスタンバイ モードに置かれます。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定します。

（注）LACP リンクを制御するスイッチ上にポートがある場合に限り、LACP ポート プライオリティは有効です。リンクを制御するスイッチの判別については、**lacp system-priority** 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。

LACP ポート プライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定に関する情報については、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、ポートで LACP ポート プライオリティを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# lacp port-priority 1000
```

設定を確認するには、**show lacp** [*channel-group-number*] **internal** 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。
lacp system-priority	LACP システム プライオリティを設定します。
show lacp [*channel-group-number*] **internal**	すべてのチャネル グループまたは指定のチャネル グループの内部情報を表示します。

lacp system-priority

Link Aggregation Control Protocol（LACP）のシステム プライオリティを設定するには、**lacp system-priority** 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。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。

lacp system-priority *priority*

no lacp system-priority

シンタックスの説明

priority	LACP のシステム プライオリティ。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルト値は 32768 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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

lacp system-priority コマンドでは、ポート プライオリティを制御する LACP リンクのスイッチが判別されます。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポート プライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）は無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システム プライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのスイッチも同じ LACP システム プライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（スイッチの MAC [メディア アクセス制御] アドレス）により制御するスイッチが判別されます。

lacp system-priority コマンドは、スイッチ上のすべての LACP EtherChannel に適用されます。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定の詳細については、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 ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、LACP のシステム プライオリティを設定する方法を示します。

```
Switch(config)# lacp system-priority 20000
```

設定を確認するには、**show lacp sys-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
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lacp port-priority	LACP ポート プライオリティを設定します。
show lacp sys-id	LACP によって使用されるシステム識別子を表示します。

location (global configuration)

エンドポイントのロケーション情報を設定するには、**location** 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。ロケーション情報を削除する場合は、このコマンドの **no** 形式を使用します。

location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

no location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

シンタックスの説明

admin-tag	管理タグまたはサイト情報を設定します。
civic-location	都市ロケーション情報を設定します。
elin-location	緊急ロケーション情報（ELIN）を設定します。
identifier *id*	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。
ストリング	サイト情報またはロケーション情報を英数字形式で指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location identifier *id* グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。このモードでは、都市ロケーションおよび郵便ロケーション情報を入力することができます。

ロケーション TLV をディセーブルにするには、**no lldp med-tlv-select location** 情報インターフェイス コンフィギュレーション コマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。詳細情報については、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 LLDP and LLDP-MED」の章を参照してください。

例

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
Switch (config)# location elin-location 14085553881 identifier 1
```

設定を確認するには、**show location elin** 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
location (interface configuration)	インターフェイスにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

location (interface configuration)

インターフェイスのロケーション情報を入力するには、**location** インターフェイス コマンドを使用します。インターフェイスのロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

no location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

シンタックスの説明

additional-location-information	ロケーションまたは場所に関する追加情報を設定します。
civic-location-id	インターフェイスにグローバル都市ロケーション情報を設定します。
elin-location-id	インターフェイスに緊急ロケーション情報を設定します。
id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。
word	追加のロケーション情報を指定する語またはフレーズを指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

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

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location-id *id* インターフェイス コンフィギュレーション コマンドを入力すると、都市ロケーション コンフィギュレーション モードに入ります。このモードでは、追加のロケーション情報を入力することができます。

例

次の例では、インターフェイスに都市ロケーション情報を入力する方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end

Switch(config-if)# interface gigabitethernet2/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

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

次の例では、インターフェイスに緊急ロケーション情報を入力する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location elin 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
link state group	エンドポイントにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

link state group

リンクステート グループのメンバーとしてポートを設定するには、**link state 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。リンクステート グループから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。

link state group [*number*] {**upstream** | **downstream**}

no link state group [*number*] {**upstream** | **downstream**}

シンタックスの説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 10 です。デフォルトは 1 です。
upstream	ポートを特定のリンクステート グループのアップストリーム ポートとして設定します。
downstream	ポートを特定のリンクステート グループのダウンストリーム ポートとして設定します。

デフォルト

デフォルトのグループは group 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

指定されたリンク ステート グループのアップストリームまたはダウンストリーム インターフェイスとしてポートを設定するには、**link state 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。グループ番号が省略されている場合、デフォルトのグループ番号は 1 です。

リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。ポートの集合（EtherChannel）、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。*ダウンストリーム インターフェイス*は、*アップストリーム インターフェイス*にバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイス呼ばれ、ディストリビューション スイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

ダウンストリーム インターフェイスとアップストリーム インターフェイス間の連動の詳細については、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 ガイドの「Configuring EtherChannels and Link-State Tracking」の章を参照してください。

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバーにはなれません。
- スイッチごとに設定できるのは、10 個のリンクステート グループだけです。

例

次の例では、group 2 でインターフェイスを **upstream** として設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/11 - 14
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

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
link state track	リンクステート グループをイネーブルにします。
show link state group	リンクステート グループ情報を表示します。
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 Configuration Fundamentals Command Reference for Release 12.2』> 「Cisco IOS File Management Commands」> 「Configuration File Commands」**を選択してください。

link state track

リンクステート グループをイネーブルにするには、**link state track** ユーザ EXEC コマンドを使用します。リンクステート グループをディセーブルにするには、このコマンドの **no** 形式を使用します。

link state track [*number*]

no link state track [*number*]

シンタックスの説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 10 です。デフォルト値は 1 です。

デフォルト

リンクステート トラッキングは、すべてのグループでディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループをイネーブルにするには、**link state track** 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、リンクステート グループの group 2 をイネーブルにする方法を示します。

```
Switch(config)# link state track 2
```

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
link state track	リンクステート グループのメンバーとしてインターフェイスを設定します。
show link state group	リンクステート グループ情報を表示します。
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 Configuration Fundamentals Command Reference for Release 12.2**』>「**Cisco IOS File Management Commands**」>「**Configuration File Commands**」を選択してください。

logging event

インターフェイス リンク ステータス変更の通知をイネーブルにするには、**logging event** 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。通知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。

logging event {bundle-status | link-status | spanning-tree | status | trunk status}

no logging event {bundle-status | link-status | spanning-tree | status | trunk status}

シンタックスの説明

bundle-status	BUNDLE および UNBUNDLE メッセージの通知をイネーブルにします。
link-status	インターフェイス データ リンク ステータス変更の通知をイネーブルにします。
spanning-tree	スパニングツリー イベントの通知をイネーブルにします。
status	スパニングツリー ステート変更メッセージの通知をイネーブルにします。
trunk-status	トランクステータス メッセージの通知をイネーブルにします。

デフォルト

イベント ロギングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

例

次の例では、スパニングツリー ロギングをイネーブルにする方法を示します。

```
Switch(config-if)# logging event spanning-tree
```

logging event power-inline-status

Power over Ethernet（PoE）イベントのロギングをイネーブルにするには、**logging event power-inline-status** 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。PoE 状態イベントのロギングをディセーブルにする場合は、このコマンドの **no** 形式を使用しますが、このコマンドの **no** 形式を使用しても、PoE エラー イベントはディセーブルになりません。

logging event power-inline-status

no logging event power-inline-status

シンタックスの説明

power-inline-status	PoE メッセージのロギングをイネーブルにします。

デフォルト

PoE イベントのロギングはイネーブルです。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

power-inline-status キーワードは、PoE インターフェイスでだけ使用できます。

例

次の例では、ポート上で PoE イベントのロギングをイネーブルにする方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

関連コマンド

コマンド	説明
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。

logging file

ロギング ファイルのパラメータを設定するには、**logging file** 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。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。

logging file *filesystem*:*filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem*:*filename* [*severity-level-number* | *type*]

シンタックスの説明

filesystem:*filename*	フラッシュ ファイル システムのエイリアスです。ログ メッセージを持つファイルのパスおよび名前を含みます。 スタック メンバーまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック マスターから、スタック メンバー上のローカル フラッシュ ファイル システムの構文： **flash** *member number*
max-file-size	（任意）ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。
nomax	（任意）最大ファイル サイズ（2147483647）を指定します。
min-file-size	（任意）ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。
severity-level-number	（任意）ログ ファイルの重大度のレベルを指定します。指定できる範囲は 0 ～ 7 です。各レベルの意味については *type* オプションを参照してください。
type	（任意）ログ タイプを指定します。次のキーワードが有効です。 • **emergencies**：システムは使用不可（重大度 0） • **alerts**：早急な対応が必要（重大度 1） • **critical**：危険な状態（重大度 2） • **errors**：エラーが発生している状態（重大度 3） • **warnings**：警告状態（重大度 4） • **notifications**：通常ではあるが、重要なメッセージ（重大度 5） • **information**：通知メッセージ（重大度 6） • **debugging**：デバッグ メッセージ（重大度 7）

デフォルト

ファイル サイズは最小で 2048 バイト、最大で 4096 バイトになります。

デフォルトの重大度のレベルは 7（**debugging** メッセージ：数字的に低いレベル）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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ログ ファイルは ASCII テキストの形式で、スタンドアロン スイッチの内部バッファに格納されます。スイッチ スタックの場合、スタック マスター上の内部バッファに格納されます。スタンドアロン スイッチまたはスタック マスターに障害が発生した場合、事前に **logging file flash:***filename* 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、フラッシュ メモリに保存していないかぎり、ログは失われます。

logging file flash:*filename* グローバル コンフィギュレーション コマンドで、ログをフラッシュ メモリに保存したあとは、**more flash:***filename* 特権 EXEC コマンドを使用してその内容を表示できます。

最小ファイル サイズが、最大ファイル サイズから 1024 引いた数より大きい場合、コマンドはその最小ファイルを拒否し、最大ファイル サイズから 1024 引いたサイズで設定されます。

level を指定すると、そのレベルのメッセージおよび数字的に低いレベルのメッセージが表示されます。

例

次の例では、フラッシュ メモリ内のファイルに情報レベルのログ メッセージを保存する方法を示します。

```
Switch(config)# logging file flash:logfile informational
```

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 Configuration Fundamentals Command Reference**』**Release 12.2 >** 「**File Management Commands**」**>** 「**Configuration File Management Commands**」を選択してください。

mac access-group

MAC（メディア アクセス制御）Access Control List（ACL）をレイヤ 2 インターフェイスに適用するには、**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。インターフェイスからすべてまたは指定の MAC ACL を削除するには、このコマンドの **no** 形式を使用します。MAC ACL を作成するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

mac access-group {*name*} **in**

no mac access-group {*name*}

シンタックスの説明

name	名前付き MAC アクセス リストを指定します。
in	ACL が入力方向に適用されるように指定します。出力 ACL はレイヤ 2 インターフェイスではサポートされていません。

デフォルト

MAC ACL 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（レイヤ 2 インターフェイスだけ）

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

MAC ACL は入力レイヤ 2 インターフェイスにだけ適用できます。レイヤ 3 インターフェイスには適用できません。

レイヤ 2 インターフェイスでは、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アクセス リストを使用して非 IP トラフィックをフィルタリングできます。インターフェイスに IP ACL と MAC ACL の両方を適用すると、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方をフィルタリングできます。同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。

MAC ACL がすでにレイヤ 2 インターフェイスに設定されており、新しい MAC ACL をインターフェイスに適用した場合、以前に設定されていた ACL は新しい ACL で置換されます。

スイッチ上でレイヤ 2 インターフェイスに ACL を適用する場合に、そのスイッチに対してレイヤ 3 ACL が適用されているか、またはインターフェイスがメンバーである VLAN に VLAN マップが適用されていれば、レイヤ 2 インターフェイスに適用された ACL が有効になります。

スイッチは、MAC ACL が適用されたインターフェイス上で入力パケットを受信すると、その ACL 内の一致条件を調べます。条件が一致すると、スイッチは ACL に従ってパケットを転送またはドロップします。

指定された ACL が存在しない場合、スイッチはすべてのパケットを転送します。

MAC 拡張 ACL を設定する方法の詳細については、このリリースのソフトウェア コンフィギュレーション ガイドの「Configuring Network Security with ACLs」の章を参照してください。

例

次の例では、*macacl2* と名付けられた MAC 拡張 ACL をインターフェイスに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mac access-group macacl2 in
```

設定を確認するには、**show mac access-group** 特権 EXEC コマンドを入力します。スイッチに設定された ACL を表示するには、**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
show access-lists	スイッチで設定される ACL を表示します。
show link state group	スイッチで設定される MAC ACL を表示します。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

mac access-list extended

非 IP トラフィックの MAC（メディア アクセス制御）アドレスに基づいたアクセス リストを作成するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。このコマンドを使用すると、拡張 MAC アクセス リスト コンフィギュレーション モードに入ります。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。

mac access-list extended *name*

no mac access-list extended *name*

シンタックスの説明

name	MAC 拡張アクセス リストに名前を割り当てます。

デフォルト

デフォルトでは、MAC アクセス リストは作成されません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

MAC 名前付き拡張リストは、VLAN マップおよびクラス マップとともに使用されます。

名前付き MAC 拡張 ACL は、VLAN マップまたはレイヤ 2 インターフェイスに適用できます。レイヤ 3 インターフェイスには適用できません。

mac access-list extended コマンドを入力すると、MAC アクセス リスト コンフィギュレーション モードがイネーブルになります。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。

- **default**：コマンドをそのデフォルトに設定します。
- **deny**：パケットを拒否するように指定します。詳細については、「deny (MAC access-list configuration)」の MAC アクセス リスト コンフィギュレーション コマンドを参照してください。
- **exit**：MAC 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、デフォルト値を設定します。
- **permit**：パケットを転送するように指定します。詳細は、permit (MAC access-list configuration) コマンドを参照してください。

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、名前付き MAC 拡張アクセス リスト *mac1* を作成し、拡張 MAC アクセス リスト コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

次の例では、名前付き MAC 拡張アクセス リスト *mac1* を削除する方法を示します。

```
Switch(config)# no mac access-list extended mac1
```

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
deny (MAC access-list configuration) **permit (MAC access-list configuration)**	MAC ACL を設定します（拡張 MAC アクセス リスト コンフィギュレーション モード）。
show access-lists	スイッチで設定されるアクセス リストを表示します。
vlan access-map	VLAN マップを定義し、アクセスマップ コンフィギュレーション モードに入ります。このモードでは、マッチングする MAC ACL と実行するアクションを指定できます。

mac address-table aging-time

ダイナミック エントリが使用または更新されたあと、MAC（メディア アクセス制御）アドレス テーブル内に維持される時間を設定するには、**mac address-table aging-time** 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。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。エージング タイムはすべての VLAN、または指定の VLAN に対して適用されます。

mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

no mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

シンタックスの説明

0	この値はエージングをディセーブルにします。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。
10-1000000	エージング タイム（秒）。指定できる範囲は 10 ～ 1000000 秒です。
vlan *vlan-id*	（任意）エージング タイムを適用する VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルト値は 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table aging-time**（ハイフン付き）コマンドが、**mac address-table aging-time**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

ホストが継続して送信しない場合、エージング タイムを長くして、より長い時間ダイナミック エントリを記録してください。時間を長くすることで、ホストが再送信した場合にフラッディングが起こりにくくなります。

特定の VLAN を指定しない場合、このコマンドはすべての VLAN に対してエージング タイムを設定します。

例

次の例では、すべての VLAN にエージング タイムを 200 秒に設定する方法を示します。

```
Switch(config)# mac address-table aging-time 200
```

show mac address-table aging-time 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 mac address-table aging-time	すべての VLAN または指定された VLAN の、MAC アドレス テーブルのエージング タイムを表示します。

mac address-table learning vlan

VLAN で MAC（メディア アクセス制御）アドレス学習をイネーブルにするには、**mac address-table learning** 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。これがデフォルトの状態になります。VLAN で MAC アドレス学習をディセーブルにして、MAC アドレスを学習できる VLAN を制御するには、このコマンドの **no** 形式を使用します。

mac address-table learning vlan *vlan-id*

no mac address-table learning vlan *vlan-id*

シンタックスの説明

vlan-id	1 つの VLAN ID、またはハイフンあるいはカンマで区切った VLAN ID の範囲を指定します。指定できる VLAN ID の範囲は、1 ～ 4094 です。VLAN は VLAN 内部には指定できません。

デフォルト

デフォルトでは、MAC アドレス学習はすべての VLAN でイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

使用上のガイドライン

VLAN で MAC アドレス学習を制御する場合、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。

1 つの VLAN ID（たとえば、**no mac address-table learning vlan 223**）または VLAN ID の範囲（たとえば、**no mac address-table learning vlan 1-20, 15**）での MAC アドレス学習をディセーブルにすることができます。

MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。たとえば、Switch Virtual Interface（SVI）を設定済みの VLAN で MAC アドレス学習をディセーブルにした場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。3 つ以上のポートを含む VLAN で MAC アドレス学習をディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。MAC アドレス学習のディセーブル化はポートを 2 つ含む VLAN だけで行い、SVI のある VLAN で MAC アドレス学習をディセーブルにする場合は十分注意してください。

スイッチが内部的に使用する VLAN で MAC アドレス学習はディセーブルにできません。**no mac address-table learning vlan** *vlan-id* コマンドに入力する VLAN ID が内部 VLAN である場合、スイッチはエラーメッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。

プライベート VLAN のプライマリまたはセカンダリ VLAN として設定された VLAN で MAC アドレス学習をディセーブルにする場合、MAC アドレスは、そのプライベート VLAN に属する別の VLAN（プライマリまたはセカンダリ）上で引き続き学習されます。

RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。

セキュア ポートを含む VLAN で MAC アドレス学習をディセーブルにする場合、セキュア ポートで MAC アドレス学習はディセーブルになりません。あとでインターフェイスのポート セキュリティをディセーブルにすると、ディセーブルになった MAC アドレス学習の状態がイネーブルになります。

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] コマンドを入力します。

例

次の例では、VLAN 2003 で MAC アドレス学習をディセーブルにする方法を示します。

```
Switch(config)# no mac address-table learning vlan 2003
```

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] コマンドを入力します。

関連コマンド

コマンド	説明
show mac address-table learning	すべての VLAN または指定した VLAN の MAC アドレス学習のステータスを表示します。

mac address-table move update

MAC（メディア アクセス制御）アドレス テーブル移行更新機能をイネーブルにするには、**mac address-table move update** 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。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。

mac address-table move update {**receive** | **transmit**}

no mac address-table move update {**receive** | **transmit**}

シンタックスの説明

receive	スイッチが MAC アドレステーブル移行更新メッセージを処理するよう指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MAC アドレステーブル移行更新メッセージをネットワークの他のスイッチに送信するよう指定します。

コマンド モード

グローバル コンフィギュレーション

デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

MAC アドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイ リンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次の例では、アップリンク スイッチが MAC アドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

設定を確認するには、**show mac address-table move update** 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 mac address-table move update	MAC アドレステーブル移行更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレステーブル移行更新メッセージ処理をデバッグします。
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。

mac address-table notification

スイッチ スタック上で MAC（メディア アクセス制御）アドレス通知機能をイネーブルにするには、**mac address-table notification** 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。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。

mac address-table notification [**history-size** *value*] | [**interval** *value*]

no mac address-table notification [**history-size** | **interval**]

シンタックスの説明

history-size *value*	（任意）MAC 通知履歴テーブルのエントリの最大数を設定します。指定できる範囲は 0 ～ 500 エントリです。
interval *value*	（任意）通知トラップ間隔を設定します。この時間量が過ぎると、スイッチ スタックは通知トラップを送信します。指定できる範囲は 0 ～ 2147483647 秒です。

デフォルト

MAC アドレス通知機能はデフォルトでディセーブルです。

デフォルトのトラップ間隔は 1 秒です。

履歴テーブルのデフォルトのエントリ数は 1 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table notification** （ハイフン付き）コマンドが、**mac address-table notification** （ハイフンなし）コマンドに替わりました。

使用上のガイドライン

MAC アドレス通知機能は、新しい MAC アドレスが転送テーブルに追加されたり、古いアドレスがそこから削除されたりするたびに、SNMP（簡易ネットワーク管理プロトコル）トラップを Network Management System（NMS; ネットワーク管理システム）に送信します。MAC 通知は、ダイナミックまたはセキュア MAC アドレスについてだけ許可されます。自アドレス、マルチキャスト アドレス、または他のスタティック アドレスについては、イベントは生成されません。

history-size オプションを設定している場合、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

mac address-table notification コマンドを使用すれば、MAC アドレス通知機能がイネーブルになります。また、**snmp trap mac-notification** インターフェイス コンフィギュレーション コマンドでインターフェイス上の MAC アドレス通知トラップをイネーブルにし、**snmp-server enable traps mac-notification** グローバル コンフィギュレーション コマンドでスイッチが MAC アドレス トラップを NMS に送信するよう設定する必要があります。

例

次の例では、MAC アドレス テーブル通知機能をイネーブルにし、通知トラップの間隔を 60 秒、履歴テーブルのサイズを 100 エントリに設定する方法を示します。

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

show mac address-table notification 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
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-server enable traps	**mac-notification** キーワードが追加された場合に SNMP MAC 通知トラップを送信します。
snmp trap mac-notification	特定のインターフェイスの SNMP MAC 通知トラップをイネーブルにします。

mac address-table static

MAC（メディア アクセス制御）アドレス テーブルにスタティック アドレスを追加するには、**mac address-table static** 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。スタティック エントリをテーブルから削除するには、このコマンドの **no** 形式を使用します。

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

シンタックスの説明

mac-addr	アドレス テーブルに追加する宛先 MAC アドレス（ユニキャストまたはマルチキャスト）。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
interface *interface-id*	受信されたパケットを転送するインターフェイス。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。

デフォルト

スタティック アドレスは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table static** コマンド（ハイフンあり）は、**mac address-table static** コマンド（ハイフンなし）に替わりました。

例

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先としてパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet6/0/1
```

設定を確認するには、**show mac address-table** 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 mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

mac address-table static drop

ユニキャスト MAC（メディア アクセス制御）アドレス フィルタリングをイネーブルにして、特定の送信元または宛先 MAC アドレスのトラフィックをドロップするようにスイッチを設定するには **mac address-table static drop** 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。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。

mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id*

シンタックスの説明

mac-addr	ユニキャスト送信元または宛先 MAC アドレス。この MAC アドレスを持つパケットはドロップされます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は、1 ～ 4094 です。

デフォルト

ユニキャスト MAC アドレス フィルタリングはディセーブルです。スイッチは、特定の送信元または宛先 MAC アドレスのトラフィックをドロップしません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

この機能を使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、最初のコマンドを上書きします。

  たとえば、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* グローバル コンフィギュレーション コマンドのあとに **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

  mac address-table static *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマンドのあとに **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

例

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

次の例では、ユニキャスト MAC アドレス フィルタリングをディセーブルにする方法を示します。

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

show mac address-table static 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

macro apply

インターフェイスにマクロを適用するか、またはインターフェイスにマクロ設定を適用してこれを追跡するには、**macro apply** 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。

macro {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

シンタックスの説明

apply	指定したインターフェイスにマクロを適用します。
trace	インターフェイスにマクロを適用し、そのマクロをデバッグするには、**trace** キーワードを使用します。
macro-name	マクロ名を指定します。
parameter *value*	（任意）インターフェイスに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

デフォルト

このコマンドにはデフォルト設定はありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(18)SE	**parameter** *value* キーワードが追加されました。

使用上のガイドライン

macro trace *macro-name* インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをインターフェイスに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、そのインターフェイスに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro apply** *macro-name* **?** コマンドを使用してマクロ内で必要な値のリストを表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

スイッチ ソフトウェアには、シスコ デフォルト Smartports マクロが埋め込まれています。**show parser macro** ユーザ EXEC コマンドを使用すると、マクロおよびマクロに含まれているコマンドを表示できます。

インターフェイスにシスコ デフォルト Smartports マクロを適用する場合は、次の注意事項に従ってください。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name** *macro-name* ユーザ EXEC コマンドを使用します。
- **$** で始まるキーワードには、一意のパラメータ値が必要です。**parameter** *value* キーワードを使用して、必要な値をシスコ デフォルト マクロに追加します。

  シスコ デフォルト マクロは **$** という文字を使用しているので、必須キーワードを識別するのに役立ちます。マクロを作成する場合、**$** という文字を使用したキーワードの定義には制限がありません。

マクロをインターフェイスに適用する場合、マクロ名が自動的にインターフェイスに追加されます。**show running-configuration interface** *interface-id* ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

インターフェイスの範囲に適用されたマクロは、単一インターフェイスに適用されたマクロと同じ動作をします。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。あるインターフェイスでマクロ コマンドが失敗した場合、残りのインターフェイスに適用されていきます。

default interface *interface-id* インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスで適用されたマクロの設定を削除できます。

例

macro name グローバル コンフィギュレーション コマンドを使用してマクロを作成したあとは、そのマクロをインターフェイスに適用できます。次の例では、**duplex** という名前のユーザ作成マクロをインターフェイスに適用する方法を示します。

```
Switch(config-if)# macro apply duplex
```

マクロをデバッグするには、**macro trace** 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、マクロがインターフェイスに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、インターフェイス上の **duplex** という名前のユーザ作成マクロをトラブルシューティングする方法を示します。

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

次の例では、シスコ デフォルト **cisco-desktop** マクロを表示する方法、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する方法を示します。

```
Switch# show parser macro cisco-desktop
-------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1
```

```
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

関連コマンド

コマンド	説明
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro auto execute

組み込みマクロのデフォルト値を置き換えて、組み込みまたはユーザ定義の Auto Smartports マクロへのイベント トリガからのマッピングを設定するには、**macro auto execute** 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。

macro auto execute *event trigger* {[**builtin** *built-in macro name* [*parameter=value*]] | [[*parameter=value*] **{** *function contents* **}**]}

no macro auto execute *event trigger* {[**builtin** *built-in macro name* [*parameter=value*]] | [[*parameter=value*] **{** *function contents* **}**]}

（注）　Cisco IOS Release 12.2(50)SE からは、**macro auto execute** コマンドが **macro name** コマンドに替わります。コマンドラインには表示されませんが、**macro name** コマンドは依然としてアクティブです。このコマンドは、将来の Cisco IOS ソフトウェア リリースで廃止される予定です。

シンタックスの説明

event trigger	イベント トリガから組み込みマクロへのマッピングを定義します。 *event trigger* 指定します。 • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • WORD：ユーザ定義のイベント トリガを適用します。

builtin *built-in macro name*	（任意）**builtin** *built-in macro name* を指定します。 • CISCO_PHONE_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) と $VOICE_VLAN=(2) を指定します。 • CISCO_SWITCH_AUTO_SMARTPORT （任意）パラメータ値：$NATIVE_VLAN=(1) を指定します。 • CISCO_ROUTER_AUTO_SMARTPORT （任意）パラメータ値：$NATIVE_VLAN=(1) を指定します。 • CISCO_AP_AUTO_SMARTPORT （任意）パラメータ値：$NATIVE_VLAN=(1) を指定します。 • CISCO_LWAP_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_DESKTOP_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_EASY_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_MAB_GUEST_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_MAB_TIMEOUT_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_AUTH_FAIL_AUTO_SMARTPORT （任意）パラメータ値：$ACCESS_VLAN=(1) を指定します。 • CISCO_DOT1X_CRITICAL_AUTO_SMARTPORT （任意）パラメータ値：$CRITICAL_VLAN=(1) を指定します。
parameter=value	（任意）*parameter=value*：**$** で始まるデフォルト値を置き換えます。新しい値をスペースで区切った名前値のペアの形式で入力します。[<name1>=<value1> <name2>=<value2>...]。デフォルト値は丸カッコ内に表示されます。
{*function contents*}	（任意）{*function contents*} ユーザ定義の名前を指定して、トリガに関連付けます。マクロの内容を波カッコ内に入力します。左波カッコで Cisco IOS シェル コマンドを開始し、右波カッコでコマンド グルーピングを終了します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

Auto Smartports 組み込みマクロのデフォルト値をスイッチに固有の値に置き換えるには、**macro auto execute** 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。

スイッチは、イベント トリガから組み込みマクロに自動的にマッピングします。組み込みマクロは、ソフトウェア イメージ内のシステム定義マクロです。シスコ IOS シェル スクリプティング機能を使用して、ユーザ定義のマクロを作成することもできます。

shell trigger 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、新しいイベント トリガを作成できます。組み込みおよびユーザ定義のトリガとマクロの内容を表示するには、**show shell** 特権 EXEC コマンドを使用します。

Auto Smartports マクロおよびアンチマクロ（アンチマクロとは、リンク ダウンで削除される、適用されたマクロの一部です）には、次のガイドラインと制限があります。

- 組み込みマクロは、削除または変更できません。ただし、同じ名前のユーザ定義のマクロを作成して上書きできます。元の組み込みマクロを復元するには、ユーザ定義のマクロを削除します。
- Auto Smartports マクロを適用するときにシステム競合を回避するには、802.1x 認証以外のすべてのポートの設定を削除します。
- マクロが元の設定と競合する場合、一部のマクロ コマンドが適用されなかったり、一部のアンチマクロ コマンドが削除されなかったりする場合があります。

  たとえば、802.1x 認証がイネーブルの場合、スイッチポート モードのアクセス設定を削除できません。スイッチポート モードの設定を削除する前に 802.1x 認証を削除します。
- Auto Smartports マクロを適用する場合、ポートは EtherChannel のメンバーとしないでください。
- 組み込みマクロのデフォルトのデータ VLAN は VLAN 1 です。デフォルトの音声 VLAN は VLAN 2 です。スイッチが別の VLAN を使用する場合は、組み込みマクロのデフォルト値を変更する必要があります。すべての組み込みマクロのデフォルト値を表示するには、**show shell** *functions* 特権 EXEC コマンドを使用します。
- 802.1x 認証または MAB では、Cisco 属性値（av）のペア **auto-smart-port**=*event trigger* をサポートするように RADIUS サーバを設定して、シスコ以外のデバイスを検出します。
- ネットワーク プリンタなどの CDP、MAB、または 802.1x 認証をサポートしない固定デバイスでは、ポート上の Auto Smartports をディセーブルにすることを推奨します。
- マクロ内の CLI コマンドの順序と対応するアンチマクロは、同じでなくても構いません。

例

次の例では、Cisco スイッチと Cisco IP Phone をスイッチに接続するために、2 つの組み込み Auto Smartports マクロを使用する方法を示します。次の例では、トランク インターフェイスのデフォルトの音声 VLAN、アクセス VLAN、およびネイティブ VLAN を変更します。

```
Switch# configure terminal
Switch(config)#!!!the next command modifies the access and voice vlans
Switch(config)#!!!for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!!the next command modifies the Native vlan used for inter switch trunks
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config)#
Switch(config)#!!!the next command enables auto smart ports globally
Switch(config)# macro auto global processing cdp-fallback
Switch(config)#
Switch(config)# exit

Switch# !!!here's the running configuration of the interface connected
Switch# !!!to another Cisco Switch after the Macro is applied
```

```
Switch#
Switch# show running-config interface Gi1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

次の例では、Cisco Digital Media Player（DMP）と呼ばれるユーザ定義のイベント トリガをユーザ定義のマクロにマッピングする方法を示します。

a. DMP を 802.1x または MAB イネーブルのスイッチ ポートに接続します。

b. RADIUS サーバで、属性値のペアを **auto-smart-port**=CISCO_DMP_EVENT に設定します。

c. スイッチで、イベント トリガ CISCO_DMP_EVENT を作成し、次に示すユーザ定義のマクロ コマンドを入力します。

d. スイッチが、RADIUS サーバからの属性値のペア =CISCO_DMP_EVENT 応答を認識し、このイベント トリガに関連付けられたマクロに適用します。

```
Switch(config)# shell trigger CISCO_DMP_EVENT Cisco DMP player
Switch(config)# macro auto execute CISCO_DMP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
 interface $INTERFACE
   macro description $TRIGGER
   switchport access vlan 1
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security violation restrict
   switchport port-security aging time 2
   switchport port-security aging type inactivity
   spanning-tree portfast
   spanning-tree bpduguard enable
   exit
fi
if [[ $LINKUP -eq NO ]]; then
conf t
interface $INTERFACE
     no macro description $TRIGGER
     no switchport access vlan 1
     if [[ $AUTH_ENABLED -eq NO ]]; then
        no switchport mode access
     fi
     no switchport port-security
     no switchport port-security maximum 1
     no switchport port-security violation restrict
     no switchport port-security aging time 2
     no switchport port-security aging type inactivity
     no spanning-tree portfast
     no spanning-tree bpduguard enable
     exit
fi
```

```
}
Switch(config)# end
```

表 2-6　サポートされるシスコ IOS シェル キーワード

コマンド	説明
{	コマンド グルーピングを開始します。
}	コマンド グルーピングを終了します。
[[	条件構造体として使用します。
]]	条件構造体として使用します。
else	条件構造体として使用します。
-eq	条件構造体として使用します。
fi	条件構造体として使用します。
if	条件構造体として使用します。
then	条件構造体として使用します。
-z	条件構造体として使用します。
$	$ 文字で始まる変数がパラメータ値に置き換えられます。
#	# 文字を使用して、コメント テキストを入力します。

表 2-7　サポートされないシスコ IOS シェル予約済みキーワード

コマンド	説明
|	パイプライン
case	条件構造体
esac	条件構造体
for	ループ構造体
function	シェル関数
in	条件構造体
select	条件構造体
time	パイプライン
until	ループ構造体
while	ループ構造体

関連コマンド

コマンド	説明
macro auto global processing	スイッチで Auto Smartports をイネーブルにします。
shell trigger	イベント トリガを作成します。
show shell	イベント トリガとマクロに関する情報を表示します。

macro auto global processing

スイッチ上で Auto Smartports をイネーブルにするには、**macro auto global processing** 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。Auto Smartports マクロ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。

macro auto global processing [**cdp-fallback**]

no macro auto global processing [**cdp-fallback**]

シンタックスの説明

cdp-fallback	（任意）ポート認証がイネーブルになっていて、RADIUS サーバがイベント トリガを送信しない場合、Cisco Discovery Protocol（CDP）機能情報を使用します。

デフォルト

Auto Smartports 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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチ上で Auto Smartports マクロをグローバルにイネーブルにするには、**macro auto global processing** 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。特定のポート上で Auto Smartports マクロをディセーブルにするには、**no macro auto processing** コマンドをインターフェイス モードで使用します。

Auto Smartports マクロは、ポート上で検出されたデバイス タイプに基づいて、ポートを動的に設定します。スイッチがポート上で新しいデバイスを検出した場合、適切な Auto Smartports マクロをポートに適用します。ポート上でリンクダウン イベントが発生した場合、スイッチはマクロを削除します。たとえば、ポートに Cisco IP Phone を接続した場合、Auto Smartports は自動的に IP Phone マクロを適用します。IP Phone マクロは、Quality of Service（QoS）、セキュリティ機能、および専用の音声 VLAN をイネーブルにして、遅延に影響されやすい音声トラフィックの適切な処理を確保します。

Auto Smartports は、イベント トリガを使用して、デバイスをマクロにマッピングします。最も一般的なイベント トリガは、接続されたデバイスからの Cisco Discovery Protocol（CDP）メッセージに基づきます。デバイスの検出によって、Cisco IP phone、Cisco ワイヤレス アクセスポイント、Cisco スイッチ、または Cisco ルータなどの CDP イベント トリガが呼び出されます。その他のイベント トリガは、MAC 認証バイパス（MAB）と 802.1x 認証メッセージを使用します。

認証がポート上でイネーブルの場合、**cdp-fallback** キーワードがイネーブルでない限り、スイッチは CDP メッセージを無視します。

802.1x または MAB 認証を使用する場合は、シスコ属性値（av）のペア **auto-smart-port**=*event trigger* をサポートするように、RADIUS サーバを設定します。

CDP を識別するデバイスが複数の機能をアドバタイズする場合、スイッチは次のプライオリティで機能を選択します。スイッチ、ルータ、アクセスポイント、Lightweight アクセス ポイント、電話機、ホスト。

Auto Smartports マクロがインターフェイスに適用されていることを確認するには、**show running config** ユーザ EXEC コマンドを使用します。

例

次の例では、スイッチ上で Auto Smartports をイネーブルにする方法と特定のインターフェイス上でこの機能をディセーブルにする方法を示します。

```
Switch(config)# macro auto global processing
Switch(config)# interface interface_id
Switch(config-if)# no macro auto processing
```

関連コマンド

コマンド	説明
macro auto execute	イベント トリガから組み込みのマクロへのマッピングを設定します。
shell trigger	イベント トリガを作成します。
show shell	イベント トリガとマクロに関する情報を表示します。

macro description

インターフェイスにどのマクロが適用されているかという内容を入力するには、**macro description** 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。説明を削除するには、このコマンドの **no** 形式を使用します。

macro description *text*

no macro description *text*

シンタックスの説明

description *text*	指定したインターフェイスに適用されたマクロについての説明を入力します。

デフォルト

このコマンドにはデフォルト設定はありません。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

インターフェイスにコメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。単一インターフェイスに複数のマクロを適用する場合、説明テキストは最後に適用したマクロのものになります。

次の例では、インターフェイスに説明を追加する方法を示します。

```
Switch(config-if)# macro description duplex settings
```

設定を確認するには、**show parser macro description** 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
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global

スイッチにマクロを適用するか、またはスイッチにマクロ設定を適用してこれを追跡するには、**macro global** 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。

macro global {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

シンタックスの説明

apply	スイッチにマクロを適用します。
trace	スイッチにマクロを適用してマクロをデバッグします。
macro-name	マクロ名を指定します。
parameter *value*	（任意）スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

macro trace *macro-name* グローバル コンフィギュレーション コマンドを使用して、スイッチ上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをスイッチに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、そのスイッチに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro global apply** *macro-name* **?** コマンドを使用してマクロ内で必要な値のリストを表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

スイッチ ソフトウェアには、シスコ デフォルト Smartports マクロが埋め込まれています。**show parser macro** ユーザ EXEC コマンドを使用すると、マクロおよびマクロに含まれているコマンドを表示できます。

スイッチにシスコ デフォルト Smartports マクロを適用するときは、次の注意事項に従ってください。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name** *macro-name* ユーザ EXEC コマンドを使用します。
- **$** で始まるキーワードには、一意のパラメータ値が必要です。**parameter** *value* キーワードを使用して、必要な値をシスコ デフォルト マクロに追加します。

  シスコ デフォルト マクロは **$** という文字を使用しているので、必須キーワードを識別するのに役立ちます。マクロを作成する場合、**$** という文字を使用したキーワードの定義には制限がありません。

マクロをスイッチに適用する場合、マクロ名が自動的にスイッチに追加されます。**show running-configuration** ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

マクロに含まれる各コマンドの **no** バージョンを入力したときにだけ、スイッチで適用されたグローバル マクロ設定を削除できます。

例

macro name グローバル コンフィギュレーション コマンドを使用して新しいマクロを作成したあとは、そのマクロをスイッチに適用できます。次の例では、**snmp** マクロを表示する方法、およびそのマクロを適用してホスト名をテスト サーバに設定し、IP precedence 値を 7 に設定する方法を示します。

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

----------------------------------------------------
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

マクロをデバッグするには、**macro global trace** 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、マクロがスイッチに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、**ADDRESS** パラメータ値が入力されなかったために `snmp-server host` コマンドが失敗した一方で、残りのマクロがスイッチに適用されていることを示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global description

スイッチに適用されているマクロに関する記述を入力するには、**macro global description** 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。説明を削除するには、このコマンドの **no** 形式を使用します。

macro global description *text*

no macro global description *text*

シンタックスの説明

description *text*	スイッチに適用されたマクロについての説明を入力します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチにコメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。複数のマクロがスイッチに適用されている場合、説明テキストは最後に適用されたマクロの説明になります。

次の例では、スイッチに説明を追加する方法を示します。

```
Switch(config)# macro global description udld aggressive mode enabled
```

設定を確認するには、**show parser macro description** 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
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro name

設定マクロを作成するには、**macro 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。マクロ定義を削除するには、このコマンドの **no** 形式を使用します。

macro name *macro-name*

no macro name *macro-name*

（注） Cisco IOS Release 12.2(50)SE からは、**macro auto execute** コマンドが **macro name** コマンドに替わります。コマンドラインには表示されませんが、**macro name** コマンドは依然としてアクティブです。このコマンドは、将来の Cisco IOS ソフトウェア リリースで廃止される予定です。

シンタックスの説明

macro-name	マクロの名前

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(20)SE	ヘルプ ストリング **# macro keywords** が追加されました。
12.2(50)SE	このコマンドは廃止されました。

使用上のガイドライン

マクロには、最大 3000 文字を含めることができます。1 行に 1 つのマクロ コマンドを入力します。マクロを終了するには @ 文字を使用します。マクロ内にコメント テキストを入力するには、行の先頭に # 文字を使用します。

ヘルプ文字列を使用してキーワードを指定し、マクロ内で必須キーワードを定義できます。**#macro keywords** *word* を入力してマクロで使用できるキーワードを定義します。スペースで分離することにより最大で 3 つのヘルプ ストリングを入力できます。4 つのキーワードを入力した場合、最初の 3 つだけが表示されます。

マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** と **macro name sample-macro** は、2 つの別個のマクロとなります。

マクロを作成する際に、**exit** や **end** コマンド、または **interface** *interface-id* コマンドを使用してコマンド モードを変更しないでください。これらのコマンドを使用すると、**exit**、**end**、または **interface** *interface-id* に続くコマンドが異なるコマンド モードで実行されることがあります。

このコマンドの **no** 形式によって、マクロ定義だけが削除されます。マクロがすでに適用されているインターフェイスの設定には、影響はありません。**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスで適用されたマクロの設定を削除できます。また、元のマクロの対応するコマンドすべての **no** 形式を含む既存のマクロの *anti-macro* を作成できます。次に anti-macro をインターフェイスに適用します。

既存のマクロと同じ名前の新しいマクロを作成して、マクロを変更することができます。新規作成されたマクロは既存のマクロを上書きしますが、元のマクロが適用されたインターフェイスの設定には影響を与えません。

例

次の例では、デュプレックス モードおよび速度を定義するマクロを作成する方法を示します。

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

次の例では、**# macro keywords** でマクロを作成する方法を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

次の例では、インターフェイスにマクロを適用する前に、必須キーワード値を表示する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# macro apply test ?
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID ?
  WORD  Value of first keyword to replace

Switch(config-if)# macro apply test $VLANID 2
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID 2 $MAX ?
  WORD  Value of second keyword to replace
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

match (access-map configuration)

VLAN マップを設定して、パケットを 1 つまたは複数のアクセス リストと照合するには、**match** アクセスマップ コンフィギュレーション コマンドを使用します。一致パラメータを削除するには、このコマンドの **no** 形式を使用します。

match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

シンタックスの説明

ip address	パケットを IP アドレス アクセス リストとマッチングするようにアクセス マップを設定します。
mac address	パケットを MAC（メディア アクセス制御）アドレス アクセス リストとマッチングするようにアクセス マップを設定します。
name	パケットをマッチングするアクセス リストの名前です。
number	パケットをマッチングするアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

デフォルト

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

コマンド モード

アクセスマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

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

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

パケットは、同じプロトコル タイプのアクセス リストに対してだけマッチングされます。IP パケットは、IP アクセス リストに対してマッチングされ、その他のパケットはすべて MAC アクセス リストに対してマッチングされます。

同じマップ エントリに、IP アドレスと MAC アドレスの両方を指定できます。

例

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

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
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	番号付き標準 Access Control List（ACL）を設定します。構文情報については、**『Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
action	パケットが ACL のエントリに一致した場合に、実行されるアクションを指定します。
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 IP Command Reference, Volume 1 of 3:Addressing and Services』Release 12.2 >「IP Services Commands」**を選択してください。
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。
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。

match (class-map configuration)

トラフィックを分類するための一致条件を定義するには、**match** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

no match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

シンタックスの説明

access-group *acl-index-or-name*	IP 標準または拡張 Access Control List（ACL）または MAC（メディア アクセス制御）ACL の番号または名前です。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
input-interface *interface-id-list*	階層ポリシー マップでインターフェイス レベルのクラス マップを適用する物理ポートを指定します。このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。ポート（1 エントリとしてカウント）、スペースで区切ったポート（各ポートを 1 エントリとしてカウント）、またはハイフンで区切ったポート範囲（2 エントリとしてカウント）を指定することによって、最大 6 つのエントリを指定することができます。
ip dscp *dscp-list*	着信パケットとのマッチングを行うための、最大 8 つまでの IP Differentiated Service Code Point（DSCP）値のリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。よく使用される値の場合は、ニーモニック名を入力することもできます。
ip precedence *ip-precedence-list*	着信パケットとのマッチングを行うための、最大 8 つの IP precedence 値のリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。よく使用される値の場合は、ニーモニック名を入力することもできます。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	**input-interface** *interface-id-list* キーワードが追加されました。

使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

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。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ip precedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマンドを入力した場合と同じ結果になります。サポートされているニーモニックのリストを表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ ストリングを表示してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface** *interface-id-list* キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定することができます。

例

次の例では、クラス マップ *class2* を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次の例では、クラス マップ *class3* を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、*acl1* を使用してトラフィックを分類する方法を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートのリストの指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 gigabitethernet2/0/2
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートの範囲の指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 - gigabitethernet2/0/5
Switch(config-cmap)# exit
```

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-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。
show class-map	Quality of Service（QoS）クラス マップを表示します。

mdix auto

インターフェイス上で Automatic Media-Dependent-Interface Crossover（Auto-MDIX）機能をイネーブルにするには、**mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。Auto MDIX 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。

mdix auto

no mdix auto

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Auto MDIX 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

コマンドの履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(18)SE	デフォルト設定が*ディセーブル*から*イネーブル*に変更されました。

使用上のガイドライン

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブル タイプ（ストレートまたはクロス）が不正でもリンクがアップします。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイス上および 10/100/1000BASE-T/TX Small Form-factor Pluggable（SFP）モジュール インターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスの Auto MDIX の動作ステートを確認するには、**show controllers ethernet-controller** *interface-id* **phy** 特権 EXEC コマンドを入力します。

mls qos

スイッチ全体の Quality of Service（QoS）をイネーブルにするには、**mls qos** グローバル コンフィギュレーション コマンドを使用します。**mls qos** コマンドを入力すると、システム内のすべてのポートでデフォルト パラメータが使用されて QoS がイネーブになります。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 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。

mls qos

no mls qos

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS はディセーブルです。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存在しません。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、ポリシング無しのベスト エフォートに分類されます）。

mls qos グローバル コンフィギュレーション コマンドによって QoS がイネーブル化され、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート（DSCP 値と CoS 値は 0 に設定される）として分類されます。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。デフォルトの入力キューおよび出力キューの設定値が有効となります。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

QoS 分類、ポリシング、マークダウンまたはドロップ、キューイング、トラフィック シェーピング機能を使用するには、QoS をグローバルにイネーブルにする必要があります。**mls qos** コマンドを入力する前に、ポリシーマップを作成しそれをポートに適用できます。ただし、**mls qos** コマンドを入力していない場合、QoS 処理はディセーブルになります。

no mls qos コマンドを入力しても、QoS を設定するために使用したポリシーマップとクラスマップは設定から削除されません。ただし、システム リソースを節約するため、ポリシーマップに対応するエントリはスイッチ ハードウェアから削除されます。以前の設定で QoS を再度イネーブルにする場合、**mls qos** コマンドを使用します。

このコマンドでスイッチの QoS 状態を切り替えることで、キューのサイズが修正（再割り当て）されます。キュー サイズの変更時には、ハードウェアを再設定する期間中キューは一時的にシャットダウンされ、スイッチはこのキューに新たに到着したパケットをドロップします。

例

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

```
Switch(config)# mls qos
```

設定を確認するには、**show mls qos** 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 mls qos	QoS 情報を表示します。

mls qos aggregate-policer

ポリサー パラメータを定義するには、**mls qos aggregate-policer** 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。これは、同一のポリシー マップ内の複数のクラスで共有できます。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

mls qos aggregate-policer *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}

no mls qos aggregate-policer *aggregate-policer-name*

シンタックスの説明

aggregate-policer-name	**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドが参照する集約ポリサーの名前です。
rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 8000 ～ 1000000000 です。
burst-byte	通常のバーストサイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
exceed-action drop	指定された伝送速度を超えると、スイッチがパケットをドロップするよう指定します。
exceed-action policed-dscp-transmit	指定された伝送速度を超えると、スイッチがパケットの Differentiated Service Code Point（DSCP）を、ポリシング設定 DSCP マップに指定された値に変更して、パケットを送信するよう指定します。

デフォルト

集約ポリサーは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ポリサーが複数のクラスによって共有されている場合は、集約ポリサーを定義します。

あるポートのポリサーを別のポートの他のポリサーと共有することはできません。2 つの異なるポートからのトラフィックは、ポリシング目的では集約できません。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません（ポートがいずれかのポリサーに割り当てられるとは保証されていません）。

集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

ポリシー マップ内で使用中の場合、集約ポリサーは削除できません。最初に、**no police aggregate** *aggregate-policer-name* 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すべてのポリシー マップから集約ポリサーを削除してから、**no mls qos aggregate-policer** *aggregate-policer-name* コマンドを使用する必要があります。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** 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。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** 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。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、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 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
police aggregate	異なるクラスによって共有されるポリサーを作成します。
show mls qos aggregate-policer	Quality of Service（QoS）集約ポリサー設定を表示します。

mls qos cos

デフォルトのポート Class of Service（CoS）値を定義したり、ポート上のすべての着信パケットにデフォルトの CoS 値を割り当てたりするには、**mls qos cos** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos cos {*default-cos* | **override**}

no mls qos cos {*default-cos* | **override**}

シンタックスの説明

default-cos	デフォルト CoS 値をポートに割り当てます。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。
override	着信パケットの CoS を無効にし、すべての着信パケットにデフォルトのポート CoS 値を適用します。

デフォルト

デフォルトのポート CoS 値は 0 です。

CoS 無効化はディセーブル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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

デフォルト値を使用して、タグなし（着信パケットが CoS 値を持たない場合）で着信したすべてのパケットに CoS 値と Differentiated Service Code Point（DSCP）値を割り当てることができます。また、**override** キーワードを使用すると、デフォルトの CoS 値と DSCP 値をすべての着信パケットに割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートから着信するパケットより高いプライオリティまたは低いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドは以前に設定済みの信頼状態を無効にし、すべての着信 CoS 値に **mls qos cos** コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、出力ポートで、ポートのデフォルト CoS を使用して変更されます。

例

次の例では、ポートのデフォルト ポート CoS 値を 4 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

次の例では、ポートで、ポートに着信するすべてのパケットにデフォルトのポート CoS 値 4 を割り当てる方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

設定を確認するには、**show mls qos 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 mls qos interface	Quality of Service（QoS）情報を表示します。

mls qos dscp-mutation

Differentiated Service Code Point（DSCP）の信頼性のあるポートに対して、DSCP/DSCP 変換マップを適用するには、**mls qos dscp-mutation** 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。マップをデフォルト設定（DSCP 変換なし）に戻すには、このコマンドの **no** 形式を使用します。

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*

シンタックスの説明

dscp-mutation-name	DSCP/DSCP 変換マップの名前。このマップは、以前は **mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドで定義されていました。

デフォルト

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

2 つの Quality of Service（QoS）ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を持つパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

入力ポートには複数の DSCP/DSCP 変換マップを設定できます。

マップは、DSCP の信頼性のあるポートにだけ適用します。DSCP 変換マップを信頼できないポート、Class of Service（CoS）または IP precedence の信頼できるポートに適用すると、コマンドはすぐには影響せず、そのポートが DSCP の信頼できるポートになってから効果を発揮します。

例

次の例では、DSCP/DSCP 変換マップ *dscpmutation1* を定義し、そのマップをポートに適用する方法を示します。

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

次の例では、DSCP/DSCP 変換マップ名 *dscpmutation1* をポートから削除し、そのマップをデフォルトにリセットする方法を示します。

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

設定を確認するには、**show mls qos maps** 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
mls qos map dscp-mutation	DSCP/DSCP 変換マップを定義します。
mls qos trust	ポートの信頼状態を設定します。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos map

Class of Service（CoS）/Differentiated Service Code Point（DSCP）マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシングされた DSCP のマップを定義するには、**mls qos map** グローバル コンフィギュレーション コマンドを使用します。デフォルトのマップに戻すには、このコマンドの **no** 形式を使用します。

mls qos map {**cos-dscp** *dscp1...dscp8* | **dscp-cos** *dscp-list* **to** *cos* | **dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp* | **ip-prec-dscp** *dscp1...dscp8* | **policed-dscp** *dscp-list* **to** *mark-down-dscp*}

no mls qos map {**cos-dscp** | **dscp-cos** | **dscp-mutation** *dscp-mutation-name* | **ip-prec-dscp** | **policed-dscp**}

シンタックスの説明

cos-dscp *dscp1...dscp8*	CoS/DSCP マップを定義します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。
dscp-cos *dscp-list* **to** ***cos***	DSCP/CoS マップを定義します。 *dscp-list* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。さらに、**to** キーワードを入力します。 *cos* には、DSCP 値と対応する 1 つの CoS 値を入力します。指定できる範囲は 0 ～ 7 です。
dscp-mutation *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを定義します。 *dscp-mutation-name* には、変換マップ名を入力します。 *in-dscp* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、**to** キーワードを入力します。 *out-dscp* には、1 つの DSCP 値を入力します。 指定できる範囲は 0 ～ 63 です。
ip-prec-dscp *dscp1...dscp8*	IP precedence/DSCP マップを定義します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。
policed-dscp *dscp-list* **to** *mark-down-dscp*	ポリシング設定 DSCP マップを定義します。 *dscp-list* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、**to** キーワードを入力します。 *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。 指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-8 に、デフォルトの CoS/DSCP マップを示します。

表 2-8　デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 2-9 に、デフォルトの DSCP/CoS マップを示します。

表 2-9　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 - 7	0
8 - 15	1
16 - 23	2
24 - 31	3
32 - 39	4
40 - 47	5
48 - 55	6
56 - 63	7

表 2-10 に、デフォルトの IP precedence/DSCP マップを示します。

表 2-10　デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

マップはすべてグローバルに定義されています。DSCP/DSCP 変換マップを除くすべてのマップは、すべてのポートに適用されます。DSCP/DSCP 変換マップは、特定のポートに適用されます。

例

次の例では、IP precedence/DSCP マップを定義し、IP precedence 値 0 ～ 7 を DSCP 値 0、10、20、30、40、50、55、および 60 にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

次の例では、ポリシング設定 DSCP マップを定義する方法を示します。DSCP 値 1、2、3、4、5、および 6 は DSCP 値 0 にマークダウンされます。明示的に設定されていないマークされた DSCP 値は変更されません。

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

次の例では、DSCP/CoS マップを定義する方法を示します。DSCP 値 20、21、22、23、および 24 は、CoS 1 にマッピングされます。DSCP 値 10、11、12、13、14、15、16、および 17 は CoS 0 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

次の例では、CoS/DSCP マップを定義する方法を示します。CoS 値 0 ～ 7 は、DSCP 値 0、5、10、15、20、25、30、および 35 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないエントリはすべて変更されません（ヌル マップ内の指定のままです）。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

設定を確認するには、**show mls qos maps** 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
mls qos dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼性のあるポートに適用します。
show mls qos maps	Quality of Service（QoS）マッピング情報を表示します。

mls qos queue-set output buffers

キューセット（各ポートの 4 つの出力キュー）にバッファを割り当てるには、**mls qos queue-set output buffers** 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。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。

mls qos queue-set output *qset-id* **buffers** *allocation1 ... allocation4*

no mls qos queue-set output *qset-id* **buffers**

シンタックスの説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。
allocation1 ... allocation4	各キュー（キュー 1 ～ 4 の 4 つのキュー）のバッファ スペース割り当て（%）です。*allocation1*、*allocation3*、*allocation4* の場合、範囲は 0 ～ 99 です。*allocation2* の場合、範囲は 1 ～ 100 です（CPU バッファを含める）。各値はスペースで区切ります。

デフォルト

すべての割り当て値は、4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファ スペースの 1/4 を持ちます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(18)SE	*allocation2* の範囲が 0 ～ 100 から 20 ～ 100 に変更されました。
12.2(20)SE	*allocation1*、*allocation3*、*allocation4* の範囲が 0 ～ 100 から 0 ～ 99 に変更されました。*allocation2* の範囲が 20 ～ 100 から 1 ～ 100 に変更されました。

使用上のガイドライン

4 つの割り当て値を指定します。各値はスペースで区切ります。

トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。

異なる特性を持つ異なるクラスのトラフィックを設定するには、**mls qos queue-set output** *qset-id* **threshold** グローバル コンフィギュレーション コマンドとともに、このコマンドを使用します。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にバッファ スペースの 40% を、出力キュー 2、3、および 4 にはそれぞれ 20% ずつ割り当てます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos queue-set** 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
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos queue-set output threshold

Weighted Tail-Drop（WTD）しきい値を設定することで、バッファの可用性を保証し、キューセット（各ポートの 4 つの出力キュー）に対して最大のメモリ割り当てを設定するには、**mls qos queue-set output threshold** 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。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。

mls qos queue-set output *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

シンタックスの説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。
queue-id	コマンドが実行されるキューセット内の特定のキューです。指定できる範囲は 1 ～ 4 です。
drop-threshold1 *drop-threshold2*	キューに割り当てられたメモリの割合（%）で表される 2 つの WTD しきい値です。指定できる範囲は 1 ～ 3200% です。
reserved-threshold	キューに対して保証（予約）されるメモリ量です。割り当てられたメモリの割合（%）で表されます。指定できる範囲は 1 ～ 100% です。
maximum-threshold	フル状態のキューが、予約量を超えるバッファを取得できるようにします。これは、キューがパケットをドロップせずに保持できる最大メモリです。指定できる範囲は 1 ～ 3200% です。

デフォルト

Quality of Service（QoS）がイネーブルなときは、WTD もイネーブルです。

表 2-11 は、デフォルトの WTD しきい値の設定値を示しています。

表 2-11　デフォルトの出力キュー WTD しきい値設定値

機能	キュー 1	キュー 2	キュー 3	キュー 4
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	100%	50%	50%
最大しきい値	400%	400%	400%	400%

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

mls qos queue-set output *qset-id* **buffers** グローバル コンフィギュレーション コマンドは、キューセット内の 4 つのキューに固定数のバッファを割り当てます。

ドロップしきい値（%）は 100% を超過することができ、最大値まで指定することができます（最大しきい値が 100% を超える場合）。

バッファ範囲により、キューセット内の個々のキューが共通のプールをさらに利用できる場合でも、各キューの最大パケット数は内部で 400%、つまりバッファに割り当てられた数の 4 倍に制限されます。1 つのパケットは 1 つまたは複数のバッファを使用できます。

Cisco IOS Release 12.2(25)SEE1 以降で、*drop-threshold*、*drop-threshold2*、*maximum-threshold* パラメータの範囲が増加しました。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

スイッチは、バッファ割り当て方式を使用して、出力キューごとに最小バッファ量を予約し、いずれかのキューまたはポートがすべてのバッファを消費しその他のキューがバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを決定します。スイッチは、ターゲット キューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か空でない（空きバッファ）かを判断します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。次の例では、ポートをキューセット 2 にマッピングする方法を示します。キュー 2 のドロップしきい値を割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos queue-set** 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
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos rewrite ip dscp

着信 IP パケットの Differentiated Service Code Point（DSCP）フィールドを変更する（書き換える）ようスイッチを設定するには、**mls qos rewrite ip dscp** 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。スイッチがパケットの DSCP フィールドを変更（書き換え）しないように設定し、DSCP 透過をイネーブルにするには、このコマンドの **no** 形式を使用します。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DSCP 透過はディセーブルです。スイッチは着信 IP パケットの DSCP フィールドを変更します。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

DSCP 透過は、出力でのパケットの DSCP フィールドにだけ影響を与えます。**no mls qos rewrite ip dscp** コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

（注）DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service（QoS）に基づきます。

DSCP 透過の設定に関係なく、スイッチは、トラフィックのプライオリティを表す Class of Service（CoS）値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

たとえば、QoS がイネーブルになっていて、着信パケットの DSCP 値が 32 である場合、スイッチは、ポリシーマップ設定に基づいて内部 DSCP 値を 16 に変更します。DSCP 透過がイネーブルになっている場合、送信 DSCP 値は 32（着信の値と同じ）です。DSCP 透過がディセーブルになっている場合、内部 DSCP 値に基づいて、送信 DSCP 値は 16 になります。

例

次の例では、DSCP 透過性をイネーブルにして、スイッチで着信 IP パケットの DSCP 値を変更しないように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

次の例では、DSCP 透過性をディセーブルにして、スイッチで着信 IP パケットの DSCP 値を変更するように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

設定を確認するには、**show running config | include rewrite** 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
mls qos	QoS をグローバルにイネーブルにします。
show mls qos	QoS 情報を表示します。
show running-config | include rewrite	DSCP 透過性設定を表示します。構文情報については、**『Cisco IOS Release 12.2 Configuration Guides and Command Reference』> 『Cisco IOS Fundamentals Command Reference』Release12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

mls qos srr-queue input bandwidth

入力キューに Shaped Round Robin（SRR）ウェイトを割り当てるには、**mls qos srr-queue input bandwidth** 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。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。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。

mls qos srr-queue input bandwidth *weight1 weight2*

no mls qos srr-queue input bandwidth

シンタックスの説明

weight1 weight2	*weight1* および *weight2* の比率により、SRR スケジューラがパケットを入力キュー 1 およびキュー 2 から送り出す頻度の比率が決まります。指定できる範囲は 1 ～ 100 です。各値はスペースで区切ります。

デフォルト

weight1 と weight2 は 4 です（帯域幅の 1/2 ずつ 2 つのキューに均等に分配されます）。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

どの入力キューがプライオリティ キューであるかを指定するには、**mls qos srr-queue input priority-queue** 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、スタックでキューの入力帯域幅を割り当てる方法を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

次の例では、キュー 2 はキュー 1 の 3 倍の帯域幅を持っています。キュー 2 には、キュー 1 の 3 倍の頻度でサービスが提供されます。

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** または **show mls qos input-queue** 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
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	Class of Service（CoS）値を入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 input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 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 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 input threshold	Weighted Tail-Drop（WTD）しきい値のパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input buffers

入力キュー間にバッファを割り当てるには、**mls qos srr-queue input buffers** 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。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。

mls qos srr-queue input buffers *percentage1 percentage2*

no mls qos srr-queue input buffers

シンタックスの説明

percentage1 *percentage2*	入力キュー 1 およびキュー 2 に割り当てられるバッファの割合（%）です。指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。

デフォルト

バッファの 90% がキュー 1 に、バッファの 10% がキュー 2 に割り当てられます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。

例

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos input-queue** 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
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入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 input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 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 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。

コマンド	説明
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD）しきい値のパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input cos-map

Class of Service（CoS）値を入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 にマッピングするには、**mls qos srr-queue input cos-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。

mls qos srr-queue input cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*}

no mls qos srr-queue input cos-map

シンタックスの説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 2 です。
cos1...cos8	CoS 値を入力キューへマッピングします。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキューのしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。

デフォルト

表 2-12 では、デフォルトの CoS 入力キューしきい値のマッピングを示します。

表 2-12　デフォルトの CoS 入力キューしきい値

CoS 値	キュー ID - しきい値 ID
0 - 4	1 - 1
5	2 - 1
6, 7	1 - 1

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた CoS によって、入力または出力のキューおよびしきい値が選択されます。

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、CoS 値 0 ～ 3 を、入力キュー 1 とドロップしきい値 50% のしきい値 ID 1 にマッピングする方法を示します。CoS 値 4 と 5 は、入力キュー 1 とドロップしきい値 70% のしきい値 ID 2 に割り当てます。

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 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
mls qos srr-queue input bandwidth	Shaped Round Robin（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 dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 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 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 input threshold	WTD しきい値のパーセントを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input dscp-map

Differentiated Service Code Point（DSCP）値を入力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue input dscp-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。

mls qos srr-queue input dscp-map queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}

no mls qos srr-queue input dscp-map

シンタックスの説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 2 です。
dscp1...dscp8	DSCP 値を入力キューにマッピングします。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。
threshold *threshold-id dscp1...dscp8*	DSCP 値をキューしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-13 は、デフォルトの DSCP 入力キューしきい値マップを示しています。

表 2-13　デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 - 39	1 - 1
40 - 47	2 - 1
48 - 63	1 - 1

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた DSCP によって、入力または出力のキューおよびしきい値が選択されます。

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20 と 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 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
mls qos srr-queue input bandwidth	Shaped Round Robin（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	Class of Service（CoS）値を入力キューにマッピングするか、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 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 input threshold	WTD しきい値のパーセントを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input priority-queue

リングが輻輳している場合、入力プライオリティ キューを設定して、スタック リング上で帯域幅を保証するには、**mls qos srr-queue input priority-queue** 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。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。

mls qos srr-queue input priority-queue *queue-id* **bandwidth** *weight*

no mls qos srr-queue input priority-queue *queue-id*

シンタックスの説明

queue-id	入力のキュー ID。指定できる範囲は 1 ～ 2 です。
bandwidth *weight*	スタック リングの帯域幅のパーセンテージ。指定できる範囲は 0 ～ 40 です。

デフォルト

プライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューはスタック リング上で帯域幅の一部が保証されており、オーバーサブスクライブ型のスタック上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューが満杯でフレームをドロップしている場合）に、遅延とジッタを軽減します。

大きい値はスタック全体に影響を与え、スタック パフォーマンスを低下させるため、保証される帯域幅の合計は制限されます。

Shaped Round Robin（SRR）は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** と入力します。

例

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** または **show mls qos input-queue** 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
mls qos srr-queue input bandwidth	Shaped Round Robin（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	Class of Service（CoS）値を入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 input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 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 input threshold	Weighted Tail-Drop（WTD）しきい値のパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input threshold

入力キューに Weighted Tail-Drop（WTD）しきい値のパーセンテージを割り当てるには、**mls qos srr-queue input threshold** 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。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。

mls qos srr-queue input threshold *queue-id threshold-percentage1 threshold-percentage2*

no mls qos srr-queue input threshold *queue-id*

シンタックスの説明

queue-id	入力キューの ID です。指定できる範囲は 1 ～ 2 です。
threshold-percentage1 *threshold-percentage2*	2 つの WTD しきい値（%）です。各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。各値はスペースで区切ります。指定できる範囲は 1 ～ 100 です。

デフォルト

Quality of Service（QoS）がイネーブルなときは、WTD もイネーブルです。

2 つの WTD しきい値は、100% 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

QoS は、CoS/ しきい値 マップまたは DSCP/ しきい値マップを使用して、どの Class of Service（CoS）値または Differentiated Service Code Point（DSCP）値をしきい値 1 としきい値 2 にマッピングするかを判別します。しきい値 1 を超えた場合は、しきい値を超えなくなるまで、このしきい値に割り当てられた CoS または DSCP を持つパケットがドロップされます。ただし、しきい値 2 に割り当てられたパケットは、2 番めのしきい値を超えることがないかぎり、引き続きキューに入れられ送信されます。

各キューには、2 つの設定可能な（明示）ドロップしきい値と 1 つの事前設定された（暗黙）ドロップしきい値（フル）があります。

CoS/ しきい値マップを設定するには、**mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用します。DSCP/ しきい値マップを設定するには、**mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、2 つのキューにテールドロップしきい値を設定する方法を示します。キュー 1 のしきい値は 50% と 100%、キュー 2 のしきい値は 70% と 100% です。

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos input-queue** 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
mls qos srr-queue input bandwidth	Shaped Round Robin（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	Class of Service（CoS）値を入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 input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 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 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。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

mls qos srr-queue output cos-map

Class of Service（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 にマッピングするには、**mls qos srr-queue output cos-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。

mls qos srr-queue output cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*}

no mls qos srr-queue output cos-map

シンタックスの説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 4 です。
cos1...cos8	CoS 値を出力キューへマッピングします。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキューのしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。

デフォルト

表 2-14 では、デフォルトの CoS 出力キューしきい値のマッピングを示します。

表 2-14　デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0, 1	2 - 1
2, 3	3 - 1
4	4 - 1
5	1 - 1
6, 7	4 - 1

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service（QoS）ソリューションを満たさないと判断した場合に限り、設定を変更することができます。

mls qos queue-set output *qset-id* **threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ～ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** 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
mls qos srr-queue output dscp-map	Differentiated Service Code Point（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 queue-set output threshold	WTD しきい値を設定して、バッファのアベイラビリティを保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos srr-queue output dscp-map

Differentiated Service Code Point（DSCP）値を出力キューにマッピングするか、または DSCP 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue output dscp-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。

mls qos srr-queue output dscp-map queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}

no mls qos srr-queue output dscp-map

シンタックスの説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 4 です。
dscp1...dscp8	DSCP 値を出力キューにマッピングします。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。
threshold *threshold-id dscp1...dscp8*	DSCP 値をキューしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-15 は、デフォルトの DSCP 出力キューしきい値マップを示しています。

表 2-15　デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 - 15	2 - 1
16 - 31	3 - 1
32 - 39	4 - 1
40 - 47	1 - 1
48 - 63	4 - 1

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

mls qos queue-set output *qset-id* **threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。DSCP 値 0 ～ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** 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
mls qos srr-queue output cos-map	Class of Service（CoS）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 queue-set output threshold	WTD しきい値を設定して、バッファのアベイラビリティを保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos trust

ポートの信頼状態を設定するには、**mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。入力トラフィックを信頼できるようになり、パケットの Differentiated Service Code Point（DSCP）、Class of Service（CoS）、または IP precedence のフィールドを調べることにより分類が実行されます。ポートを信頼できない状態に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust [**cos** | **device cisco-phone** | **dscp** | **ip-precedence**]

no mls qos trust [**cos** | **device** | **dscp** | **ip-precedence**]

シンタックスの説明

cos	（任意）パケットの CoS 値を使用して、入力パケットを分類します。タグのないパケットについては、ポートのデフォルト CoS 値を使用します。
device cisco-phone	（任意）信頼設定に応じて、Cisco IP Phone（信頼される境界）から送信された CoS または DSCP 値を信頼することにより入力パケットを分類します。
dscp	（任意）パケット DSCP 値（8 ビット サービスタイプ フィールドの上位 6 ビット）を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグなしパケットの場合は、デフォルトのポート CoS 値が使用されます。
ip-precedence	（任意）パケットの IP precedence 値（8 ビット サービスタイプ フィールドの上位 3 ビット）を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。

デフォルト

ポートは信頼されていません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**device cisco-phone** キーワードが追加されました。
12.2(20)SE	使用上のガイドラインが改訂されて、Cisco IP Phone がスイッチまたはルーテッド ポートに接続された場合のスイッチの信頼状態の設定方法が説明されています。

使用上のガイドライン

Quality of Service（QoS）ドメインに着信するパケットは、ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートはいずれか 1 つの信頼状態に設定できます。ポートが信頼されているかどうか、またどのパケットのフィールドがトラフィックの分類に使用されるのかを指定する場合に、このコマンドを使用します。

ポートに信頼 DSCP または信頼 IP precedence が設定され、着信パケットが非 IP パケットの場合は、CoS/DSCP マップを使用して、CoS 値から対応する DSCP 値が導き出されます。CoS は、トランクポートの場合はパケット CoS、非トランク ポートの場合はデフォルトのポート CoS となります。

DSCP が信頼されている場合、IP パケットの DSCP フィールドは変更されません。ただし、パケットの CoS 値を（DSCP/CoS マップに基づいて）変更することは可能です。

CoS が信頼されている場合、パケットの CoS フィールドは変更されませんが、IP パケットである場合には（CoS/DSCP マップに基づいて）DSCP を変更することはできます。

信頼境界機能は、ユーザがネットワーク化された Cisco IP Phone から PC を切断し、これをスイッチポートに接続して信頼された CoS または DSCP 設定を利用する場合のセキュリティ問題の発生を防止します。スイッチおよび IP Phone に接続されたポートで Cisco Discovery Protocol（CDP）をグローバルにイネーブルにする必要があります。IP Phone が検出されなかった場合、信頼境界機能はスイッチまたはルーテッド ポートの信頼設定をディセーブルにし、高プライオリティ キューが誤って使用されないようにします。

DSCP または IP precedence の信頼設定を行うと、着信パケットの DSCP 値または IP precedence 値が信頼されます。IP Phone に接続するスイッチ ポートで **mls qos cos override** インターフェイス コンフィギュレーション コマンドを設定すると、スイッチは着信音声およびデータパケットの CoS を無効にし、デフォルトの CoS 値をそれらに割り当てます。

QoS ドメイン間境界の場合は、ポートを DSCP 信頼状態に設定し、DSCP 値が QoS ドメイン間で異なる場合は DSCP/DSCP 変換マップを適用することができます。

ポート信頼状態を使用した分類（たとえば、**mls qos trust** [**cos** | **dscp** | **ip-precedence**]）とポリシーマップ（たとえば、**service-policy input** *policy-map-name*）は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

例

次の例では、着信パケットの IP precedence フィールドを信頼するようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust ip-precedence
```

次の例では、ポートに接続している Cisco IP Phone が信頼できる装置であると指定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust device cisco-phone
```

設定を確認するには、**show mls qos 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
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 dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼できるポートに適用します。
mls qos map	CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義します。
show mls qos interface	QoS 情報を表示します。

mls qos vlan-based

物理ポート上で VLAN ベースの Quality of Service（QoS）をイネーブルにするには、**mls qos vlan-based** 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。

mls qos vlan-based

no mls qos vlan-based

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

VLAN ベースの QoS 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

コマンドの履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

階層ポリシー マップを Switch Virtual Interface（SVI）に適用するには、階層ポリシー マップのセカンダリ インターフェイス レベルでポートを指定するときに、物理ポートで **mls qos vlan-based** 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。

階層ポリシングを設定すると、階層ポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに反映されます。インターフェイス レベルのトラフィック分類における個々のポリサーは、分類に従って指定された物理ポートだけに反映されます。

階層型ポリシー マップを設定する詳細な手順については、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「Classifying, Policing, and Marking Traffic by Using Hierarchical Policy Maps」の項を参照してください。

例

次の例では、物理ポート上で VLAN ベースのポリシングをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos vlan-based
```

show mls qos interface 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 mls qos interface	QoS 情報を表示します。

monitor session

新規に Switched Port Analyzer（SPAN）セッションまたは Remote SPAN（RSPAN）の送信元または宛先セッションを開始するには、**monitor session** 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。これにより、ネットワーク セキュリティ デバイス（Cisco IDS センサー アプライアンスなど）の宛先ポート上にある入力トラフィックをイネーブルにして、既存の SPAN または RSPAN セッションでのインターフェイスまたは VLAN の追加または削除を実行し、SPAN 送信元トラフィックを特定 VLAN に制限（フィルタリング）します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元/宛先インターフェイスまたはフィルタを削除したりするには、このコマンドの **no** 形式を使用します。宛先インターフェイスに対してこのコマンドの **no** 形式を使用すると、カプセル化オプションは無視されます。

monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

monitor session *session_number* **filter vlan** *vlan-id* [, | -]

monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

no monitor session {*session_number* | **all** | **local** | **remote**}

no monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

no monitor session *session_number* **filter vlan** *vlan-id* [, | -]

no monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

シンタックスの説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は 1 ～ 66 です。
destination	SPAN または RSPAN の宛先を指定します。宛先は物理ポートである必要があります。
interface *interface-id*	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバー、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 48 です。
encapsulation replicate	（任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。
ingress	（任意）入トラフィック転送をイネーブルにします。
dot1q vlan *vlan-id*	デフォルト VLAN として指定された VLAN で IEEE 802.1Q カプセル化を持つ着信パケットを受け入れます。

isl	ISL（スイッチ間リンク）カプセル化を使用して入力トラフィックを転送するように指定します。
untagged vlan *vlan-id*	デフォルト VLAN として指定された VLAN でタグなしカプセル化を持つ着信パケットを受け入れます。
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入トラフィックにデフォルトの VLAN を設定します。
remote vlan *vlan-id*	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークン リングおよび FDDI VLAN に予約済）になることはできません。
,	（任意）一連のインターフェイスまたは VLAN を指定します。または、以前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
filter vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
source	SPAN または RSPAN の送信元を指定します。物理ポート、ポート チャネル、VLAN が送信元になることができます。
both、**rx**、**tx**	（任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
source vlan *vlan-id*	VLAN ID として SPAN の送信元インターフェイスを指定します。指定できる範囲は 1 ～ 4094 です。
all、**local**、**remote**	すべての SPAN および RSPAN、すべてのローカル SPAN、すべての RSPAN セッションをクリアするため、**no monitor session** コマンドに **all**、**local**、**remote** を指定します。

デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタされます。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートでは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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*} キーワードが追加されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

スイッチ スタック上で、最大 64 の宛先ポートを保有できます。

SPAN または RSPAN の宛先ポートとして 10 ギガビット イーサネット ポートを設定すると、リンクの回線速度は低下します。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,** | **-]** オプションを使用することにより、一連のインターフェイスまたはインターフェイス範囲、一連の VLAN または VLAN 範囲を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。EtherChannel グループのメンバーである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

個々のポートはそれらが EtherChannel に参加している間もモニタすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証はディセーブルです。IEEE 802.1x 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。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。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元になることができません。

入トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- 他のキーワードなしで、**monitor session** *session_number* **destination interface** *interface-id* を入力した場合、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session** *session_number* **destination interface** *interface-id* **ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q**、**isl**、または **untagged** のいずれであるかによって決まります。
- その他のキーワードを指定せずに、**monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** を入力した場合は、出力カプセル化は送信元インターフェイス カプセル化を複製し、入力トラフィック転送はイネーブルにはなりません。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスのカプセル化を複製し、入力カプセル化はそのあとに続くキーワードが、**dot1q**、**isl**、または **untagged** のいずれであるかによって決まります。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバー 1 の送信元ポート 1 からスタック メンバー 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Switch(config)# no monitor session 2 destination gigabitethernet1/0/2
```

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次の例では、複数の送信元インターフェイスをモニタする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、モニタされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
replicate ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN および RSPAN 設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

関連コマンド

コマンド	説明
remote-span	vlan コンフィギュレーション モードで RSPAN VLAN を設定します。
show monitor	SPAN および RSPAN セッション情報を表示します。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

mvr (global configuration)

スイッチ上の Multicast VLAN Registration（MVR）機能をイネーブルにするには、キーワードを指定せずに **mvr** 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。このコマンドをキーワードとともに使用すると、スイッチの MVR モードの設定、MVR IP マルチキャスト アドレスの設定、またはグループ メンバシップからのポートの削除を行う前に、クエリーの返答を待つ最大時間の設定、または MVR マルチキャスト VLAN の指定が行われます。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。

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

シンタックスの説明

group *ip-address*	スイッチの MVR グループ IP マルチキャスト アドレスをスタティックに設定します。 スタティックに設定した IP マルチキャスト アドレスまたは連続アドレスを削除したり、IP アドレスが入力されない場合にすべてのスタティックに設定された MVR IP マルチキャスト アドレスを削除したりする場合は、このコマンドの **no** 形式を使用します。
count	（任意）複数の連続 MVR グループ アドレスを設定します。指定できる範囲は 1 ～ 256 です。デフォルト値は 1 です。
mode	（任意）MVR の動作モードを指定します。 デフォルトは compatible モードです。
compatible	MVR モードを設定して、Catalyst 2900 XL および Catalyst3500XL スイッチと互換性を持つようにします。このモードでは、送信元ポートでのダイナミック メンバシップ加入は使用できません。
dynamic	MVR モードを設定して、送信元ポートでダイナミック MVR メンバシップを使用できるようにします。
querytime *value*	（任意）レシーバー ポートで IGMP レポート メンバシップを待機する最大時間を設定します。この時間は、レシーバー ポート脱退処理にだけ適用されます。IGMP クエリーがレシーバー ポートから送信された場合、スイッチは、デフォルトまたは設定された MVR クエリー時間が経過するまで IGMP グループ メンバシップ レポートを待ってから、ポートをマルチキャスト グループ メンバシップから削除します。 この値は 10 分の 1 秒単位の応答時間です。指定できる範囲は 1 ～ 100 です。デフォルトは 5/10 秒つまり 1/2 秒です。 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。
vlan *vlan-id*	（任意）MVR マルチキャスト データの受信が予想される VLAN を指定します。これは、すべての送信元ポートが属する VLAN でもあります。指定できる範囲は 1 ～ 4094 です。デフォルト値は VLAN 1 です。

デフォルト

MVR はデフォルトでディセーブルです。

デフォルトの MVR モードは、compatible モードです。

IP マルチキャスト アドレスは、デフォルトではスイッチで設定されます。

デフォルトのグループ IP アドレス カウントは 0 です。

デフォルトのクエリー応答時間は 5/10 秒つまり 1/2 秒です。

デフォルトの MVR 用マルチキャスト VLAN は VLAN 1 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

最大 256 の MVR マルチキャスト グループを 1 つのスイッチで設定できます。

MVR に属するすべての IP マルチキャスト アドレスをスタティックに設定する場合は、**mvr group** コマンドを使用します。設定したマルチキャスト アドレスに送信されたマルチキャスト データは、スイッチのすべての送信元ポートおよびその IP マルチキャスト アドレスでデータを受信するよう登録されたすべてのレシーバー ポートに送信されます。

MVR はスイッチのエイリアス IP マルチキャスト アドレスをサポートします。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。

mvr querytime コマンドはレシーバー ポートだけに適用されます。

スイッチ MVR が、Catalyst 2900 XL または Catalyst 3500 XL スイッチと相互動作している場合は、マルチキャスト モードを compatible に設定してください。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR はスイッチで IGMP スヌーピングと共存できます。

マルチキャスト ルーティングおよび MVR はスイッチ上で共存できません。MVR がイネーブルになっている状態で、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにした場合、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態で、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作はキャンセルされ、エラー メッセージが表示されます。

例

次の例では、MVR をイネーブルにする方法を示します。

```
Switch(config)# mvr
```

show mvr 特権 EXEC コマンドを使用すると、最大のマルチキャスト グループの現在の設定を表示できます。

次の例では、228.1.23.4 を IP マルチキャスト アドレスとして設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.4
```

次の例では、228.1.23.1 ～ 228.1.23.10 のマルチキャスト アドレスとともに 10 の連続 IP 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)# mvr group 228.1.23.1 10
```

スイッチで設定された IP マルチキャスト グループ アドレスを表示する場合は、**show mvr members** 特権 EXEC コマンドを使用します。

次の例では、最大クエリー応答時間を 1 秒（10/10）に設定する方法を示します。

```
Switch(config)# mvr querytime 10
```

次の例では、VLAN 2 をマルチキャスト VLAN として設定する方法を示します。

```
Switch(config)# mvr vlan 2
```

設定を確認するには、**show mvr** 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
mvr (interface configuration)	MVR ポートを設定します。
show mvr	MVR グローバル パラメータまたはポート パラメータを表示します。
show mvr interface	設定された MVR インターフェイスをそのタイプ、ステータス、および即時脱退設定とともに表示します。インターフェイスがメンバーであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャスト グループのメンバーであるすべてのポートを表示します。グループにメンバーがいない場合、そのステータスは Inactive として表示されます。

mvr (interface configuration)

レイヤ 2 のポートを Multicast VLAN Registration（MVR）のレシーバーまたは送信元ポートとして設定することで、即時脱退機能を設定し、IP マルチキャスト VLAN と IP アドレスにポートをスタティックに割り当てるには、**mvr** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mvr [**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* **group** [*ip-address*]]

no mvr [**immediate** | **type** {**source** | **receiver**}| **vlan** *vlan-id* **group** [*ip-address*]]

シンタックスの説明

immediate	（任意）ポートの MVR の即時脱退機能をイネーブルにします。この機能をディセーブルにするには、**no mvr immediate** コマンドを使用します。
type	（任意）ポートを MVR レシーバー ポートまたは送信元ポートとして設定します。 デフォルト ポート タイプは、MVR 送信元ポートおよびレシーバー ポートのどちらでもありません。**no mvr type** コマンドは、送信元ポートおよびレシーバー ポートのどちらでもないポートとしてポートをリセットします。
receiver	ポートを、マルチキャスト データの受信だけが可能な加入者ポートとして設定します。レシーバー ポートはマルチキャスト VLAN に属することはできません。
source	ポートを、設定済みのマルチキャスト グループとのマルチキャスト データの送受信が可能なアップリンク ポートとして設定します。スイッチの送信元ポートはすべて単一のマルチキャスト VLAN に属します。
vlan *vlan-id* **group**	（任意）ポートを、指定された VLAN ID を持つマルチキャストグループのスタティック メンバーとして追加します。 **no mvr vlan** *vlan-id* **group** コマンドは、IP マルチキャスト アドレス グループのメンバシップから VLAN 上のポートを削除します。
ip-address	（任意）指定されたマルチキャスト VLAN ID の指定された MVR IP マルチキャスト グループ アドレスをスタティックに設定します。これは、ポートが加入しているマルチキャスト グループの IP アドレスです。

デフォルト

ポートはレシーバーとしても送信元としても設定されません。

即時脱退機能はすべてのポートでディセーブルです。

レシーバー ポートはどの設定済みマルチキャスト グループにも属していません。

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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ポートが設定されたマルチキャスト グループ向けマルチキャスト データを送受信できるようにする場合は、ポートを送信元ポートとして設定します。マルチキャスト データは送信元ポートとして設定されているすべてのポートで受信されます。

レシーバー ポートはトランク ポートになることはできません。スイッチのレシーバー ポートは異なる VLAN に属していても構いませんが、マルチキャスト VLAN に属することはできません。

MVR に参加していないポートは、MVR レシーバー ポートまたは送信元ポートとして設定しないでください。非 MVR ポートは通常のスイッチ ポートであり、通常のスイッチ動作でマルチキャスト データを送受信することができます。

即時脱退機能がイネーブルの場合、レシーバー ポートはより短時間でマルチキャスト グループから脱退します。即時脱退機能がなく、スイッチがレシーバー ポートのグループから IGMP Leave メッセージを受信した場合、スイッチは、そのポートに IGMP MAC（メディア アクセス制御）ベースのクエリーを送信し、IGMP グループ メンバシップ レポートを待ちます。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能では、IGMP Leave を受信したレシーバー ポートから IGMP MAC ベースのクエリーは送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち時間が短縮されます。

即時脱退機能をイネーブルにするのは、レシーバー装置が 1 つだけ接続されているレシーバー ポートに限定してください。

mvr vlan group コマンドは、IP マルチキャスト アドレスへ送信されたマルチキャスト トラフィックを受信するようにポートをスタティックに設定します。グループのメンバーとしてスタティックに設定されたポートは、スタティックに削除されるまではそのグループのメンバーのままです。compatible モードでは、このコマンドはレシーバー ポートだけに適用されます。dynamic モードでは送信元ポートにも適用されます。レシーバー ポートは、IGMP Join メッセージを使用してダイナミックにマルチキャスト グループに加入することもできます。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR ポートはプライベート VLAN ポートにはなれません。

例

次の例では、MVR レシーバー ポートとしてポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

設定されたレシーバー ポートおよび送信元ポートを表示するには、**show mvr interface** 特権 EXEC コマンドを使用します。

次の例では、ポートの即時脱退機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 のポートを IP マルチキャスト グループ 228.1.23.4 のスタティック メンバーとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

設定を確認するには、**show mvr 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
mvr (global configuration)	スイッチ上で Multicast VLAN Registration（MVR）をイネーブルにして、設定します。
show mvr	MVR グローバル パラメータまたはポート パラメータを表示します。
show mvr interface	設定済みの MVR インターフェイスを表示するか、またはレシーバー ポートが所属するマルチキャスト グループを表示します。インターフェイスがメンバーであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャスト グループのメンバーであるすべてのレシーバー ポートを表示します。

network-policy

インターフェイスにネットワークポリシー プロファイルを適用するには、**network-policy** インターフェイス コンフィギュレーション コマンドを使用します。ポリシーを削除する場合は、このコマンドの **no** 形式を使用します。

network-policy *profile number*

no network-policy

シンタックスの説明

profile number	ネットワークポリシー プロファイルの番号を指定します。

デフォルト

ネットワークポリシー プロファイルは適用されません。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

インターフェイスにプロファイルを適用するには、**network-policy** *profile number* 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。

最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan** *vlan-id* がすでにインターフェイス上に設定されている場合、ネットワークポリシー プロファイルをインターフェイス上に適用できます。その後、インターフェイスは、インターフェイス上に適用された音声または音声シグナリング VLAN ネットワークポリシー プロファイルを使用します。

例

次の例では、インターフェイスにネットワークポリシー プロファイル 60 を適用する方法を示します。

```
Switch(config)# interface_id
Switch(config-if)# network-policy profile 60
```

関連コマンド

コマンド	説明
network-policy profile (global configuration)	ネットワークポリシー プロファイルを作成します。
network-policy profile (network-policy configuration)	ネットワークポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

network-policy profile (global configuration)

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーション モードに入るには、**network-policy 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。ポリシーを削除し、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。

network-policy profile *profile number*

no network-policy profile *profile number*

シンタックスの説明

profile number	ネットワークポリシー プロファイルの番号を指定します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

ネットワークポリシー プロファイル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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードに入るには、**network-policy 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。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service（CoS）、Differentiated Service Code Point（DSCP）の値、およびタギング モードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

その後、これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）の **network-policy** Time Length Value（TLV）に含まれます。

例

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile (network-policy configuration)	ネットワークポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

network-policy profile (network-policy configuration)

network-policy profile グローバル コンフィギュレーション コマンドを使用して作成されたネットワーク ポリシー プロファイルを設定するには、**network-policy profile** コンフィグレーション モード コマンドを使用します。プロファイルを削除する場合は、追加パラメータなしでこのコマンドの **no** 形式を使用します。設定された属性を変更する場合は、パラメータとともにこのコマンドの **no** 形式を使用します。

network-policy profile *profile number* {**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**]

no network-policy profile *profile number* {**voice** | **voice-signaling**} **vlan** [*vlan-id* | {**cos** *cvalue*} | {**dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue*} | {**dscp** *dvalue*}] | **none** | **untagged**]

シンタックスの説明

voice	音声アプリケーション タイプを指定します。
voice-signaling	音声シグナリング アプリケーション タイプを指定します。
vlan	音声トラフィック用のネイティブ VLAN を指定します。
vlan-id	（任意）音声トラフィック用の VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
cos *cvalue*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 0 です。
dscp *dvalue*	（任意）設定された VLAN に対する Differentiated Service Code Point（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 0 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	（任意）IP Phone をタグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。

デフォルト

ネットワーク ポリシーは定義されていません。

コマンド モード

ネットワークポリシー コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ネットワークポリシー プロファイルの属性を設定するには、**network-policy profile** コマンドを使用します。

voice アプリケーション タイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データ アプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

voice-signaling アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが **voice policy** TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーション タイプはアドバタイズしないでください。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)#voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile (global configuration)	ネットワークポリシー プロファイルを作成します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

nmsp

Network Mobility Services Protocol（NMSP）をスイッチ上でイネーブルにするには、**nmsp** 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。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。

nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

no nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

シンタックスの説明

enable	NMSP 機能をスイッチ上でイネーブルにします。
notification interval	NMSP 通知間隔を指定します。
attachment	アタッチメント通知間隔を指定します。
location	ロケーション通知間隔を指定します。
interval-seconds	スイッチが MSE にロケーションまたはアタッチメントの更新を送信するまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。

デフォルト

NMSP 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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

NMSP ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine（MSE; モビリティ サービス エンジン）に送信するようにスイッチをイネーブルにするには、**nmsp** 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、スイッチ上で NMSP をイネーブルにし、ロケーション通知時間を 10 秒に設定する方法を示します。

```
Switch(config)#nmsp enable
Switch(config)#nmsp notification interval location 10
```

関連コマンド

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。
nmsp attachment suppress	特定のインターフェイスからのアタッチメント情報のレポートを抑制します。
show nmsp	NMSP 情報を表示します。

nmsp attachment suppress

特定のインターフェイスからのアタッチメント情報のレポートを抑制するには、**nmsp attachment suppress** インターフェイス コンフィギュレーション モード コマンドを使用します。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。

nmsp attachment suppress

no nmsp attachment suppress

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドにはデフォルト設定はありません。

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

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine（MSE）に送信しないようにインターフェイスを設定するには、**nmsp attachment suppress** 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、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Switch(config)# switch interface interface-id
Switch(config-if)# nmsp attachment suppress
```

関連コマンド

コマンド	説明
nmsp	スイッチ上で Network Mobility Services Protocol（NMSP）をイネーブルにします。
show nmsp	NMSP 情報を表示します。

nsf

Open Shortest Path First（OSPF）または Enhanced IGRP（EIGRP）ルーティングの Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）をイネーブルにし、設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**nsf** ルータ コンフィギュレーション コマンドを使用します。NSF 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。

nsf [**enforce global**]

no nsf

シンタックスの説明

enforce global	（任意）非 NSF 認識ネイバが検出された場合、OSPF NSF の再起動をキャンセルします。このキーワードは、OSPF ルータ コンフィギュレーション モードでだけ表示されます。

デフォルト

NSF はディセーブルです。

enforce global オプションはイネーブルです（OSPF 限定）。

コマンド モード

ルータ コンフィギュレーション（OSPF または EIGRP）

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

nsf コマンドはルータ コンフィギュレーション コマンドで、指定のルーティング プロセスが適用されたすべてのインターフェイスに影響します。スイッチは、OSPF および EIGRP プロトコルに対する Cisco NSF をサポートしています。

NSF がイネーブルで、スタック マスターのスイッチオーバーが検出された場合、NSF 対応ルータは NSF 認識ネイバまたは NSF 対応ネイバからのルーティング情報を再構築し、再起動を待機しません。

例

次の例では、OSPF NSF をイネーブルにする方法を示します。

```
Switch(config)# router ospf 100
Switch(config-router)# nsf
```

show ip ospf 特権 EXEC コマンドを使用して、OSPF NSF がイネーブルであることを確認します。

次の例では、EIGRP NSF をイネーブルにする方法を示します。

```
Switch(config)# router eigrp 1
Switch(config-router)# nsf
```

show ip protocols 特権 EXEC コマンドを使用して、EIGRP NSF がイネーブルであることを確認します。

関連コマンド

コマンド	説明
router *protocol-id number*	ルーティング プロセスをイネーブルにします。

pagp learn-method

EtherChannel ポートから受信する着信パケットの送信元アドレスを学習するには、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp learn-method {aggregation-port | physical-port}

no pagp learn-method

シンタックスの説明

aggregation-port	論理ポート チャネルで学習するアドレスを指定します。スイッチは、EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートで学習するアドレスを指定します。スイッチは、送信元アドレスを学習したものと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャネルの一方の終端は、特定の宛先 MAC（メディア アクセス制御）または IP アドレスのチャネルのポートと同一のポートを使用します。

デフォルト

デフォルトは aggregation-port（論理ポート チャネル）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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

（注）CLI（コマンドライン インターフェイス）を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** 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、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

次の例では、学習方式を設定し、EtherChannel 内のポート チャネル上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 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
pagp port-priority	EtherChannel を経由するすべてのトラフィックが送信されるポートを選択します。
show pagp	PAgP チャネル グループ情報を表示します。
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 Configuration Fundamentals Command Reference』Release 12.2 > 「File Management Commands」> 「Configuration File Management Commands」**を選択してください。

pagp port-priority

EtherChannel を経由するすべての Port Aggregation Protocol（PAgP）トラフィックが送信されるポートを選択するには、**pagp port-priority** 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。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼動状態にできます。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。

pagp port-priority *priority*

no pagp port-priority

シンタックスの説明

priority	プライオリティ番号は 0 ～ 255 です。

デフォルト

デフォルト値は 128 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

（注）CLI（コマンドライン インターフェイス）を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** 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 プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 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
pagp learn-method	着信パケットの送信元アドレスを学習する機能を提供します。
show pagp	PAgP チャネル グループ情報を表示します。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

permit (ARP access-list configuration)

Dynamic Host Configuration Protocol（DHCP）バインディングとの照合に基づいて Address Resolution Protoco（ARP）パケットを許可するには、**permit** ARP 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。Access Control List（ACL）から指定された Access Control Entry（ACE）を削除するには、このコマンドの **no** 形式を使用します。

permit {[**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 permit {[**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**]

シンタックスの説明

request	（任意）ARP 要求の照合を要求します。**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	送信側 IP アドレスを指定します。
any	すべての IP アドレスまたは MAC（メディア アクセス制御）アドレスを許可します。
host *sender-ip*	指定された送信側 IP アドレスを許可します。
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 アドレスを指定します。
host *sender-mac*	指定された送信側 MAC アドレスを許可します。
sender-mac sender-mac-mask	指定された範囲の送信側 MAC アドレスを許可します。
response ip	ARP 応答の IP アドレス値を定義します。
host *target-ip*	（任意）指定されたターゲット IP アドレスを許可します。
target-ip target-ip-mask	（任意）指定された範囲のターゲット IP アドレスを許可します。
mac	ARP 応答の MAC アドレス値を指定します。
host *target-mac*	（任意）指定されたターゲット MAC アドレスを許可します。
target-mac target-mac-mask	（任意）指定された範囲のターゲット MAC アドレスを許可します。
log	（任意）ACE と一致するパケットを記録します。**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 **matchlog** キーワードも設定している場合は、一致するパケットはロギングされます。

デフォルト

デフォルト設定はありません。

コマンド モード

ARP アクセス リスト コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

permit 句を追加すると、一部の一致条件に基づいて ARP パケットを転送できます。

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 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 ACL を定義します。
deny (ARP access-list configuration)	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。
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。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

permit (IPv6 access-list configuration)

IPv6 アクセス リストの許可条件を設定するには、**permit** IPv6 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。許可条件を削除するには、このコマンドの **no** 形式を使用します。

permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

no permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

（注）　**flow-label**、**reflect**、および **routing** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

Internet Control Message Protocol（ICMP）

permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol（UDP）

permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]

（注）　**flow-label**、**reflect**、および **routing** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

シンタックスの説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/*prefix-length*	許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および Extended Universal Identifier（EUI）ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	許可条件の設定先である送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/ *prefix-length*	許可条件を設定する宛先 IPv6 ネットワーク、またはネットワークのクラス。 この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
host *destination-ipv6-address*	許可条件の設定先である宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Service Code Point（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。

fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、初期状態でないフラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。
log	（任意）エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します （コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します）。 メッセージには、アクセス リスト名、シーケンス番号、パケットが許可されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で許可されたパケット数を含めて生成されます。
log-input	（任意）**log** キーワードと同じ機能を提供します（ただし、ロギング メッセージには受信インターフェイスも表示されます）。
timeout *value*	（任意）再帰 IPv6 アクセス リストがタイムアウトになる前のアイドル時間の間隔（秒単位）。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 180 秒です。
sequence *value*	（任意）アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）許可ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。ICMP パケットは ICMP メッセージ タイプによってフィルタリングできます。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってフィルタリングできます。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージ名、または ICMP メッセージ タイプおよびコードによってフィルタリングできます。使用可能な名前については、「使用上のガイドライン」の項を参照してください。
ack	（任意）TCP プロトコルの場合の ACK ビット設定
established	（任意）TCP プロトコルの場合に限り、接続が確立済みであることを意味します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り、PSH ビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCP プロトコルの場合に限り RST ビットを設定します。
syn	（任意）TCP プロトコルの場合に限り SYN ビットを設定します。
urg	（任意）TCP プロトコルの場合に限り URG ビットを設定します。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

permit（IPv6 アクセス リスト コンフィギュレーション モード）コマンドは、IPv6 専用である点を除き **permit**（IPv4 アクセス リスト コンフィギュレーション モード）コマンドと類似しています。

IPv6 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、パケットがアクセス リストを通過する条件を定義するには、**ipv6 access-list** コマンドの後ろに **permit**（IPv6）コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力しないで、**permit**、**deny**、または **remark** ステートメントを既存のアクセス リストに追加できます。リストの最後以外の場所に新しいステートメントを追加するには、挿入する場所を示す、既存の 2 つのエントリ番号の間にある適切なエントリ番号を持った新しいステートメントを作成します。

IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注）すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探索プロセスと同等の Address Resolution Protocol（ARP）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィクスはトラフィックの送信元に基づいて、宛先プレフィクスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクスと EUI ベースの /128 プレフィクスだけをサポートします。

fragments キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

例

次の例では、OUTBOUND および INBOUND という名の IPv6 アクセス リスト 2 つを設定し、そのアクセス リストをレイヤ 3 インターフェイス上の発信および着信トラフィックに適用する方法を示します。OUTBOUND リストの最初と 2 番めの許可エントリは、ネットワーク 2001:ODB8:0300:0201::/64 からの TCP および UDP パケットすべてがインターフェイスで送信されるのを許可します。OUTBOUND リストの拒否エントリは、ネットワーク FE80:0:0:0201::/64 でのすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとして、リンクローカル プレフィクス FE80:0:0:0201 のあるパケット）がインターフェイスで送信されるのを防ぎます。OUTBOUND リストの 3 番めの許可エントリは、すべての ICMP パケットがインターフェイスで送信されるのを許可します。

INBOUND リストの許可エントリは、すべての ICMP パケットをインターフェイスで受信するのを許可します。

```
Switch(config)#ipv6 access-list OUTBOUND
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# permit udp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# deny FE80:0:0:0201::/64 any
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)#ipv6 access-list INBOUND
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter OUTBOUND out
Switch(config-if)# ipv6 traffic-filter INBOUND in
```

（注） **permit any any** ステートメントが OUTBOUND または INBOUND アクセス リストの最後のエントリとして含まれていない場合、TCP、UDP、および ICMP パケットだけがインターフェイスの双方向（着信および発信）で許可されます（アクセス リストの末尾にある、暗黙の条件によりインターフェイス上のその他のパケット タイプはすべて拒否されます）。

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 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。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
deny (IPv6 access-list configuration)	IPv6 アクセス リストに拒否条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストすべての内容を表示します。

permit (MAC access-list configuration)

条件が一致した場合に転送される非 IP トラフィックを許可するには、**permit** MAC（メディア アクセス制御）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。許可条件を拡張 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。

{**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **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 {**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **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**]

（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。

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
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）パケットの Ethertype 番号と、Ethernet II または Subnetwork Access Protocol（SNAP）カプセル化を使用して、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、マッチングを行う前に 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 までの任意の Class of Service（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）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *mask* は、マッチングを行う前に 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）を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを選択します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。表 2-16 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 2-16　IPX フィルタ基準

IPX カプセル化タイプ		
Cisco IOS 名	**Novell 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

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 Access Control List（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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

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

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

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

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

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

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

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

関連コマンド

コマンド	説明
deny (MAC access-list configuration)	条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
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。
show access-lists	スイッチに設定された ACL を表示します。

police

分類されたトラフィックのポリサーを定義するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no police *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

シンタックスの説明

rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 1000000 ～ 1000000000 です。
burst-byte	通常のバーストサイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
exceed-action drop	（任意）指定された伝送速度を超えた場合は、スイッチがパケットをドロップするように指定します。
exceed-action policed-dscp-transmit	（任意）指定された伝送速度を超えた場合、スイッチがパケットの Differentiated Service Code Point（DSCP）をポリシング設定 DSCP マップに指定された値に変え、パケットを送信するように指定します。

デフォルト

ポリサーは定義されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

階層ポリシーマップを設定する場合、セカンダリ インターフェイス レベルのポリシーマップで使用できるのは **police** ポリシーマップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

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。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** 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。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** 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。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。

ポリシー マップの **police aggregate** コマンドを 10 ギガビット イーサネット インターフェイスで使用すると、エラーになります。

例

次の例では、トラフィックがバースト サイズ 20 KB で平均伝送速度 1 Mb/s を超えた場合に、ポリサーがパケットをドロップするように設定する方法を示します。着信パケットの DSCP が信頼され、パケットは変更されません。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
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	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。
mls qos map policed-dscp	ポリシング設定 DSCP マップを DSCP の信頼できるポートに適用します。
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。

police aggregate

同一のポリシー マップにある複数のクラスにアグリゲート ポリサーを適用するには、**police aggregate** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。指定されたポリサーを削除するには、このコマンドの **no** 形式を使用します。

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

シンタックスの説明

aggregate-policer-name	集約ポリサーの名前です。

デフォルト

集約ポリサーは定義されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

集約ポリサー パラメータを設定するには、**mls qos aggregate-policer** 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。集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

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。

police aggregate コマンドを使用するポリシー マップを 10 ギガビット イーサネット インターフェイスに適用すると、エラーになります。

階層ポリシーマップで集約ポリサーを設定することはできません。

例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 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
mls qos aggregate-policer	ポリシー マップ内の複数のクラスが共有できるポリサー パラメータを定義します。
show mls qos aggregate-policer	Quality of Service（QoS）集約ポリサー設定を表示します。

policy-map

複数の物理ポートまたは Switch Virtual Interface（SVI）に適用可能なポリシーマップを作成または変更し、ポリシーマップ コンフィギュレーション モードを開始するには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。既存のポリシー 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。

policy-map *policy-map-name*

no policy-map *policy-map-name*

シンタックスの説明

policy-map-name	ポリシー マップ名です。

デフォルト

ポリシー マップは定義されません。

デフォルトの動作は、パケットが IP パケットの場合には Differentiated Service Code Point（DSCP）を 0 に設定し、パケットがタグ付きの場合には Class of Service（CoS）を 0 に設定します。ポリシングは実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	SVI のポリシー マップのサポートが追加されました。

使用上のガイドライン

policy-map コマンドを入力すると、ポリシーマップ 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。

- **class**：指定したクラス マップの分類一致基準を定義します。詳細については、「class」（P.2-68）を参照してください。
- **description**：ポリシー マップを説明します（最大 200 文字）。
- **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、グローバル コンフィギュレーション モードに戻ります。
- **no**：以前定義したポリシー マップを削除します。
- **rename**：現在のポリシー マップの名前を変更します。

グローバル コンフィギュレーション モードに戻る場合は、**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。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシー マップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシー マップのクラス ポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラス マップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

1 つの入力ポートまたは SVI では、1 つのポリシー マップだけがサポートされています。同じポリシー マップを複数の物理ポートまたは SVI に適用できます。

物理ポートまたは SVI に非階層ポリシー マップを適用できます。ただし、階層ポリシー マップを適用できるのは SVI だけです。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

プライマリ VLAN レベル ポリシー マップでは、信頼状態の設定、あるいはパケットでの新しい DSCP または IP precedence 値の設定だけが可能です。セカンダリ インターフェイス レベル ポリシー マップでは、SVI に属する物理ポートの個々のポリサーの設定だけが可能です。

階層ポリシー マップを SVI に適用すると、インターフェイス レベル ポリシー マップを変更したり、階層ポリシー マップから削除したりすることはできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。

階層ポリシー マップの詳細については、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 ガイドで「Configuring QoS」の章の「Policing on SVIs」の項を参照してください。

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。入力ポートに適用した場合、*class1* で定義されたすべての着信トラフィックのマッチングを行い、IP DSCP を 10 に設定し、平均伝送速度 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。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した 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
```

次の例では、ポリシー マップ *policymap2* に複数のクラスを設定する方法を示します。

```
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

次の例は、階層ポリシー マップを作成し、SVI に適用する方法を示しています。

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet2/0/2 - gigabitethernet2/0/3
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

次の例では、*policymap2* を削除する方法を示します。

```
Switch(config)# no policy-map policymap2
```

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	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定義します（**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）。
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。
service-policy	ポートにポリシー マップを適用します。
show mls qos vlan	SVI に適用されている Quality of Service（QoS）ポリシー マップを表示します。
show policy-map	QoS ポリシー マップを表示します。

port-channel load-balance

EtherChannel のポート間で負荷分散方式を設定するには、**port-channel load-balance** 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。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。

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

シンタックスの説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散。
dst-mac	宛先ホストの MAC（メディア アクセス制御）アドレスに基づいた負荷分散。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいた負荷分散。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散。
src-mac	送信元 MAC アドレスに基づいた負荷分散。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。

デフォルト

デフォルトは、**src-mac** 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

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

これらの転送方式をどのような場合に使用するかについての詳細は、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 ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、負荷分散方式を **dst-mac** に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 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
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 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 Configuration Fundamentals Command Reference』Release 12.2 > 「File Management Commands」> 「Configuration File Management Commands」**を選択してください。

power inline

Power over Ethernet（PoE）ポート上で電力管理モードを設定にするには、**power inline** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

power inline {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]}

no power inline {**auto** | **never** | **static**}

シンタックスの説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。
max *max-wattage*	（任意）ポートに供給される電力を制限します。指定できる範囲は 4000 ～ 15400 ミリワットです。値を指定しない場合は、最大電力が供給されます。
never	装置の検出とポートへの電力供給をディセーブルにします。
static	受電装置の検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます（確保します）。

デフォルト

デフォルトの設定は **auto**（イネーブル）です。

最大ワット数は、15400 ミリワットです。

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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(25)SE	**static** および **max** *max-wattage* オプションが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline auto
                  ^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全ポートでサポートされます。

max *max-wattage* オプションを使用して、受電装置の電力が制限を超えないようにします。この設定によって、受電装置が最大ワット数より多い電力を要求する Cisco Discovery Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル パワー バジェットに送られます。

（注）　**power inline max** *max-wattage* コマンドが 15.4 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電装置への電力供給を拒否する場合（受電装置が CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは power-deny ステートになります。スイッチはシステム メッセージを生成し、**show power inline** ユーザ EXEC コマンド出力の Oper カラムに *power-deny* が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max** *max-wattage* コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。電力が事前割り当てされているので、最大ワット数以下の電力を使用する受電装置は、スタティック ポートに接続されていれば電力が保証されます。ただし、受電装置の IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電装置が最大ワット数を超えた量を要求していることをスイッチが認識すると、受電装置がシャットダウンします。

ポートが static モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、パワー バジェット全体がすでに別の自動ポートまたはスタティック ポートに割り当てられているなど）、次のメッセージが表示されます。`Command rejected: power inline static: pwr not available`。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電装置であるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別されたあと、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定する場合、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電装置が接続されている場合は、**power inline never** コマンドでポートを設定しないでください。ポートで不正なリンクアップが生じ、errdisable ステートになる可能性があります。

例

次の例では、受電装置の検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電装置を受け入れるように PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline never
```

設定を確認するには、**show power inline** 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
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline consumption

各受電装置が使用するワット数を指定することにより、デバイスの IEEE 分類によって指定された電力量を無効にするには、**power inline consumption** グローバルまたはインターフェイス コンフィギュレーション コマンドを使用します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

power inline consumption default *wattage*

no power inline consumption default

（注）　**default** キーワードは、グローバル コンフィギュレーション コマンドでだけ表示されます。

シンタックスの説明

wattage	スイッチがポート用に確保する電力を指定します。指定できる範囲は 4000 ～ 15400 ミリワットです。

デフォルト

Power over Ethernet（PoE）ポートのデフォルトの電力は 15400 ミリワットです。

コマンド モード

グローバル コンフィギュレーション

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol（CDP）を使用して*実際に*装置が消費する電力量を決定して、それに応じてパワー バジェットを調整します。この機能は、IEEE サードパーティの受電装置には適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じてパワー バジェットを調整します。受電装置が Class 0（クラス ステータスは不明）または Class 3 である場合、実際に必要な電力量に関係なく、スイッチは装置用に 15400 ミリワットの電力を確保します。受電装置が実際の電力消費量よりも高いクラスであるか、または電力分類（デフォルトで Class 0）をサポートしない場合、スイッチは IEEE クラス情報を使用してグローバル パワー バジェットを追跡するので、少しの装置にしか電力を供給しません。

power inline consumption *wattage* コンフィギュレーション コマンドを使用することで、IEEE 分類で指定されたデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル パワー バジェットに入れられます。したがって、スイッチのパワー バジェットを拡張してもっと効率的に使用できます。

たとえば、スイッチが各 PoE ポートで 15400 ミリワットの電力を確保した場合、Class0 の受電装置を 24 台だけしか接続できません。Class0 の装置の電力要件が実際には 5000 ミリワットである場合、消費ワット数を 5000 ミリワットに設定すると、最大 48 台の装置を接続できます。24 ポートまたは 48 ポート スイッチで利用できる PoE 総出力電力は 370,000 ミリワットです。

注意　慎重にスイッチのパワー バジェットを計画し、電源装置がオーバーサブスクライブ状態にならないようにしてください。

power inline consumption default *wattage* または **no power inline consumption default** 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か、**power inline consumption** *wattage* または **no power inline consumption** 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、次の注意メッセージが表示されます。

```
%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

（注）　手動でパワー バジェットを設定する場合、スイッチと受電装置の間のケーブルでの電力消失を考慮する必要があります。

IEEE 分類に関する詳細については、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 ガイドの「Configuring Interface Characteristics」の章を参照してください。

このコマンドは、PoE 対応ポートだけでサポートされています。PoE をサポートしていないスイッチまたはポートでこの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。

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全スイッチまたはポートでサポートされます。

例

次の例では、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、各 PoE ポートに 5000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

次の例では、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 PoE ポートに接続された受電装置に 12000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline consumption 12000
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

設定を確認するには、**show power inline consumption** 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
power inline	PoE ポート上で電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

priority-queue

ポート上で出力緊急キューをイネーブルにするには、**priority-queue** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

priority-queue out

no priority-queue out

シンタックスの説明

out	出力緊急キューをイネーブルにします。

デフォルト

出力緊急キューは、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

コマンドの履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

priority-queue out コマンドを設定する場合、Shaped Round Robin（SRR）に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** 内の *weight1* または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドが無視されることを意味します（比率計算に使用されません）。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して shared モードでサービスを提供します。

例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

次の例では、SRR のシェーピングおよび共有された重みが設定されたあと、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは、共有モードを無効にします。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

show mls qos interface *interface-id* **queueing** または **show running-config** 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mls qos interface queueing	キューイング方法（SRR、プライオリティ キューイング）、キューに相応する重み、および Class of Service（CoS）から出力キューへのマップを表示します。
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。

private-vlan

プライベート VLAN を設定して、プライベート VLAN のプライマリおよびセカンダリ VLAN 間のアソシエーションを設定するには、**private-vlan** VLAN コンフィギュレーション コマンドを使用します。通常の VLAN 設定に VLAN を戻すには、このコマンドの **no** 形式を使用します。

private-vlan {association [**add** | **remove**] *secondary-vlan-list* | **community** | **isolated** | **primary}**

no private-vlan {association | **community** | **isolated** | **primary}**

シンタックスの説明

association	プライマリ VLAN とセカンダリ VLAN とのアソシエーションを作成します。
secondary-vlan-list	プライベート VLAN 内のプライマリ VLAN に関連付ける 1 つまたは複数のセカンダリ VLAN を指定します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアします。
community	VLAN をコミュニティ VLAN として指定します。
isolated	VLAN をコミュニティ VLAN として指定します。
primary	VLAN をコミュニティ VLAN として指定します。

デフォルト

デフォルトでは、プライベート VLAN が設定されていません。

コマンド モード

VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

プライベート VLAN を設定する前に、VLAN Trunking Protocol（VTP）をディセーブル（VTP 透過モード）にする必要があります。プライベート VLAN を設定したあとで、VTP モードをクライアントまたはサーバに変更できません。

VTP は、プライベート VLAN の設定を伝播しません。レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定して、レイヤ 2 データベースを結合し、プライベート VLAN トラフィックのフラッディングを防ぐ必要があります。

プライベート VLAN には、VLAN 1 または VLAN 1002 ～ 1005 を設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に設定できます。

セカンダリ（隔離またはコミュニティ）VLAN を 1 つのプライマリ VLAN だけに**関連付ける**ことができます。プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。

- セカンダリ VLAN をプライマリ VLAN として設定できません。
- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。
- プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN に関連付けられたポートが非アクティブになります。

コミュニティ VLAN は、コミュニティ ポート間、およびコミュニティ ポートから対応するプライマリ VLAN の混合ポートにトラフィックを伝送します。

隔離 VLAN は、混合ポートと通信を行うために隔離ポートによって使用されます。同一のプライマリ VLAN ドメインで他のコミュニティ ポートまたは隔離ポートにトラフィックを伝送しません。

プライマリ VLAN は、ゲートウェイからプライベート ポートのカスタマー エンド ステーションにトラフィックを伝送する VLAN です。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

VLAN コンフィギュレーション モードを終了するまで、**private-vlan** コマンドは作用しません。

プライベート VLAN ポートを EtherChannel として設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。

プライベート VLAN を Remote Switched Port Analyzer（RSPAN）VLAN として設定しないでください。

プライベート VLAN を音声 VLAN として設定しないでください。

プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。

プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは 1 つの Spanning Tree Protocol（STP）インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

ホスト ポートおよび混合ポートの設定に関する情報については、**switchport mode private-vlan** コマンドを参照してください。

プライベート VLAN の他の機能との相互作用に関する詳細については、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、VLAN 20 をプライマリ VLAN に、VLAN 501 を隔離 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、プライベート VLAN に関連付ける方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

設定を確認するには、**show vlan private-vlan** または **show interfaces status** 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 status	所属する VLAN を含むインターフェイスのステータスを表示します。
show vlan private-vlan	スイッチ スタックで設定されたプライベート VLAN および VLAN アソシエーションを表示します。
switchport mode private-vlan	ホスト ポートまたは混合ポートとしてプライベート VLAN ポートを設定します。

private-vlan mapping

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 間でマッピングを作成して、両方の VLAN で同じプライマリ VLAN Switch Virtual Interface（SVI）を共有できるようにするには、**private-vlan mapping** 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。SVI からプライベート VLAN のマッピ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。

private-vlan mapping {[**add** | **remove**] *secondary-vlan-list*}

no private-vlan mapping

シンタックスの説明

secondary-vlan-list	プライマリ VLAN SVI にマッピングされる 1 つまたは複数のセカンダリ VLAN を指定します。
add	（任意）セカンダリ VLAN をプライマリ VLAN SVI にマッピングします。
remove	（任意）セカンダリ VLAN とプライマリ VLAN SVI 間のマッピングを削除します。

デフォルト

デフォルトでは、プライベート VLAN SVI のマッピングが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

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

プライベート VLAN を設定する場合は、スイッチが VTP 透過モードになっている必要があります。

プライマリ VLAN の SVI は、レイヤ 3 で作成されます。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。

セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN の SVI によってルーティングされます。

セカンダリ VLAN は、1 つのプライマリ SVI だけにマッピングできます。プライマリ VLAN がセカンダリ VLAN として設定されると、このコマンドで指定されたすべての SVI はダウンします。

有効なレイヤ 2 プライベート VLAN のアソシエーションがない 2 つの VLAN 間のマッピングを設定する場合、マッピングの設定は作用しません。

例

次の例では、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする方法を示します。

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

次の例では、セカンダリ VLAN 303 ～ 305、および 307 からのセカンダリ VLAN トラフィックのルーティングを VLAN 20 SVI を介して許可する方法を示します。

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

設定を確認するには、**show interfaces private-vlan mapping** 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 private-vlan mapping	VLAN SVI に対するプライベート VLAN のマッピング情報を表示します。

queue-set

キューセットに対してポートをマッピングするには、**queue-set** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

queue-set *qset-id*

no queue-set *qset-id*

シンタックスの説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。

デフォルト

キューセット ID は 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** 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
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 queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

radius-server dead-criteria

RADIUS サーバが使用不可または *デッド*状態であると考えられる場合に決定する条件を設定するには、**radius-server dead-criteria** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

no radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

シンタックスの説明

time *seconds*	（任意）RADIUS サーバからの有効な応答をスイッチが取得するのに必要としない時間（秒）を設定します。指定できる範囲は 1 ～ 120 秒です。
tries *number*	（任意）サーバが使用不可と見なされる前に RADIUS サーバから有効な応答をスイッチが取得するのに必要としない回数を指定します。指定できる範囲は 1 ～ 100 です。

デフォルト

スイッチは、10 ～ 60 秒の *seconds* 値を動的に決定します。

スイッチは、10 ～ 100 の *tries* 値を動的に決定します。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

次の *seconds* および *number* パラメータを設定することを推奨します。

- IEEE 802.1x 認証が期限切れになる前に RADIUS サーバへの応答を待機する時間（秒）を指定するには、**radius-server timeout** *seconds* 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。スイッチは、10 ～ 60 秒のデフォルトの *seconds* 値を動的に決定します。
- RADIUS サーバが使用不能と見なされる前に RADIUS サーバへの送信を試行する時間（秒）を指定するには、**radius-server retransmit** *retries* 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。スイッチは、10 ～ 100 のデフォルトの *tries* 値を動的に決定します。
- *seconds* パラメータは、IEEE 802.1x 認証が期限切れになる前に再送信を試行する秒数以下か、または同じです。
- *tries* パラメータは、再送信試行回数と同じである必要があります。

例

次の例では、RADIUS サーバが使用不可と見なされた場合に決定する条件として、**時間**に 60 を設定し、**試行**回数に 10 を設定する方法を示します。

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

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
dot1x critical (global configuration)	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 critical (interface configuration)	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、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 を設定します。
radius-server retransmit *retries*	RADIUS サーバが使用不可と見なされる前にスイッチが RADIUS サーバに送信を試行する回数を指定します。構文情報については、**『Cisco IOS Security Command Reference』Release 12.2 >「Server Security Protocols」>「RADIUS Commands」**を選択してください。
radius-server timeout *seconds*	IEEE 802.1x 認証が期限切れになる前にスイッチが RADIUS サーバへの応答を待機する時間（秒）を指定します。構文情報については、**『Cisco IOS Security Command Reference』Release 12.2 >「Server Security Protocols」>「RADIUS Commands」**を選択してください。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

radius-server host

RADIUS アカウンティングおよび RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]

no radius-server host *ip-address*

シンタックスの説明

ip-address	RADIUS サーバの IP アドレスを指定します。
acct-port *udp-port*	（任意）RADIUS アカウンティング サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
auth-port *udp-port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
test *username* *name*	（任意）RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
idle-time *time*	（任意）スイッチがテスト パケットをサーバに送信したあとの間隔（分）を設定します。指定できる範囲は 1 ～ 35791 分です。
ignore-acct-port	（任意）RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。
ignore-auth-port	（任意）RADIUS サーバ認証ポートのテストをディセーブルにします。
key *string*	（任意）スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。

デフォルト

RADIUS アカウンティング サーバの UDP ポートは 1646 です。

RADIUS 認証サーバの UDP ポートは 1645 です。

自動サーバ テストはディセーブルです。

アイドル時間は 60 分（1 時間）です。

自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。

認証鍵および暗号鍵（*string*）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

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。

RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定するには、**test username** *name* キーワードを使用します。

radius-server host *ip-address* **key** *string* または **radius-server key** {**0** *string* | **7** *string* | *string*} 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認証鍵および暗号鍵を設定できます。必ずこのコマンドの最終項目として key を設定してください。

例

次の例では、アカウンティング サーバの UDP ポートを 1500、認証サーバの UDP ポートを 1510 に設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

次の例では、アカウンティング サーバおよび認証サーバの UDP ポートを設定し、RADIUS サーバ ステータスの自動テストをイネーブルにし、使用されるユーザ名を指定し、キー ストリングを設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

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
dot1x critical (global configuration)	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 critical (interface configuration)	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、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 を設定します。
radius-server key {**0** *string* | **7** *string* | *string*}	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。構文情報については、**『Cisco IOS Security Command Reference』Release 12.2 >「Server Security Protocols」>「RADIUS Commands」**を選択してください。
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 Configuration Fundamentals Command Reference』Release 12.2 >「File Management Commands」>「Configuration File Management Commands」**を選択してください。

rcommand

Telnet セッションを開始し、クラスタ コマンド スイッチまたはスイッチ スタックからクラスタ メンバー スイッチのコマンドを実行するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **rcommand** ユーザ EXEC コマンドを使用します。セッションを終了するには、**exit** コマンドを入力します。

rcommand {*n* | **commander** | **mac-address** *hw-addr*}

シンタックスの説明

n	クラスタ メンバーを識別する番号を提供します。指定できる範囲は 0 ～ 15 です。
commander	クラスタ メンバー スイッチからクラスタ コマンド スイッチへアクセスできるようにします。
mac-address *hw-addr*	クラスタ メンバー スイッチの MAC（メディア アクセス制御）アドレス

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スイッチ スタックまたはクラスタ コマンド スイッチに限られます。

スイッチがクラスタ コマンド スイッチで、クラスタ メンバー スイッチ *n* が存在していない場合、エラー メッセージが表示されます。スイッチ番号を得るには、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。

このコマンドを使用してクラスタ コマンド スイッチ プロンプトからクラスタ メンバー スイッチにアクセスしたり、メンバー スイッチ プロンプトからクラスタ コマンド スイッチにアクセスしたりすることができます。

Catalyst 2900 XL、Catalyst 3500 XL、Catalyst 2950、Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、および Catalyst 3750 スイッチの場合、Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチ CLI（コマンドライン インターフェイス）にアクセスします。たとえば、このコマンドをクラスタ コマンド スイッチからユーザ レベルで入力した場合、メンバー スイッチはユーザ レベルでアクセスされます。このコマンドをクラスタ コマンド スイッチからイネーブル レベルで使用した場合、コマンドはイネーブル レベルでリモート デバイスにアクセスします。*権限レベル*よりも低い中間イネーブル レベルを使用した場合、クラスタ メンバー スイッチはユーザ レベルとなります。

Standard Edition ソフトウェアが稼動している Catalyst 1900 および Catalyst 2820 スイッチの場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションはメニュー コンソール（メニュー方式インターフェイス）にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 であれば、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。クラスタ コマンド スイッチの権限レベルは、Standard Edition ソフトウェアが稼動しているクラスタ メンバー スイッチに次のようにマッピングします。

- クラスタ コマンド スイッチの権限レベルが 1 ～ 14 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 1 で行われます。
- クラスタ コマンド スイッチの権限レベルが 15 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 15 で行われます。

Catalyst 1900 および Catalyst 2820 の CLI が利用できるのは、スイッチで Enterprise Edition ソフトウェアが稼動している場合に限られます。

クラスタ コマンド スイッチの vty ラインにアクセス クラス コンフィギュレーションがある場合、このコマンドは機能しません。

クラスタ メンバー スイッチはクラスタ コマンド スイッチのパスワードを継承するため、クラスタ メンバー スイッチがクラスタに加入してもパスワードを要求するプロンプトは表示されません。

例

次の例では、メンバー 3 でセッションを開始する方法を示します。**exit** コマンドを入力するか、あるいはセッションを閉じるまで、このコマンドに続くすべてのコマンドは、メンバー 3 へ向けられます。

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

関連コマンド

コマンド	説明
show cluster members	クラスタ メンバーに関する情報を表示します。

reload

スタック メンバーをリロードし、設定の変更を有効にするには、**reload** 特権 EXEC コマンドを使用します。

reload [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]

シンタックスの説明

LINE	リロードする理由を指定します。
at	リロードを実行する時間（hh:mm）を指定します。
cancel	中断しているリロードをキャンセルします。
in	リロードを実行する時間間隔（mmm または hhh:mm）を指定します。
slot *stack-member-number*	指定のスタック メンバー上で変更を保存し、再起動します。
standby-cpu	スタンバイ Route Processor（RP; ルート プロセッサ）をリロードします。

デフォルト

スタック メンバーをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチ スタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
Switch(config)# reload
System configuration has been modified.Save?[yes/no]: y
Proceed to reload the whole Stack?[confirm] y
```

次の例では、特定のスタック メンバーをリロードする方法を示します。

```
Switch(config)# reload slot 6
Proceed with reload?[confirm]y
```

次の例では、単一スイッチのスイッチ スタック（メンバー スイッチが 1 つだけ）をリロードする方法を示します。

```
Switch(config)# reload slot 3
System configuration has been modified.Save?[yes/no]: y
Proceed to reload the whole Stack?[confirm] y
```

関連コマンド

コマンド	説明
rcommand	特定のスタック メンバーにアクセスします。
switch	スタック メンバーのプライオリティ値を変更します。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

remote command

すべてのまたは指定のスタック メンバーをモニタするには、**remote command** 特権 EXEC コマンドを使用します。

remote command {**all** | *stack-member-number*} *LINE*

シンタックスの説明

all	すべてのスタック メンバーに適用します。
stack-member-number	スタック メンバーを指定します。指定できる範囲は 1 ～ 9 です。
LINE	実行するコマンドを指定します。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ストリングを実行する LINE コマンドで使用するコマンド（**debug**、**show**、または **clear** など）は、指定のスタック メンバーまたはスイッチ スタックに適用されます。

例

次の例では、スイッチ スタックで **undebug** コマンドを実行する方法を示します。

```
Switch(config)# remote command all undebug all
Switch :1 :
------------
All possible debugging has been turned off
Switch :5 :
------------
All possible debugging has been turned off
Switch :9 :
------------
All possible debugging has been turned off
```

次の例では、スタック メンバー 5 で **debug udld event** コマンドを実行する方法を示します。

```
Switch(config)# remote command 5 undebug all
Switch :5 :
------------
UDLD events debugging is on
```

関連コマンド

コマンド	説明
reload	特定のスタック メンバーにアクセスします。
switch	スタック メンバーのプライオリティ値を変更します。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

remote-span

VLAN を Remote Switched Port Analyzer（RSPAN）VLAN として設定するには、**remote-span** VLAN コンフィギュレーション コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span

no remote-span

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション（config-VLAN）

コマンドの履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

RSPAN VLAN を設定できるのは config-VLAN モードの場合だけです（このモードは、**vlan** グローバル コンフィギュレーション コマンドで開始します）。**vlan database** 特権 EXEC コマンドを使用して開始された VLAN コンフィギュレーション モードでは設定できません。

VLAN Trunking Protocol（VTP）がイネーブルで、VLAN ID が 1005 未満の場合は、RSPAN 機能は VTP によって伝達されます。RSPAN VLAN ID が拡張範囲内の場合は、手動で中間スイッチを設定する必要があります（送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定）。

RSPAN **remote-span** コマンドを設定する前に、**vlan**（グローバル コンフィギュレーション）コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックだけが流れます。
- Spanning-Tree Protocol（STP）は RSPAN VLAN 内では稼動できますが、RSPAN 宛先ポートでは稼動しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

例

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

show vlan remote-span ユーザ EXEC コマンドを入力すると、設定を確認することができます。

関連コマンド

コマンド	説明
monitor session	ポートで Switched Port Analyzer（SPAN）および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。
vlan (global configuration)	VLAN 1 ～ 4094 を設定できる config-vlan モードに変更します。

renew ip dhcp snooping database

Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

renew ip dhcp snooping database [{**flash**[*number*]*:/filename* | **ftp:***//user:password@host/filename* | **nvram:***/filename* | **rcp:***//user@host/filename* | **tftp:***//host/filename*}] [**validation none**]

シンタックスの説明

flash[*number*]**:**/*filename*	（任意）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。スタック マスターのスタック メンバー番号を指定するには、*number* パラメータを使用します。*number* に指定できる範囲は 1 ～ 9 です。
ftp://*user*:*password*@*host*/*filename*	（任意）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（ファイル転送プロトコル）サーバにあることを指定します。
nvram:/*filename*	（任意）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 NVRAM（不揮発性 RAM）にあることを指定します。
rcp://*user*@*host*/*filename*	（任意）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 Remote Control Protocol（RCP）サーバにあることを指定します。
tftp://*host*/*filename*	（任意）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（簡易ファイル転送プロトコル）サーバにあることを指定します。
validation none	（任意）URL によって指定されたバインディング ファイルのエントリに対して、Cyclic Redundancy Check（CRC; 巡回冗長検査）を検証しないようにスイッチに指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

URL を指定しない場合は、スイッチは設定された URL からファイルを読み込もうとします。

例

次の例では、ファイル内の CRC 値のチェックを省略して、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

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。

reserved-only

Dynamic Host Configuration Protocol（DHCP）アドレス プールに予約済みのアドレスだけ割り当てるには、**reserved-only** DHCP プール コンフィギュレーション モード コマンドを使用します。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。

reserved-only

no reserved-only

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、プール アドレスは制限されません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

reserved-only コマンドを入力すると、DHCP プールから事前設定された予約への割り当てが制限されます。ネットワークまたはプール上の範囲の一部である予約されていないアドレスがクライアントには提供されず、他のクライアントはプールによるサービスを受けられません。

このコマンドの入力により、ユーザは、共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視する DHCP プールを持つスイッチのグループを設定できます。

DHCP プール コンフィギュレーション モードにアクセスするには、**ip dhcp pool** *name* グローバル コンフィギュレーション コマンドを入力します。

例

次の例では、予約済みのアドレスだけを割り当てるように DHCP プールを設定する方法を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

設定を確認するには、**show ip dhcp pool** 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 dhcp pool	DHCP アドレス プールを表示します。

reserved-only