Catalyst 2960 スイッチ Cisco IOS コマンド

aaa accounting dot1x

Authentication, Authorization, and Accounting（AAA; 認証、許可、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、回線単位またはインターフェイス単位で 802.1x セッションの特定のアカウンティング方式を定義する方式リストを作成するには **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場合は、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {*name* | **default**} **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **...**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...]}

no aaa accounting dot1x {*name* | **default**}

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードのあとに入力する場合のオプションです。
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	プロセスの最初にアカウンティング開始通知を送信し、プロセスの終了時にアカウンティング終了通知を送信します。アカウンティング開始レコードは、バックグラウンドで送信されます。アカウンティング開始通知がアカウンティング サーバで受信されたかどうかにかかわらず、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。最初のサーバが使用不可の場合、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 **group** キーワードは、**broadcast group** および **group** キーワードのあとに入力する場合のオプションです。複数のオプション **group** 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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

次に、IEEE 802.1x アカウンティングを設定する例を示します。

```
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に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 つまたは複数の AAA を指定します。
aaa new-model	AAA アクセス制御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	定期的再認証をイネーブルまたはディセーブルにします。
dot1x timeout reauth-period	再認証の間隔（秒）を指定します。

aaa authentication dot1x

IEEE 802.1x に準拠したポートで使用する Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）方式を指定するには、**aaa authentication 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場合は、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**}

構文の説明

default	この引数に続ける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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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場合は、**show running-config** イネーブル 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行します。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** イネーブル 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 アクセス制御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。

archive download-sw

新しいイメージを TFTP サーバから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するには、**archive download-sw** イネーブル EXEC コマンドを使用します。

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

構文の説明

/force-reload	ソフトウェア イメージのダウンロードが成功したあと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あと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あとに、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。
/overwrite	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	設定が変更され、それが保存されていないという場合に限り、イメージのダウンロードに成功したあと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前には、新しいソフトウェア イメージ用の領域を作るための現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。

source-url	ローカルまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP（ファイル転送プロトコル）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** • Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）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

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

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 イメージを指定するよう変更されます。

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 形式で提供されます。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

/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** オプションを使用すると、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を失敗させるようにできます。ソフトウェアをそのまま残し、メモリ領域の制約によって新しいイメージがフラッシュ メモリにうまく収まらない場合は、結果として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を上書きしなかった場合、**delete** イネーブル 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。詳細は、「delete」（p.2-56）を参照してください。

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

/overwrite オプションなしでこのコマンドを指定すると、ダウンロード アルゴリズムは、新しいイメージがスイッチ フラッシュ デバイスのイメージと同じではないことを確認します。イメージが同じである場合には、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あとで、**reload** イネーブル 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、**archive download-sw** コマンドの **/reload** オプションまたは **/force-reload** オプションを指定してください。

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あとで古いソフトウェア バージョンを保存する方法を示します。

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

関連コマンド

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

archive tar

tar ファイルの作成、tar ファイルのファイル一覧表示、または tar ファイルからのファイルの抽出を実行するには、**archive tar** イネーブル EXEC コマンドを使用します。

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

構文の説明

/create *destination-url* **flash:**/*file-url*	ローカルまたはネットワーク ファイル システムに新しい tar ファイルを作成します。 *destination-url* には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスおよび作成する tar ファイルの名前を指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 **flash:** • FTP の構文 **ftp:**[[//*username*[**:***password*]@*location*]/*directory*]/*tar-filename***.tar** • HTTP サーバの構文 **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア 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で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、抽出が行われる 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。*dir/file...* オプションを使用して、tar ファイル内から抽出す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　設定なし

コマンド モード　イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 メモリに存在する *c2960-lanbase-tar.12-25.FX* 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:c2960-lanbase-tar.12-25.FX.tar
info (219 bytes)

c2960-lanbase-mz.12-25.FX/(directory)
c2960-lanbase-mz.12-25.FX (610856 bytes)
c2960-lanbase-mz.12-25.FX/info (219 bytes)
info.ver (219 bytes)
```

この例では、*c2960-lanbase-12-25.FX/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:c2960-lanbase-12-25.FX.tar c2960-lanbase-12-25/html
c2960-lanbase-mz.12-25.FX/html/(directory)
c2960-lanbase-mz.12-25.FX/html/const.htm (556 bytes)
c2960-lanbase-mz.12-25.FX/html/xhome.htm (9373 bytes)
c2960-lanbase-mz.12-25.FX/html/menu.css (1654 bytes)
<output truncated>
```

この例では、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。このコマンドは、*new-configs* ディレクトリだけを、ローカル フラッシュ ファイル システムのルート（root）ディレクトリへ抽出します。*saved.tar* ファイル内の残りのファイルは無視されます。

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

関連コマンド

コマンド	説明
archive download-sw	新しいイメージを TFTP サーバからスイッチに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

既存のスイッチ イメージをサーバにアップロードするには、**archive upload-sw** イネーブル EXEC コマンドを使用します。

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

構文の説明

/version *version_string*	（任意）アップロードするイメージの指定バージョン文字列を指定します。
destination-url	ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスです。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文 : **flash:** • FTP（ファイル転送プロトコル）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** • Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）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

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

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、172.20.140.2 の TFTP サーバへ現在稼働中のイメージをアップロードする方法を示します。

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

関連コマンド

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

auto qos voip

Quality of Service（QoS; サービス品質）ドメイン内で Voice over IP（VoIP）の QoS を自動的に設定するには、**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。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**]

構文の説明

cisco-phone	このポートが Cisco IP Phone に接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。
cisco-softphone	このポートが Cisco SoftPhone が動作している装置に接続されていると判断し、自動的に VoIP の QoS を設定します。
trust	このポートが信頼され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。

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] CoS	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 Services Code Point
4. CoS = Class of Service（サービス クラス）

表 2-2 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 2-2　出力キューに対する 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	10%	16%	10%
SRR 共有	2	3、6、7	10%	6%	10%
SRR 共有	3	2、4	60%	17%	26%
SRR 共有	4	0、1	20%	61%	54%

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、スイッチのルーテッド ポートに接続された Cisco IP Phone を使用する VoIP、および Cisco SoftPhone アプリケーションが稼働するデバイスを使用する VoIP 用に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) 以降のみをサポートします。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。

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*あと*に、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かのように、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 コンフィギュレーションでは、生成されたコマンドの適用が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、現在のコンフィギュレーション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 をイネーブル化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、スイッチは信頼される境界の機能をイネーブルにします。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかまたは存在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。Cisco IP Phone が存在しない場合、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。
- 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。
- ネットワーク内部へ接続するポートで **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチは入力パケット内の非ルーテッド ポートの CoS 値を信頼します（これは、トラフィックがすでに他のエッジ装置によって分類されていることが前提です）。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（仮想 LAN）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 が動作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 アプリケーションのみをサポートします。

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た QoS 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ギングをイネーブルにします。**debug auto qos** イネーブル 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 をイネーブル化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 はディセーブルとみなされます

（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 QoS、DSCP、および IP precedence 値は変更されない）ため、信頼されるポートまたは信頼されないポートといった概念はありません。トラフィックはパススルー モードでスイッチングされます（パケットは、書き直されずにスイッチングされ、ポリシングされずにベストエフォートとして分類されます）。

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され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 gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

show auto qos interface *interface-id* イネーブル 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
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、または CoS 値をキューとスレッシュホールド 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、または DSCP 値をキューとスレッシュホールド 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、またはキューとスレッシュホールド 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、またはキューとスレッシュホールド 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	キューセットに対するポートをマッピングします。
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出力キュー 4 つで帯域幅をシェーピングします。
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出力キュー 4 つで帯域幅を共有します。

boot boothlpr

特別な Cisco IOS イメージをロードするには、**boot boothlpr** 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。メモリにロードすると、次の Cisco IOS イメージをメモリにロードして開始することができます。この変数が使用されるのは、内部開発およびテスト時だけです。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。

boot boothlpr *filesystem*:*/file-url*

no boot boothlpr

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	起動可能なヘルパー イメージのパス（ディレクトリ）および名前です。

デフォルト

ヘルパー イメージはロードされません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、BOOTHLPR 環境変数の設定を変更します。詳細は、付録 A「Catalyst 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート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、**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

構文の説明

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

デフォルト

デフォルトのコンフィギュレーション ファイルは、flash:config.text です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート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、**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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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あとで Break キーを押して、自動ブート プロセスを中断することができます。

（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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート環境変数の設定を表示します。

boot helper

ブート ローダ初期化中に動的にファイルをロードして、ブート ローダの機能を拡張またはパッチするには、**boot helper** グローバル コンフィギュレーション コマンドを使用します。このコマンドを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。

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

no boot helper

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	ローダ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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

この変数が使用されるのは、内部開発およびテスト時だけです。

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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート環境変数の設定を表示します。

boot helper-config-file

Cisco IOS ヘルパー イメージ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するには、**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場合は、このコマンドの **no** 形式を使用します。

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

no boot helper-config file

構文の説明

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

デフォルト

ヘルパー コンフィギュレーション ファイルは指定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

この変数が使用されるのは、内部開発およびテスト時だけです。

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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート環境変数の設定を表示します。

boot manual

次のブート サイクル中に手動スイッチ起動をイネーブルにするには、**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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

手動起動はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

次回システムを再起動すると、スイッチはブート ローダ モードで起動します。これは *switch:* プロンプトによってわかります。システムをブートするには、**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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート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、**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

構文の説明

filename	プライベート コンフィギュレーション ファイルの名前です。

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、*private-config* です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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	ブート環境変数の設定を表示します。

boot system

次のブート サイクル中にロードする Cisco IOS イメージを指定するには、**boot system** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no boot system

構文の説明

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

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な縦型検索を行って、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

archive download-sw イネーブル 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 2960 スイッチ ブート ローダ コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	ブート環境変数の設定を表示します。

channel-group

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

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

no channel-group

PAgP 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**

構文の説明

channel-group-number	チャネル グループ番号を指定します。指定できる範囲は 1 ～ 6 です。
mode	EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol（LACP）をイネーブルにします。 active モードは、ポートをネゴシエーション ステートにします。この場合、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は、デフォルトでサイレント動作となります。
desirable	PAgP を無条件で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 **auto** または **desirable** キーワードとともに PAgP モードで使用します。
on	**on** モードをイネーブルにします。 **on** モードでは、接続している両方のポート グループが **on** モードの場合にのみ、使用可能な EtherChannel が存在します。
passive	PAgP 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、ポートは受信する 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られません。

モードは設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 コマンドを使用します。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* と同じ番号を使用することもできれば、新しい番号を使用することもできます。新しい番号を使用すると、**channel-group** コマンドが動的に新しいポート チャネルを作成します。

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、その設定を適用しているポートだけに影響します。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みなされます。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。この場合は、物理ポートで PAgP を稼働して、ポートが動作可能にならないようにします。ただし、PAgP によって、ポートは動作可能となり、そのポートをチャネル グループへ接続したり、伝送用として使用したりすることができます。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 モードの場合、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 モードを使用する場合は、注意して使用してください。これは手動設定であり、EtherChannel の両端のポートは同一の設定である必要があります。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP と LACP が稼働している EtherChannel は、同じスイッチに共存できます。個々の EtherChannel グループは PAgP または LACP のどちらかを稼働できますが、それらを相互に稼働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 メンバーを 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 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。

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。

設定時の注意事項の完全なリストは、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 EtherChannels」の章を参照してください。

例

次の例では、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 gigabitethernet0/1 -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、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 gigabitethernet0/1 -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
```

設定を確認するには、**show running-config** イネーブル 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

ポートで使用されるプロトコルを制限して、チャネル化を管理するには、**channel-protocol** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no channel-protocol

構文の説明

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

デフォルト

プロトコルは EtherChannel に割り当てられていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

LACP または PAgP に制限する場合にだけ、**channel-protocol** コマンドを使用してください。**channel-protocol** 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。

EtherChannel パラメータを設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**channel-group** コマンドを使用して、EtherChannel のモードを設定することもできます。

EtherChannel グループで PAgP と LACP の両方のモードをイネーブルにすることはできません。

PAgP と LACP は非互換です。チャネルの両側で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
```

show etherchannel [*channel-group-number*] **protocol** イネーブル 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
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。

class

特定のクラスマップ名のトラフィック分類の一致基準を（**police**、**set**、および **trust** ポリシーマップ クラス コンフィギュレーション コマンドを使用して）定義するには、**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*

構文の説明

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 マップは定義されません。

コマンド モード

ポリシーマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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に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。イネーブル 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 Services Code Point（DSCP）を 10 に設定し、平均レート 1 Mbps、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** イネーブル 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比較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	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
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; サービス品質）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マッチングを行うためのクラス 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 モードに戻る場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

match-all	（任意）このクラス マップ内のすべての一致ステートメントの論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
match-any	（任意）このクラス マップ内の一致ステートメントの論理和をとります。1 つまたは複数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 マップは定義されません。

match-all または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

クラス マップ一致基準を作成または変更したい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。

ポートごとに適用されるグローバルに名付けられたサービス 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; サービス品質）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** イネーブル 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（クラスマップ コンフィギュレーション）** コマンドを参照してください。
- **no**：クラス マップから一致ステートメントを削除します。
- **rename**：現在のクラス マップの名前を変更します。クラス マップ名をすでに使用されている名前に変更すると、`A class-map with this name already exists` 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 つずつのみ **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; アクセス制御リスト）は 1 つだけです。ACL には複数の Access Control Entry（ACE; アクセス制御エントリ）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 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 イネーブル 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
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシーマップ クラス コンフィギュレーション コマンドによる）を定義します。
match（クラスマップ コンフィギュレーション）	トラフィックを分類するための一致条件を定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
show class-map	QoS クラス マップを表示します。

clear ip dhcp snooping database

DHCP バインディング データベース エージェント統計情報をクリアするには、**clear ip dhcp snooping database** イネーブル EXEC コマンドを使用します。

clear ip dhcp snooping database statistics

構文の説明

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

clear ip dhcp snooping database statistics コマンドを入力すると、統計情報がクリアされるまで、スイッチはバインディング データベース内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 エージェント統計情報をクリアする方法を示します。

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

show ip dhcp snooping database イネーブル EXEC コマンドを入力すると、統計情報がクリアされたことを確認できます。

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。

clear lacp

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

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

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 6 です。
counters	トラフィック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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

clear lacp counters コマンドを使用すると、すべてのカウンタをクリアできます。また、**clear lacp** *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 lacp counters
```

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

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

show lacp counters または **show lacp 4 counters** イネーブル EXEC コマンドを入力すると、情報が削除されたかどうか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 lacp	LACP チャネル グループ情報を表示します。

clear mac address-table

MAC（メディア アクセス制御）アドレス テーブルから特定のダイナミック アドレス、特定のインターフェイスのすべてのダイナミック アドレス、または特定の VLAN（仮想 LAN）のすべてのダイナミック アドレスを削除するには、**clear mac address-table** イネーブル EXEC コマンドを使用します。このコマンドは、MAC アドレス通知グローバル カウンタもクリアします。

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

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

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

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

show mac address-table イネーブル EXEC コマンドを入力すると、情報が削除されたかどうかを確認することができます。

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 address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification	特定のインターフェイスの 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 テーブル移動更新関連カウンタをクリアするには、**clear mac address-table move update** イネーブル EXEC コマンドを使用します。

clear mac address-table move update

構文の説明

このコマンドには、引数またはキーワードはありません。

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

イネーブル EXEC

コマンド履歴

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 テーブル移動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 イネーブル EXEC コマンドを入力すると、情報がクリアされたかどうかを確認することができます。

関連コマンド

コマンド	説明
mac address-table move update {**receive** | **transmit**}	スイッチの MAC アドレス テーブル移動更新を設定します。
show mac address-table move update	スイッチの MAC アドレス テーブル移動更新情報を表示します。

clear pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）チャネル グループ情報をクリアするには、**clear pagp** イネーブル EXEC コマンドを使用します。

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

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 6 です。
counters	トラフィック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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

clear pagp counters コマンドを使用すると、すべてのカウンタをクリアできます。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 カウンタをクリアする方法を示します。

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

show pagp イネーブル EXEC コマンドを入力すると、情報が削除されたかどうか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 pagp	PAgP チャネル グループ情報を表示します。

clear port-security

MAC（メディア アクセス制御）アドレス テーブルからスイッチ上またはインターフェイス上のすべてのセキュア アドレスまたは特定のタイプ（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** イネーブル 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**}}]]

構文の説明

all	すべてのセキュア MAC アドレスを削除します。
configured	設定済みセキュア MAC アドレスを削除します。
dynamic	ハードウェアによって自動学習されたセキュア MAC アドレスを削除します。
sticky	自動学習または設定されたセキュア 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（仮想 LAN）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、以下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 でない場合のみ利用可能です。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	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 gigabitethernet0/1
```

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 イネーブル EXEC コマンドを入力すると、情報が削除されたかどうかを確認することができます。

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** イネーブル EXEC コマンドを使用します。

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

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニングツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN（仮想 LAN）、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 チャネルは 1 ～ 6 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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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（強制的に近接スイッチと再度ネゴシエートさせる）するには、**clear spanning-tree detected-protocols** イネーブル EXEC コマンドを使用します。

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

構文の説明

interface *interface-id*	（任意）指定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（仮想 LAN）、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 チャネルは 1 ～ 6 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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルまたは Multiple Spanning-Tree Protocol（MSTP）が稼働するスイッチは、組み込み済みのプロトコル移行メカニズムをサポートしています。それによって、スイッチはレガシー IEEE 802.1D スイッチと相互に動作できるようになります。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）スイッチは、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）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 gigabitethernet0/1
```

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）クライアントによって保持される統計情報をクリアするには、**clear vmps statistics** イネーブル EXEC コマンドを使用します。

clear vmps statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	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 メンバーシップ 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
```

show vmps statistics イネーブル EXEC コマンドを入力すると、情報が削除されたかどうか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 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; VLAN トランキング プロトコル）およびプルーニング カウンタをクリアするには、**clear vtp counters** イネーブル EXEC コマンドを使用します。

clear vtp counters

構文の説明

このコマンドには、引数またはキーワードはありません。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	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
```

show vtp counters イネーブル EXEC コマンドを入力すると、情報が削除されたかどうか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 vtp	VTP 管理ドメイン、ステータス、およびカウンタの一般情報を表示します。

cluster commander-address

このコマンドの入力は不要です。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（メディア アクセス制御）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メンバー 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** 形式を入力します。

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

no cluster commander-address

構文の説明

mac-address	クラスタ コマンド スイッチの MAC アドレスです。
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）です。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチでのみ使用できます。

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することができます。通常、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入力します。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のみクラスタ 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

次の例は、クラスタ メンバーの実行コンフィギュレーションの出力の一部です。

```
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
```

show cluster イネーブル 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
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 discovery hop-count

コマンド スイッチから候補スイッチの拡張検出を行うためのホップ カウント制限を設定するには、**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

構文の説明

number	クラスタ コマンド スイッチが候補の検出を制限するクラスタ エッジからのホップ数。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 に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチに対してのみ使用できます。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 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ポイントです。

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 スイッチで実行します。

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

show cluster イネーブル 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
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

コマンド対応スイッチで使用され、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、**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場合は、このコマンドの **no** 形式を使用します。

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

no cluster enable

構文の説明

name	クラスタ名（最大 31 文字）です。指定できる文字は、英数字、ダッシュ、および下線です。
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。

これがクラスタ 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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
```

クラスタ コマンド スイッチで **show cluster** イネーブル 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
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 スイッチまたはクラスタ メンバー スイッチ）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、**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

構文の説明

holdtime-in-secs	スイッチ（コマンド スイッチまたはクラスタ 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タイムは 80 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチでのみ **cluster timer** グローバル コンフィギュレーション コマンドとともに使用します。設定がクラスタ内のすべてのスイッチ間で一貫性を持つように、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（**クラスタ タイマー**）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、（ホールド時間 / 間隔）（いずれも単位は秒）回のハートビート メッセージの数が連続して抜けています。

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 タイマーおよび期間を変更する方法を示します。

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

show cluster イネーブル 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
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 コマンド スイッチから候補をクラスタに追加するには、**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場合は、このコマンドの **no** 形式を使用します。

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

no cluster member *n*

構文の説明

n	クラスタ メンバーを識別する番号です。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）です。
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（仮想 LAN）ID です。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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 スイッチでのみ入力することができます。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
```

クラスタ コマンド スイッチで **show cluster members** イネーブル 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
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

メンバーが IP アドレスなしでクラスタ外部の装置と通信できるように、クラスタ 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するには、**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

構文の説明

interface-id	外部インターフェイスとして機能するインターフェイスです。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（仮想 LAN）があります。ポート チャネル範囲は 1 ～ 6 です。指定できる VLAN 範囲は 1 ～ 4094 です。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドが入力できるのは、クラスタ コマンド スイッチだけです。クラスタ メンバー スイッチ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。

例

次の例では、VLAN 1 への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** イネーブル 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのスイッチでクラスタリングがイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

クラスタ コマンド スイッチで **no cluster run** コマンドを入力すると、そのクラスタ 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はできません。

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、このクラスタ 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はできません。

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はできません。

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
```

show cluster イネーブル 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
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）スタンバイ グループへクラスタをバインドすることにより、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と、同じ HSRP グループを使用して、クラスタ コマンド スイッチ冗長とルーティング冗長を確立できます。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。

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

no cluster standby-group

構文の説明

HSRP-group-name	クラスタにバインドされる HSRP グループの名前です。グループ名は 32 文字までです。
routing-redundancy	（任意）同じ HSRP スタンバイ グループを使用して、クラスタ コマンド スイッチ冗長とルーティング冗長を確立できます。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドが入力できるのは、クラスタ コマンド スイッチだけです。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。

このクラスタ 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。そうでないとコマンドを入力したときにエラーが発生します。

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してください。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った名前を使用することができます）。

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 スイッチ上だけで実行します。

```
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 スイッチで実行され、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
```

show cluster イネーブル 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。出力は、クラスタ内の冗長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、**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

構文の説明

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

デフォルト

間隔は 8 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチでのみ **cluster holdtime** グローバル コンフィギュレーション コマンドとともに使用します。設定がクラスタ内のすべてのスイッチ間で一貫性を持つように、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（**クラスタ タイマー**）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、（ホールド時間 / 間隔）（いずれも単位は秒）回のハートビート メッセージの数が連続して抜けています。

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 インターバル 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
```

show cluster イネーブル 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
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場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

macro-name	インターフェイス範囲マクロの名前（最大 32 文字）です。
interface-range	インターフェイス範囲です。インターフェイス範囲の有効値については、「使用上の注意事項」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がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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（仮想 LAN）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 0/1 - 2** ならば範囲は指定されますが、**gigabitethernet 0/1-2** では指定されません。

type および *interface* の有効値は次のとおりです。

- **vlan** *vlan-id*、ここで、VLAN ID は 1 ～ 4094 です。

（注）　コマンドライン インターフェイスには複数の VLAN ID を設定するオプションがありますが、これはサポートされていません。

VLAN インターフェイスは、**interface vlan** コマンドで設定してください（**show running-config** イネーブル 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-ranges* では使用できません。

- **port-channel** *port-channel-number*、ここで、*port-channel-number* は 1 ～ 6 です。
- **fastethernet** module/{*first port*} - {*last port*}

- **gigabitethernet** module/{*first port*} - {*last port*}

物理インターフェイスの場合は、次のとおりです。

- モジュールは常に 0 です。
- 範囲は、*type* **0**/*number* - *number* です（たとえば、**gigabitethernet 0/1 - 2**）。

範囲を定義するときは、ハイフン（-）の前後に間にスペースが必要です。例：

gigabitethernet0/1 - 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、最初のエントリとカンマ（,）の間にスペースが必要です。カンマの後ろのスペースは任意です。例：

fastethernet0/3, gigabitethernet0/1 – 2

fastethernet0/3 –4, gigabitethernet0/1 – 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 fastethernet0/1 - 2, gigabitethernet0/1
- 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで同時にコマンドを実行します。
show running-config	定義されたマクロを含む現在稼働中の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。

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するには、**delete** イネーブル EXEC コマンドを使用します。

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

構文の説明

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

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

/force キーワードを使用すると、削除プロセスの最初に 1 回だけ削除の確認を要求するプロンプトが表示されます。

/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、新しいイメージが正常にダウンロードされたあとに、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***:** イネーブル EXEC コマンドを入力すると、ディレクトリが削除されたかどうかを確認することができます。

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へダウンロードし、既存のイメージを上書きまたは保持します。

deny（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非 IP トラフィックが転送されるのを防ぐには、**deny** 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。拒否条件を名前付き MAC アクセス リスト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。

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

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

構文の説明

any	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 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 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、ハードウェアでのみ実行可能です。**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）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ていますが、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 フィルタリング条件

IPX カプセル化タイプ		
Cisco IOS 名	**Novel 名**	**フィルタ条件**
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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

mac access-list extended グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

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

Access Control Entry（ACE; アクセス制御エントリ）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。すなわち、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
```

show access-lists イネーブル 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
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit（MAC アクセス リスト コンフィギュレーション）	条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定された ACL を表示します。

dot1x

IEEE 802.1x 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 {**system-auth-control**} | {**guest-vlan supplicant**}

no dot1x {**system-auth-control**} | {**guest-vlan supplicant**}

構文の説明

system-auth-control	スイッチで IEEE 802.1x をグローバルにイネーブルにします。
guest-vlan supplicant	スイッチでオプションのゲスト VLAN（仮想 LAN）の動作をグローバルにイネーブルにします。

デフォルト

IEEE 802.1x がディセーブルで、オプションのゲスト VLAN の動作もディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

IEEE 802.1x をグローバルにイネーブルにする前に、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザの認証に使用されるシーケンスと認証方式を記述したものです。

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

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

guest-vlan supplicant キーワードを使用して、スイッチでオプションの IEEE 802.1x ゲスト VLAN の動作をイネーブルにすることができます。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、スイッチの IEEE 802.1x 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、スイッチの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
```

show dot1x [**interface** *interface-id*] イネーブル 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
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	ポートの許可ステートの手動制御をイネーブルにします。
show dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x auth-fail max-attempts

許容可能な最大回数の認証試行のあとにポートが制限付き VLAN に移動されるように設定するには、**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

構文の説明

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

デフォルト

デフォルト値は 3 回の試行です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

VLAN によって許容される最大認証試行回数を再設定する場合には、変更は再認証タイマーが時間切れになったあとに有効になります。

例

次の例では、ポートがポート 3 の制限付き VLAN に移動されるまでに許容される最大認証試行回数を *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 gigabitethernet0/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

show dot1x [**interface** *interface-id*] イネーブル 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
dot1x auth-fail vlan [*vlan id*]	オプションの制限付き VLAN 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高回数を指定します。
show dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x auth-fail vlan

ポートに対して制限付き 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 *vlan-id*

構文の説明

vlan-id	1 ～ 4094 の範囲で VLAN を指定します。

デフォルト

制限付き VLAN は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

制限付き VLAN は、次のように設定されたポートに対して設定できます。

- シングルホスト（デフォルト）モード
- 許可が自動モード

再認証をイネーブルにする必要があります。制限付き VLAN 内のポートは、再認証がディセーブルにされている場合には、再認証要求を受信しません。再認証プロセスを開始するには、制限付き VLAN はリンクダウン イベントまたは Extensible Authentication Protocol（EAP）ログオフ イベントをポートから受信する必要があります。ホストがハブ経由で接続されている場合には、ホストが切断されてもポートはリンクダウン イベントを受信せず、その結果として次の再認証試行が行われるまで、新規ホストを検出できません。

サプリカントが認証に失敗すると、ポートは制限付き VLAN に移動され、EAP *success* メッセージがサプリカントに送信されます。サプリカントは実際の認証失敗を通知されないため、この制限付きネットワーク アクセスについて混乱する場合があります。EAP success メッセージは次の理由で送信されます。

- EAP success メッセージが送信されない場合には、サプリカントは 60 秒ごとに EAP-start メッセージを送信して認証を試行します。
- 一部のホスト（Windows XP を実行しているデバイスなど）は、EAP success メッセージを受信するまで DHCP を実装できません。

サプリカントはオーセンティケータから EAP success メッセージを受信した後に、不正なユーザ名とパスワードをキャッシュし、その情報を再認証のたびに再利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、ポートは制限付き VLAN に留まります。

レイヤ 3 ポートに使用される内部 VLAN は、制限付き VLAN として設定できません。

VLAN を制限付き VLAN と音声 VLAN の両方に設定することはできません。これを行うと、syslog メッセージが生成されます。

制限付き VLAN ポートが無許可ステートに移行すると、認証プロセスが再開されます。サプリカントが再度認証プロセスに失敗すると、オーセンティケータは保留ステートで待機します。サプリカントが正しく再認証を行うと、すべての IEEE 802.1x ポートは再初期化され、通常の IEEE 802.1x ポートとして扱われます。

制限付き VLAN を別の VLAN として再設定すると、制限付き VLAN 内のすべてのポートも移行され、各ポートは現在の許可ステートに留まります。

制限付き VLAN をシャットダウンするかまたは VLAN データベースから削除すると、制限付き VLAN 内のすべてのポートはただちに無許可ステートに移行し、認証プロセスが再開されます。制限付き VLAN 設定がまだ存在するため、オーセンティケータは保留ステートで待機しません。制限付き VLAN が非アクティブの間もすべての認証試行はカウントされるため、制限付き VLAN がアクティブになると、ポートはただちに制限付き VLAN に置かれます。

制限付き VLAN はシングルホスト モード（デフォルト ポート モード）でのみサポートされます。そのため、ポートが制限付き VLAN に置かれた場合には、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、ポートに現れたその他の 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。

例

次の例では、ポート 1 に制限付き VLAN を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch(config)# end
Switch#
```

show dot1x [**interface** *interface-id*] イネーブル 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
dot1x auth-fail max-attempts [*max-attempts*]	ユーザを制限付き VLAN に割り当てるまでに許容される認証試行の回数を設定します。
show dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x control-direction

ポート制御を単方向制御または双方向制御に切り替えるには、**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 {**in** | **both**}

no dot1x control-direction {**in** | **both**}

構文の説明

in	ポートの単方向制御をイネーブルにします。
both	ポートの双方向制御をイネーブルにします。

デフォルト

ポートは双方向モードに設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

キーワード **both** の使用と、このコマンドの **no** 形式の使用は同一コマンドとなります。

キーワード **both** と、このコマンドの **no** 形式は、ポートをデフォルト設定の双方向に変更します。

例

次の例では、単方向制御をイネーブルにする方法を示します。

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

次の例では、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
Switch(config-if)# no dot1x control-direction
```

show dot1x all イネーブル 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。

show dot1x all イネーブル EXEC コマンド出力は、ポート名とポートの状態を除き、すべてのスイッチで同一です。ポートにホストが接続されていてまだ認証されていない場合には、次のように表示されます。

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

単方向制御をイネーブルにするために **dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを入力すると、**show dot1x all** コマンド出力には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 コマンドを入力したが、設定の不整合のためにポートがこのモードをサポートできない場合には、**show dot1x all** コマンド出力に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の制御方向ポート設定ステータスを表示します。

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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト値は次のとおりです。

- ポート単位の IEEE 802.1x プロトコルのイネーブル ステートはディセーブルです（force-authorized）。
- 再認証試行の間隔（秒数）は、3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機期間は 60 秒です。
- 再送信時間は 30 秒間です。
- 最大再送信回数は、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 タイムアウト期間は、30 秒間です。
- 認証サーバ タイムアウト期間は、30 秒間です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、ポート上の IEEE 802.1x パラメータをリセットする方法を示します。

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

show dot1x [**interface** *interface-id*] イネーブル 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 dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x guest-vlan

アクティブ VLAN（仮想 LAN）を IEEE 802.1x 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

構文の説明

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

デフォルト

ゲスト VLAN は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	使用上の注意事項が修正されました。

使用上の注意事項

ゲスト VLAN は次のスイッチ ポートに対して設定できます。

- 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 ポートに接続されたすべてのホストは、状態確認が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。スイッチはスイッチ上の プライマリ プライベート VLAN アソシエーションとセカンダリ プライベート VLAN アソシエーションを使用してプライマリ プライベート VLAN を決定します。

スイッチの IEEE 802.1x ポートごとに、ゲスト VLAN を設定して、IEEE 802.1x 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することができますが、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、スイッチが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しない場合、または EAPOL パケットがクライアントから送信されない場合には、スイッチ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 パケット履歴を保存します。リンクの存続中にインターフェイスで別の EAPOL パケットが検出されると、ゲスト VLAN 機能はディセーブルされます。ポートがすでにゲスト VLAN ステートの場合には、ポートは無許可ステートに戻され、認証が再起動されます。リンクが切れると、EAPOL 履歴はリセットされます。

dot1x guest-vlan supplicant グローバル コンフィギュレーション コマンドを入力すると、この動作はディセーブルされます。

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

ゲスト VLAN は、シングルホスト モードとマルチホスト モードの IEEE 802.1x ポートでサポートされます。

Remote Switched Port Analyzer（RSPAN）VLAN または音声 VLAN 以外の任意のアクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、トランク ポートではサポートされず、アクセス ポートでのみサポートされています。

Dynamic Host Configuration Protocol（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少します（**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）。設定を減少する量は、接続されている IEEE 802.1x クライアント タイプに依存します。

例

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

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

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

```
Switch(config-if)# dot1x timeout 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 gigabitethernet0/1
Switch(config-if)# dot1x guest-vlan 5
```

show dot1x [**interface** *interface-id*] イネーブル 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
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*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x host-mode

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** に設定された IEEE 802.1x 認証ポートで単一のホスト（クライアント）または複数のホストを許可するには、**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。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**}

no dot1x host-mode [**multi-host** | **single-host**]

構文の説明

multi-host	スイッチのマルチホスト モードをイネーブルにします。
single-host	スイッチのシングルホスト モードをイネーブルにします。

デフォルト

デフォルトは、シングルホスト モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 つが許可されると、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。

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てください。

例

次の例では、IEEE 802.1x をグローバルにイネーブルにし、ポートの IEEE 802.1x 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 gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

show dot1x [**interface** *interface-id*] イネーブル 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 dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x initialize

ポートで新しい認証セッションを開始する前に、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** イネーブル EXEC コマンドを使用します。

dot1x initialize interface *interface-id*

構文の説明

interface *interface-id*	初期化されるポートです。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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すると、ポート ステータス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 gigabitethernet0/2
```

show dot1x [**interface** *interface-id*] イネーブル EXEC コマンドを入力すると、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*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x max-reauth-req

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高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

構文の説明

count	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数です。指定できる範囲は 0 ～ 10 です。

デフォルト

デフォルトは 2 回です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上の注意事項

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
```

show dot1x [**interface** *interface-id*] イネーブル 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
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（応答を受信しないと仮定して）を認証サーバに送信する最高回数を設定します。
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*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x max-req

スイッチが認証プロセスを再起動する前に、(応答を受信しないと仮定して)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高回数を設定するには、**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

構文の説明

count	認証プロセスを再起動する前に、スイッチが認証サーバから EAP フレームを再送信する回数。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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、スイッチが認証サーバからクライアントに EAP フレームを送信する回数を 5 回に設定する方法を示します。

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

show dot1x [**interface** *interface-id*] イネーブル 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
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*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x port-control

ポートの許可ステートの手動制御をイネーブルにするには、**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

構文の説明

auto	ポートで IEEE 802.1x 認証をイネーブルにし、スイッチおよびクライアント間の IEEE 802.1x 認証交換に基づきポートを許可または無許可ステートに変更します。
force-authorized	ポートで IEEE 802.1x 認証をディセーブルにすれば、認証情報の交換を必要とせずに、ポートを許可ステートに移行します。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することができません。

デフォルト

デフォルトは、force-authorized です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

特定のポートの IEEE 802.1x 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 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 プロトコルは、レイヤ 2 スタティック アクセス ポートと音声 VLAN ポート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 **auto** キーワードを使用することができます。

- トランク ポート ― トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、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 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、IEEE802.1x 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 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 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。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）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 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 はディセーブルになっています。SPAN または RSPAN 送信元ポートでは IEEE 802.1x をイネーブルにすることができます。

スイッチの IEEE 802.1x 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 をディセーブルにするには、**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 をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

show dot1x [**interface** *interface-id*] イネーブル 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 dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x re-authenticate

指定された、IEEE 802.1x がイネーブルされたポートの再認証を手動で起動するには、**dot1x re-authenticate** イネーブル EXEC コマンドを使用します。

dot1x re-authenticate interface *interface-id*

構文の説明

interface *interface-id*	再認証するインターフェイスのモジュールおよびポート番号です。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドを使用すると、再認証（re-authperiod）および自動再認証の間の設定秒数を待たずにクライアントを再認証することができます。

例

次の例では、ポートに接続された装置を手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

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	再認証の間隔（秒）を指定します。

dot1x reauthentication

クライアントの定期的再認証をイネーブルにするには、**dot1x re-authentication** 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

定期的な再認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、定期的再認証の試行間隔の時間を設定します。

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
```

show dot1x [**interface** *interface-id*] イネーブル 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
dot1x re-authenticate	IEEE 802.1x がイネーブルされたポートすべての再認証を手動で起動します。
dot1x timeout reauth-period	再認証の間隔（秒）を指定します。
show dot1x [**interface** *interface-id*]	指定したポートの IEEE 802.1x ステータスを表示します。

dot1x timeout

IEEE 802.1x 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* | **reauth-period** {*seconds* | **server**} | **server-timeout** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

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

構文の説明

quiet-period *seconds*	スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数。指定できる範囲は 1 ～ 65535 です。
reauth-period {*seconds* | **server**}	再認証の間隔（秒）を指定します。 キーワードの意味は次のとおりです。 • *seconds* — 秒数を 1 ～ 65535 の範囲で設定します。デフォルトは 3600 秒です。 • **server** — 秒数を Session-Timeout RADIUS アトリビュート（Attribute[27]）の値として設定します。
server-timeout *seconds*	スイッチが認証サーバ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。
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 5 ～ 65535 です。

デフォルト

デフォルト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。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	**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。

使用上の注意事項

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 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、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドで定期的な再認証をイネーブルにした場合にだけスイッチの動作に影響を与えます。

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起動しません。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

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、Session-Timeout RADIUS アトリビュートの値を再認証の間隔の秒数として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、スイッチと認証サーバ間の再送信時間を 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 フレームのスイッチとクライアント間の再送信時間を 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
```

show dot1x イネーブル 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
dot1x max-req	スイッチが、認証プロセスを再起動する前に、EAP-Request/Identity フレームを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。

duplex

ポートのデュプレックス動作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

構文の説明

auto	自動デュプレックス設定をイネーブルにします。ポートは、接続する装置のモードに応じて、全二重または半二重のどちらのモードで稼働する必要があるかを自動的に検出します。
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 Mbps または 100 Mbps で動作するインターフェイス用のみ）。1000 Mbps または 10000 Mbps 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、および - LX）SFP モジュールに対するデフォルトは **full** です。

1000BASE-*x*（*-x* は -BX、-CWDM、-LX、-SX、および -ZX）SFP モジュールではデュプレックス オプションはサポートされません。

各スイッチがサポートする SFP モジュールについては、製品リリース ノートを参照してください。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ファスト 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場合にポートを **auto** に設定すると、**full** を指定するの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できません。

特定のポートを全二重または半二重のどちらかに設定することができます。このコマンドの適用可能性は、このスイッチが接続されている装置によって異なります。

回線の両方のエンドが自動ネゴシエーションをサポートしている場合は、デフォルトの自動ネゴシエーション設定を使用することを強く推奨します。一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、もう一方のエンドがサポートしていない場合は、両方のインターフェイスのデュプレックスと速度を設定します。サポートされる側には、**auto** を設定します。

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は、速度が **auto** に設定されている場合に設定可能です。

注意　インターフェイス速度とデュプレックス モード コンフィギュレーションを変更すると、インターフェイスをシャットダウンし、再設定中に再度イネーブルにする場合があります。

スイッチ速度とデュプレックス パラメータの設定については、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。

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 gigabitethernet0/1
Switch(config-if)# duplex full
```

設定を確認するには、**show interfaces** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	スイッチのインターフェイス設定を表示します。
speed	10/100 Mbps または 10/100/1000 Mbps インターフェイスに速度を設定します。

errdisable detect cause

特定の原因またはすべての原因の 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** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap**}

no errdisable detect cause {**all** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **link-flap** | **pagp-flap**}

構文の説明

all	すべての errdisable 原因の検出をイネーブルにします。
dhcp-rate-limit	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）フラッピングのエラー検出をイネーブルにします。
gbic-invalid	無効な GBIC（ギガビット インターフェイス コンバータ）用のエラー検出をイネーブルにします。 **（注）** Catalyst 2960 スイッチ上では、このエラーは無効な Small Form-factor Pluggable（SFP）モジュールを意味します。
link-flap	リンク ステート フラッピングの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のエラー検出をイネーブルにします。
pagp-flap	Port Aggregation Protocol（PAgP; ポート集約プロトコル）フラップの errdisable 原因のエラー検出をイネーブルにします。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

原因（**all**、**dhcp-rate-limit** など）は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、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。

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、原因の回復メカニズムが設定されている場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出し、動作を再試行できます。回復メカニズムが設定されていない場合は、手動でインターフェイスを errdisable ステートから回復するために、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力する必要があります。

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
```

show errdisable detect イネーブル 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
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。

errdisable recovery

回復メカニズム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** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **udld** | **vmps**} | {**interval** *interval*}

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

構文の説明

cause	errdisable メカニズムをイネーブルにして、特定の原因から回復します。
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。
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	無効な GBIC（ギガビット インターフェイス コンバータ）モジュールの errdisable ステートから回復するタイマーをイネーブルにします。 **（注）** Catalyst 2960 スイッチ上では、このエラーは無効な Small Form-factor Pluggable（SFP）errdisable ステートを意味します。
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; ポート集約プロトコル）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。
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。
udld	UniDirectional Link Detection（UDLD; 単一方向リンク検出）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）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。同じ間隔がすべての原因に適用されます。デフォルト間隔は 300 秒です。 （注）　errdisable 回復タイマーは、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。

（注）　**ilpower**、**storm-control**、および **unicast-flood** 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ていますが、サポートされていません。

デフォルト

回復はすべての原因に対してディセーブルです。

デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

原因（**all**、**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。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、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。その原因に対して errdisable の回復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 ステートに置かれます。原因の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できるようになります。

それを行わない場合、手動でインターフェイスを errdisable ステートから回復するには、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力します。

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
```

show errdisable recovery イネーブル 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
show errdisable recovery	errdisable 回復タイマー情報を表示します。
show interfaces status err-disabled	インターフェイスのステータス、または errdisable ステートにあるインターフェイスのリストを表示します。

exception crashinfo

Cisco IOS イメージの障害時に拡張 crashinfo ファイルを作成するようにスイッチを設定するには、**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場合は、このコマンドの **no** 形式を使用します。

exception crashinfo

no exception crashinfo

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは拡張 crashinfo ファイルを作成します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

基本 crashinfo ファイルには、障害が発生した Cisco IOS 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ために役立つその他の情報が含まれます。

exception crashinfo グローバル コンフィギュレーション コマンドをスタック マスターで入力すると、スタック メンバーで Cisco IOS イメージの障害が発生した場合にすべてのスタック メンバーが拡張 crashinfo ファイルを作成するように設定されます。

拡張 crashinfo ファイルを作成しないようにスイッチを設定するには、**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、拡張 crashinfo ファイルを作成しないようにスイッチを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** イネーブル 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稼働中の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。

flowcontrol

インターフェイスの受信フロー制御ステートを設定するには、**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 **send** が動作可能でオンになっており、接続のもう一方の側で輻輳を検出した場合、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** がオンであり、休止フレームを受信した場合、データ パケットの送信を停止します。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。

receive off キーワードを使用すると、フロー制御はディセーブルになります。

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

（注）　Catalyst 2960 スイッチは休止フレームを受信できますが、送信はできません。

構文の説明

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働させることができます。
off	接続装置がフロー制御パケットをインターフェイスへ送信する機能をオフにします。
on	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼働させることができます。

デフォルト

デフォルトは、**flowcontrol receive off** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチは、フロー制御休止フレームの送信をサポートしていません。

on および **desired** キーワードの結果は同じであ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**：ポートは休止フレームを送信できませんが、休止フレームを必要とするかまたは休止フレームを送信できる接続装置とともに稼働できます。ポートは休止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、設定を組み合わせることによりローカル装置およびリモート装置で生じるフロー制御の結果を示したものです。この表は、**receive desired** キーワードの結果が **receive on** キーワードを使用した場合と同じであることを前提にしています。

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	
ローカル装置	**リモート装置**	**ローカル装置**	**リモート装置**
send off/receive on	**send on/receive on**	受信のみ行います。	送受信を行います。
	send on/receive off	受信のみ行います。	送信のみ行います。
	send desired/receive on	受信のみ行います。	送受信を行います。
	send desired/receive off	受信のみ行います。	送信のみ行います。
	send off/receive on	受信のみ行います。	受信のみ行います。
	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 gigabitethernet0/1
Switch(config-if)# flowcontrol receive off
```

設定を確認するには、**show interfaces** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

interface port-channel

ポート チャネル論理インターフェイスのアクセスまたは作成を行うには、**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*

構文の説明

port-channel-number	ポート チャネル番号です。指定できる範囲は 1 ～ 6 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 コマンドを使用します。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* と同じ番号を使用することもできれば、新しい番号を使用することもできます。新しい番号を使用すると、**channel-group** コマンドが動的に新しいポート チャネルを作成します。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

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。

設定時の注意事項の完全なリストは、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 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
```

show running-config イネーブル EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** イネーブル 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
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

インターフェイス範囲コンフィギュレーション モードを開始したり、同時に複数のポートでコマンドを実行したりするには、**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*}

構文の説明

port-range	ポート範囲。*port-range* の有効値のリストについては、「使用上の注意事項」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がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

インターフェイス範囲コンフィギュレーション モードを開始すると、入力するすべてのインターフェイス パラメータが範囲内のすべてのインターフェイスに適用されます。

VLAN（仮想 LAN）については、既存の VLAN Switch Virtual Interface（SVI）でだけ **interface range** コマンドを使用することができます。VLAN SVI を表示する場合は、**show running-config** イネーブル 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すべての設定変更は、NVRAM（不揮発性 RAM）に保存されますが、interface range 自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力することができます。

- 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 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することができます。

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*、ここで、VLAN ID は 1 ～ 4094 です。

（注） コマンドライン インターフェイス（CLI）には複数の VLAN を設定するオプションがありますが、これはサポートされていません。

- **fastethernet** module/{*first port*} - {*last port*}、module は常に **0** です。
- **gigabitethernet** module/{*first port*} - {*last port*}、module は **0** です。
  物理インターフェイスの場合は、次のとおりです。
  — モジュールは常に 0 です。
  — 範囲は、*type* **0**/*number* - *number* です（たとえば、**gigabitethernet 0/1 - 2**）。
- **port-channel** *port-channel-number* - *port-channel-number*、*port-channel-number* は 1 ～ 6 です。

（注） **interface range** コマンドに port-channel を指定する場合、範囲の先頭と最後のポート チャネルはアクティブなポート チャネルでなければなりません。

範囲を定義するときは、最初のエントリとハイフン（-）の間にスペースが必要です。

```
interface range gigabitethernet0/1 -2
```

複数の範囲を定義するときは、最初のエントリとカンマ（,）の間にスペースが必要です。

```
interface range fastethernet0/1 - 2, gigabitethernet0/1 - 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。

port-range に単一のインターフェイスを指定することもできます。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。

インターフェイス範囲の設定方法の詳細については、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、**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 gigabitethernet0/1 - 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 gigabitethernet0/1 - 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マクロを作成します。
show running-config	スイッチで現在稼働中の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

VLAN（仮想 LAN）を作成または VLAN へアクセスし、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。VLAN 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*

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN は、特定の VLAN に対して、最初に **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、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。

no interface vlan *vlan-id* コマンドで VLAN 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** イネーブル 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。

削除され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と、削除された VLAN を復元できます。インターフェイスは復元されますが、以前の設定は失われます。

例

次の例では、VLAN ID 23 の新しい VLAN 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* イネーブル 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 interfaces vlan *vlan-id*	すべてのインターフェイスまたは指定された 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 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場合は、このコマンドの **no** 形式を使用します。

ip access-group {*access-list-number* | *name*} {**in**}

no ip access-group [*access-list-number* | *name*] {**in**}

構文の説明

access-list-number	IP Access Control List（ACL; アクセス制御リスト）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。

デフォルト

アクセス リストは、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

名前付きまたは番号付きの標準 / 拡張 IP アクセス リストをインターフェイスに適用できます。名前を付けてアクセス リストを定義するには、**ip access-list** グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストを定義するには、**access list** グローバル コンフィギュレーション コマンドを使用します。1 ～ 99 および 1300 ～ 1999 の範囲の番号付き標準アクセス リスト、または 100 ～ 199 および 2000 ～ 2699 の範囲の番号付き拡張アクセス リストを使用できます。

このコマンドを使用して、アクセス リストをレイヤ 2 インターフェイスに適用できます。ただし、次のポート ACL の制限に注意してください。

- 入力方向にのみ ACL を適用できます。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC（メディア アクセス制御）ACL のみを適用できます。
- ポート ACL はロギングをサポートしていません。IP ACL に **log** キーワードが指定されていても、それは無視されます。
- 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リングします。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。

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廃棄します。

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 gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
```

show ip interface、**show access-lists**、または **show ip access-lists** イネーブル 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
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る ACL を表示します。
show ip access-lists	スイッチで設定される 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場合は、このコマンドの **no** 形式を使用します。

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

構文の説明

ip-address	IP アドレスです。
subnet-mask	関連する IP サブネットのマスクです。
secondary	（任意）設定済みアドレスがセカンダリ IP アドレスであることを指定します。このキーワードを省略すると、設定済み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ません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Telnet セッションを使用してスイッチ IP アドレスを削除すると、そのスイッチへの接続は切断されます。

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、ICMP Mask Reply メッセージでこの要求に応答します。

no ip address コマンドで IP アドレスを削除することで、特定インターフェイスの IP 処理をディセーブルにすることができます。スイッチは、その IP アドレスのいずれかを使用するホストを検出すると、エラー メッセージをコンソールに送ります。

任意のキーワード **secondary** を使用して、数に制限なくセカンダリ アドレスを指定できます。セカンダリ アドレスは、システムがセカンダリ送信元アドレスを持つルーティング アップデート以外生成しない点を除いて、プライマリ アドレスと同様に扱われます。IP ブロードキャストと ARP 要求は、IP ルーティング テーブル内のインターフェイス ルートと同様に、適切に処理されます。

（注）　ネットワーク セグメント上のルータがセカンダリ アドレスを使用している場合は、同じセグメント上の他のすべての装置も同じネットワークまたはサブネットのセカンダリ アドレスを使用する必要があります。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、すぐにルーティング ループを引き起こす可能性があります。

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 サーバは再びアドレスを割り当てることはできません。

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ています。

```
Switch(config)# interface vlan 1
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** イネーブル 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 dhcp snooping

Dynamic Host Configuration Protocol（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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピングは、ディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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（仮想 LAN）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
```

show ip dhcp snooping イネーブル 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
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 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 binding

DHCP スヌーピング バインディング データベースを設定し、バインディング エントリをデータベースに追加するには、**ip dhcp snooping binding** イネーブル 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*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。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時間（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 データベースは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドはスイッチのテストまたはデバッグの際に使用します。

DHCP スヌーピング バインディング データベース内の、バインディングとも呼ばれる各データベース エントリには、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進形式）、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属する VLAN が含まれます。このデータベースには最大 8192 のバインディングを含むことができます。

設定済みのバインディングのみを表示するには、**show ip dhcp snooping binding** ユーザ EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポートに有効時間 1000 秒の DHCP バインディング設定を作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
gigabitethernet0/1 expiry 1000
```

show ip dhcp snooping binding イネーブル 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
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 データベースに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。

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 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。エージェントをディセーブルし、timeout 値をリセットするか、または write-delay 値をリセットするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {{**flash:**/*filename* | **ftp:**//*user:password@host/filename* | **http:**//*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar** | **rcp:**//*user@host/filename* | **tftp:**//*host/filename*} | **timeout** *seconds* | **write-delay** *seconds*}

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

構文の説明

flash:/*filename*	データベース エージェントまたはバインディング ファイルがフラッシュ メモリ内にあることを指定します。
ftp://*user*:*password*@*host*/*filename*	データベース エージェントまたはバインディング ファイルが FTP サーバ上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 サーバ上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 Control Protocol（RCP）サーバ上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 サーバ上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の終了を待機する時間（秒）を指定します。 デフォルト値は 300 秒です。範囲は 0 ～ 86400 です。無期限を指定するには 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 データベースの内容が変化した後、転送を行うまでの遅延時間（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 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。

timeout 値は 300 秒（5 分）です。

write-delay 値は 300 秒（5 分）です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

DHCP スヌーピング バインディング データベースには最大 8192 のバインディングを含むことができます。

データベース内のリース時間の精度を保証するには、Network Time Protocol（NTP）をイネーブルし、以下の機能を設定することを推奨します。

- 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 ソース IP アドレス

NTP が設定されると、スイッチはシステム クロックが NTP に同期されている時のみバインディングの変更をバインディング ファイルに書き込みます。

NVRAM とフラッシュ メモリのストレージ容量には限りがあるため、バインディング ファイルは TFTP サーバに保存することを推奨します。スイッチが、指定された URL 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には、あらかじめネットワークベース URL（TFTP および FTP など）上の設定された URL に空ファイルを作成する必要があります。

DHCP スヌーピング バインディング データベースを NVRAM に保存するには、**ip dhcp snooping database flash:***filename* コマンドを使用します。**ip dhcp snooping database timeout** を 0 秒に設定し、データベースを TFTP ファイルに書き込んでいる場合には、TFTP サーバがダウンすると、データベース エージェントは無期限に転送の試行を続けます。この転送の継続中は、新たな転送は起動できません。サーバがダウンしているとファイルを書き込むことはできないため、これは問題にはなりません。

エージェントをディセーブルするには、**no ip dhcp snooping database** コマンドを使用します。

timeout 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。

write-delay 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、バインディング ファイルを IP アドレス 10.1.1.1 の *directory* という名前のディレクトリに保存する方法を示します。*file* という名前のファイルが TFTP サーバ上に存在する必要があります。

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

次の例では、*file01.txt* という名前のバインディング ファイルを NVRAM に保存する方法を示します。

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

show ip dhcp snooping database イネーブル 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
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 データベース情報を設定します。
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

Dynamic Host Configuration Protocol（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するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option

no ip dhcp snooping information option

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP オプション 82 データが挿入されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 機能がイネーブルにされており、スイッチがホストからの DHCP 要求を受信した場合、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）のポート識別子が含まれます。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 アドレス値制限などのポリシーを適用することができます。さらに 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 データを最初から挿入したかを確認します。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
```

show ip dhcp snooping イネーブル 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 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た、信頼されていないポートで受信されたオプション 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチはエッジ スイッチに接続された信頼されていないポートで受信されたオプション 82 情報を持つ DHCP パケットを廃棄します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、エッジ スイッチにホストを接続したいユーザ、アグリケーション スイッチでは DHCP スヌーピングなどの DHCP セキュリティ機能もイネーブルにできます。しかしながら、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、スイッチは信頼されてい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廃棄し、信頼され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。

ホストが接続されたエッジ スイッチがオプション 82 情報を挿入し、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場合は、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 スイッチは信頼されていないポートで 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できます。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、信頼されるポートとして設定する必要があります。

（注）　信頼されてい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、信頼されてい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、エッジ スイッチからの信頼されていないパケットのオプション 82 情報を確認せず、パケットを受け入れるようにアクセス スイッチを設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

show ip dhcp snooping イネーブル 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 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 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 Dynamic Host Configuration Protocol（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

構文の説明

rate	インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数。指定できる範囲は 1 ～ 2048 です。

デフォルト

DHCP スヌーピング レート制限は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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（仮想 LAN）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にされていない場合、**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
```

show ip dhcp snooping イネーブル 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
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）スヌーピング目的でポートを信頼でき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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピング信頼は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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された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され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
```

show ip dhcp snooping イネーブル 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 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

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 ハードウェア アドレスと一致する信頼されないポートをスイッチが確認するよう設定するには、**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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

サービスプロバイダー ネットワークで、スイッチが信頼されないポートの 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廃棄します。

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
```

show ip dhcp snooping イネーブル 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 ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

VLAN（仮想 LAN）上で 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*

構文の説明

vlan *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られています。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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
```

show ip dhcp snooping イネーブル 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 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 igmp filter

Internet Group Management Protocol（IGMP）プロファイルをインターフェイスに適用することで、レイヤ 2 インターフェイス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

構文の説明

profile number	適用される IGMP プロファイル番号です。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

IGMP フィルタは適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

IGMP フィルタはレイヤ 2 物理インターフェイスのみに適用できます。IGMP フィルタを EtherChannel グループに属するポートに適用することはできません。

IGMP プロファイルは 1 つまたは複数のスイッチ ポート インターフェイスに適用できますが、1 つのポートに適用可能なプロファイルは 1 つだけです。

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 gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

設定を確認するには、**show running-config** イネーブル EXEC コマンドを入力し、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 igmp profile	指定の IGMP プロファイルの特性を表示します。
show running-config interface *interface-id*	スイッチ インターフェイスに適用されている IGMP プロファイル（ある場合）を含む、そのインターフェイス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 igmp max-groups

レイヤ 2 インターフェイスが加入できる Internet Group Management Protocol（IGMP）グループの最大数を設定する、またはエントリの最大数が転送テーブルにある場合に IGMP スロットリング アクションを設定するには、**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（レポートを廃棄）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

構文の説明

number	インターフェイスが加入できる IGMP グループの最大数です。指定できる範囲は 0 ～ 4294967294 で、デフォルトは無制限です。
action deny	IGMP スヌーピング転送テーブル内に最大数のエントリがある場合は、次の IGMP 加入レポートを廃棄します。これは、デフォルトのアクションです。
action replace	IGMP スヌーピング転送テーブル内に最大数のエントリがある場合には、IGMP レポートが受信された既存グループが新規グループで置換されます。

デフォルト

デフォルトの最大グループ数は、無制限です。

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 レポートを廃棄し、インターフェイスに IGMP グループのエントリを追加しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドをレイヤ 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のみ使用できます。EtherChannel グループに属するポートの IGMP 最大グループを設定することができません。

IGMP スロットリング アクションを設定するときには、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、最大グループ制限を設定する場合は、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廃棄します。
- スロットリング アクションを **replace** として設定し、最大グループ制限を設定する場合は、以前転送テーブルにあったエントリは削除されます。転送テーブル内に最大数のエントリがある場合は、スイッチは無作為に選択されたマルチキャスト エントリを受信された IGMP レポートで置換します。
- 最大グループ制限が、デフォルト（上限なし）に設定された場合は、**ip igmp max-groups** {**deny** | **replace**} コマンドを使用しても無効です。

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 gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、転送テーブル内に最大数のエントリがある場合に、IGMP レポートが受信された既存グループを新規グループで置換するようにスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** イネーブル EXEC コマンドを入力し、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加入できる最大 IGMP グループ数およびスロットリング アクションを含む、スイッチ インターフェイス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 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 メンバーシップ レポートをフィルタするための 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場合は、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*

no ip igmp profile *profile number*

構文の説明

profile number	設定される IGMP プロファイル番号です。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ません。設定されている場合、IGMP プロファイルに一致したときのデフォルト アクションは、一致アドレスの拒否です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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してプロファイルを作成できます。

- **deny**：一致アドレスを拒否するように指定します。これはデフォルトの条件です。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルトにリセットします。
- **permit**：一致アドレスを許可するように指定します。
- **range**：プロファイルの IP アドレスの範囲を指定します。単一の IP アドレスでも、開始アドレスと終了アドレスを持つ範囲でも構いません。

  範囲の入力時は、最小の IP マルチキャスト アドレス、スペース、最大の IP マルチキャスト アドレスの順に入力します。

IGMP プロファイルは 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、指定の IP マルチキャスト アドレスの範囲を許可する IGMP プロファイル 40 を設定する方法を示します。

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

show ip igmp profile イネーブル EXEC コマンドを入力すると、コマンド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
ip igmp filter	IGMP プロファイルを指定のインターフェイスに適用します。
show ip igmp profile	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）スヌーピングをグローバルまたは VLAN（仮想 LAN）単位で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*]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は、1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

IGMP スヌーピングは、スイッチでグローバルにイネーブルです。

IGMP スヌーピングは VLAN インターフェイスでイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 用に確保されていて、IGMP スヌーピングには使用できません。

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
```

show ip igmp snooping イネーブル 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
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 クエリー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）設定可能脱退タイマーをグローバルまたは VLAN 単位で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**

構文の説明 t

vlan *vlan-id*	(任意)指定された VLAN で IGMP スヌーピングおよび脱退タイマーをイネーブルにします。指定できる範囲は、1 ～ 1001 および 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 ～ 5000 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 用に確保されていて、IGMP スヌーピングには使用できません。

VLAN 上に脱退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 設定可能脱退時間は、IGMP バージョン 2 を実行するデバイスでのみサポートされます。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、IGMP 脱退タイマーを 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 脱退タイマーを 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
```

show ip igmp snooping イネーブル 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
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN で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 ネットワークで Internet Group Management Protocol（IGMP）クエリア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**]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび 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 および 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 アドレスを使用しようとします。
max-response-time *response-time*	（任意）IGMP クエリア レポートを待機する最大時間を設定します。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; トポロジー変更通知）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 の間隔中に実行する 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。1 または 2 を選択します。

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ディセーブルにされています。

イネーブルの場合、マルチキャスト対応デバイスからの IGMP トラフィックを検出すると、IGMP スヌーピング クエリア自身が機能をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

querier 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 *Version 2*（IGMPv2）を使用するデバイスを検出するように IGMP スヌーピング クエリアが設定されており、IGMP *Version 1*（IGMPv1）を使用しているクライアントを検出しません。デバイスが IGMPv2 を使用する場合は、手動で **max-response-time** 値を設定できます。デバイスが IGMPv1 を使用する場合は、**max-response-time** を設定できません（値を設定することができず、0 に設定されています）。

IGMPv1 が稼働している RFC に準拠しないデバイスは、**max-response-time** 値として 0 以外の値を持つ IGMP の一般的なクエリー メッセージを拒否する可能性があります。デバイスが IGMP の一般的なクエリー メッセージを受け入れるようにする場合、IGMPv1 を稼働するように IGMP スヌーピング クエリアを設定します。

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

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
```

show ip igmp snooping イネーブル 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
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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IGMP レポート抑制は、イネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートおよび IGMPv2 レポートが含まれる場合にのみサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれる場合はサポートされません。

このスイッチは、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 1 つの IGMP レポートだけをマルチキャスト 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）にされている場合は、スイッチは最初の IGMP レポート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 ルータに転送します。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 ルータに転送しません。この機能は、マルチキャスト デバイスに複製レポートが転送されるのを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートの要求だけが含まれる場合は、スイッチは最初の IGMPv1 または IGMPv2 レポートのみ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 ルータに転送します。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 コマンドを使用して IGMP レポート抑制をディセーブルにする場合は、すべての IGMP レポートがすべてのマルチキャスト ルータに転送されます。

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
```

show ip igmp snooping イネーブル 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
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN で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; トポロジー変更通知）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**}

構文の説明

flood query count *count*	マルチキャスト トラフィックがフラッディングされる IGMP の一般的なクエリーの数を指定します。指定できる範囲は 1 ～ 10 です。
query solicit	TCN イベントによって引き起こされたフラッディング モードからの復旧プロセスを加速するために、IGMP 脱退メッセージ（グローバル脱退）を送信します。

デフォルト

TCN flood query count は 2 です。

TCN クエリー送信請求はディセーブルされています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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され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 flood query count を 1 に設定すると、一般的なクエリーを 1 つ受信した後にフラッディングが停止します。count を 7 に設定すると、一般的なクエリーが 7 つ受信されるまで 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が続きます。グループは TCN イベント中に受信された一般的なクエリーに基づいて再学習します。

スイッチがスパニングツリー ルートであるか否かにかかわらずスイッチがグローバル脱退メッセージを送信できるようにするには、**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。このコマンドにより、TCN イベントに起因するフラッディング モードからの復旧プロセスも加速します。

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される IGMP の一般的なクエリーの数を 7 に指定する方法を示します。

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

show ip igmp snooping イネーブル 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
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping tcn flood	インターフェイスで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 動作に指定します。
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

Internet Group Management Protocol（IGMP）スプーフィング スパニングツリー Topology Change Notification（TCN; トポロジー変更通知）の動作をマルチキャスト フラッディングに設定するには、**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場合は、このコマンドの **no** 形式を使用します。

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スパニングツリー TCN イベントの間、インターフェイスでマルチキャスト フラッディングがイネーブルされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、すべてのポートにマルチキャスト トラフィックがフラッディングされます。スイッチに多数のポートがあり、接続されているホストが属するマルチキャストグループが複数ある場合は、フラッディングがリンクの容量を超過し、パケットを喪失する場合があります。

ip igmp snooping tcn flood query count *count* グローバル コンフィギュレーション コマンドを使用すると、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する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

show ip igmp snooping イネーブル 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
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping tcn	スイッチの IGMP TCN 動作を設定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping vlan immediate-leave

VLAN 単位で 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**

構文の説明

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 および 1006 ～ 4094 です。

デフォルト

IGMP 即時脱退処理はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

VLAN 内の各ポートに最大 1 つのレシーバーしか存在しない場合は、即時脱退機能のみ設定する必要があります。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 が稼働しているホストだけです。

例

次の例では、VLAN 1 で IGMP 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

show ip igmp snooping イネーブル 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
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 クエリー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 ポートを追加するか、またはマルチキャスト学習方式を設定するには、**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**}}

構文の説明

vlan-id	IGMP スヌーピングをイネーブルにし、マルチキャスト ルータ ポートとして、ポートを指定された VLAN に追加します。指定できる範囲は、1 ～ 1001 および 1006 ～ 4094 です。
interface *interface-id*	次のホップの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 ～ 6 です。
learn {**cgmp** | **pim-dvmrp**}	マルチキャスト ルータ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設定します。 • **pim-dvmrp —** IGMP クエリーおよび Protocol-Independent Multicasting-Distance Vector Multicast Routing Protocol（PIM-DVMRP）パケット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 クエリーと PIM-DVMRP パケットをスヌーピングします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

CGMP 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 gigabitethernet0/2
```

次の例では、マルチキャスト ルータ学習方式を 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
```

show ip igmp snooping イネーブル 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
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 クエリー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、マルチキャスト グループノメンバーとしてレイヤ 2 ポートを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 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*

構文の説明

vlan-id	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 および 1006 ～ 4094 です。
ip-address	レイヤ 2 ポートを、指定のグループ IP アドレスを持つマルチキャスト グループのメンバーとして追加します。
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 ～ 6 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指定されているポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

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で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
gigabitethernet0/1
Configuring port gigabitethernet0/1 on group 0100.5e02.0203
```

show ip igmp snooping イネーブル 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
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。

コマンド	説明
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 クエリーの設定および動作情報を表示します。

ip ssh

スイッチが Secure Shell（SSH; セキュア シェル）バージョン 1 または SSH バージョン 2 を実行するように設定するには、**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、スイッチが暗号化ソフトウェア イメージを実行している場合にのみ使用可能です。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。

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

構文の説明

1	（任意）スイッチが SSH version 1（SSHv2; SSH バージョン 2）を実行するように設定します。
2	（任意）スイッチが SSH version 2（SSHv2; SSH バージョン 2）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 クライアントによってサポートされる最新の SSH バージョンです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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場合は、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は、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、スイッチは SSHv1 クライアントをサポートします。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, and Adelman（RSA）キー ペアは、SSHv2 サーバで使用することができます。その逆の場合も同様です。

例

次の例では、SSHv2 を実行するようにスイッチを設定する方法を示します。

```
Switch(config)# ip ssh version 2
```

show ip ssh または **show ssh** イネーブル 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 ip ssh	SSH サーバがイネーブルにされているかどうかを表示し、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。

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

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 グループ内に 9 つ以上のポートがある場合に、どのポートがバンドルされ、どのポートがホットスタンバイ モードにされるかを指定します。

LACP チャネル グループには、同一タイプのイーサネット ポートを最大 16 個含むことができます。最大 8 個のポートをアクティブにでき、最大 8 個のポートをスタンバイ モードにできます。

port-priority の比較では、数値的に*小さな*値ほど*高い*プライオリティとなります。LACP チャネル グループ内に 9 つ以上のポートが含まれる場合には、LACP ポート プライオリティが小さな値（高いプライオリティ）の 8 つのポートがチャネル グループにバンドルされ、低プライオリティのポートがホットスタンバイ モードになります。2 つ以上のポートが同一の LACP ポート プライオリティを持つ場合には（デフォルト設定の 65535 に設定されている場合など）、内部ポート番号値がプライオリティの決定に使用されます。

（注）　LACP ポート プライオリティは、LACP リンクを制御するスイッチ上のポートでのみ有効です。どのスイッチがリンクを制御しているかを調べるには、**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** イネーブル EXEC コマンドを使用します。

物理ポートで LACP 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 EtherChannels」の章を参照してください。

例

次の例では、ポートの 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 gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000
```

show lacp [*channel-group-number*] **internal** イネーブル 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
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

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

lacp system-priority コマンドは、LACP リンク内の、ポート プライオリティを制御するスイッチを決定します。

LACP チャネル グループには、同一タイプのイーサネット ポートを最大 16 個含むことができます。最大 8 個のポートをアクティブにでき、最大 8 個のポートをスタンバイ モードにできます。LACP チャネルグループ内に 9 つ以上のポートが含まれる場合には、リンクの制御端のスイッチは、ポート プライオリティを使用して、どのポートがチャネルにバンドルされ、どのポートがホットスタンバイ モードになるかを決定します。他のスイッチ（リンクの非制御端）のポート プライオリティは無視されます。

プライオリティの比較では、数値的に小さい値ほどプライオリティが高くなります。そのため、LACP システム プライオリティが小さな値（高プライオリティ値）が制御システムになります。両方のスイッチが同一の LACP システム プライオリティの場合には（両方がデフォルト設定の 32768 に設定されている場合など）、LACP システム ID（スイッチの MAC アドレス）によって制御を行うスイッチが決定されます。

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

どのポートがホットスタンバイ モードであるかを確認するには、**show etherchannel summary** イネーブル EXEC コマンドを使用します（H ポートステート フラグが出力表示に示される）。

物理ポートで LACP 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 EtherChannels」の章を参照してください。

例

次の例では、LACP 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
```

show lacp sys-id イネーブル 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
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。

logging file

ロギング ファイル 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*]

構文の説明

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 メッセージが格納されるファイルのパスと名前が含まれます。 ローカル フラッシュ ファイル システムの構文 **flash:**
max-file-size	（任意）最大のロギング ファイル 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）最小のロギング ファイル 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）ロギング重大度を指定します。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）ロギング タイプを指定します。次のキーワードが有効です。 • **emergencies** — システムが使用不能（重大度 0） • **alerts** — すぐに対処が必要（重大度 1） • **critical** — クリティカル状態（重大度 2） • **errors** — エラー状態（重大度 3） • **warnings** — 警告状態（重大度 4） • **notifications** — 通常動作だ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

最小ファイル サイズは 2048 バイト、最大ファイル サイズは 4096 バイトです。

デフォルトの重大度レベルは 7 です（**debugging** メッセージと数値の小さいレベル）

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ログ ファイルは、スイッチの内部バッファに ASCII テキスト形式で格納されます。記録されたシステム メッセージには、スイッチの CLI（コマンドライン インターフェイス）を使用するか、適切に設定された Syslog サーバに保存することで、アクセスできます。スイッチに障害が生じた場合は、それ以前に **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 メモリにログを保存していないかぎり、ログは失われてしまいます。

logging file flash:*filename* グローバル コンフィギュレーション コマンドによってログをフラッシュ メモリに保存したあとは、**more flash***filename* イネーブル EXEC コマンドを使用してその内容を表示することができます。

コマンドは、最小ファイル サイズが最大ファイル サイズから 1024 を引いたサイズより大きい場合は、それを拒否します。そのあと、最小ファイル サイズは、最大ファイル サイズから 1024 を引いたサイズになります。

level を指定すると、指定したレベル以下（数値的に）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通知ログ 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** イネーブル 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; アクセス制御リスト）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 を削除する場合は、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*}

構文の説明

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 インターフェイスのみ）

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 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廃棄します。

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 gigabitethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

show mac access-group イネーブル 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。**show access-lists** イネーブル EXEC コマンドを入力すれば、スイッチに設定された ACL を表示することができます。

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 mac access-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）アドレスに基づきアクセス 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*

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

MAC 拡張リストはクラス マップとともに使用されます。

MAC 拡張 ACL はレイヤ 2 インターフェイスにだけ適用できます。

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。次のコンフィギュレーション コマンドが利用できます。

- **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 アクセス リスト コンフィギュレーション）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 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。

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
```

show access-lists イネーブル 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
deny（MAC アクセス リスト コンフィギュレーション）	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）。
permit（MAC アクセス リスト コンフィギュレーション）	
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。

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 テーブル内に保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（仮想 LAN）または指定の VLAN に適用されます。

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

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

構文の説明

0	この値はエージング タイムをディセーブルにします。スタティック アドレス エントリは、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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ホストが継続して送信しない場合、エージング タイムを増やして、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。時間を増やすと、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 に対してエージング 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 イネーブル 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 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 move update

MAC（メディア アクセス制御）アドレス テーブル移動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**}

構文の説明

receive	スイッチが MAC アドレス テーブル移動更新メッセージを処理することを指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクがアップになった場合に、スイッチが MAC アドレス テーブル移動更新メッセージをネットワーク内の他のスイッチに送信することを指定します。

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 テーブル移動更新機能はディセーブルです。

コマンド履歴

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。

使用上の注意事項

MAC アドレス テーブル移動更新機能により、プライマリ（フォワーディング）リンクがダウンしてスタンバイ リンクがトラフィックの転送を開始した場合に、スイッチは素早く双方向の収束を行うことができます。

アクセス スイッチは、プライマリ リンクがダウンしてスタンバイ リンクがアップになった場合に、MAC アドレス テーブル移動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 スイッチは、MAC アドレス テーブル移動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 スイッチを MAC アドレス テーブル移動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 スイッチを MAC アドレス テーブル移動更新メッセージを受信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** イネーブル 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 テーブル移動更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレス テーブル移動更新メッセージ処理をデバッグします。
show mac address-table move update	スイッチの MAC アドレス テーブル移動更新情報を表示します。

mac address-table notification

スイッチの 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**]

構文の説明

history-size *value*	（任意）MAC 通知履歴テーブルの最大エントリ数を設定します。指定できる範囲は 0 ～ 500 エントリです。
interval *value*	（任意）通知トラップの間隔を設定します。スイッチは、この時間量が経過した時点で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

デフォルトでは、MAC アドレス通知機能はディセーブルです。

デフォルトのトラップ間隔は 1 秒です。

デフォルトの履歴テーブルのエントリ数は 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

MAC アドレス通知機能は、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 MAC アドレスまたはセキュア MAC アドレスについてのみ許可されます。自身のアドレス、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 コマンドを使用すると、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
```

設定を確認するには、**show mac address-table notification** イネーブル 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 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 アドレス通知トラップをイネーブルにします。

mac address-table static

スタティック アドレスを MAC（メディア アクセス制御）アドレス テーブルに追加するには、**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場合は、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*]

構文の説明

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）です。この宛先アドレスを持つパケットが指定した VLAN（仮想 LAN）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です。有効なインターフェイスとしては、物理ポートおよびポート チャネルがあります。

デフォルト

スタティック アドレスは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	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
gigabitethernet0/1
```

show mac address-table イネーブル 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 エントリのみを表示します。

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、特定の送信元または宛先 MAC アドレスを持つトラフィックを廃棄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*

構文の説明

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廃棄されます。
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（仮想 LAN）ID 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廃棄しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

この機能を使用するときには、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 に転送されたパケットも、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廃棄します。次に入力したコマンドは、最初に入力したコマンドを無効にします。

  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廃棄します。

  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、スイッチはスタティック アドレスとして MAC アドレスを追加します。

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廃棄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 VLAN 4 上で受信された場合、パケットが廃棄されます。

```
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
```

設定を確認するには、**show mac address-table static** イネーブル 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 エントリのみを表示します。

macro apply

インターフェイスにマクロを適用、またはインターフェイス上にマクロ設定を適用し追跡するには、**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*}]

構文の説明

apply	指定されたインターフェイスにマクロを適用します。
trace	**trace** キーワードを使用してマクロをインターフェイスに適用し、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）インターフェイスに固有の一意なパラメータ値を指定します。最大 3 つのキーワード値のペアを入力できます。パラメータ キーワードのマッチングでは、大文字と小文字が区別されます。キーワードが一致すると、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がありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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することができます。

マクロを適用したときに構文エラーまたは設定エラーによりコマンドがエラーになった場合、マクロはインターフェイスへのそれ以外のコマンドの適用を継続します。

一意な値を割り当てる必要があるマクロを作成するとき、**parameter** *value* キーワードを使用して、インターフェイスに固有の値を指定します。

キーワードのマッチングでは、大文字と小文字が区別されます。キーワードが一致すると、すべて対応する値に置き換えられます。キーワードが長い文字列の一部であっても、キーワードが完全に一致する場合は一致とみなされ、対応する値に置き換えられます。

マクロの中にはパラメータ値を必要とするキーワードが含まれているものもあります。**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すると、コマンドは無効になり適用されません。

スイッチのソフトウェアに Cisco-default SmartPort マクロが組み込まれています。**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することができます。

インターフェイスに Cisco-default SmartPort マクロを適用する場合、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、スイッチのマクロをすべて表示します。**show parser macro name** *macro-name* ユーザ EXEC コマンドを使用して、特定のマクロの内容を表示します。
- **$** で始まるキーワードは、一意なパラメータ値が必要であることを示します。**parameter** *value* キーワードを使用して、Cisco-default マクロに必要な値を追加します。

  Cisco-default マクロでは **$** 文字を使用して必要なキーワードを識別しやすくしています。マクロを作成する際にキーワードを定義するための **$** 文字の使用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、マクロ名は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することができます。

インターフェイス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ような動作をします。インターフェイス範囲を使用する場合は、マクロは範囲内の各インターフェイスに順に適用されます。マクロが 1 つのインターフェイスで失敗した場合でも、残りのインターフェイスに適用されます。

default interface *interface-id* インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上のマクロが適用された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、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された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することができます。次の例では、インターフェイスに **duplex** という名前のユーザ作成された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、Cisco-default **cisco-desktop** マクロを表示し、マクロを適用してインターフェイス上のアクセス 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 gigabitethernet0/4
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るマクロ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、追跡します。
macro global description	スイッチに適用されるマクロ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されたマクロのマクロ定義を表示します。

macro description

インターフェイスに適用されているマクロの説明を入力するには、**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。説明を削除する場合は、このコマンドの **no** 形式を使用します。

macro description *text*

no macro description *text*

構文の説明

description *text*	指定されたインターフェイスに適用されるマクロ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がありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

description キーワードを使用して、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ます。複数のマクロが単一のインターフェイス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となります。

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** イネーブル 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、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、追跡します。
macro global description	スイッチに適用されるマクロ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され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、またはスイッチ上にマクロ設定を適用し追跡するには、**macro global** 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 global {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

構文の説明

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なパラメータ値を指定します。最大 3 つのキーワード値のペアを入力できます。パラメータ キーワードのマッチングでは、大文字と小文字が区別されます。キーワードが一致すると、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がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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することができます。

マクロを適用したときに構文エラーまたは設定エラーによりコマンドがエラーになった場合、マクロはスイッチへのそれ以外のコマンドの適用を継続します。

一意な値を割り当てる必要があるマクロを作成する場合、**parameter** *value* キーワードを使用して、スイッチに固有の値を指定します。

キーワードのマッチングでは、大文字と小文字が区別されます。キーワードが一致すると、すべて対応する値に置き換えられます。キーワードが長い文字列の一部であっても、キーワードが完全に一致する場合は一致とみなされ、対応する値に置き換えられます。

マクロの中にはパラメータ値を必要とするキーワードが含まれているものもあります。**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すると、コマンドは無効になり適用されません。

スイッチのソフトウェアに Cisco-default SmartPort マクロが組み込まれています。**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することができます。

スイッチに Cisco-default SmartPort マクロを適用する場合、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、スイッチのマクロをすべて表示します。**show parser macro name** *macro-name* ユーザ EXEC コマンドを使用して、特定のマクロの内容を表示します。

- **$** で始まるキーワードは、一意なパラメータ値が必要であることを示します。**parameter** *value* キーワードを使用して、Cisco-default マクロに必要な値を追加します。

  Cisco-default マクロでは **$** 文字を使用して必要なキーワードを識別しやすくしています。マクロを作成する際にキーワードを定義するための **$** 文字の使用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、マクロ名は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することができます。

マクロに含まれている各コマンドの **no** バージョンを入力した場合のみスイッチ上でグローバルにマクロが適用された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、そのマクロをスイッチに適用できます。次に、**snmp** マクロを表示し、マクロを適用し、ホスト名をテスト サーバに設定して IP precedence 値を 7 に設定する例を示します。

```
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することができます。この例では、**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ものの、残りのマクロがスイッチに適用されます。

```
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、追跡します。
macro description	インターフェイスに適用されるマクロの説明を追加します。
macro global description	スイッチに適用されるマクロ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され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の説明を入力するには、**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。説明を削除する場合は、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*

構文の説明

description *text*	スイッチに適用されるマクロ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がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

description キーワードを使用して、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となります。

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** イネーブル 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、追跡します。
macro description	インターフェイスに適用されるマクロ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、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され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場合は、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*

構文の説明

macro-name	マクロ名

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

マクロには、最大 3000 文字を含めることができます。各行に 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。行の最初に **#** 文字を使用して、マクロ内にコメント テキストを入力します。

ヘルプ ストリングを使用してキーワードを指定することにより、マクロ内に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で最大で 3 つのヘルプ ストリングを入力できます。4 つ以上のマクロ キーワードを指定した場合、最初の 3 つのみ表示されます。

マクロ名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** および **macro name sample-macro** は 2 つの別々のマクロになります。

マクロを作成する際に、**exit** または **end** コマンドを使用したり、**interface** *interface-id* を使用してコマンド モードを変更しないでください。これらのコマンドは、**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原因になる可能性があります。

このコマンドの **no** 形式は、マクロ定義だけを削除します。マクロはすでに適用されたインターフェイスの設定に影響を与えません。**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上のマクロが適用された設定を削除できます。また、元のマクロの相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* を作成することができます。次に、anti-macro をインターフェイスに適用します。

既存のマクロと同一の名前の新規マクロを作成することによってマクロを修正できます。新しく作成されたマクロは、既存のマクロを無効にしますが、元のマクロが適用されたインターフェイスの設定に影響しません。

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
@
```

次に、**# macro keywords** を使用してマクロを作成する例を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

次に、インターフェイスをマクロに適用する前に必須キーワード値を表示する例を示します。

```
Switch(config)# interface gigabitethernet0/1
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、追跡します。
macro description	インターフェイスに適用されるマクロ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、追跡します。
macro global description	スイッチに適用されるマクロの説明を追加します。
show parser macro	すべてのマクロまたは指定されたマクロのマクロ定義を表示します。

match（クラスマップ コンフィギュレーション）

トラフィックを分類するための一致基準を定義するには、**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場合は、このコマンドの **no** 形式を使用します。

match {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

no match {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

構文の説明

access-group *acl-index-or-name*	IP 標準または拡張 Access Control List（ACL; アクセス制御リスト）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。
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 Services 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。また、一般的な値にニーモニック名を入力できます。
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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 のマッチングのみ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 つずつのみ **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。サポートされるニーモニック名のリストについては、**match ip dscp ?** コマンドまたは **match ip precedence ?** コマンドを入力して、コマンドライン ヘルプ ストリングを参照してください。

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
```

show class-map イネーブル 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
class-map	名前を指定したクラスとパケットとの比較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; サービス品質）クラス マップを表示します。

mdix auto

インターフェイスの自動 Medium-Dependent Interface crossover（MDIX; メディア依存型インターフェイス クロス）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。自動 MDIX がイネーブルにされている場合、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。自動 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

自動 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

インターフェイスの自動 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、インターフェイスの速度とデュプレックスも **auto** に設定する必要があります。

自動 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。

自動 MDIX はすべての 10/100 Mbps および 10/100/1000 Mbps インターフェイスでサポートされます。自動 MDIX は、1000BASE-SX または -LX Small Form-factor Pluggable（SFP）モジュール ポートではサポートされません。

例

次の例では、ポートの自動 MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

show controllers ethernet-controller *interface-id* **phy** イネーブル EXEC コマンドを入力すると、インターフェイスの自動 MDIX の動作ステートを確認できます。

関連コマンド

コマンド	説明
show controllers ethernet-controller *interface-id* **phy**	自動 MDIX の動作ステートを含む、インターフェイスの内部レジスタに関する一般的な情報を表示します。

media-type

インターフェイスと dual-purpose アップリンク ポートのタイプを手動で選択するか、または最初にリンクアップするタイプの動的選択をイネーブルにするには、**media-type** 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。

media-type {**auto-select** | **rj45** | **sfp**}

no media-type

構文の説明

auto-select	最初にリンクアップしたタイプに基づいた、動的選択をイネーブルにします。
rj45	RJ-45 インターフェイスを選択します。
sfp	Small Form-factor Pluggable（SFP）モジュール インターフェイスを選択します。

デフォルト

デフォルトは、スイッチが動的に選択する **auto-select** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

dual-purpose アップリンクを冗長リンクとして使用することはできません。

dual-purpose アップリンクの速度またはデュプレックスを設定するには、インターフェイス タイプを選択する必要があります。タイプを変更すると、速度とデュプレックスの設定は削除されます。スイッチは両方のタイプの、速度とデュプレックスの両方を自動ネゴシエーション（デフォルト）に設定します。

auto-select を選択すると、スイッチは最初にリンクアップするタイプを動的に選択します。リンクアップすると、スイッチはアクティブ リンクがダウンするまでの間、他のタイプをディセーブルにします。アクティブ リンクがダウンすると、スイッチはいずれかがリンクアップするまで、両方のタイプをイネーブルにします。auto-select モードでは、スイッチは両方のタイプの、速度とデュプレックスの両方を自動ネゴシエーション（デフォルト）に設定します。

rj45 を選択すると、スイッチは SFP モジュール インターフェイスをディセーブルにします。このポートにケーブルを接続した場合、RJ-45 側がダウンまたは接続されていなくても、リンクアップすることはできません。このモードでは、dual-purpose ポートは 10/100/1000BASE-TX インターフェイスのように動作します。このインターフェイス タイプに合わせて速度とデュプレックスを設定できます。

sfp を選択すると、スイッチは RJ-45 インターフェイスをディセーブルにします。このポートにケーブルを接続した場合、SFP モジュール側がダウンまたは SFP モジュールが存在しなくても、リンクアップすることはできません。取り付けられている SFP モジュールのタイプに基づいて、このインターフェイス タイプに合わせて速度とデュプレックスを設定できます。

スイッチの電源をオンにするか、または **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 コマンドを使用して dual-purpose アップリンク ポートをイネーブルにすると、スイッチは SFP モジュール インターフェイスを初期設定状態にします。その他の場合には、スイッチは最初にリンクアップしたタイプに基づいてアクティブ リンクを選択します。

auto-select に設定すると、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドによる設定はできません。

Catalyst 2960 スイッチと 100BASE-X（-X は -BX、-FX、-FE、-LX のいずれか）SFP の組み合わせでは以下のように動作します。

- 100BASE -X SFP がモジュール スロットに挿入され、RJ-45 側にリンクが存在しない場合には、スイッチは RJ-45 インターフェイスをディセーブルにし、SFP モジュール インターフェイスを選択します。SFP 側にケーブルが接続されておらず、リンクがない場合でも、このような動作になります。
- 100BASE-X SFP モジュールが挿入されており、RJ-45 側にリンクが存在する場合には、スイッチはそのリンクを使用します。リンクがダウンすると、スイッチは RJ-45 側をディセーブルにし、SFP モジュール インターフェイスを選択します。
- 100BASE-X SFP モジュールが取り外されると、スイッチはタイプの動的選択（**auto-select**）に戻り、RJ-45 側を再度イネーブルにします。

スイッチは 100BASE-FX-GE SFP モジュールに対しては、このような動作はしません。

例

次の例では、SFP インターフェイスを選択する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# media-type sfp
```

show interfaces *interface-id* **capabilities** または **show interfaces** *interface-id* **transceiver properties** イネーブル EXEC コマンドを使用すると、設定を確認できます。

関連コマンド

コマンド	説明
show interfaces capabilities	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の能力を表示します。
show interfaces transceiver properties	インターフェイスの速度とデュプレックスの設定を表示します。

mls qos

スイッチ全体の Quality of Service（QoS; サービス品質）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 パラメータを使用して QoS がイネーブルになります。すべての QoS 関連の統計情報をリセットし、スイッチ全体の 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

構文の説明

このコマンドには、引数またはキーワードはありません。

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、信頼されるポートまたは信頼されないポートといった概念は存在しません。トラフィックはパススルー モードでスイッチングされます（パケットは、書き直されずにスイッチングされ、ポリシングされずにベストエフォートとして分類されます）。

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。すべてのポートのデフォルトのポート信頼状態は、信頼されない状態（untrusted）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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

QoS 分類、ポリシング、マークダウンまたは廃棄、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** コマンドを入力するまで、QoS 処理はディセーブルになっています。

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、ポリシーマップに関連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には、**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 ステータスを切り替えると、キューのサイズが変更（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間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廃棄します。

例

次の例では、スイッチで QoS をイネーブルにする方法を示します。

```
Switch(config)# mls qos
```

show mls qos イネーブル 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	QoS 情報を表示します。

mls qos aggregate-policer

同じポリシー マップ内の複数のクラスによって共有可能なポリサー 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。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場合は、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*

構文の説明

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（bps）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	指定された伝送速度を超えると、スイッチがパケットを廃棄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、スイッチはパケットの Differentiated Services 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 個のポリサーと 1 個の **no** 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最大ポリサー数は 64 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
```

show mls qos aggregate-policer イネーブル 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
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; サービス品質）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; サービス クラス）値を定義したり、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**}

構文の説明

default-cos	デフォルト CoS 値をポートに割り当てます。タグなしパケットの場合、デフォルトの CoS 値はパケットの 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 Services 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、他のポートからのパケットより高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 gigabitethernet0/1
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 gigabitethernet0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

show mls qos interface イネーブル 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	QoS 情報を表示します。

mls qos dscp-mutation

Differentiated Services Code Point（DSCP）/DSCP 変換マップを DSCP の信頼されるポートに適用するには、**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）に戻す場合は、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*

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

2 つの Quality of Service（QoS; サービス品質）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のみ適用します。DSCP 変換マップを信頼されないポート、Class of Service（CoS; サービス クラス）または IP precedence の信頼され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 の信頼され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 gigabitethernet0/1
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 *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
```

show mls qos maps イネーブル 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
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 マッピング情報を表示します。

mls qos map

Class of service（CoS; サービス クラス）/Differentiated Services Code Point（DSCP）マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP 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場合は、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**}

構文の説明

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 個の 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 個の DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。そのあと、続けて **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。 *dscp-list* には、各値をスペースで区切って最大 8 個の 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 個の 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 個の 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 2-6 に、デフォルトの CoS/DSCP マップを示します。

表 2-6　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 2-7 に、デフォルトの DSCP/CoS マップを示します。

表 2-7　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 2-8 に、デフォルトの IP precedence/DSCP マップを示します。

表 2-8　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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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
```

show mls qos maps イネーブル 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
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; サービス品質）マッピング情報を表示します。

mls qos queue-set output buffers

バッファをキューセット（ポートあたり 4 つの出力キュー）に割り当てるには、**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**

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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　デフォルト設定は、たいていの場合に適します。出力キューに関して深く理解し、この設定が QoS ソリューションを満たさない場合のみ、設定を変更する必要があります。

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。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 gigabitethernet0/1
Switch(config-if)# queue-set 2
```

show mls qos interface [*interface-id*] **buffers** または **show mls qos queue-set** イネーブル 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
mls qos queue-set output threshold	Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッシュホールドを設定し、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	キューセットに対するポートをマッピングします。
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 queue-set output threshold

Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッシュホールドの設定、バッファの可用性の保証、およびキューセット（ポートあたり 4 つの出力キュー）への最大メモリ割り当ての設定を行うには、**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*]

構文の説明

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 スレッシュホールドです。指定できる範囲は 1 ～ 400% 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廃棄せずに保持できる最大メモリです。指定できる範囲は 1 ～ 400% です。

デフォルト

Quality of Service（QoS; サービス品質）がイネーブルなときは、WTD もイネーブルです。

表 2-9 は、デフォルトの WTD スレッシュホールドの設定値を示しています。

表 2-9　デフォルトの出力キュー WTD スレッシュホールド設定値

機能	キュー 1	キュー 2	キュー 3	キュー 4
WTD 廃棄スレッシュホールド 1	100%	200%	100%	100%
WTD 廃棄スレッシュホールド 2	100%	200%	100%	100%
予約済みスレッシュホールド	50%	100%	50%	50%
最大スレッシュホールド	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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 つのキューに固定量のバッファを割り当てます。

廃棄スレッシュホールド値（%）は、100% を超え、最大値（最大スレッシュホールドが 100% を超える場合）まで指定することができます。

（注）　出力キュー　デフォルト設定は、たいていの場合に適します。出力キューに関して深く理解し、この設定が QoS ソリューションを満たさない場合のみ、設定を変更する必要があります。

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廃棄します。

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。キュー 2 の廃棄スレッシュホールド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廃棄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 gigabitethernet0/1
Switch(config-if)# queue-set 2
```

show mls qos interface [*interface-id*] **buffers** または **show mls qos queue-set** イネーブル 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
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	キューセットに対するポートをマッピングします。
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

スイッチで着信 IP パケットの Differentiated Services Code Point（DSCP）フィールドを変更する（書き換える）ように設定するには、**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。スイッチでパケットの DSCP フィールドを変更しないようにして、DSCP 透過性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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DSCP 透過性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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

DSCP 透過性は、出力のパケットの DSCP フィールドだけに反映されます。**no mls qos rewrite ip dscp** コマンドを使用して DSCP 透過性をイネーブルにすると、スイッチでは着信パケットの DSCP フィールドは変更されず、発信パケットの DSCP フィールドは、着信パケットの DSCP フィールドと同じになります。

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; サービス品質）を基にします。

DSCP 透過性設定に関係なく、スイッチは、トラフィックのプライオリティを示す Class of Service（CoS; サービス クラス）値の生成に使用するパケットの内部 DSCP 値を変更します。スイッチは、出力キューおよびスレッシュホールドを選択する場合にも内部 DSCP 値を使用します。

たとえば、QoS はイネーブルで、着信パケットの DSCP 値が 32 の場合、スイッチは、ポリシー マップ設定を基に内部 DSCP 値を変更し、内部 DSCP 値を 16 に変更します。DSCP 透過性がイネーブルにされている場合には、発信 DSCP 値は 32（着信値と同一）です。DSCP 透過性がディセーブルの場合、発信 DSCP 値は、内部 DSCP 値を基にするため 16 になります。

例

次の例は、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** イネーブル 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 References** > **Cisco IOS Fundamentals Command Reference, Release 12.2** > **File Management Commands** > **Configuration File Management Commands** を選択してください。

mls qos srr-queue input bandwidth

Shaped Round Robin（SRR）の重みを入力キューに割り当てるには、**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

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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。そのあと SRR は、**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重みの指定どおりに、残りの帯域幅を両方の入力キューに分配し、それらにサービスを提供します。

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、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、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、帯域幅の 10% が割り当てられたプライオリティ 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、最初に 10% の帯域幅が設定済みであるキュー 1（プライオリティ キュー）にサービスを提供します。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
```

show mls qos interface [*interface-id*] **queueing** または **show mls qos input-queue** イネーブル 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
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、CoS 値をキューおよびスレッシュホールド 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 値をキューおよびスレッシュホールド 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; 重み付きテール廃棄）スレッシュホールドのパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定値を表示します。
show mls qos interface queueing	QoS 情報を表示します。

mls qos srr-queue input buffers

入力キューの間で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

構文の説明

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 19% 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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
```

show mls qos interface [*interface-id*] **buffers** または **show mls qos input-queue** イネーブル 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
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	CoS 値を入力キューにマッピングするか、CoS 値をキューおよびスレッショルド 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 値をキューおよびスレッショルド 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; 重み付きテール廃棄）スレッショルドのパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定値を表示します。
show mls qos interface buffers	QoS 情報を表示します。

mls qos srr-queue input cos-map

Class of Service（CoS; サービス クラス）値を入力キューにマッピングしたり、CoS 値をキューおよびスレッシュホールド ID にマッピングしたりするには、**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。デフォルト値に戻す場合は、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

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* に指定できる範囲は 1 ～ 2 です。
cos1...cos8	CoS 値を入力キューにマッピングします。 *cos1...cos8* 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 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキュー スレッシュホールド ID にマッピングします。 *threshold-id* に指定できる範囲は 1 ～ 3 です。 *cos1...cos8* 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 ～ 7 です。

デフォルト

表 2-10 は、デフォルトの CoS 入力キュー スレッシュホールド マップを示しています。

表 2-10　デフォルトの CoS 入力キュー スレッシュホールド マップ

CoS 値	キュー ID ― スレッシュホールド 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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スレッシュホールドが選択されます。

スレッシュホールド 3 の廃棄スレッシュホールド値（%）は事前に定義されています。つまり、queue-full ステートに設定されています。**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; 重み付きテール廃棄）スレッシュホールド値（%）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スレッシュホールド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。

例

次の例では、CoS 値 0 ～ 3 を、入力キュー 1 と廃棄スレッショルド 50% のスレッショルド 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 と廃棄スレッショルド 70% のスレッショルド 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
```

show mls qos maps イネーブル 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
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 値をキューおよびスレッショルド 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 スレッショルドのパーセントを入力キューに割り当てます。
show mls qos maps	QoS マッピング情報を表示します。

mls qos srr-queue input dscp-map

Differentiated Services Code Point（DSCP）値を入力キューにマッピングしたり、DSCP 値をキューおよびスレッショルド ID にマッピングしたりするには、**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。デフォルト値に戻す場合は、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

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* に指定できる範囲は 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 スレッショルド ID にマッピングします。 *threshold-id* に指定できる範囲は 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 2-11 は、デフォルトの DSCP 入力キュー スレッショルド マップを示しています。

表 2-11　デフォルトの DSCP 入力キュー スレッショルド マップ

DSCP 値	キュー ID ― スレッショルド 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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スレッショルドが選択されます。

スレッショルド 3 の廃棄スレッショルド値（%）は事前に定義されています。つまり、queue-full ステートに設定されています。**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; 重み付きテール廃棄）スレッショルド値（%）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スレッショルド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 と廃棄スレッショルド 50% のスレッショルド 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 と廃棄スレッショルド 70% のスレッショルド 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
```

show mls qos maps イネーブル 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
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; サービス クラス）値を入力キューにマッピングするか、CoS 値をキューおよびスレッショルド 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 スレッショルドのパーセントを入力キューに割り当てます。
show mls qos maps	QoS マッピング情報を表示します。

mls qos srr-queue input priority-queue

入力プライオリティ キューを設定し、リングが輻輳している場合には内部リングの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*

構文の説明

queue-id	入力キュー ID です。指定できる範囲は 1 ～ 2 です。
bandwidth *weight*	内部リングの帯域幅の割合（%）です。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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

優先的に処理する必要のあるトラフィック（たとえば、遅延とジッタを最小限に抑える必要のある音声トラフィック）に対してのみプライオリティ キューを使用するべきです。

プライオリティ キューは、内部リングの帯域幅の保証された部分です。これは、オーバーサブスクライブされたリング上に過剰なネットワーク トラフィックが発生した場合（バックプレーンが搬送可能なトラフィック量を超え、キューがいっぱいでフレームを廃棄している状態）に、遅延とジッタを削減します。

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。そのあと SRR は、**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重みの指定どおりに、残りの帯域幅を両方の入力キューに分配し、それらにサービスを提供します。

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、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、帯域幅の 10% が割り当てられたプライオリティ 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、最初に 10% の帯域幅が設定済みであるキュー 1（プライオリティ キュー）にサービスを提供します。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
```

show mls qos interface [*interface-id*] **queueing** または **show mls qos input-queue** イネーブル 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
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、CoS 値をキューおよびスレッショルド 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 値をキューおよびスレッショルド ID にマッピングします。
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッショルドのパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定値を表示します。
show mls qos interface queueing	QoS 情報を表示します。

mls qos srr-queue input threshold

Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッショルド値（%）を入力キューに割り当てるには、**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*

構文の説明

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 スレッショルド値（%）です。各スレッショルド値は、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; サービス品質）がイネーブルなときは、WTD もイネーブルです。

2 つの WTD スレッショルドは、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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

QoS は、CoS/ スレッショルド マップまたは DSCP/ スレッショルド マップを使用して、どの Class of Service（CoS; サービス クラス）値または Differentiated Services Code Point（DSCP）値をスレッショルド 1 とスレッショルド 2 にマッピングするかを判別します。スレッショルド 1 を超えた場合は、スレッショルドを超えなくなるまで、このスレッショルドに割り当てられた CoS または DSCP を持つパケットが廃棄されます。ただし、スレッショルド 2 に割り当てられたパケットは、2 番めのスレッショルド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）廃棄スレッショルドと 1 つの事前設定された（暗黙）廃棄スレッショルド（フル）があります。

CoS/ スレッショルド 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/ スレッショルド 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廃棄スレッショルドを設定する方法を示します。キュー 1 のスレッショルドは 50% と 100%、キュー 2 のスレッショルドは 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
```

show mls qos interface [*interface-id*] **buffers** または **show mls qos input-queue** イネーブル 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
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、CoS 値をキューおよびスレッショルド 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 値をキューおよびスレッショルド 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	入力キューの設定値を表示します。
show mls qos interface buffers	QoS 情報を表示します。

mls qos srr-queue output cos-map

Class of Service（CoS; サービス クラス）値を出力キューにマッピングしたり、CoS 値をキューおよびスレッショルド ID にマッピングしたりするには、**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。デフォルト値に戻す場合は、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

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* に指定できる範囲は 1 ～ 4 です。
cos1...cos8	CoS 値を出力キューにマッピングします。 *cos1...cos8* 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 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキュー スレッショルド ID にマッピングします。 *threshold-id* に指定できる範囲は 1 ～ 3 です。 *cos1...cos8* 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 ～ 7 です。

デフォルト

表 2-12 は、デフォルトの CoS 出力キュー スレッショルド マップを示しています。

表 2-12　デフォルトの CoS 出力キュー スレッショルド マップ

CoS 値	キュー ID ― スレッショルド 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スレッシュホールド 3 の廃棄スレッシュホールド値（%）は事前に定義されています。つまり、queue-full ステートに設定されています。

（注）　出力キュー　デフォルト設定は、たいていの場合に適します。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 Quality of Service（QoS; サービス品質）ソリューションを満たさない場合のみ、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; 重み付きテール廃棄）スレッシュホールド値（%）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スレッシュホールド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。

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 1 ～ 3 を出力キュー 1 とスレッシュホールド ID 1 にマッピングします。キュー 1 の廃棄スレッシュホールド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廃棄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 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 gigabitethernet0/1
Switch(config-if)# queue-set 1
```

show mls qos maps、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** イネーブル 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
mls qos srr-queue output dscp-map	Differentiated Services Code Point（DSCP）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos queue-set output threshold	WTD スレッシュホールドを設定して、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	キューセットに対するポートをマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos maps	QoS 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 Services Code Point（DSCP）値を出力キューにマッピングしたり、DSCP 値をキューおよびスレッショルド ID にマッピングしたりするには、**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。デフォルト値に戻す場合は、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

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* に指定できる範囲は 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 スレッショルド ID にマッピングします。 *threshold-id* に指定できる範囲は 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 出力キュー スレッショルド マップを示しています。

表 2-13　デフォルトの DSCP 出力キュー スレッショルド マップ

DSCP 値	キュー ID ― スレッショルド 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スレッシュホールド 3 の廃棄スレッシュホールド値（%）は事前に定義されています。つまり、queue-full ステートに設定されています。

（注）　出力キュー　デフォルト設定は、たいていの場合に適します。出力キューに関して深く理解し、この設定が QoS ソリューションを満たさない場合のみ、設定を変更する必要があります。

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; 重み付きテール廃棄）スレッシュホールド値（%）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スレッシュホールド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 とスレッシュホールド ID 1 にマッピングします。キュー 1 の廃棄スレッシュホールド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廃棄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 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 gigabitethernet0/1
Switch(config-if)# queue-set 1
```

show mls qos maps、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** イネーブル 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
mls qos srr-queue output cos-map	Class of Service（CoS; サービス クラス）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos queue-set output threshold	WTD スレッシュホールドを設定して、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	キューセットに対するポートをマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos maps	QoS 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 Services Code Point（DSCP）、Class of Service（CoS; サービス クラス）、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。ポートを信頼されない状態に戻す場合は、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**]

構文の説明

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。タグなしパケットの場合は、ポートのデフォルトの 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 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）を使用することにより、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。タグのないパケットについては、ポート デフォルト 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。キーワードが指定されず、コマンドが入力されている場合、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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Quality of Service（QoS; サービス品質）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**]）およびポリシー 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で、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 gigabitethernet0/1
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 が信頼される装置であると指定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust device cisco-phone
```

show mls qos interface イネーブル 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
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 の信頼され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。

monitor session

新たな Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）セッションまたは Remote SPAN（RSPAN; リモート SPAN）送信元もしく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。さらに、ネットワーク セキュリティ装置（Cisco IDS Sensor Appliance など）用のトラフィックが宛先ポートに入力できるようにしたり、既存 SPAN または RSPAN セッションとやり取りするインターフェイスや VLAN（仮想 LAN）を追加または削除したり、SPAN 送信元トラフィックを特定の VLAN に制限（フィルタ）したりします。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場合は、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、encapsulation オプションは無視されます。

monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {**dot1q** ***vlan*** *vlan-id* | **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** {**dot1q** | **replicate**}] [**ingress** {**dot1q** ***vlan*** *vlan-id* | **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*}

構文の説明

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 宛先を指定します。宛先は物理ポートでなければなりません。
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です（タイプとポート番号を含む）。**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 ～ 6 です。
encapsulation dot1q	（任意）宛先インターフェイスが IEEE 802.1Q カプセル化方式を使用することを指定します。 これらのキーワードはローカル SPAN に対してのみ有効です。RSPAN に対しては、RSPAN VLAN ID が元の 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。
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。 これらのキーワードはローカル SPAN に対してのみ有効です。RSPAN に対しては、RSPAN VLAN ID が元の 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）入力トラフィックの転送をイネーブルにします。

dot1q *vlan* *vlan-id*	指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。
untagged *vlan* *vlan-id*	指定された VLAN をデフォルト VLAN として、タグなしでカプセル化された着信パケットを受け入れます。
vlan *vlan-id*	**ingress** キーワードだけが指定された場合に、入力トラフィック用のデフォルト 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 および 1006 ～ 4094 です。 RSPAN VLAN として、VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングと FDDI VLAN 用に予約済み）を指定す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*	トランク送信元ポートのフィルタとして VLAN のリストを指定し、SPAN 送信元トラフィックを特定の VLAN に限定します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
source	SPAN または RSPAN 送信元を指定します。送信元は、物理ポート、ポート チャネル、または VLAN のいずれかになります。
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が指定されなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方をモニタします。
source vlan *vlan-id*	VLAN ID として SPAN 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、またはすべての RSPAN セッションを切断するには、**no monitor session** コマンドに ***all*、*local*、**または ***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たトランク インターフェイスでは、すべての VLAN がモニタされます。

ローカル SPAN 宛先ポートに **encapsulation replicate** が指定されなかった場合、パケットはカプセル化タグなしのネイティブ形式で送信されます。

入力トラフィックの転送は宛先ポートではディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 を使用してモニタすることができます。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することができません。

最大で 2 つのローカル SPAN セッションと RSPAN 送信元セッションを組み合わせて設定できます。1 つのスイッチで合計 66 の SPAN および RSPAN セッションを保持することができます。

1 つのスイッチで最大 64 の宛先ポートを持つことができます。

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。各セッションには複数の宛先ポートを含めることができます。

VLAN ベースの SPAN（VSPAN）を使用して 1 つまたは一連の VLAN 内のネットワーク トラフィックを分析する場合は、送信元 VLAN 内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、モニタ対象の VLAN ID を持つパケットだけが宛先ポートへ送信されます。

1 つのポートまたは VLAN、一連または一定範囲のポートまたは VLAN 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、一連または一定範囲のインターフェイスまたは VLAN 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 グループに属する物理ポートは宛先ポートとして使用できますが、SPAN 宛先である間は EtherChannel グループに参加することはできません。

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 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 はディセーブルです（IEEE 802.1x がポート上で使用できない場合、スイッチはエラー メッセージを戻します）。SPAN または RSPAN 送信元ポートでは IEEE 802.1x をイネーブルにすることができます。

VLAN フィルタリングとは、指定されたトランク送信元ポートの一連の VLAN のネットワーク トラフィックを分析することです。デフォルトでは、トランク送信元ポートのすべての VLAN がモニタされます。**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 だけに限定することができます。

VLAN モニタリングと VLAN フィルタリングは互いに排他的です。VLAN が送信元である場合、VLAN フィルタリングをイネーブルにすることはできません。VLAN フィルタリングが設定されている場合は、VLAN が送信元になることはできません。

ネットワーク セキュリティ装置に対して入力トラフィック転送がイネーブルな場合、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、次の方法で動作するように設定できます。

- その他のキーワードを指定せずに、**monitor session** *session_number* **destination interface** *interface-id* を入力した場合は、出力カプセル化はタグなしで、入力トラフィック転送はイネーブルにはなりません。

- **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**、または **untagged** のいずれであるかによって決まります。
- 他のキーワードを指定せずに **monitor session** *session_number* **destination interface** *interface-id* **encapsulation dot1q** を入力すると、出力カプセル化には IEEE 802.1Q カプセル化方式が使用されます。（これは、ローカル SPAN だけに適用されます。RSPAN は **dot1q カプセル化**をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation dot1q ingress** を入力した場合は、出力カプセル化には IEEE 802.1Q カプセル化が使用され、入力カプセル化はそのあとに続くキーワードが、**dot1q** 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 だけに適用されます。RSPAN は **dot1q カプセル化**をサポートしていません）。
- 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 だけに適用されます。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** 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 だけに適用されます。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 を作成して、送信元ポート 1 と、宛先ポート 2 の送信トラフィックと受信トラフィックの両方をモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

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 gigabitethernet0/2
```

次の例では、既存セッションの SPAN トラフィックを特定の VLAN のみに限定する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 304
```

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 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 gigabitethernet0/1
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、モニタ対象の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 gigabitethernet0/2
```

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 gigabitethernet0/2
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。入力トラフィックにタグはありません。

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
encapsulation replicate ingress untagged vlan 5
```

show monitor イネーブル 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。
show running-config イネーブル 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、出力の終わり近くに表示されます。

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（グローバル コンフィギュレーション）

キーワードなしでスイッチの Multicast VLAN Registration（MVR）をイネーブルにするには、**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。このコマンドはキーワードとともに使用すると、スイッチの MVR モードを設定したり、MVR IP マルチキャスト アドレスを設定したり、ポートをグループ メンバーシップから削除したりする前に、クエリーの返答を待つ最大時間を設定したり、MVR マルチキャスト VLAN（仮想 LAN）を指定したりします。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 [**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*]

構文の説明

group *ip-address*	スイッチの MVR グループ IP マルチキャスト アドレスを静的に設定します。 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 Catalyst 3500 XL 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 MVR メンバー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 メンバー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 メンバー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 メンバーシップ 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 メンバー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 秒すなわち 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

最大 256 個の 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。

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 イネーブル 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 個の連続 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** イネーブル 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
```

show mvr イネーブル 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
mvr（インターフェイス コンフィギュレーション）	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（インターフェイス コンフィギュレーション）

レイヤ 2 ポートを Multicast VLAN Registration（MVR）レシーバーまたは送信元ポートとして設定し、即時脱退機能を設定してポートを IP マルチキャスト VLAN（仮想 LAN）と IP アドレスに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*]]

構文の説明

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 データの受信のみ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 グループのメンバーシップから 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 アドレスを静的に設定します。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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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したい場合には、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 メンバーシップ 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 メンバー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 メンバー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静的に設定します。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動的にマルチキャスト 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。

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 gigabitethernet0/1
Switch(config-if)# mvr type receiver
```

show mvr interface イネーブル EXEC コマンドを使用すると、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できます。

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 gigabitethernet0/1
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 gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

show mvr members イネーブル 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
mvr（グローバル コンフィギュレーション）	スイッチ上で 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 グループに属するすべてのレシーバー ポートを表示します。

pagp learn-method

EtherChannel ポートから受信した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

構文の説明

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し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。アグリゲート ポート ラーニングの場合、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 内の物理ポートでのアドレス ラーニングを指定します。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。チャネルのもう一方のエンドは、特定の宛先 MAC（メディア アクセス制御）または IP アドレスに対してチャネル内の同じ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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

リンクの両方のエンドで同じ学習方式を設定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、Catalyst 2960 スイッチがサポートするのは、アグリゲート ポートでのアドレス ラーニングだけです。**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 コマンドはスイッチのハードウェアには影響しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習のみをサポートするデバイスとの PAgP 相互運用性のために必要とされます。

Catalyst 2960 スイッチのリンク相手が物理ラーナーの場合には、**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 ラーナーに設定し、**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負荷分散方式を送信元　MAC　アドレスに基づく方式に設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような状況でのみ使用してください。

例

次の例では、EtherChannel 内の物理ポートでアドレスを学習するように学習方式を設定する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel 内のポート チャネルでアドレスを学習するように学習方式を設定する方法を示します。

```
Switch(config-if)# pagp learn-method aggregation-port
```

show running-config イネーブル EXEC コマンドまたは **show pagp** *channel-group-number* **internal** イネーブル 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
pagp port-priority	EtherChannel を通るすべてのトラフィックが送信時に経由す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 を通るすべての Port Aggregation Protocol（PAgP）トラフィックが送信時に経由す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 内の未使用のポートがすべてホットスタンバイ モードで、現在選択されているポートとリンクに障害が生じた場合は、それらが動作を引き継ぎます。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

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最高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、Catalyst 2960 スイッチがサポートするのは、アグリゲート ポートでのアドレス ラーニングだけです。**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 コマンドはスイッチのハードウェアには影響しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習のみをサポートするデバイスとの PAgP 相互運用性のために必要とされます。

Catalyst 2960 スイッチのリンク相手が物理ラーナーの場合には、**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 ラーナーに設定し、**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負荷分散方式を送信元 MAC アドレスに基づく方式に設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような状況でのみ使用してください。

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
```

show running-config イネーブル EXEC コマンドまたは **show pagp** *channel-group-number* **internal** イネーブル 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
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（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非 IP トラフィックが転送されるのを許可するには、**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場合は、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ていますが、一致条件としてはサポートされていません。

構文の説明

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 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; 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、ハードウェアでのみ実行可能です。**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 2-14 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 2-14　IPX フィルタリング条件

IPX カプセル化タイプ		
Cisco IOS 名	**Novell 名**	**フィルタ条件**
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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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; アクセス制御エントリ）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。すなわち、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
```

show access-lists イネーブル 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
deny（MAC アクセス リスト コンフィギュレーション）	条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
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

トラフィックを分類するため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場合は、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**}]

構文の説明

rate-bps	平均トラフィック伝送速度をビット / 秒（bps）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廃棄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 Services 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 個のポリサーと 1 個の **no** 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最大ポリサー数は 64 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。イネーブル 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。

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 Mbps を超えた場合に、ポリサーがパケットを廃棄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** イネーブル 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 の信頼されるポートに適用します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
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; サービス品質）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

同じポリシー マップ内の複数のクラスに集約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*

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 個のポリサーと 1 個の **no** 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最大ポリサー数は 64 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。イネーブル EXEC モードに戻るには、**end** コマンドを使用します。

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 1000000 8000 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
```

show mls qos aggregate-policer イネーブル 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
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; サービス品質）集約ポリサー設定を表示します。

policy-map

複数の物理ポートに適用できるポリシー 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 モードに戻る場合は、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*

構文の説明

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 Services 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; サービス クラス）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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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。詳細は、「class」（p.2-27）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。イネーブル 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** コマンドを入力しても、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。

サポートされるポリシー マップは、入力ポートに 1 つのみです。同じポリシー マップを複数のポートに適用できます。

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。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 Mbps、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 1000000 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 1000000 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** イネーブル 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比較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 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

構文の説明

dst-ip	負荷分散は宛先ホスト IP アドレスに基づいています。
dst-mac	負荷分散は宛先ホスト MAC（メディア アクセス制御）アドレスに基づいています。同じ宛先へのパケットは同じポートで送信されますが、異なる宛先へのパケットはチャネル内の異なるポートで送信されます。
src-dst-ip	負荷分散は送信元および宛先ホスト IP アドレスに基づいています。
src-dst-mac	負荷分散は送信元および宛先ホスト MAC アドレスに基づいています。
src-ip	負荷分散は送信元ホスト IP アドレスに基づいています。
src-mac	負荷分散は送信元ホスト MAC アドレスに基づいています。異なるホストからのパケットはチャネル内の異なるポートを使用しますが、同じホストからのパケットは同じ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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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、このリリースのソフトウェア 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
```

show running-config イネーブル EXEC コマンドまたは **show etherchannel load-balance** イネーブル 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
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。

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

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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 の重みを無効にします。

```
Switch(config)# interface gigabitethernet0/2
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。shaped モードは、shared モードを無効にします。

```
Switch(config)# interface gigabitethernet0/2
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** イネーブル 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 queueing	（任意）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 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出力キュー 4 つで帯域幅をシェーピングします。
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出力キュー 4 つで帯域幅を共有します。

queue-set

ポートをキューセットに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*

構文の説明

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

コマンド履歴

リリース	変更内容
12.2(25)FX	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 gigabitethernet0/1
Switch(config-if)# queue-set 2
```

show mls qos interface [*interface-id*] **buffers** イネーブル 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
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; 重み付きテール廃棄）スレッシュホールドを設定し、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	QoS 情報を表示します。

rcommand

Telnet セッションを開始し、クラスタ コマンド スイッチからクラスタ メンバー スイッチでコマンドを実行するには、**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場合は、**exit** コマンドを入力します。

rcommand {*n* | **commander** | **mac-address** *hw-addr*}

構文の説明

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）アドレスです。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチに対してのみ使用できます。

スイッチがクラスタ コマンド スイッチであるがクラスタ メンバー スイッチ *n* が存在しない場合、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** イネーブル 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、クラスタ 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 レベルでリモート装置にアクセスします。*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 スイッチへのアクセスはユーザ レベルとなります。

Standard Edition ソフトウェアが稼働している 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 ソフトウェアが稼働しているクラスタ 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 ソフトウェアが稼働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引き継ぐため、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。

remote-span

VLAN（仮想 LAN）を Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）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 から削除する場合は、このコマンドの **no** 形式を使用します。

remote-span

no remote-span

構文の説明

このコマンドには、引数またはキーワードはありません。

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）

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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** イネーブル 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; VLAN トランキング プロトコル）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）。

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 トラフィックのみが流れます。
- Spanning-Tree Protocol（STP; スパニングツリー プロトコル）は RSPAN VLAN 内では稼働できますが、RSPAN 宛先ポートでは稼働しません。

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; スイッチド ポート アナライザ）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（グローバル コンフィギュレーション）	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

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** イネーブル EXEC コマンドを使用します。

renew ip dhcp snooping database [{**flash**:/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **nvram:**/*filename* | **rcp:**//*user*@*host*/*filename* | **tftp:**//*host*/*filename*}] [**validation none**]

構文の説明

flash:/*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 メモリ内にあることを指定します。
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 サーバ上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 内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）サーバ上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 サーバ上にあることを指定します。
validation none	（任意）URL で指定されたバインディング ファイル内のエントリに対してスイッチが Cyclic Redundancy Check（CRC; 巡回冗長検査）の確認を行わないことを指定します。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

URL を指定しない場合は、スイッチは設定済み URL からのファイルの読み出しを試行します。

例

次の例では、ファイル内の CRC 値をチェックすることなく 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
```

show ip dhcp snooping database イネーブル 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
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 データベース情報を設定します。
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。

rmon collection stats

イーサネット グループ統計情報を収集するには、**rmon collection stats** 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。イーサネット グループ統計情報には、ブロードキャストおよびマルチキャスト パケットについての使用統計情報、および Cyclic Redundancy Check（CRC; 巡回冗長検査）アライメント エラーおよびコリジョンについてのエラー統計情報が含まれます。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。

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *index* [**owner** *name*]

構文の説明

index	Remote Network Monitoring（RMON）収集制御インデックスです。指定できる範囲は 1 ～ 65535 です。
owner *name*	（任意）RMON 収集の所有者です。

デフォルト

RMON 統計情報収集はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

RMON 統計情報収集コマンドはハードウェア カウンタに基づいています。

例

次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

show rmon statistics イネーブル 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
show rmon statistics	RMON 統計情報を表示します。 構文情報については、**Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands** を選択してください。

sdm prefer

Switch Database Management（SDM）リソース割り当てで使用されるテンプレートを設定するには、**sdm prefer** グローバル コンフィギュレーション コマンドを使用します。テンプレートは、アプリケーションで使用される機能を最適にサポートするようにシステム リソースを割り当てるために使用できます。デフォルト テンプレートに戻す場合は、このコマンドの **no** 形式を使用します。

sdm prefer {**default** | **qos**}

no sdm prefer

構文の説明

default	すべての機能に対してバランスを取ります。
qos	最大限のシステム リソースを Quality of Service（QoS; サービス品質）Access Control Entry（ACE; アクセス制御エントリ）に割り当てます。

デフォルト

デフォルト テンプレートはすべての機能に対してバランスを取ります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

設定を有効にするには、スイッチをリロードする必要があります。

reload イネーブル EXEC コマンドを入力する前に **show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドは現在使用中のテンプレートおよびリロード後にアクティブになるテンプレートを表示します。

スイッチをデフォルト デスクトップ テンプレートに設定するには、**no sdm prefer** コマンドを使用します。

各テンプレートでサポートされる、各リソースの概略数を表 2-15 に示します。

表 2-15　各テンプレートで許容される機能リソースの概略数

リソース	デフォルト	QoS
ユニキャスト MAC アドレス	8 K	8 K
IPv4 IGMP グループ	256	256
IPv4 MAC QoS ACE	128	384
IPv4 MAC セキュリティ ACE	384	128

例

次の例では、QoS テンプレートの使用方法を示します。

```
Switch(config)# sdm prefer qos
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show sdm prefer** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show sdm prefer	現在使用中の SDM テンプレートの表示、または使用可能なテンプレートを機能ごとの概略リソース割り当てとともに表示します。

service password-recovery

パスワード回復メカニズム（デフォルト）をイネーブルにするには、**service password-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。このメカニズムでは、スイッチに物理的にアクセスするエンド ユーザは、スイッチの電源投入時に **Mode** ボタンを押してブート プロセスを中断し、新しいパスワードを割り当てることができます。パスワード回復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。パスワード回復メカニズムがディセーブルになると、ユーザがシステムをデフォルト設定に戻すことに同意した場合のみブート プロセスを中断できます。

service password-recovery

no service password-recovery

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

パスワード回復メカニズムはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

システム管理者が **no service password-recovery** コマンドを使用すると、エンド ユーザがシステムをデフォルト設定に戻すことに同意するだけでパスワードをリセット可能にすることにより、パスワード回復機能の一部をディセーブルにできます。

パスワード回復手順を実行するには、スイッチに物理的にアクセスするユーザはスイッチの電源投入時、およびポート 1X の上にある LED が消灯してから 1 ～ 2 秒後に **Mode** ボタンを押します。ボタンを放すと、システムは初期化を続けます。パスワード回復メカニズムをディセーブルにした場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

ユーザがシステムをデフォルト設定にリセットしない場合、**Mode** ボタンを押さない場合と同じように通常の起動プロセスを続けます。ユーザがシステムをデフォルト設定にリセットする場合、フラッシュ メモリのコンフィギュレーション ファイルが削除され、VLAN（仮想 LAN）データベース ファイル、*flash:vlan.dat* がある場合にはこのファイルも削除されます。

（注）　**no service password-recovery** コマンドを使用してエンド ユーザがパスワードにアクセスするのを制御する場合、エンド ユーザがパスワード回復手順を実行してシステムをデフォルトに戻すとき、スイッチから離れた場所にコンフィギュレーション ファイルのコピーを保存することを推奨します。コンフィギュレーション ファイルのコピーをスイッチ上に保持しないでください。

スイッチが VTP トランスペアレント モードで稼働している場合には、vlan.dat ファイルのコピーもスイッチから離れた場所に保存することを推奨します。

show version イネーブル EXEC コマンドを入力すると、パスワード回復がイネーブルかまたはディセーブルかを確認できます。

例

次の例では、システムをデフォルト設定に戻すことに同意するだけでユーザがパスワードをリセットできるように、スイッチでパスワード回復をディセーブルにする方法を示します。

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

関連コマンド

コマンド	説明
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。

service-policy

policy-map コマンドで定義されたポリシー マップを、物理ポートの入力に適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で **service-policy** インターフェイス コンフィギュレーション コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

構文の説明

input *policy-map-name*	物理ポートの入力に、指定したポリシー マップを適用します。

（注）　**history** 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ていますが、サポートされていません。このキーワードが収集した統計情報は無視します。**output** キーワードもサポートされていません。

デフォルト

ポートにポリシー マップは適用されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ポリシー マップは物理ポート上に設定できます。

ポリシー マップは物理ポート上の着信トラフィックに適用できます。

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**]）およびポリシー 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で、前の設定が上書きされます。

例

次の例では、物理入力ポートに *plcmap1* を適用します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから *plcmap2* を削除します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy input plcmap2
```

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

関連コマンド

コマンド	説明
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
show policy-map	QoS ポリシー マップを表示します。
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。

set

パケットに Differentiated Services Code Point（DSCP）値、または IP precedence 値を設定して、IP トラフィックを分類するには、**set** 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。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

set {**dscp** *new-dscp* | [**ip**] **precedence** *new-precedence*}

no set {**dscp** *new-dscp* | [**ip**] **precedence** *new-precedence*}

構文の説明

dscp *new-dscp*	分類されたトラフィックに割り当てられる新しい DSCP 値です。指定できる範囲は、0 ～ 63 です。また、一般的な値にニーモニック名を入力できます。
[**ip**] **precedence** *new-precedence*	分類されたトラフィックに割り当てられる新しい IP precedence 値です。指定できる範囲は 0 ～ 7 です。また、一般的な値にニーモニック名を入力できます。

デフォルト

トラフィックの分類は定義されていません。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	**ip** キーワードはオプションです。

使用上の注意事項

set ip dscp コマンドを使用した場合には、スイッチはこのコマンドをスイッチ コンフィギュレーション内の **set dscp** コマンドに変換します。**set ip dscp** コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。

Cisco IOS リリース 12.2(25)SED 以降では、**set ip precedence** コマンドまたは **set precedence** コマンドを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。

同じポリシーマップ内では、**set** コマンドと **trust** ポリシーマップ クラス コンフィギュレーション コマンドを同時に指定できません。

set dscp *new-dscp* コマンドまたは **set ip precedence** *new-precedence* コマンドについては、一般的な値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set ip precedence critical** コマンドを入力できます。これは **set ip precedence 5** コマンドの入力と同じです。サポートされているニーモニック名について、コマンドラインのヘルプ ストリングを表示するには、**set dscp ?** コマンドまたは **set ip precedence ?** コマンドを入力します。

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。イネーブル EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、ポリサーが設定されていないすべてのFTPトラフィックにDSCP値10を割り当てます。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

設定を確認するには、**show policy-map** イネーブル 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。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
show policy-map	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。

setup

スイッチを初期設定にするには、**setup** イネーブル EXEC コマンドを使用します。

setup

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

setup コマンドを使用する場合、次の情報を確認します。

- IP アドレスとネットワーク マスク
- 使用する環境のパスワード設定方法
- スイッチをクラスタ コマンド スイッチおよびクラスタ名として使用します。

setup コマンドを入力すると、System Configuration Dialog と呼ばれるインタラクティブ ダイアログが表示されます。コンフィギュレーション プロセスとプロンプトにより、情報の説明を行います。各プロンプトの次のカッコ内の値は、**setup** コマンド機能または **configure** イネーブル EXEC コマンドによって最後に設定されたデフォルト値です。

各プロンプトでは、ヘルプを提供しています。ヘルプにアクセスするには、プロンプトの疑問符（**?**）キーを押します。

System Configuration Dialog で変更せず、また実行せずにイネーブル EXEC プロンプトに戻るには、**Ctrl-C** を押します。

変更を完了すると、セットアップ プログラムは、セットアップ セッション中に作成したコンフィギュレーション コマンド スクリプトを表示します。設定を NVRAM（不揮発性 RAM）に保存する、あるいは設定を保存せずにセットアップ プログラムまたはコマンドライン プロンプトに戻ることができます。

例

次に **setup** コマンドの出力例を示します。

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

```
Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet0/1         unassigned      YES unset  up                    up

GigabitEthernet0/2         unassigned      YES unset  up                    down

（テキスト出力は省略）

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

Would you like to enable as a cluster command switch? [yes/no]: yes

Enter cluster name: cluster-name

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!

cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.
```

```
[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

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。
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。

setup express

Express Setup モードをイネーブルにするには、**setup express** 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。Express Setup モ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。

setup express

no setup express

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Express Setup はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Express Setup が新しい（未設定の）スイッチでイネーブルの場合、Mode ボタンを 2 秒間押して Express Setup を起動します。IP アドレス 10.0.0.1 を使用するとイーサネット ポート経由でスイッチにアクセスできます。そのあと、スイッチを Web ベースの Express Setup プログラム、または CLI（コマンドライン インターフェイス）ベースのセットアップ プログラムで設定できます。

設定したスイッチで Mode ボタンを 2 秒間押すと、Mode ボタンの上にある LED が点滅し始めます。Mode ボタンを計 10 秒間押した場合、スイッチ コンフィギュレーションは削除され、スイッチを再起動します。Web ベースの Express Setup プログラム、または CLI ベースのセットアップ プログラムによって、スイッチを新しく設定できます。

（注）　（CLI ベースのセットアップ プログラムの始めで *no* を入力することを含む）スイッチ コンフィギュレーションの変更を行うとすぐに、Express Setup によるコンフィギュレーションを利用できなくなります。Mode ボタンを 10 秒間押し続けると、再度 Express Setup のみを稼働できます。これにより、スイッチ コンフィギュレーションは削除され、スイッチを再起動します。

Express Setup がスイッチでアクティブな場合、**write memory** または **copy running-configuration startup-configuration** イネーブル EXEC コマンドを入力すると Express Setup は不活性となります。IP アドレス 10.0.0.1 はスイッチで無効となり、この IP アドレスを使用した接続も終了します。

no setup express コマンドの主な目的は、Mode ボタンを 10 秒間押すことによるスイッチ コンフィギュレーションの削除を防ぐことです。

例

次の例では、Express Setup モードをイネーブルにする方法を示します。

```
Switch(config)# setup express
```

Mode ボタンを押すと、Express Setup モードがイネーブルであることを確認できます。

- 未設定のスイッチでは、Mode ボタンの上にある LED は 3 秒後にグリーンになります。
- 設定したスイッチでは、モードLEDは2秒後に点滅し始め、10秒後に固定のグリーンになります。

注意　Mode ボタンを計 10 秒間*押し続けた*場合、コンフィギュレーションは削除され、スイッチを再起動します。

次の例では、Express Setup モードをディセーブルにする方法を示します。

```
Switch(config)# no setup express
```

Mode ボタンを押すと、Express Setup モードがディセーブルであることを確認できます。Express Setup モードがスイッチでイネーブルでない場合、モード LED は固定のグリーンにならない、またはグリーンに点滅し始めます。

関連コマンド

コマンド	説明
show setup express	Express Setup モードがアクティブな場合に表示します。

show access-lists

スイッチに設定された Access Control List（ACL; アクセス制御リスト）を表示するには、**show access-lists** イネーブル EXEC コマンドを使用します。

show access-lists [*name* | *number* | **hardware counters | ipc**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

name	（任意）ACL の名前です。
number	（任意）ACL の番号です。指定できる範囲は 1 ～ 2699 です。
hardware counters	（任意）切り替えられ、ルーティングされたパケットのグローバル ハードウェア ACL 統計情報を表示します。
ipc	（任意）Interprocess Communication（IPC）プロトコル アクセス リスト コンフィギュレーションのダウンロード情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

（注） **rate-limit** 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ていますが、サポートされていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチは IP 標準および拡張アクセス リストのみをサポートします。したがって、1 ～ 199 と 1300 ～ 2699 のみが許可されます。

このコマンドでは、設定済みの MAC ACL も表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show access-lists** コマンドの出力を示します。

```
Switch# show access-lists
Standard IP access list 1
    10 permit 1.1.1.1
    20 permit 2.2.2.2
    30 permit any
    40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
    10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    10 permit 10.10.10.10
Extended IP access list 121
    10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny   ip any any
    10 deny ip any host 19.19.11.11
    20 deny ip any host 10.11.12.13
    Dynamic Cluster-NAT permit ip any any
    10 permit ip host 10.99.100.128 any
    20 permit ip host 10.46.22.128 any
    30 permit ip host 10.45.101.64 any
    40 permit ip host 10.45.20.64 any
    50 permit ip host 10.213.43.128 any
    60 permit ip host 10.91.28.64 any
    70 permit ip host 10.99.75.128 any
    80 permit ip host 10.38.49.0 any
```

次の例では、**show access-lists hardware counters** コマンドの出力を示します。

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0
```

```
L2 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 232983
    Forwarded:           All bytes count: 16825661
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0

L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

関連コマンド

コマンド	説明
access-list	スイッチに標準または拡張番号アクセス リストを設定します。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	スイッチに指定された IP アクセス リストを設定します。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。
mac access-list extended	スイッチに、指定されたまたは番号のついた MAC（メディア アクセス制御）アクセス リストを設定します。

show archive status

HTTP または TFTP プロトコルでスイッチにダウンロードされた新しいイメージのステータスを表示するには、**show archive status** イネーブル EXEC コマンドを使用します。

show archive status [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

archive download-sw イネーブル EXEC コマンドを使用してイメージを TFTP サーバにダウンロードする場合、**archive download-sw** コマンドの出力にはダウンロードのステータスが表示されます。

TFTP サーバがない場合、HTTP を使用してイメージをダウンロードするには、Network Assistant または組み込みデバイス マネージャを使用します。**show archive status** コマンドは、ダウンロードの進捗を表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

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

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

関連コマンド

コマンド	説明
archive download-sw	新しいイメージを TFTP サーバからスイッチにダウンロードします。

show auto qos

Automatic QoS（auto-QoS）がイネーブルのインターフェイスで入力された Quality of Service（QoS; サービス品質）コマンドを表示するには、**show auto qos** ユーザ EXEC コマンドを使用します。

show auto qos [**interface** [*interface-id*]]

構文の説明

interface [*interface-id*]	（任意）指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。指定できるインターフェイスとして、物理ポートも含まれます。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show auto qos コマンドの出力には、各インターフェイスに入力された auto-QoS コマンドのみが表示されます。**show auto qos interface** *interface-id* コマンド出力は、特定のインターフェイスに入力された auto-QoS コマンドを表示します。

auto-QoS 設定およびユーザ変更を表示する場合は、**show running-config** イネーブル EXEC コマンドを使用します。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

例

次の例では、**auto qos voip cisco-phone** および **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の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
GigabitEthernet0/4
auto qos voip cisco-softphone

GigabitEthernet0/5
auto qos voip cisco-phone

GigabitEthernet0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface** *interface-id* command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch> show auto qos interface gigabitethernet 0/5
GigabitEthernet0/5
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** および **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の **show running-config** イネーブル EXEC コマンドの出力を示します。

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3  af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
   set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
   set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
...
```

```
!
interface GigabitEthernet0/4
 switchport mode access
 switchport port-security maximum 400
 service-policy input AutoQoS-Police-SoftPhone
 speed 100
 duplex half
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 auto qos voip cisco-softphone
!
interface GigabitEthernet0/5
 switchport mode access
 switchport port-security maximum 1999
 speed 100
 duplex full
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface GigabitEthernet0/6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 2
 switchport mode access
 speed 10
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
(テキスト出力は省略)
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show auto qos interface fastethernet0/2
FastEthernet0/2
auto qos voip cisco-phone
```

次の例では、auto-QoS がスイッチでディセーブルの場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
AutoQoS not enabled on any interface
```

次の例では、auto-QoS がインターフェイスでディセーブルの場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet0/1
AutoQoS is disabled
```

関連コマンド

コマンド	説明
auto qos voip	QoS ドメイン内の Voice over IP(VoIP) に QoS を自動設定します。
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。

show boot

ブート環境変数の設定を表示するには、**show boot** イネーブル EXEC コマンドを使用します。

show boot [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show boot** コマンドの出力を示します。表 2-16 に、表示される各フィールドの説明を示します。

```
Switch# show boot
BOOT path-list: flash:c2960-lanbase-mz.122-25.FX.bin
Config file:         flash:/config.text
Private Config file: flash:/private-config
Enable Break:        no
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
      buffer size:   32768
```

表 2-16　show boot のフィールドの説明

フィールド	説明
BOOT path-list	自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリストを表示します。 BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に見つかった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。 BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。
Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Private Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Enable Break	起動中のブレークがイネーブルか、またはディセーブルかを表示します。yes、on、または 1 に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押して、自動起動プロセスを中断することができます。
Manual Boot	スイッチが自動で起動するか、または手動で起動するかを表示します。no または 0 に設定されている場合、ブート ローダはシステムを自動的に起動しようとします。それ以外に設定されている場合は、ブート ローダ モードから手動でスイッチを起動する必要があります。
Helper path-list	ブート ローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを表示します。ヘルパー ファイルは、ブート ローダの機能を拡張したり、パッチを当てます。
NVRAM/Config file buffer size	メモリにコンフィギュレーション ファイルのコピーを保持するために Cisco IOS が使用するバッファのサイズを表示します。コンフィギュレーション ファイルは、バッファ サイズの割り当てを超えてはなりません。

関連コマンド

コマンド	説明
boot config-file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を指定します。
boot enable-break	自動起動プロセスを中断することができます。
boot manual	次の起動サイクル時の手動スイッチ起動をイネーブルにします。
boot private-config-file	Cisco IOS がプライベート コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を指定します。
boot system	次の起動サイクル中にロードする Cisco IOS イメージを指定します。

show cable-diagnostics tdr

Time Domain Reflector（TDR）結果を表示するには、**show cable-diagnostics tdr** イネーブル EXEC コマンドを使用します。

show cable-diagnostics tdr interface *interface-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	TDR が実行されているインターフェイスを指定します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

TDR は、10/100 および 10/100/1000 の銅線のイーサネット ポートでのみサポートされます。SFP モジュール ポートではサポートされません。TDR 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。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi0/2     auto  Pair A     0    +/- 2  meters N/A         Open

              Pair B     0    +/- 2  meters N/A         Open
              Pair C     0    +/- 2  meters N/A         Open
              Pair D     0    +/- 2  meters N/A         Open
```

表 2-17 に、**show cable-diagnostics tdr** コマンドで出力されるフィールドの説明を示します。

表 2-17　show cable-diagnostics tdr コマンドで出力されるフィールドの説明

フィールド	説明
Interface	TDR が実行されたインターフェイス
Speed	接続速度
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名

表 2-17　show cable-diagnostics tdr コマンドで出力されるフィールドの説明（続き）

フィールド	説明
Pair length	使用するスイッチについて、問題が発生したケーブルの場所。次の場合に、TDR は場所を特定します。 • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mbps である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合にのみ、TDR はリモート ペアについて確認します。
Pair status	TDR が稼働しているワイヤ ペアのステータス • Normal — ワイヤ ペアが正しく接続されています。 • Not completed — テストが実行され、まだ完了していません。 • Not supported — インターフェイスは TDR をサポートしません。 • Open — ワイヤ ペアが断線しています。 • Shorted — ワイヤ ペアがショートしています。

次の例では、TDR が動作しているときの **show interface** *interface-id* コマンドの出力を示します。

```
Switch# show interface gigabitethernet0/2
gigabitethernet0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が動作していないときの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
% TDR test was never issued on Gi0/2
```

インターフェイスが TDR をサポートしていない場合、次のメッセージが表示されます。

```
% TDR test is not supported on switch 1
```

関連コマンド

コマンド	説明
test cable-diagnostics tdr	インターフェイスで TDR をイネーブルにし、実行します。

show class-map

show class-map ユーザ EXEC コマンドは、トラフィックを分類するための一致基準を定義する Quality of Service（QoS; サービス品質）クラス マップを表示します。

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

class-map-name	（任意）指定されたクラス マップの内容を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show class-map** コマンドの出力を示します。

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

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比較に使用されるクラス マップを作成します。
match（クラスマップ コンフィギュレーション）	トラフィックを分類するための一致条件を定義します。

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するには、**show cluster** ユーザ EXEC コマンドを使用します。このコマンドは、クラスタ コマンド スイッチとクラスタ メンバー スイッチ上だけで入力します。

show cluster [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

クラスタのメンバーでないスイッチに対してこのコマンドを入力すると、エラー メッセージ `Not a management cluster member` が表示されます。

クラスタ メンバー スイッチに対してこのコマンドを入力すると、クラスタ コマンド スイッチの ID、そのスイッチ メンバーの番号、およびクラスタ コマンド スイッチとの接続状態が表示されます。

クラスタ コマンド スイッチに対してこのコマンドを入力すると、クラスタ名およびメンバーの総数が表示されます。また、ステータス変更後のクラスタのステータスおよび時間も表示されます。冗長構成がイネーブルの場合は、プライマリおよびセカンダリ コマンド スイッチの情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、アクティブなクラスタ コマンド スイッチに対して **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 2 minutes
        Redundancy:                     Enabled
                Standby command switch: Member 1
                Standby Group:          Ajang_standby
                Standby Group Number:   110
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

次の例では、クラスタ メンバー スイッチに対して **show cluster** コマンドを入力した場合の出力を示します。

```
Switch1> show cluster
Member switch for cluster "hapuna"
        Member number:                  3
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

次の例では、スタンバイ クラスタ コマンド スイッチとして設定されたクラスタ メンバー スイッチに対して **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  3 (Standby command switch)
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

次の例では、メンバー 1 との接続が切断されているクラスタ コマンド スイッチに対して **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 5 minutes
        Redundancy:                     Disabled
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

次の例では、クラスタ コマンド スイッチとの接続が切断されているクラスタ メンバー スイッチに対して **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  <UNKNOWN>
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

関連コマンド

コマンド	説明
cluster enable	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、およびオプションとしてメンバー番号を割り当てます。
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。

show cluster candidates

候補スイッチのリストを表示するには、**show cluster candidates** イネーブル EXEC コマンドを使用します。

show cluster candidates [**detail** | **mac-address** *H.H.H.*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）すべての候補に関する詳細を表示します。
mac-address *H.H.H.*	（任意）クラスタ候補の MAC（メディア アクセス制御）アドレスです。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチに対してのみ使用できます。

スイッチがクラスタ コマンド スイッチでない場合は、プロンプトに空行が表示されます。

出力内の SN は、*スイッチ メンバー番号* を意味します。SN 列の値が E の場合、スイッチは拡張検出によって検出されています。SN 列の値が E でない場合、*スイッチ メンバー番号* のスイッチは、候補スイッチのアップストリーム側ネイバです。ホップ数は、クラスタ コマンド スイッチから候補スイッチまでのデバイス数です。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates
                                                                  |---Upstream---|
       MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC
       00d0.7961.c4c0 StLouis-2    WS-C2960-12T     Gi0/1        2   1  Fa0/11
       00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL      Fa0/7        1   0  Fa0/24
       00e0.1e7e.be80 1900_Switch  1900             3        0   1   0  Fa0/11
       00e0.1e9f.7a00 Surfers-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
       00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL      Fa0/4        1   0  Fa0/7
       00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
```

次の例では、クラスタ コマンド スイッチに直接接続されクラスタ メンバー スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C2960-12T
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Gi0/1   FEC number:
        Upstream port:          GI0/11  FEC Number:
Hops from cluster edge: 1
        Hops from command device: 1
```

次の例では、クラスタ エッジからのホップ数が 3 であるクラスタ メンバー スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
        Device type:            cisco WS-C2912MF-XL
        Upstream MAC address:   0010.7bb6.1cd4
        Local port:             Fa2/1   FEC number:
        Upstream port:          Fa0/24  FEC Number:
        Hops from cluster edge: 3
        Hops from command device: -
```

次の例では、**show cluster candidates detail** コマンドの出力を示します。

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C3512-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 1)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
        Device type:            cisco 1900
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 2)
        Local port:             3       FEC number: 0
        Upstream port:          Fa0/11  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
        Device type:            cisco WS-C2924-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 3)
        Local port:             Fa0/5   FEC number:
        Upstream port:          Fa0/3   FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
```

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 members	クラスタ メンバーに関する情報を表示します。

show cluster members

クラスタ メンバーに関する情報を表示するには、**show cluster members** イネーブル EXEC コマンドを使用します。

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

n	（任意）クラスタ メンバーを識別する番号です。指定できる範囲は 0 ～ 15 です。
detail	（任意）すべてのクラスタ メンバーに関する詳細を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、クラスタ コマンド スイッチに対してのみ使用できます。

クラスタ内にメンバーがない場合は、プロンプトに空行が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show cluster members** コマンドの出力を示します。出力内の SN は、*スイッチ番号* を意味します。

```
Switch# show cluster members
                                              |---Upstream---|
SN MAC Address    Name          PortIf FEC Hops   SN PortIf  FEC  State
0  0002.4b29.2e00 StLouis1                 0                    Up   (Cmdr)
1  0030.946c.d740 tal-switch-1 Fa0/13      1     0  Gi0/1       Up
2  0002.b922.7180 nms-2820     10      0   2     1  Fa0/18      Up
3  0002.4b29.4400 SanJuan2     Gi0/1       2     1  Fa0/11      Up
4  0002.4b28.c480 GenieTest    Gi0/2       2     1  Fa0/9       Up
```

次の例では、クラスタ メンバー 3 に対する **show cluster members** の出力を示します。

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C2960
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/1   FEC number:
        Upstream port:          GI0/11  FEC Number:
        Hops from command device: 2
```

次の例では、**show cluster members detail** コマンドの出力を示します。

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
        Device type:            cisco WS-C2960
        MAC address:            0002.4b29.2e00
        Upstream MAC address:
        Local port:                     FEC number:
        Upstream port:                  FEC Number:
        Hops from command device: 0
Device 'tal-switch-14' with member number 1
        Device type:            cisco WS-C3548-XL
        MAC address:            0030.946c.d740
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Fa0/13  FEC number:
        Upstream port:          Gi0/1   FEC Number:
        Hops from command device: 1
Device 'nms-2820' with member number 2
        Device type:            cisco 2820
        MAC address:            0002.b922.7180
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             10      FEC number: 0
        Upstream port:          Fa0/18  FEC Number:
        Hops from command device: 2
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C2960
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/1   FEC number:
        Upstream port:          Fa0/11  FEC Number:
        Hops from command device: 2
Device 'GenieTest' with member number 4
        Device type:            cisco SeaHorse
        MAC address:            0002.4b28.c480
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/2   FEC number:
        Upstream port:          Fa0/9   FEC Number:
        Hops from command device: 2
Device 'Palpatine' with member number 5
        Device type:            cisco WS-C2924M-XL
        MAC address:            00b0.6404.f8c0
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Gi2/1   FEC number:
        Upstream port:          Gi0/7   FEC Number:
        Hops from command device: 1
```

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 controllers cpu-interface

CPU ネットワーク インターフェイス Application Specific Integrated Circuit（ASIC; 特定用途向け IC）のステートを表示し、CPU に達するパケットに関する統計情報を送受信するには、**show controllers cpu-interface** イネーブル EXEC コマンドを使用します。

show controllers cpu-interface [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチのトラブルシューティングを行うシスコのテクニカル サポート担当者にとって有益となる情報を表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show controllers cpu-interface** コマンドの出力の一部を示します。

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
----------------- ---------- ---------- ---------- ----------
rpc               4523063    0          0          0
stp               1545035    0          0          0
ipc               1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol       79596      0          0          0
remote console    0          0          0          0
sw forwarding     5756       0          0          0
host              225646     0          0          0
broadcast         46472      0          0          0
cbt-to-spt        0          0          0          0
igmp snooping     68411      0          0          0
icmp              0          0          0          0
logging           0          0          0          0
rpf-fail          0          0          0          0
queue14           0          0          0          0
cpu heartbeat     1710501    0          0          0

Supervisor ASIC receive-queue parameters
----------------------------------------
 queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
 queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
 queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
 queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

(テキスト出力は省略)
```

```
Supervisor ASIC Mic Registers
-----------------------------
MicDirectPollInfo               80000800
MicIndicationsReceived          00000000
MicInterruptsReceived           00000000
MicPcsInfo                      0001001F
MicPlbMasterConfiguration       00000000
MicRxFifosAvailable             00000000
MicRxFifosReady                 0000BFFF
MicTimeOutPeriod:       FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

(テキスト出力は省略)

MicTransmitFifoInfo:
Fifo0:    StartPtrs:     038C2800        ReadPtr:        038C2C38
         WritePtrs:      038C2C38        Fifo_Flag:      8A800800
         Weights:        001E001E
Fifo1:   StartPtr:       03A9BC00        ReadPtr:        03A9BC60
         WritePtrs:      03A9BC60        Fifo_Flag:      89800400
         writeHeaderPtr: 03A9BC60
Fifo2:   StartPtr:       038C8800        ReadPtr:        038C88E0
         WritePtrs:      038C88E0        Fifo_Flag:      88800200
         writeHeaderPtr: 038C88E0
Fifo3:   StartPtr:       03C30400        ReadPtr:        03C30638
         WritePtrs:      03C30638        Fifo_Flag:      89800400
         writeHeaderPtr: 03C30638
Fifo4:   StartPtr:       03AD5000        ReadPtr:        03AD50A0
         WritePtrs:      03AD50A0        Fifo_Flag:      89800400
         writeHeaderPtr: 03AD50A0
Fifo5:   StartPtr:       03A7A600        ReadPtr:        03A7A600
         WritePtrs:      03A7A600        Fifo_Flag:      88800200
         writeHeaderPtr: 03A7A600
Fifo6:   StartPtr:       03BF8400        ReadPtr:        03BF87F0
         WritePtrs:      03BF87F0        Fifo_Flag:      89800400

(テキスト出力は省略)
```

関連コマンド

コマンド	説明
show controllers ethernet-controller	ハードウェアまたはインターフェイス内部レジスタから読み込んだインターフェイスごとの送受信統計情報を表示します。
show interfaces	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の管理ステータスおよび動作ステータスを表示します。

show controllers ethernet-controller

ハードウェアから読み込んだ送受信に関するインターフェイス単位の統計情報をキーワードなしで表示するには、**show controllers ethernet-controller** イネーブル EXEC コマンドを使用します。**phy** キーワードはインターフェイス内部レジスタを表示し、**port-asic** キーワードはポート Application Specific Integrated Circuit（ASIC; 特定用途向け IC）に関する情報を表示します。

show controllers ethernet-controller [*interface-id*] [**phy** [**detail**]] [**port-asic** {**configuration** | **statistics**}] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	タイプ、モジュール、ポート番号を含む、物理インターフェイス
phy	（任意）デバイス、またはインターフェイスのスイッチの物理層（PHY）デバイスの内部レジスタ ステータスを表示します。インターフェイスの Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能の動作ステートを表示に含めます。
detail	（任意）PHY 内部レジスタの詳細を表示します。
port-asic	（任意）ポート ASIC 内部レジスタの詳細を表示します。
configuration	ポート ASIC 内部レジスタ コンフィギュレーションを表示します。
statistics	Rx/Sup Queue およびその他の統計情報を含むポート ASIC 統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC（ユーザ EXEC モードの *interface-id* キーワードでのみサポート）

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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の基本的な RMON 統計情報を含むトラフィック統計情報をキーワードなしで表示します。

phy または **port-asic** キーワードを入力した場合、表示された情報は主にスイッチのトラブルシューティングを行うシスコのテクニカル サポート担当者にとって有益な情報です。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、インターフェイスに対する **show controllers ethernet-controller** コマンドの出力を示します。表 2-18 は、*Transmit* フィールドについて説明します。表 2-19 は、*Receive* フィールドについて説明します。

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1            Receive
         0 Bytes                               0 Bytes
         0 Unicast frames                      0 Unicast frames
         0 Multicast frames                    0 Multicast frames
         0 Broadcast frames                    0 Broadcast frames
         0 Too old frames                      0 Unicast bytes
         0 Deferred frames                     0 Multicast bytes
         0 MTU exceeded frames                 0 Broadcast bytes
         0 1 collision frames                  0 Alignment errors
         0 2 collision frames                  0 FCS errors
         0 3 collision frames                  0 Oversize frames
         0 4 collision frames                  0 Undersize frames
         0 5 collision frames                  0 Collision fragments
         0 6 collision frames
         0 7 collision frames                  0 Minimum size frames
         0 8 collision frames                  0 65 to 127 byte frames
         0 9 collision frames                  0 128 to 255 byte frames
         0 10 collision frames                 0 256 to 511 byte frames
         0 11 collision frames                 0 512 to 1023 byte frames
         0 12 collision frames                 0 1024 to 1518 byte frames
         0 13 collision frames                 0 Overrun frames
         0 14 collision frames                 0 Pause frames
         0 15 collision frames                 0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                     0 Invalid frames, too large
         0 VLAN discard frames                 0 Valid frames, too large
         0 Excess defer frames                 0 Invalid frames, too small
         0 64 byte frames                      0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                     0 Too old frames
         0 511 byte frames                     0 Valid oversize frames
         0 1023 byte frames                    0 System FCS error frames
         0 1518 byte frames                    0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

表 2-18　Transmit のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で送信されたバイトの総数
Unicast Frames	ユニキャスト アドレスに送信されたフレームの総数
Multicast frames	マルチキャスト アドレスに送信されたフレームの総数
Broadcast frames	ブロードキャスト アドレスに送信されたフレームの総数
Too old frames	パケットが有効期限切れのため出力ポートで廃棄されたフレームの数
Deferred frames	時間が 2* 最大パケット時間を超えたあとで送信されなかったフレームの数
MTU exceeded frames	最大許可フレーム サイズを超えたフレームの数
1 collision frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
2 collision frames	2 回の衝突後、インターフェイス上で正常に送信されたフレームの数
3 collision frames	3 回の衝突後、インターフェイス上で正常に送信されたフレームの数
4 collision frames	4 回の衝突後、インターフェイス上で正常に送信されたフレームの数
5 collision frames	5 回の衝突後、インターフェイス上で正常に送信されたフレームの数
6 collision frames	6 回の衝突後、インターフェイス上で正常に送信されたフレームの数
7 collision frames	7 回の衝突後、インターフェイス上で正常に送信されたフレームの数

表 2-18　Transmit のフィールドの説明（続き）

フィールド	説明
8 collision frames	8 回の衝突後、インターフェイス上で正常に送信されたフレームの数
9 collision frames	9 回の衝突後、インターフェイス上で正常に送信されたフレームの数
10 collision frames	10 回の衝突後、インターフェイス上で正常に送信されたフレームの数
11 collision frames	11 回の衝突後、インターフェイス上で正常に送信されたフレームの数
12 collision frames	12 回の衝突後、インターフェイス上で正常に送信されたフレームの数
13 collision frames	13 回の衝突後、インターフェイス上で正常に送信されたフレームの数
14 collision frames	14 回の衝突後、インターフェイス上で正常に送信されたフレームの数
15 collision frames	15 回の衝突後、インターフェイス上で正常に送信されたフレームの数
Excessive collisions	16 回の衝突後、インターフェイス上で送信できなかったフレームの数
Late collisions	フレームが送信されたあとで、フレームの送信時に検出されたレイト コリジョンによって廃棄されたフレームの数
VLAN discard frames	CFI[1] ビットが設定されたことによりインターフェイス上で廃棄されたフレームの数
Excess defer frames	時間が最大パケット時間を超えたあとで送信されなかったフレームの数
64 byte frames	インターフェイス上で送信された 64 バイトのフレームの総数
127 byte frames	インターフェイス上で送信された 65 ～ 127 バイトのフレームの総数
255 byte frames	インターフェイス上で送信された 128 ～ 255 バイトのフレームの総数
511 byte frames	インターフェイス上で送信された 256 ～ 511 バイトのフレームの総数
1023 byte frames	インターフェイス上で送信された 512 ～ 1023 バイトのフレームの総数
1518 byte frames	インターフェイス上で送信された 1024 ～ 1518 バイトのフレームの総数
Too large frames	インターフェイス上で送信された最大許可フレーム サイズを超えたフレームの数
Good (1 coll) frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 1 回の衝突後、インターフェイス上で正常に送信されなかったフレームの数は含まれません。

1. CFI = Canonical Format Indicator（フォーマット形式表示）

表 2-19　Receive のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で受信されたフレームによって使用されたメモリ（バイト）の総量。FCS[1] 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Unicast frames	インターフェイス上で正常に受信されたユニキャスト アドレスに向けられたフレームの総数
Multicast frames	インターフェイス上で正常に受信されたマルチキャスト アドレスに向けられたフレームの総数
Broadcast frames	インターフェイス上で正常に受信されたブロードキャスト アドレスに向けられたフレームの総数
Unicast bytes	インターフェイス上で受信されたユニキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Multicast bytes	インターフェイス上で受信されたマルチキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。

表 2-19　Receive のフィールドの説明（続き）

フィールド	説明
Broadcast bytes	インターフェイス上で受信されたブロードキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Alignment errors	インターフェイス上で受信されたアライメント エラーを持つフレームの総数
FCS errors	インターフェイス上で受信された有効な長さ（バイト）を持ち、正常な FCS 値を持たないフレームの総数
Oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数
Undersize frames	インターフェイス上で受信された 64 バイト未満のフレームの数
Collision fragments	インターフェイス上で受信されたコリジョン フラグメントの数
Minimum size frames	最小フレーム サイズのフレームの総数
65 to 127 byte frames	65 ～ 127 バイトのフレームの総数
128 to 255 byte frames	128 ～ 255 バイトのフレームの総数
256 to 511 byte frames	256 ～ 511 バイトのフレームの総数
512 to 1023 byte frames	512 ～ 1023 バイトのフレームの総数
1024 to 1518 byte frames	1024 ～ 1518 バイトのフレームの総数
Overrun frames	インターフェイス上で受信されたオーバーラン フレームの総数
Pause frames	インターフェイス上で受信されたポーズ フレームの数
Symbol error frames	インターフェイス上で受信されたシンボル エラーを持つフレームの数
Invalid frames, too large	許可 MTU[2] サイズ（FCS ビットを含み、フレーム ヘッダーを含まない）を超え、FCS エラーまたはアライメント エラーのどちらかを持つ受信されたフレームの数
Valid frames, too large	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数
Invalid frames, too small	64 バイト（FCS ビットを含み、フレーム ヘッダーを含まない）未満で、FCS エラーまたはアライメント エラーのどちらかを持つ受信されたフレームの数
Valid frames, too small	64 バイト（または VLAN タグ付きフレームでは 68 バイト）未満で、有効な FCS 値を持つインターフェイスで受信されたフレームの数。フレーム サイズには、FCS ビットが含まれ、フレーム ヘッダー ビットは含まれません。
Too old frames	パケットが有効期限切れのため入力ポートで廃棄されたフレームの数
Valid oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超え、有効な FCS 値を持つフレームの数。フレーム サイズには、FCS 値が含まれ、VLAN タグは含まれません。
System FCS error frames	インターフェイス上で受信された有効な長さ（バイト）を持ち、正常な FCS 値を持たないフレームの総数
RxPortFifoFull drop frames	入力キューが一杯であるため廃棄された、インターフェイス上で受信されたフレームの総数

1. FCS = frame check sequence（フレーム チェック シーケンス）
2. MTU = Maximum Transmission Unit（最大伝送ユニット）

次の例では、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller gigabitethernet0/2 phy
GigabitEthernet0/2 (gpn: 2, port-number: 2)
------------------------------------------------------------
============================================================
Port    Conf-Media   Active-Media Attached
------- ------------ ------------ --------------------------
Gi0/1   auto-select  none         0 -Not Present
Gi0/2   auto-select  none         0 -Not Present
============================================================
Other Information
------------------------------------------------------
Port asic num         : 0
Port asic port num    : 1
XCVR init completed   : 0
Embedded PHY          : not present
SFP presence index    : 0
SFP iter cnt          : 2564163d
SFP failed oper flag  : 0x00000000
IIC error cnt         : 0
IIC error dsb cnt     : 0
IIC max sts cnt       : 0
Chk for link status   : 1
Link Status           : 0
(テキスト出力は省略)
```

次の例では、**show controllers ethernet-controller port-asic configuration** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic configuration
================================================================================
Switch 1, PortASIC 0 Registers
--------------------------------------------------------------------------------
DeviceType                          : 000101BC
Reset                               : 00000000
PmadMicConfig                       : 00000001
PmadMicDiag                         : 00000003
SupervisorReceiveFifoSramInfo       : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo      : 000001D0 000001D0 40000000
GlobalStatus                        : 00000800
IndicationStatus                    : 00000000
IndicationStatusMask                : FFFFFFFF
InterruptStatus                     : 00000000
InterruptStatusMask                 : 01FFE800
SupervisorDiag                      : 00000000
SupervisorFrameSizeLimit            : 000007C8
SupervisorBroadcast                 : 000A0F01
GeneralIO                           : 000003F9 00000000 00000004
StackPcsInfo                        : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                      FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                        : 73001630 00000003 7F001644 00000003
                                      24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                  : 18E418E0
stackControlStatusMask              : FFFFFFFF
TransmitBufferFreeListInfo          : 00000854 00000800 00000FF8 00000000
                                      0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo                : 00000016 00000016 40000000 00000000
                                      0000000C 0000000C 40000000 00000000
TransmitBufferInfo                  : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount           : 00000F7A
TransmitBufferCommonCountPeak       : 0000001E
TransmitBufferCommonCommonEmpty     : 000000FF
NetworkActivity                     : 00000000 00000000 00000000 02400000
DroppedStatistics                   : 00000000
FrameLengthDeltaSelect              : 00000001
SneakPortFifoInfo                   : 00000000
MacInfo                             : 0EC0801C 00000001 0EC0801B 00000001
                                      00C0001D 00000001 00C0001E 00000001
```

（テキスト出力は省略）

次の例では、**show controllers ethernet-controller port-asic statistics** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic statistics
================================================================================
 Switch 1, PortASIC 0 Statistics
--------------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
   4118966 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

         0 RxQ-1, wt-0 enqueue frames            0 RxQ-1, wt-0 drop frames
       296 RxQ-1, wt-1 enqueue frames            0 RxQ-1, wt-1 drop frames
   2836036 RxQ-1, wt-2 enqueue frames            0 RxQ-1, wt-2 drop frames

         0 RxQ-2, wt-0 enqueue frames            0 RxQ-2, wt-0 drop frames
         0 RxQ-2, wt-1 enqueue frames            0 RxQ-2, wt-1 drop frames
    158377 RxQ-2, wt-2 enqueue frames            0 RxQ-2, wt-2 drop frames

         0 RxQ-3, wt-0 enqueue frames            0 RxQ-3, wt-0 drop frames
         0 RxQ-3, wt-1 enqueue frames            0 RxQ-3, wt-1 drop frames
         0 RxQ-3, wt-2 enqueue frames            0 RxQ-3, wt-2 drop frames


        15 TxBufferFull Drop Count               0 Rx Fcs Error Frames
         0 TxBufferFrameDesc BadCrc16            0 Rx Invalid Oversize Frames
         0 TxBuffer Bandwidth Drop Cou           0 Rx Invalid Too Large Frames
         0 TxQueue Bandwidth Drop Coun           0 Rx Invalid Too Large Frames
         0 TxQueue Missed Drop Statist           0 Rx Invalid Too Small Frames
        74 RxBuffer Drop DestIndex Cou           0 Rx Too Old Frames
         0 SneakQueue Drop Count                 0 Tx Too Old Frames
         0 Learning Queue Overflow Fra           0 System Fcs Error Frames
         0 Learning Cam Skip Count

        15 Sup Queue 0 Drop Frames               0 Sup Queue 8 Drop Frames
         0 Sup Queue 1 Drop Frames               0 Sup Queue 9 Drop Frames
         0 Sup Queue 2 Drop Frames               0 Sup Queue 10 Drop Frames
         0 Sup Queue 3 Drop Frames               0 Sup Queue 11 Drop Frames
         0 Sup Queue 4 Drop Frames               0 Sup Queue 12 Drop Frames
         0 Sup Queue 5 Drop Frames               0 Sup Queue 13 Drop Frames
         0 Sup Queue 6 Drop Frames               0 Sup Queue 14 Drop Frames
         0 Sup Queue 7 Drop Frames               0 Sup Queue 15 Drop Frames
================================================================================
 Switch 1, PortASIC 1 Statistics
--------------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
        52 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames
```

（テキスト出力は省略）

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC のステートを表示し、CPU に達するパケットに関する統計情報を送受信します。
show controllers tcam	システム内のすべての Temary CAM（TCAM）と CAM コントローラである TCAM インターフェイス ASIC のレジスタ ステートを表示します。

show controllers tcam

システムのすべての Ternary CAM（TCAM）、および CAM コントローラである TCAM インターフェイス Application Specific Integrated Circuit（ASIC; 特定用途向け IC）のレジスタのステートを表示するには、**show controllers tcam** イネーブル EXEC コマンドを使用します。

show controllers tcam [**asic** [**number**]] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

asic	（任意）ポート ASIC TCAM 情報を表示します。
number	（任意）指定されたポート ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 15 です。
detail	（任意）TCAM レジスタ情報に関する詳細を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチのトラブルシューティングを行うシスコのテクニカル サポート担当者にとって有益となる情報を表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次に **show controllers tcam** コマンドの出力例を示します。

```
Switch# show controllers tcam
---------------------------------------------------------------------------
TCAM-0 Registers
---------------------------------------------------------------------------
  REV:    00B30103
  SIZE:   00080040
  ID:     00000000
  CCR:    00000000_F0000020

  RPID0:  00000000_00000000
  RPID1:  00000000_00000000
  RPID2:  00000000_00000000
  RPID3:  00000000_00000000

  HRR0:   00000000_E000CAFC
  HRR1:   00000000_00000000
  HRR2:   00000000_00000000
  HRR3:   00000000_00000000
  HRR4:   00000000_00000000
  HRR5:   00000000_00000000
  HRR6:   00000000_00000000
  HRR7:   00000000_00000000
(テキスト出力は省略)

  GMR31:  FF_FFFFFFFF_FFFFFFFF
  GMR32:  FF_FFFFFFFF_FFFFFFFF
  GMR33:  FF_FFFFFFFF_FFFFFFFF

===========================================================================
 TCAM related PortASIC 1 registers
===========================================================================
LookupType:                   89A1C67D_24E35F00
LastCamIndex:                 0000FFE0
LocalNoMatch:                 000069E0
ForwardingRamBaseAddress:
                              00022A00 0002FE00 00040600 0002FE00 0000D400
                              00000000 003FBA00 00009000 00009000 00040600
                              00000000 00012800 00012900
```

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC のステートを表示し、CPU に達するパケットに関する統計情報を送受信します。
show controllers ethernet-controller	ハードウェアまたはインターフェイス内部レジスタから読み込んだインターフェイスごとの送受信統計情報を表示します。

show controllers utilization

スイッチまたは特定のポートの帯域利用率を表示するには、**show controllers utilization** ユーザ EXEC コマンドを使用します。

show controllers [*interface-id*] **utilization** [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）スイッチ インターフェイスの ID です。
| begin	（任意）指定した *expression* と一致する行から表示を開始します。
| exclude	（任意）指定した *expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例は、**show controllers utilization** コマンドの出力を示しています。

```
Switch> show controllers utilization
Port        Receive Utilization  Transmit Utilization
Fa0/1             0                    0
Fa0/2             0                    0
Fa0/3             0                    0
Fa0/4             0                    0
Fa0/5             0                    0
Fa0/6             0                    0
Fa0/7             0                    0
(テキスト出力は省略)

(テキスト出力は省略)

Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

次の例は、特定のポートでの **show controllers utilization** コマンドの出力を示します。

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

表 2-20　show controllers utilization のフィールドの説明

フィールド	説明
Receive Bandwidth Percentage Utilization	スイッチの受信帯域利用率を表示します。これは、すべてのポートの受信トラフィックの合計をスイッチの受信容量で割ったものです。
Transmit Bandwidth Percentage Utilization	スイッチの送信帯域利用率を表示します。これは、すべてのポートの送信トラフィックの合計をスイッチの送信容量で割ったものです。
Fabric Percentage Utilization	スイッチの送信と受信の両方の帯域利用率の平均を表示します。

関連コマンド

コマンド	説明
show controllers ethernet-controller	インターフェイスの内部レジスタを表示します。

show dot1x

スイッチまたは指定されたポートの 802.1x 統計情報、管理ステータス、および動作ステータスを表示するには、**show dot1x** イネーブル EXEC コマンドを使用します。

show dot1x [**all** | **interface** *interface-id* | **statistics interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all	（任意）すべてのポートの IEEE 802.1x ステータスを表示します。
interface *interface-id*	（任意）タイプ、モジュール、ポート番号を含む、指定されたポートの IEEE 802.1x ステータスを表示します。
statistics interface *interface-id*	（任意）タイプ、モジュール、ポート番号を含む、指定されたポートの IEEE 802.1x 統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	表示は authorization state machine state フィールドおよび port status フィールドに **auth-fail-vlan** を含むよう拡張されました。
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ポートを指定しない場合は、グローバル パラメータおよびサマリーが表示されます。ポートを指定する場合、ポートの詳細が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show dot1x** および **show dot1x all** イネーブル EXEC コマンドの出力を示します。

```
Switch# show dot1x
Sysauthcontrol                  = Enabled
Supplicant Allowed In Guest Vlan  = Disabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both

Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
----------------------------------------------------
Supplicant MAC 00d0.b71b.35de
   AuthSM State      = CONNECTING
   BendSM State      = IDLE
PortStatus        = UNAUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
ControlDirection  = Both
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

次の例では、制限付き VLAN が設定された場合の **show dot1x all** イネーブル EXEC コマンドの出力例を示します。

```
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet2/0/3
----------------------------------------------------
Supplicant MAC 0002.b3eb.0df6
AuthSM State          = AUTHENTICATED(AUTH-FAIL-VLAN)
BendSM State          = IDLE
Posture               = N/A
PortStatus            = AUTHORIZED(AUTH-FAIL-VLAN)
MaxReq                = 2
MaxAuthReq            = 2
HostMode              = Single
PortControl           = Auto
ControlDirection      = Both
QuietPeriod           = 10 Seconds
Re-authentication     = Disabled
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
TxPeriod              = 10 Seconds
Guest-Vlan            = 3
AuthFail-Vlan         = 4
AuthFail-Max-Attempts = 3
```

次の例では、制限付き VLAN が設定された場合の **show dot1x interface** *interface-id* イネーブル EXEC コマンドの出力例を示します。

```
Switch# show dot1x interface gigabitethernet0/1
    Supplicant MAC 0010.a492.db59
    AuthSM State           = AUTHENTICATED(AUTH-FAIL-VLAN)
    BendSM State           = IDLE
    Posture                = N/A
       ReAuthPeriod       = 3600 Seconds (Locally Configured)
       ReAuthAction       = Reauthenticate
       TimeToNextReauth   = 2753
    PortStatus             = AUTHORIZED(AUTH-FAIL-VLAN)
    MaxReq                 = 2
    MaxAuthReq             = 2
    HostMode               = Single
    PortControl            = Auto
    ControlDirection       = Both
    QuietPeriod            = 60 Seconds
    Re-authentication      = Enabled
    ReAuthPeriod           = 3600 Seconds
    ServerTimeout          = 30 Seconds
    SuppTimeout            = 30 Seconds
    TxPeriod               = 30 Seconds
    Guest-Vlan             = 0
    AuthFail-Vlan          = 1001
    AuthFail-Max-Attempts = 3
    Critical Port          = Disabled
```

次の例では、**show dot1x statistics interface** *interface-id* コマンドの出力例を示します。表 2-21 に、この出力で表示されるフィールドの説明を示します。

```
Switch# show dot1x statistics interface gigabitethernet0/1
PortStatistics Parameters for Dot1x
---------------------------------------------
TxReqId = 15     TxReq = 0       TxTotal = 15
RxStart = 4      RxLogoff = 0    RxRespId = 1     RxResp = 1
RxInvalid = 0    RxLenErr = 0    RxTotal= 6
RxVersion = 1    LastRxSrcMac 00d0.b71b.35de
```

表 2-21　show dot1x statistics のフィールドの説明

フィールド	説明
TxReqId	送信された Extensible Authentication Protocol（EAP）-Request/Identity フレームの個数
TxReq	送信された EAP-Request フレーム（Request/Identity フレーム以外）の個数
TxTotal	送信されたすべてのタイプの Extensible Authentication Protocol over LAN（EAPOL）フレームの個数
RxStart	受信された有効な EAPOL-Start フレームの個数
RxLogoff	受信された EAPOL-Logoff フレームの個数
RxRespId	受信された EAP-Response/Identity フレームの個数
RxResp	受信された有効な EAP-Response フレーム（Response/Identity フレーム以外）の個数
RxInvalid	受信された EAPOL フレームのうち、フレーム タイプを認識できないフレームの個数
RxLenError	受信された EAPOL フレームのうち、パケット本体の長さを示すフィールドが無効なフレームの個数
RxTotal	受信されたすべてのタイプの有効な EAPOL フレームの個数

表 2-21　show dot1x statistics のフィールドの説明（続き）

フィールド	説明
RxVersion	IEEE 802.1x バージョン 1 形式で受信されたパケットの個数
LastRxSrcMac	最後に受信した EAPOL フレームで伝送された送信元 MAC アドレス

関連コマンド

コマンド	説明
dot1x default	IEEE 802.1x パラメータをデフォルト値に戻します。

show dtp

スイッチ、または指定されたインターフェイスの Dynamic Trunking Protocol（DTP）情報を表示するには、**show dtp** イネーブル EXEC コマンドを使用します。

show dtp [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスとしては、タイプ、モジュール、およびポート番号を含む物理ポートがあります。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次に **show dtp** コマンドの出力例を示します。

```
Switch# show dtp
Global DTP information
        Sending DTP Hello packets every 30 seconds
        Dynamic Trunk timeout is 300 seconds
        21 interfaces using DTP
```

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

```
Switch# show dtp interface gigabitethernet0/1
DTP information for GigabitEthernet0/1:
  TOS/TAS/TNS:                              ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                              NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:                       000943A7D081
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       1/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S2:ACCESS
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:                                   no

  Statistics
  ----------
  3160 packets received (3160 good)
  0 packets dropped
      0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
  6320 packets output (6320 good)
      3160 native
  0 output errors
  0 trunk timeouts
  1 link ups, last link up on Mon Mar 01 1993, 01:02:29
  0 link downs
```

関連コマンド

コマンド	説明
show interfaces trunk	インターフェイス トランキング情報を表示します。

show env

ファン、温度、Redundant Power System（RPS; 冗長電源システム）のアベイラビリティ、およびスイッチの電源情報を表示するには、**show env** ユーザ EXEC コマンドを使用します。

show env {**all** | **fan** | **power** | **rps**| **temperature**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all	ファンと温度環境の両方のステータスを表示します。
fan	スイッチ ファンのステータスを表示します。
power	スイッチ電源のステータスを表示します。
rps	RPS 300 冗長電源システムがスイッチに接続されているかを表示します。
temperature	スイッチ温度のステータスを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show env all** コマンドの出力を示します。

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is AVAILABLE
```

次の例では、**show env fan** コマンドの出力を示します。

```
Switch> show env fan
FAN is OK
```

show errdisable detect

errdisable 検出ステータスを表示するには、**show errdisable detect** ユーザ EXEC コマンドを使用します。

show errdisable detect [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

表示された `gbic-invalid` エラーの理由は、無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show errdisable detect** コマンドの出力を示します。

```
Switch> show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
channel-misconfig    Enabled
psecure-violation    Enabled
vmps                 Enabled
loopback             Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
unicast-flood        Enabled
storm-control        Enabled
ilpower              Enabled
```

（注）　出力には表示されていますが、ilpower、storm-control、および unicast-flood フィールドは無効です。

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の errdisable 検出をイネーブルにします。
show errdisable flap-values	エラー条件の認識情報を表示します。
show errdisable recovery	errdisable 回復タイマー情報を表示します。
show interfaces status	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。

show errdisable flap-values

原因として認められるエラーを引き起こす条件を表示するには、**show errdisable flap-values** ユーザ EXEC コマンドを使用します。

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Flaps 列では、指定されたインターバル以内にステートに対する変更を何回行うと、エラーが検出されポートがディセーブルになるかを表示します。たとえば、3 つの Dynamic Trunking Protocol（DTP）ステート（ポート モード アクセス / トランク）、または Port Aggregation Protocol（PAgP; ポート集約プロトコル）フラップが 30 秒間隔で変更された場合、または 5 つのリンク ステート（リンク アップ / ダウン）が 10 秒間隔で変更された場合、エラーとみなしポートがシャットダウンします。

```
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3        30
dtp-flap               3        30
link-flap              5        10
```

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show errdisable flap-values** コマンドの出力を示します。

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3        30
dtp-flap               3        30
link-flap              5        10
```

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の errdisable 検出をイネーブルにします。
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	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。

show errdisable recovery

errdisable 回復タイマー情報を表示するには、**show errdisable recovery** ユーザ EXEC コマンドを使用します。

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

gbic-invalid error-disable の理由は、無効な Small Form-factor Pluggable（SFP）インターフェイスを意味します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show errdisable recovery** コマンドの出力を示します。

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
loopback             Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi0/2        link-flap             279
```

（注）　出力には表示されていますが、unicast-flood フィールドは無効です。

関連コマンド

コマンド	説明
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 flap-values	エラー条件の認識情報を表示します。
show interfaces status	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。

show etherchannel

チャネルの EtherChannel 情報を表示するには、**show etherchannel** ユーザ EXEC コマンドを使用します。

show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 6 です。
detail	EtherChannel の詳細を表示します。
load-balance	ポート チャネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	EtherChannel ポート情報を表示します。
port-channel	ポート チャネル情報を表示します。
protocol	EtherChannel で使用されるプロトコルを表示します。
summary	各チャネル グループのサマリーを 1 行で表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

channel-group を指定しない場合は、すべてのチャネル グループが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show etherchannel 1 detail** コマンドの出力を示します。

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
               Ports in the group:
               -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi0/1     SA      bndl      32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

               Port-channels in the group:
               ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

次の例では、**show etherchannel 1 summary** コマンドの出力を示します。

```
Switch> show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi0/1(P)    Gi0/2(P)
```

次の例では、**show etherchannel 1 port-channel** コマンドの出力を示します。

```
Switch> show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:24m:44s    Gi0/2
```

次の例では、**show etherchannel protocol** コマンドの出力を示します。

```
Switch# show etherchannel protocol
                Channel-group listing:
                ----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

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。
channel-protocol	チャネリングを管理する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 flowcontrol

フロー制御ステータスおよび統計情報を表示するには、**show flowcontrol** ユーザ EXEC コマンドを使用します。

show flowcontrol [**interface** *interface-id* | **module** *number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）特定のインターフェイスのフロー制御ステータスおよび統計情報を表示します。
module *number*	（任意）スイッチ上のすべてのインターフェイスのフロー制御ステータスおよび統計情報を表示します。有効なモジュール番号は 1 だけです。このオプションは、特定のインターフェイス ID を入力したときは利用できません。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチまたは特定のインターフェイスのフロー制御ステータスおよび統計情報を表示するには、このコマンドを使用します。

スイッチ インターフェイス情報をすべて表示するには、**show flowcontrol** コマンドを使用します。**show flowcontrol** コマンドの出力は、**show flowcontrol module** *number* コマンドの出力と同じです。

特定のインターフェイスの情報を表示するには、**show flowcontrol interface** *interface-id* コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

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

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/1      Unsupp.  Unsupp.  off      off         0       0
Gi0/2      desired  off      off      off         0       0
Gi0/3      desired  off      off      off         0       0
(テキスト出力は省略)
```

次の例では、**show flowcontrol interface** *interface-id* コマンドの出力を示します。

```
Switch> show flowcontrol gigabitethernet0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/2      desired  off      off      off         0       0
```

関連コマンド

コマンド	説明
flowcontrol	インターフェイスの受信フロー制御ステートを設定します。

show interfaces

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の管理ステータスおよび動作ステータスを表示するには、**show interfaces** イネーブル EXEC コマンドを使用します。

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] | **transceiver** [**properties** | **detail**] [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）タイプ、モジュール、およびポート番号を含む、有効なインターフェイスは、物理ポートやポート チャネルなどです。ポート チャネル範囲は 1 ～ 6 です。
vlan *vlan-id*	（任意）VLAN（仮想 LAN）ID です。指定できる範囲は 1 ～ 4094 です。
accounting	（任意）アクティブ プロトコル、入出力パケット、オクテットを含む、インターフェイスのアカウンティング情報を表示します。
capabilities	（任意）インターフェイスで設定できる機能とオプションを含む、すべてのインターフェイス、または特定のインターフェイスの機能を表示します。このオプションはコマンドラインのヘルプに表示されていますが、VLAN ID に使用できません。
module *number*	（任意）スイッチ上の全インターフェイスの **capabilities**、**switchport** コンフィギュレーション、または **transceiver** 特性を表示します（先行するキーワードに左右されます）。有効なモジュール番号は 1 だけです。このオプションは、特定のインターフェイス ID を入力したときは利用できません。
counters	（任意）**show interfaces counters** コマンドを参照してください。
description	（任意）特定のインターフェイスに設定された管理ステータスおよび説明を表示します。
etherchannel	（任意）インターフェイス EtherChannel 情報を表示します。
flowcontrol	（任意）インターフェイス flowcontrol 情報を表示します。
pruning	（任意）インターフェイス トランク VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）プルーニング情報を表示します。
stats	（任意）インターフェイスのスイッチング パスによる入出力パケットを表示します。
status	（任意）インターフェイスのステータスを表示します。Type フィールドの *unsupported* のステータスは、Cisco 以外の Small Form-Factor Pluggable（SFP）モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	（任意）errdisable ステートのインターフェイスを表示します。
switchport	（任意）ポート ブロッキング、ポート保護設定など、スイッチングポートの管理ステータスおよび動作ステータスを表示します。
backup	（任意）スイッチ上の指定したインターフェイスまたはすべてのインターフェイスの、Flex Link バックアップ インターフェイス コンフィギュレーションおよびステータスを表示します

transceiver [**detail** | **properties**]	（任意）CWDM[1] または DWDM[2] Small Form-Factor（SFP）モジュール インターフェイスの物理プロパティを表示します。キーワードの意味は次のとおりです。 • **detail** — （任意）高低値やアラーム情報などの、調整プロパティを表示します。 • **properties** — （任意）インターフェイスの速度とデュプレックス設定を表示します。
trunk	インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブなトランキング ポートの情報のみが表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

1. Coarse Wavelength Division Multiplexing（CWDM; 低密度波長分割多重）
2. Dense Wavelength Division Multiplexing（DWDM; 高密度波長分割多重）

（注）　**crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、**rate-limit**、および **shape** 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ていますが、サポートされていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

キーワードが異なる **show interfaces capabilities** コマンドを使用した結果は次のとおりです。

- スイッチ上のすべてのインターフェイス機能を表示するには、**show interface capabilities module 1** を使用します。他の番号を入力すると無効になります。
- 特定のインターフェイスの機能を表示するには、**show interfaces** *interface-id* **capabilities** を使用します。
- スイッチ上のすべてのインターフェイス機能を表示するには、**show interfaces capabilities**（モジュール番号もインターフェイス ID もなし）を使用します。
- スイッチ上のすべてのインターフェイスのスイッチ ポート特性を表示するには、**show interface switchport module 1** を使用します。他の番号を入力すると無効になります。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次に **show interfaces** コマンドの出力例を示します。

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang
never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2 packets input, 1040 bytes, 0 no buffer
     Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     4 packets output, 1040 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

次の例では、**show interfaces accounting** コマンドの出力を示します。

```
Switch# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP    1094395  131900022     559555   84077157
           Spanning Tree     283896   17033760         42       2520
                     ARP      63738    3825680        231      13860
Interface Vlan2 is disabled
Vlan7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Vlan31
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

（テキスト出力は省略）

次の例では、インターフェイスの **show interfaces capabilities** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
  Model:                 WS-C2960G-24TC-L
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
  Multiple Media Types:  rj45, sfp, auto-select
```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを *Connects to Marketing* として指定した場合の **show interfaces** *interface* **description** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi0/2       up             down     Connects to Marketing
```

次の例では、スイッチにポート チャネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

次の例では、VTP ドメイン内でプルーニングがイネーブルの場合の **show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigibitethernet0/2 pruning
Port    Vlans pruned for lack of request by neighbor
Gi0/2     3,4

Port    Vlans traffic requested of neighbor
Gi0/2     1-3
```

次の例では、特定のインターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/1                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/2                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/3                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/4                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/5                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/6                        notconnect   1            auto   auto 10/100/1000BaseTX
```

（テキスト出力は省略）

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステートのインターフェイスのステータスを表示します。

```
Switch# show interfaces status err-disabled
Port      Name               Status       Reason
Gi0/2                        err-disabled dtp-flap
```

次の例では、1 つのポートに対する **show interfaces switchport** コマンドの出力を示します。表 2-22 に、表示されるフィールドの説明を示します。

（注）　プライベート VLAN はこのリリースではサポートされないので、フィールドは適用されません。

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

表 2-22　show interfaces switchport のフィールドの説明

フィールド	説明
Name	ポートの名前を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この表示の場合、ポートはスイッチポート モードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキング ネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニング適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル（True）であるか、またはディセーブル（False）であるかを表示します。

表 2-22　show interfaces switchport のフィールドの説明（続き）

フィールド	説明
Unknown unicast blocked Unknown multicast blocked	インターフェイス上で未知のマルチキャスト、および未知のユニキャスト トラフィックがブロックされたかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Appliance trust	IP Phone のデータ パケットの Class of Service（CoS; サービス クラス）設定を表示します。

次の例では、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
     Active Interface    Backup Interface    State
     ------------------------------------------------------------
     Fa0/1               Fa0/2             Active Up/Backup Standby
     Fa0/3               Fa0/5             Active Down/Backup Up
     Po1                 Po2               Active Standby/Backup Up
```

次の例では、**show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigibitethernet0/2 pruning
Port    Vlans pruned for lack of request by neighbor
```

次の例では、**show interfaces** *interface-id* **trunk** コマンドの出力を示します。ポートのトランキング情報が表示されます。

```
Switch# show interfaces gigabitethernet0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi0/1        auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi0/1        1-4094

Port          Vlans allowed and active in management domain
Gi0/1        1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1         1-4
```

次の例では、**show interfaces** *interface-id* **transceiver properties** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: N/A
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
Configured Media: sfp
Active Media: sfp
Attached: 10/100/1000BaseTX SFP-10/100/1000BaseTX
```

次の例では、**show interfaces** *interface-id* **transceiver detail** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.

                           High Alarm  High Warn  Low Warn   Low Alarm
        Temperature        Threshold   Threshold  Threshold  Threshold
Port     (Celsius)         (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------ ----------  ---------  ---------  ---------
Gi0/3   41.5               110.0       103.0      -8.0       -12.0

                           High Alarm  High Warn  Low Warn   Low Alarm
         Voltage           Threshold   Threshold  Threshold  Threshold
Port     (Volts)           (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------   ----------  ---------  ---------  ---------
Gi0/3    3.20              4.00        3.70       3.00       2.95

                           High Alarm  High Warn  Low Warn   Low Alarm
         Current           Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)    (mA)        (mA)       (mA)       (mA)
-------  ----------------  ----------  ---------  ---------  ---------
Gi0/3    31.0              84.0        70.0       4.0        2.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Transmit Power    Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  ----------------  ----------  ---------  ---------  ---------
Gi0/3    -0.0 ( -0.0)      -0.0        -0.0       -0.0       -0.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Receive Power     Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  ----------------  ----------  ---------  ---------  ---------
Gi0/3    N/A  ( -0.0) --   -0.0        -0.0       -0.0       -0.0
```

関連コマンド

コマンド	説明
switchport access	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport block	インターフェイス上で未知のユニキャスト、または未知のマルチキャスト トラフィックをブロックします。
switchport backup interface	相互バックアップを提供するレイヤ 2 インターフェイスのペアである Flex Link を設定します。
switchport mode	ポートの VLAN（仮想 LAN）メンバーシップ モードを設定します。
switchport protected	同じスイッチの他の保護されたポートから送信されるレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーニング適格リストを設定します。

show interfaces counters

スイッチまたは指定されたインターフェイスの各カウンタを表示するには、**show interfaces counters** イネーブル EXEC コマンドを使用します。

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **etherchannel** | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）タイプ、モジュール、ポート番号を含む、物理インターフェイスの ID です。
errors	（任意）エラー カウンタを表示します。
etherchannel	（任意）送受信されたオクテット、ブロードキャスト パケット、マルチキャスト パケット、ユニキャスト パケットなど EtherChannel カウンタを表示します。
protocol status	（任意）インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	（任意）トランク カウンタを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

（注）　**vlan** *vlan-id* 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ていますが、サポートされていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

キーワードを指定しない場合は、すべてのインターフェイスのすべてのカウンタが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi0/1                  0              0              0              0
Gi0/2                  0              0              0              0
```

（テキスト出力は省略）

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan20: Other, IP, ARP
 Vlan30: Other, IP, ARP
 Vlan40: Other, IP, ARP
 Vlan50: Other, IP, ARP
 Vlan60: Other, IP, ARP
 Vlan70: Other, IP, ARP
 Vlan80: Other, IP, ARP
 Vlan90: Other, IP, ARP
 Vlan900: Other, IP, ARP
 Vlan3000: Other, IP
 Vlan3500: Other, IP
 FastEthernet0/1: Other, IP, ARP, CDP
 FastEthernet0/2: Other, IP
 FastEthernet0/3: Other, IP
 FastEthernet0/4: Other, IP
 FastEthernet0/5: Other, IP
 FastEthernet0/6: Other, IP
 FastEthernet0/7: Other, IP
 FastEthernet0/8: Other, IP
 FastEthernet0/9: Other, IP
 FastEthernet0/10: Other, IP, CDP
```

（テキスト出力は省略）

次の例では、**show interfaces counters trunk** コマンドの出力を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1               0              0           0
Gi0/2               0              0           0
Gi0/3           80678           4155           0
Gi0/4           82320            126           0
Gi0/5               0              0           0
```

（テキスト出力は省略）

関連コマンド

コマンド	説明
show interfaces	追加のインターフェイスの特性を表示します。

show inventory

ハードウェアの Product Identification（PID）情報を表示するには、**show inventory** ユーザ EXEC コマンドを使用します。

show inventory [***entity-name*** | **raw**] [| {**begin** | **exclude** | **include**} ***expression***]

構文の説明

entity-name	（任意）指定されたエンティティを表示します。たとえば、Small Form-factor Pluggable（SFP）モジュールが取り付けられているインターフェイス（gigabitethernet0/1 など）を入力します。
raw	（任意）デバイス内のすべてのエンティティを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、大文字と小文字を区別します。引数がない場合、**show inventory** コマンドは製品識別情報を持つすべての識別可能なエンティティのコンパクト ダンプを生成します。コンパクト ダンプには、エンティティの場所（スロット ID）、エンティティの説明、およびそのエンティティの Unique Device Indicator（UDI）（PID、VID、および SN）が表示されます。

（注）　PID がない場合、ユーザが **show inventory** コマンドを入力しても出力はありません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次に **show inventory** コマンドの出力例を示します。

```
Switch> show inventory
NAME: "1", DESCR: "WS-C2960-48TC-L"
PID: WS-C2960-24TC-L   , VID: 02 , SN: FHH0923D075

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10D SFP"
PID:                      , VID:    , SN: NEC09050251

NAME: "GigabitEthernet0/2", DESCR: "100BaseBX-10U SFP"
PID:                      , VID:    , SN: NEC09050020
```

show ip dhcp snooping

Dynamic Host Configuration Protocol（DHCP）スヌーピング設定を表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip dhcp snooping** コマンドの出力を示します。

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet0/1               yes         unlimited
GigabitEthernet0/2               yes         unlimited
```

関連コマンド

コマンド	説明
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。

show ip dhcp snooping binding

スイッチ上にある全インターフェイスの Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディングデータベースおよび設定情報を表示するには、**show ip dhcp snooping binding** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

ip-address	（任意）バインディング エントリ IP アドレスを指定します。
mac-address	（任意）バインディング エントリ MAC（メディアアクセス制御）アドレスを指定します。
interface *interface-id*	（任意）バインディング入力インターフェイスを指定します。
vlan *vlan-id*	（任意）バインディング エントリ VLAN を指定します。
| begin	*expression* と一致する行から表示を開始します。
| exclude	*expression* と一致する行を表示から除外します。
| include	指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show ip dhcp snooping binding コマンド出力は、動的に設定されたバインディングのみを表示します。DHCP スヌーピング バインディング データベース内に、動的に設定されたバインディング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** イネーブル EXEC コマンドを使用します。

DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、スイッチは静的に設定されたバインディングは削除しません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、スイッチの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
01:02:03:04:05:06   10.1.2.150       9837        dhcp-snooping  20
GigabitEthernet0/1
00:D0:B7:1B:35:DE   10.1.2.151       237         dhcp-snooping  20
GigabitEthernet0/2
Total number of bindings: 2
```

次の例では、特定の IP アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 10.1.2.150
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
01:02:03:04:05:06   10.1.2.150       9810        dhcp-snooping  20
GigabitEthernet0/1
Total number of bindings: 1
```

次の例では、特定の MAC アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 0102.0304.0506
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
01:02:03:04:05:06   10.1.2.150       9788        dhcp-snooping  20
GigabitEthernet0/2
Total number of bindings: 1
```

次の例では、ポートの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding interface gigabitethernet0/2
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:30:94:C2:EF:35   10.1.2.151       290         dhcp-snooping  20
GigabitEthernet0/2
Total number of bindings: 1
```

次の例では、VLAN 20 の DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding vlan 20
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
01:02:03:04:05:06   10.1.2.150       9747        dhcp-snooping  20
GigabitEthernet0/1
00:00:00:00:00:02   10.1.2.151       65          dhcp-snooping  20
GigabitEthernet0/2
Total number of bindings: 2
```

表 2-23 は、**show ip dhcp snooping binding** コマンド出力のフィールドを説明しています。

表 2-23　show ip dhcp snooping binding コマンド出力

フィールド	説明
MacAddress	クライアント ハードウェアの MAC アドレス
IpAddress	DHCP サーバに割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレスに対する残りのリース時間
Type	バインディング タイプ
VLAN	クライアント インターフェイスの VLAN 番号

表 2-23　show ip dhcp snooping binding コマンド出力（続き）

フィールド	説明
Interface	DHCP クライアント ホストに接続するインターフェイス
Total number of bindings	スイッチに設定される合計バインディング数 （注）　コマンド出力では、合計バインディング数が表示されないこともあります。たとえば、200 バインディングがスイッチに設定されてすべてのバインディングが表示される前に表示を停止させた場合、合計数は変更されません。

関連コマンド

コマンド	説明
ip dhcp snooping binding	DHCP スヌーピング バインディング データベース情報を設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

show ip dhcp snooping 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 エージェントのステータスを表示するには、**show ip dhcp snooping database** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping database [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）詳細ステータスおよび統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、**show ip dhcp snooping database** コマンドの出力を示します。

```
Switch> show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

次の例では、**show ip dhcp snooping database detail** コマンドの出力例を示します。

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
```

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	DHCP スヌーピング情報を表示します。

show ip igmp profile

設定されたすべての Internet Group Management Protocol（IGMP）プロファイル、または指定された IGMP プロファイルを表示するには、**show ip igmp profile** イネーブル EXEC コマンドを使用します。

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

profile number	（任意）表示される IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号を入力しない場合、すべての IGMP プロファイルが表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**|exclude output** と入力した場合、*output* を含む行は表示されませんが *Output* を含む行は表示されます。

例

次に、プロファイル番号を指定した場合と指定しない場合の **show ip igmp profile** イネーブル EXEC コマンドの出力例を示します。プロファイル番号を入力しない場合、スイッチで設定されたプロファイルすべてが表示されます。

```
Switch# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

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 igmp snooping

スイッチまたは VLAN（仮想 LAN）の Internet Group Management Protocol（IGMP）スヌーピング設定を表示するには、**show ip igmp snooping** ユーザ EXEC コマンドを使用します。

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

groups	（任意）**show ip igmp snooping groups** コマンドを参照してください。
mrouter	（任意）**show ip igmp snooping mrouter** コマンドを参照してください。
querier	（任意）**show ip igmp snooping querier** コマンドを参照してください。
vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 および 1006 ～ 4094 です（イネーブル EXEC モードでのみ使用可能）。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、スイッチまたは特定の VLAN のスヌーピング設定を表示します。

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping vlan 1** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping (minimal) :Enabled
Report suppression        :Enabled
TCN solicit query         :Disabled
TCN flood query count     :2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                         :Enabled
Immediate leave                       :Disabled
Multicast router learning mode        :pim-dvmrp
Source only learning age timer        :10
CGMP interoperability mode            :IGMP_ONLY
Last member query interval : 100
```

次の例では、**show ip igmp snooping** コマンドの出力を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping               : Enabled
IGMPv3 snooping (minimal)   : Enabled
Report suppression          : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Last member query interval  : 100

Vlan 1:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 100

Vlan 2:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 333
```

（テキスト出力は省略）

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping last-member-query-interval	IGMP スヌーピング設定可能脱退タイマーをイネーブルにします。
ip igmp snooping querier	IGMP クエリア機能をレイヤ 2 ネットワークでイネーブルにします。
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
ip igmp snooping tcn	IGMP トポロジー変更通知の動作を設定します。
ip igmp snooping tcn flood	IGMP スパニングツリー トポロジー変更通知の動作としてマルチキャスト フラッディングを指定します。
ip igmp snooping vlan immediate-leave	VLAN での IGMP スヌーピング即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加するか、またはマルチキャスト学習方式を設定します。
ip igmp snooping vlan static	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静的に追加します。
show ip igmp snooping groups	スイッチの IGMP スヌーピング マルチキャスト テーブルを表示します。
show ip igmp snooping mrouter	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト 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 クエリーの設定および動作情報を表示します。

show ip igmp snooping groups

スイッチの Internet Group Management Protocol（IGMP）スヌーピング マルチキャスト テーブル、またはマルチキャスト情報を表示するには、**show ip igmp snooping groups** イネーブル EXEC コマンドを使用します。指定されたマルチキャスト VLAN のマルチキャスト テーブル、または特定のマルチキャスト情報を表示するには、**vlan** キーワードを使用します。

show ip igmp snooping groups [**count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

count	（任意）実際のエントリの代わりに、指定されたコマンド オプションのエントリの総数を表示します。
dynamic	（任意）IGMP スヌーピングにより学習されたエントリを表示します。
user	（任意）ユーザ設定のマルチキャスト エントリのみを表示します。
ip_address	（任意）指定されたグループ IP アドレスを持つマルチキャスト グループの特性を表示します。
vlan *vlan-id*	（任意）VLAN（仮想 LAN）を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

マルチキャスト情報またはマルチキャスト テーブルを表示するには、このコマンドを使用します。

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、キーワードを使用しない場合の **show ip igmp snooping groups** コマンドの出力を示します。スイッチのマルチキャスト テーブルが表示されます。

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

次の例では、**show ip igmp snooping groups count** コマンドの出力を示します。スイッチ上のマルチキャスト グループの総数が表示されます。

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

次の例では、**show ip igmp snooping groups dynamic** コマンドの出力を示します。IGMP スヌーピングにより学習されたエントリのみを表示します。

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Fa0/15
104       224.1.4.3       igmp        v2          Gi0/1, Fa0/15
```

次の例では、**show ip igmp snooping groups vlan** *vlan-id ip-address* コマンドの出力を示します。指定された IP アドレスを持つグループのエントリを表示します。

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Fa0/15
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを設定します。
ip igmp snooping vlan static	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静的に追加します。
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。
show ip igmp snooping mrouter	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show ip igmp snooping mrouter

スイッチまたは指定されたマルチキャスト VLAN（仮想 LAN）の、動的に学習された Internet Group Management Protocol（IGMP）スヌーピングと、手動で設定されたマルチキャスト ルータ ポートを表示するには、**show ip igmp snooping mrouter** イネーブル EXEC コマンドを使用します。

show ip igmp snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）VLAN（仮想 LAN）を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、スイッチまたは特定の VLAN のマルチキャスト ルータ ポートを表示します。

VLAN ID 1002 ～ 1005 はトークンリングおよび FDDI VLAN 用に確保されていて、IGMP スヌーピングには使用できません。

Multicast VLAN Registration（MVR）をイネーブルにすると、**show ip igmp snooping mrouter** コマンドは MVR マルチキャスト ルータ情報と IGMP スヌーピングを表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping mrouter** コマンドの出力を示します。ここでは、スイッチでマルチキャスト ルータ ポートを表示する方法を示します。

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi0/1(dynamic)
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加します。
ip igmp snooping vlan static	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静的に追加します。
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。
show ip igmp snooping groups	スイッチまたは指定されたパラメータの 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 querier

スイッチに設定された IGMP クエリアの設定および動作情報を表示するには、**show ip igmp snooping querier detail** ユーザ EXEC コマンドを使用します。

show ip igmp snooping querier [**detail** | **vlan** ***vlan-id*** [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）詳細な IGMP クエリア情報を表示します。
vlan *vlan-id* [**detail**]	（任意）指定された VLAN（仮想 LAN）の IGMP クエリア情報を表示します。指定できる範囲は、1 ～ 1001 および 1006 ～ 4094 です。詳細情報を表示するには、**detail** キーワードを使用します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

querier とも呼ばれる IGMP クエリー メッセージを送信する検出装置の IGMP バージョンおよび IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットには複数のマルチキャスト ルータを設定できますが、設定できるIGMPクエリアは1つだけです。IGMPv2 が実行されているサブネットの場合、マルチキャスト ルータの 1 つをクエリアとして選択します。レイヤ 3 スイッチをクエリアにすることもできます。

show ip igmp snooping querier コマンド出力には、クエリアが検出された VLAN およびインターフェイスも表示されます。スイッチがクエリアの場合、コマンド出力では *Port* フィールドに *Router* が表示されます。クエリアがルータの場合、コマンド出力では、*Port* フィールドにクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに類似しています。ただし、**show ip igmp snooping querier** はスイッチ クエリアによって最後に検出されたデバイスの IP アドレスだけを表示します。

show ip igmp snooping querier detail は、スイッチ クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報を表示します。

- VLAN（仮想 LAN）で選択されている IGMP クエリア
- VLAN に設定されているスイッチ クエリアに関連する設定および動作情報（存在する場合）

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping querier** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
--------------------------------------------------
1         172.20.50.11    v3                  Gi0/1
2         172.20.40.20    v2                  Router
```

次の例では、**show ip igmp snooping querier detail** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version   Port
-----------------------------------------------------------
1         1.1.1.1         v2             Fa0/1

Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10

Vlan 1:   IGMP switch querier status

-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをスイッチまたは VLAN でイネーブルにします。
ip igmp snooping querier	IGMP クエリア機能をレイヤ 2 ネットワークでイネーブルにします。
show ip igmp snooping	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show lacp

Link Aggregation Control Protocol（LACP）チャネル グループ情報を表示するには、**show lacp** ユーザ EXEC コマンドを使用します。

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 6 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバ情報を表示します。
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。システム識別子は、LACP システム プライオリティとスイッチ MAC アドレスで構成されています。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show lacp コマンドを入力すると、アクティブ チャネル グループの情報が表示されます。特定のチャネル情報を表示するには、チャネル グループ番号を指定して **show lacp** コマンドを入力します。

チャネル グループを指定しない場合は、すべてのチャネル グループ情報が表示されます。

channel-group-number オプションを入力すると、**sys-id** を除いたすべてのキーワードのチャネル グループが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。表 2-24 に、表示されるフィールドの説明を示します。

```
Switch> show lacp counters
               LACPDUs          Marker      Marker Response    LACPDUs
Port          Sent    Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group:1
Gi0/1         19      10       0      0        0      0         0
Gi0/2         14      6        0      0        0      0         0
```

表 2-24　show lacp counters のフィールドの説明

フィールド	説明
LACPDUs Sent/Recv	ポートによって送受信された LACP パケット数
Marker Sent/Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent/Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts Err	ポートの LACP によって受信された、未知で不正なパケット数

次の例では、**show lacp internal** コマンドの出力を示します。

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port        Flags   State   Priority      Key       Key     Number   State
Gi0/1       SA      bndl    32768         0x3       0x3     0x4      0x3D
Gi0/2       SA      bndl    32768         0x3       0x3     0x5      0x3D
```

表 2-25 に、この出力で表示されるフィールドの説明を示します。

表 2-25　show lacp internal のフィールドの説明

フィールド	説明
State	特定ポートのステート。許可された値には次のものがあります。 • 磨怎 |ートは unknown ステートです。 • **bndl** — ポートはアグリゲータに適用され、その他ポートとともにバンドルされます。 • **susp** — ポートは suspended ステートです。アグリゲータに適用されません。 • **hot-sby** — ポートは hot-standby ステートです。 • **indiv** — ポートをその他ポートとともにバンドルできません。 • **indep** — ポートは independent ステート（バンドルされませんがデータ トラフィックを切り替えます。この場合、LACP は相手側ポートで稼働していません）です。 • **down** — ポートがダウンしています。
LACP Port Priority	ポート プライオリティ設定。互換ポートの統合を妨げるようなハードウェア制限がある場合に、LACP はポート プライオリティを使用するとポートをスタンバイ モードにします。
Admin Key	このポートに割り当てられた管理キー。LACP は、管理キー値を 16 進数で自動的に生成します。管理キーは、その他ポートと統合するポートの機能を定義します。その他ポートと統合するポートの機能は、ポートの物理特性（たとえば、データ転送速度やデュプレックス機能）と設定制限によって判断されます。
Oper Key	このポートで使用されるランタイム動作キー。LACP は、この値を 16 進数で自動的に生成します。
Port Number	ポート番号

表 2-25　show lacp internal のフィールドの説明（続き）

フィールド	説明
Port State	8 ビットの各ビットに割り付けられたポートのステート変数。意味は次のとおりです。 • ビット 0：LACP_Activity • ビット 1：LACP_Timeout • ビット 2：Aggregation • ビット 3：Synchronization • ビット 4：Collecting • ビット 5：Distributing • ビット 6：Defaulted • ビット 7：Expired （注）　上記のリストでは、ビット 7 が MSB でビット 0 が LSB です。

次の例では、**show lacp neighbor** コマンドの出力を示します。

```
Switch> show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/1     32768,0007.eb49.5e80  0xC              19s        SP

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          32768                0x3             0x3C

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/2     32768,0007.eb49.5e80  0xD              15s        SP

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          32768                0x3             0x3C
```

次の例では、**show lacp sys-id** コマンドの出力を示します。

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

システム識別子は、システム プライオリティとシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティで、後ろの 6 バイトはシステムに関連付けられ、グローバルに管理される各 MAC アドレスです。

関連コマンド

コマンド	説明
clear lacp	LACP チャネル グループ情報を消去します。
lacp port-priority	LACP ポート プライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。

show mac access-group

特定のインターフェイスまたはスイッチに設定されている MAC（メディア アクセス制御）Access Control List（ACL; アクセス制御リスト）を表示するには、**show mac access-group** ユーザ EXEC コマンドを使用します。

show mac access-group [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）特定のインターフェイスで設定された MAC ACL を表示します。有効なインターフェイスは物理ポートとポート チャネルです。ポート チャネル範囲は 1 ～ 6 です（イネーブル EXEC モードでのみ使用可能）。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac-access group** ユーザ EXEC コマンドの出力を示します。この表示の場合、ポート 2 には、適用される MAC アクセス リスト *macl_e1* があります。MAC ACL は他のインターフェイスに適用されません。

```
Switch> show mac access-group
Interface GigabitEthernet0/1:
   Inbound access-list is not set
Interface GigabitEthernet0/2:
   Inbound access-list is macl_e1
Interface GigabitEthernet0/3:
   Inbound access-list is not set
Interface GigabitEthernet0/4:
   Inbound access-list is not set

(テキスト出力は省略)
```

次の例では、**show mac access-group interface gigabitethernet0/1** コマンドの出力を示します。

```
Switch# show mac access-group interface gigabitethernet0/1
Interface GigabitEthernet0/1:
   Inbound access-list is macl_e1
```

関連コマンド

コマンド	説明
mac access-group	インターフェイスに MAC アクセス グループを適用します。

show mac address-table

特定の MAC（メディア アクセス制御）アドレス テーブル スタティック エントリおよびダイナミック エントリ、または特定インターフェイスまたは VLAN（仮想 LAN）の MAC アドレス テーブル スタティック エントリおよびダイナミック エントリを表示するには、**show mac address-table** ユーザ EXEC コマンドを使用します。

show mac address-table [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table** コマンドの出力を示します。

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
 All    0000.0000.0001    STATIC      CPU
 All    0000.0000.0002    STATIC      CPU
 All    0000.0000.0003    STATIC      CPU
 All    0000.0000.0009    STATIC      CPU
 All    0000.0000.0012    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
   1    0030.9441.6327    DYNAMIC     Gi0/4
Total Mac Addresses for this criterion: 12
```

関連コマンド

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスのMACアドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table address

指定された MAC（メディア アクセス制御）アドレスの MAC アドレス テーブル情報を表示するには、**show mac address-table address** ユーザ EXEC コマンドを使用します。

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

mac-address	48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です。
interface *interface-id*	（任意）特定のインターフェイスの情報を表示します。指定できるインターフェイスとしては、物理ポートおよびポート チャネルがあります。
vlan *vlan-id*	（任意）特定の VLAN（仮想 LAN）のエントリのみを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table address** コマンドの出力を示します。

```
Switch# show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

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 のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスのMACアドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table aging-time

特定のアドレス テーブル インスタンスのエージング タイムと、特定の VLAN（仮想 LAN）上、または特定の VLAN が指定されていない場合はすべての VLAN 上のアドレス テーブル インスタンスのエージング タイムすべてを表示するには、**show mac address-table aging-time** ユーザ EXEC コマンドを使用します。

show mac address-table aging-time [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）特定の VLAN のエージング タイム情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN 番号が指定されていない場合、すべての VLAN のエージング タイムが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table aging-time** コマンドの出力を示します。

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

次の例では、**show mac address-table aging-time vlan 10** コマンドの出力を示します。

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

関連コマンド

コマンド	説明
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 テーブル内に保持される時間を設定します。
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table count

すべての VLAN（仮想 LAN）または指定された VLAN に存在するアドレス数を表示するには、**show mac address-table count** ユーザ EXEC コマンドを使用します。

show mac address-table count [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）特定の VLAN のアドレス数を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN 番号が指定されていない場合、すべての VLAN のアドレス カウントが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table count** コマンドの出力を示します。

```
Switch# show mac address-table count
Mac Entries for Vlan    : 1
---------------------------
Dynamic Address Count   : 2
Static  Address Count   : 0
Total Mac Addresses     : 2
```

関連コマンド

コマンド	説明
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table dynamic

ダイナミック MAC（メディア アクセス制御）アドレス テーブル エントリのみを表示するには、**show mac address-table dynamic** ユーザ EXEC コマンドを使用します。

show mac address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

address *mac-address*	（任意）48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です（イネーブル EXEC モードでのみ利用できます）。
interface *interface-id*	（任意）マッチングを行う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としては、物理ポートおよびポート チャネルがあります。
vlan *vlan-id*	（任意）特定の VLAN のエントリを指定します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table dynamic** コマンドの出力を示します。

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table interface

特定の VLAN（仮想 LAN）で指定されたインターフェイスの MAC（メディア アクセス制御）アドレス テーブル情報を表示するには、**show mac address-table interface** ユーザ コマンドを使用します。

show mac address-table interface *interface-id* [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイス タイプを指定します。有効なインターフェイスとしては、物理ポートおよびポート チャネルがあります。
vlan *vlan-id*	（任意）特定のVLANのエントリを指定します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table interface** コマンドの出力を示します。

```
Switch> show mac address-table interface gigabitethernet0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定のVLANのMACアドレス テーブル情報を表示します。

show mac address-table move update

スイッチの MAC アドレス テーブル移動更新情報を表示するには、**show mac address-table move update** ユーザ EXEC コマンドを使用します。

show mac address-table move update [| {**begin** | **exclude** | **include**} **expression**]

構文の説明

| **begin**	（任意）*expression* と一致する行から表示を開始します。
| **exclude**	（任意）*expression* と一致する行を表示から除外します。
| **include**	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、|**exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Switch> show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
switch#
```

関連コマンド

コマンド	説明
clear mac address-table move update	MAC アドレス テーブル移動更新カウンタをクリアします。
mac address-table move update {**receive** | **transmit**}	スイッチの MAC アドレス テーブル移動更新を設定します。

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（メディア アクセス制御）アドレス通知設定を表示するには、**show mac address-table notification** ユーザ EXEC コマンドを使用します。

show mac address-table notification [**interface** [*interface-id*]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface	（任意）すべてのインターフェイスの情報を表示します。指定できるインターフェイスとしては、物理ポートおよびポート チャネルがあります。
interface-id	（任意）指定されたインターフェイスの情報を表示します。指定できるインターフェイスとしては、物理ポートおよびポート チャネルがあります。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

キーワードを指定しないで **show mac address-table notification** コマンドを使用すると、機能がイネーブルかディセーブルか、MAC 通知間隔、履歴テーブルの最大許容エントリ数、および履歴テーブル内容を表示します。

interface キーワードを使用すると、すべてのインターフェイスのフラグを表示します。*interface-id* が含まれる場合、指定したインターフェイスのフラグのみが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table notification** コマンドの出力を示します。

```
Switch> show mac address-table notification
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

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 address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table static

スタティック MAC（メディア アクセス制御）アドレス テーブル エントリのみを表示するには、**show mac address-table static** ユーザ EXEC コマンドを使用します。

show mac address-table static [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

address *mac-address*	（任意）48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です（イネーブル EXEC モードでのみ利用できます）。
interface *interface-id*	（任意）マッチングを行う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としては、物理ポートおよびポート チャネルがあります。
vlan *vlan-id*	（任意）特定の VLAN のアドレスを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table static** コマンドの出力を示します。

```
Switch> show mac address-table static

          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

関連コマンド

コマンド	説明
mac address-table static	MAC アドレス テーブルにスタティック アドレスを追加します。
mac address-table static drop	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、特定の送信元または宛先 MAC アドレスを持つトラフィックを廃棄するようにスイッチを設定します。
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table vlan

指定された VLAN（仮想 LAN）の MAC（メディア アクセス制御）アドレス テーブル情報を表示するには、**show mac address-table vlan** ユーザ EXEC コマンドを使用します。

show mac address-table vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan-id	（任意）特定の VLAN のアドレスを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table vlan 1** コマンドの出力を示します。

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

関連コマンド

コマンド	説明
show mac address-table address	特定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN に存在するアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。

show mls qos

グローバルな Quality of Service（QoS; サービス品質）設定情報を表示するには、**show mls qos** ユーザ EXEC コマンドを使用します。

show mls qos [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、QoS がイネーブルで、Differentiated Services Code Point（DSCP）透過性がディセーブルの場合の **show mls qos** コマンドの出力を示します。

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is disabled
```

次の例では、QoS および DSCP 透過性がイネーブルの場合の **show mls qos** コマンドの出力を示します。

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

関連コマンド

コマンド	説明
mls qos	スイッチ全体に対して QoS をイネーブルにします。

show mls qos aggregate-policer

Quality of Service（QoS; サービス品質）アグリゲート ポリサー設定を表示するには、**show mls qos aggregate-policer** ユーザ EXEC 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。

show mls qos aggregate-policer [*aggregate-policer-name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

aggregate-policer-name	（任意）指定された名前のポリシー設定を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos aggregate-policer** コマンドの出力を示します。

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

関連コマンド

コマンド	説明
mls qos aggregate-policer	ポリシー マップ内で複数のクラスが共有するポリサー パラメータを定義します。

show mls qos input-queue

入力キューの Quality of Service（QoS; サービス品質）を表示するには、**show mls qos input-queue** ユーザ EXEC コマンドを使用します。

show mls qos input-queue [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos input-queue** コマンドの出力を示します。

```
Switch> show mls qos input-queue
Queue     :       1       2
-------------------------------------------
buffers   :       90      10
bandwidth :       4       4
priority  :       0       10
threshold1:       100     100
threshold2:       100     100
```

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	割り当てられた Class of Service（CoS; サービス クラス）値を入力キューにマッピングし、CoS 値をキューとスレッシュホールド ID に割り当てます。
mls qos srr-queue input dscp-map	割り当てられた Differentiated Services Code Point（DSCP）値を入力キューにマッピングし、DSCP 値をキューとスレッシュホールド ID に割り当てます。
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; 重み付きテール廃棄）スレッシュホールドのパーセントを入力キューに割り当てます。

show mls qos interface

Quality of Service（QoS; サービス品質）情報をポート レベルで表示するには、**show mls qos interface** ユーザ EXEC コマンドを使用します。

show mls qos interface [*interface-id*] [**buffers** | **queueing** | **statistics**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）指定されたポートの QoS 情報を表示します。指定できるインターフェイスとして、物理ポートも含まれます。
buffers	（任意）キュー間のバッファ割り当てを表示します。
queueing	（任意）キューイング方法（共有、またはシェーピング）とキューに対応する重みを表示します。
statistics	（任意）送受信された Differentiated Services Code Point（DSCP）の統計情報、Class of Service（CoS; サービス クラス）値、キューに入れられた、または出力キュー単位で削除されたパケット数、各ポリサーのプロファイル内外のパケット数を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

（注）　**policers** 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ていますが、サポートされていません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、VLAN ベース QoS がイネーブルの場合の **show mls qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet0/1
GigabitEthernet0/1
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:vlan-based
```

次の例では、VLAN ベース QoS がディセーブルの場合の **show mls qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet0/2
GigabitEthernet0/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based
```

次の例では、**show mls qos interface** *interface-id* **buffers** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet0/2 buffers
GigabitEthernet0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

次の例では、**show mls qos interface** *interface-id* **queueing** コマンドの出力を示します。出力緊急キューは、設定された Shaped Round Robin（SRR）の重みを無効にします。

```
Switch> show mls qos interface gigabitethernet0/2 queueing
GigabitEthernet0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth is limited to: 100%
The port is mapped to qset : 1
```

次の例では、**show mls qos interface** *interface-id* **statistics** コマンドの出力を示します。表 2-26 に、表示されるフィールドの説明を示します。

```
Switch> show mls qos interface gigabitethernet0/2 statistics
GigabitEthernet0/2

  dscp: incoming
-------------------------------

  0 -  4 :      4213          0          0          0          0
  5 -  9 :         0          0          0          0          0
 10 - 14 :         0          0          0          0          0
 15 - 19 :         0          0          0          0          0
 20 - 24 :         0          0          0          0          0
 25 - 29 :         0          0          0          0          0
 30 - 34 :         0          0          0          0          0
 35 - 39 :         0          0          0          0          0
 40 - 44 :         0          0          0          0          0
 45 - 49 :         0          0          0          6          0
 50 - 54 :         0          0          0          0          0
 55 - 59 :         0          0          0          0          0
 60 - 64 :         0          0          0          0
  dscp: outgoing
-------------------------------

  0 -  4 :    363949          0          0          0          0
  5 -  9 :         0          0          0          0          0
 10 - 14 :         0          0          0          0          0
 15 - 19 :         0          0          0          0          0
 20 - 24 :         0          0          0          0          0
 25 - 29 :         0          0          0          0          0
 30 - 34 :         0          0          0          0          0
 35 - 39 :         0          0          0          0          0
 40 - 44 :         0          0          0          0          0
 45 - 49 :         0          0          0          0          0
 50 - 54 :         0          0          0          0          0
 55 - 59 :         0          0          0          0          0
 60 - 64 :         0          0          0          0
  cos: incoming
-------------------------------

  0 -  4 :    132067          0          0          0          0
  5 -  9 :         0          0          0
  cos: outgoing
-------------------------------

  0 -  4 :    739155          0          0          0          0
  5 -  9 :        90          0          0

Policer: Inprofile:        0 OutofProfile:        0
```

表 2-26　show mls qos interface statistics のフィールドの説明

フィールド		説明
dscp	incoming	DSCP 値ごとに受信したパケット数
	outgoing	DSCP 値ごとに送信したパケット数
CoS	incoming	CoS 値ごとに受信したパケット数
	outgoing	CoS 値ごとに送信したパケット数
Policer	Inprofile	ポリサーごとのプロファイル内パケット数
	OutofProfile	ポリサーごとのプロファイル外パケット数

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; 重み付きテール廃棄）スレッシュホールドを設定し、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。
mls qos srr-queue input bandwidth	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、または CoS 値をキューとスレッシュホールド 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、または DSCP 値をキューとスレッシュホールド 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 スレッシュホールドのパーセントを入力キューに割り当てます。
mls qos srr-queue output cos-map	CoS 値を出力キュー、またはキューとスレッシュホールド 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、またはキューとスレッシュホールド ID にマッピングします。
policy-map	ポリシー マップを作成、または変更します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対するポートをマッピングします。
srr-queue bandwidth limit	ポートでの最大出力を制限します。
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出力キュー 4 つで帯域幅をシェーピングします。
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出力キュー 4 つで帯域幅を共有します。

show mls qos maps

Quality of Service（QoS; サービス品質）マッピング情報を表示するには、**show mls qos maps** ユーザ EXEC コマンドを使用します。分類では、QoS はマッピング テーブルを使用してトラフィックのプライオリティを表示し、受信した Class of Service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP）、または IP precedence 値から対応する CoS または DSCP 値を取得します。

show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

cos-dscp	（任意）CoS/DSCP マップを表示します。
cos-input-q	（任意）CoS 入力キュー スレッシュホールド マップを表示します。
cos-output-q	（任意）CoS 出力キュー スレッシュホールド マップを表示します。
dscp-cos	（任意）DSCP/CoS マップを表示します。
dscp-input-q	（任意）DSCP 入力キュー スレッシュホールド マップを表示します。
dscp-mutation *dscp-mutation-name*	（任意）指定された DSCP/DSCP-mutation マップを表示します。
dscp-output-q	（任意）DSCP 出力キュー スレッシュホールド マップを表示します。
ip-prec-dscp	（任意）IP precedence/DSCP マップを表示します。
policed-dscp	（任意）ポリシング設定 DSCP マップを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

ポリシング設定 DSCP、DSCP/CoS、および DSCP/DSCP-mutation マップは、マトリックスとして表示されます。d1 列では、DSCP で最も重要度の高い桁を指定します。d2 行では、DSCP で最も重要度の低い桁を指定します。d1 値および d2 値の共通部分では、ポリシング設定 DSCP、CoS、または Mutated-DSCP値を提供します。たとえば、DSCP/CoSマップでは、DSCP値43はCoS値5に対応します。

DSCP 入力キュー スレッシュホールドおよび DSCP 出力キュー スレッシュホールド マップは、マトリックスとして表示されます。d1 列では、最も重要度の高い DSCP 番号の桁を指定します。d2 行では、最も重要度の低い DSCP 番号の桁を指定します。d1 値および d2 値の共通部分は、キュー ID とスレッシュホールド ID を示します。たとえば、DSCP 入力キュー スレッシュホールド マップでは、DSCP 値 43 はキュー 2 とスレッシュホールド 1（02-01）に対応します。

CoS 入力キュー スレッシュホールドおよび CoS 出力キュー スレッシュホールド マップでは、1 番めの行に CoS 値、および 2 番めの行に対応するキュー ID とスレッシュホールド ID を示します。たとえば、CoS 入力キュー スレッシュホールド マップでは、CoS 値 5 はキュー 2 とスレッシュホールド 1（2-1）に対応します。

例

次の例では、**show mls qos maps** コマンドの出力を示します。

```
Switch> show mls qos maps
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07

Cos-dscp map:
     cos:   0  1  2  3  4  5  6  7
  --------------------------------
    dscp:   0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  8 16 24 32 40 48 56

Dscp-outputq-threshold map:
  d1 :d2    0     1     2     3     4     5     6     7     8     9
  ------------------------------------------------------------------------
   0 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
   1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
   2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
   3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
   5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   6 :    04-01 04-01 04-01 04-01

Dscp-inputq-threshold map:
    d1 :d2    0     1     2     3     4     5     6     7     8     9
    ------------------------------------------------------------------------
     0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
     5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

   Cos-inputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1
```

```
Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

関連コマンド

コマンド	説明
mls qos map	CoS/DSCPマップ、DSCP/CoSマップ、DSCP/DSCP-mutation 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。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピングする、または CoS 値をキューとスレッシュホールド 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、または DSCP 値をキューとスレッシュホールド ID にマッピングします。
mls qos srr-queue output cos-map	CoS 値を出力キュー、またはキューとスレッシュホールド 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、またはキューとスレッシュホールド ID にマッピングします。

show mls qos queue-set

出力キューの Quality of Service（QoS; サービス品質）を表示するには、**show mls qos queue-set** ユーザ EXEC コマンドを使用します。

show mls qos queue-set [*qset-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

qset-id	（任意）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。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos queue-set** コマンドの出力を示します。

```
Switch> show mls qos queue-set
Queueset: 1
Queue     :        1       2       3       4
----------------------------------------------
buffers   :       25      25      25      25
threshold1:       100     200     100     100
threshold2:       100     200     100     100
reserved  :       50      50      50      50
maximum   :       400     400     400     400
Queueset: 2
Queue     :        1       2       3       4
----------------------------------------------
buffers   :       25      25      25      25
threshold1:       100     200     100     100
threshold2:       100     200     100     100
reserved  :       50      50      50      50
maximum   :       400     400     400     400
```

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; 重み付きテール廃棄）スレッシュホールドを設定し、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 vlan

Switch Virtual Interface（SVI）に適用されているポリシー マップを表示するには、**show mls qos vlan** ユーザ EXEC コマンドを使用します。

show mls qos vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan-id	ポリシー マップを表示するために SVI の VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show mls qos vlan コマンドからの出力は、VLAN ベースの Quality of Service（QoS; サービス品質）がイネーブルでポリシー マップが設定されている場合のみ意味があります。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos vlan** コマンドの出力を示します。

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

関連コマンド

コマンド	説明
policy-map	複数のポートに適用できるポリシー 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 モードを開始します。

show monitor

スイッチ上の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）、および Remote SPAN（RSPAN）セッションに関する情報を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。特定のセッション、すべてのセッション、すべてのローカル セッション、またはすべてのリモート セッションを表示する場合は、キーワードを指定して、このコマンドを使用します。

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

session	（任意）指定された SPAN セッションに関する情報を表示します。
session_number	SPAN または RSPAN セッションの番号を指定します。指定できる範囲は 1 ～ 66 です。
all	すべての SPAN セッションを表示します。
local	ローカル SPAN セッションのみを表示します。
range *list*	SPAN セッションの範囲を表示します。*list* は有効なセッション範囲で、1 つのセッション、または 2 つの番号を、小さい番号を前にしてハイフンで区切って指定するセッション範囲のいずれかです。カンマで区切られたパラメータ間、またはハイフンで指定された範囲にスペースを入力しないでください。 **（注）** このキーワードは、イネーブル EXEC モードの場合のみ使用可能です。
remote	リモート SPAN セッションのみを表示します。
detail	（任意）指定されたセッションに関する詳細情報を表示します。
| begin	*expression* と一致する行から表示を開始します。
| exclude	*expression* と一致する行を表示から除外します。
| include	指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show monitor コマンドと **show monitor session all** コマンドの場合、出力は同じです。

例

次に **show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
Encapsulation : Replicate
Ingress : Disabled

Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi0/2
Destination Ports : Gi0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
---------
Type : Local Session
Source Ports :
Both : Gi0/8
Destination Ports : Gi0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

関連コマンド

コマンド	説明
monitor session	SPAN または RSPAN セッションを、開始または変更します。

show mvr

現在の Multicast VLAN Registration（MVR）グローバル パラメータ値を表示するには、キーワードを指定しないで **show mvr** イネーブル EXEC コマンドを入力します。表示されるのは、MVR がイネーブルであるかどうか、MVR マルチキャスト VLAN（仮想 LAN）、最大クエリー応答時間、マルチキャスト グループ数、および MVR モード（ダイナミックまたはコンパティブル）です。

show mvr [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr** コマンドの出力を示します。

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

上記の例では、マルチキャスト グループの最大数は 256 です。MVR モードは、コンパティブル（Catalyst 2900 XL および Catalyst 3500 XL スイッチと連動する場合）またはダイナミック（動作が IGMP スヌーピング動作と一貫性があり、送信元ポート上でダイナミック MVR メンバーシップがサポートされている場合）のいずれかです。

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で MVR をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr interface	コマンドに **interface** および **members** キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するマルチキャスト グループが表示されます。
show mvr members	MVR マルチキャスト グループに属するポートすべてを表示します。グループ内にメンバーがいない場合、グループは非アクティブであることを示します。

show mvr interface

Multicast VLAN Registration（MVR）レシーバーおよび送信元ポートを表示するには、キーワードを指定しないで **show mvr interface** イネーブル EXEC コマンドを入力します。キーワードを指定してこのコマンドを入力すると、特定のレシーバー ポートの MVR パラメータが表示されます。

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイスの MVR タイプ、ステータス、および即時脱退設定を表示します。 有効なインターフェイスとしては、タイプ、モジュール、ポート番号を含む物理ポートがあります。
members	（任意）指定されたインターフェイスが属する MVR グループをすべて表示します。
vlan *vlan-id*	（任意）VLAN（仮想 LAN）上の MVR グループ メンバーをすべて表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

入力したポートが非 MVR ポートまたは送信元ポートの場合は、エラー メッセージが戻されます。入力したポートがレシーバー ポートの場合は、ポート タイプ、ポート単位のステータス、および即時脱退設定が表示されます。

members キーワードを入力すると、インターフェイス上の MVR グループ メンバーがすべて表示されます。VLAN ID を入力すると、VLAN の MVR グループ メンバーがすべて表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface
Port        Type            Status          Immediate Leave
----        ----            -------         ---------------
Gi0/1       SOURCE          ACTIVE/UP       DISABLED
Gi0/2       RECEIVER        ACTIVE/DOWN     DISABLED
```

上記の Status の定義は、次のとおりです。

- ACTIVE は、ポートが VLAN に含まれていることを意味します。
- UP/DOWN は、ポートが転送中、または転送中ではないかを示します。
- INACTIVE は、ポートが VLAN に含まれていないことを意味します。

次の例では、指定されたインターフェイスの **show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

次の例では、**show mvr interface** *interface-id* **members** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet0/2 members
239.255.0.0     DYNAMIC ACTIVE
239.255.0.1     DYNAMIC ACTIVE
239.255.0.2     DYNAMIC ACTIVE
239.255.0.3     DYNAMIC ACTIVE
239.255.0.4     DYNAMIC ACTIVE
239.255.0.5     DYNAMIC ACTIVE
239.255.0.6     DYNAMIC ACTIVE
239.255.0.7     DYNAMIC ACTIVE
239.255.0.8     DYNAMIC ACTIVE
239.255.0.9     DYNAMIC ACTIVE
```

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で MVR をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr members	MVR マルチキャスト グループに属するすべてのレシーバー ポートを表示します。

show mvr members

現在 IP マルチキャスト グループに属するすべてのレシーバーおよび送信元ポートを表示するには、**show mvr members** イネーブル EXEC コマンドを使用します。

show mvr members [*ip-address*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

ip-address	（任意）IP マルチキャスト アドレスです。IP マルチキャスト アドレスを入力すると、マルチキャスト グループに属するすべてのレシーバーおよび送信元ポートが表示されます。IP マルチキャスト アドレスを入力しない場合は、Multicast VLAN Registration（MVR）グループのすべてのメンバーが表示されます。グループ内にメンバーがない場合は、グループは Inactive として表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show mvr members コマンドは、レシーバーおよび送信元ポートに適用されます。MVR 互換モードの場合、すべての送信元ポートは、すべてのマルチキャスト グループに属します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr members** コマンドの出力を示します。

```
Switch# show mvr members
MVR Group IP    Status          Members
------------    ------          -------
239.255.0.1     ACTIVE          Gi0/1(d), Gi0/5(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None
```

（テキスト出力は省略）

次の例では、**show mvr members** *ip-address* コマンドの出力を示します。次のアドレスを持った IP マルチキャスト グループのメンバーを表示します。

```
Switch# show mvr members 239.255.0.2
239.255.003.--22     ACTIVE          Gi0/1(d), Gi0/2(d), Gi0/3(d),
                                     Gi0/4(d), Gi0/5(s)
```

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で MVR をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr interface	コマンドに **members** キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するマルチキャスト グループが表示されます。

show pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）チャネル グループ情報を表示するには、**show pagp** ユーザ EXEC コマンドを使用します。

show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 6 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバ情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show pagp コマンドを入力すると、アクティブ チャネル グループの情報が表示されます。非アクティブ ポート チャネルの情報を表示するには、チャネル グループ番号を指定して **show pagp** コマンドを入力します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show pagp 1 counters** コマンドの出力を示します。

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi0/1      45     42       0      0
  Gi0/2      45     41       0      0
```

次の例では、**show pagp 1 internal** コマンドの出力を示します。

```
Switch> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1       SC    U6/S7   H       30s      1        128        Any      16
Gi0/2       SC    U6/S7   H       30s      1        128        Any      16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Switch> show pagp 1 neighbor
    Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
            A - Device is in Auto mode.        P - Device learns on physical port.

    Channel group 1 neighbors
                Partner             Partner          Partner           Partner Group
    Port        Name                Device ID        Port         Age  Flags   Cap.
    Gi0/1       switch-p2           0002.4b29.4600   Gi0/1          9s SC      10001
    Gi0/2       switch-p2           0002.4b29.4600   Gi0/2         24s SC      10001
```

関連コマンド

コマンド	説明
clear pagp	PAgP チャネル グループ情報を消去します。

show parser macro

スイッチ上の設定されたすべてのマクロまたは 1 つのマクロに対するパラメータを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

show parser macro [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

brief	（任意）各マクロ名を表示します。
description [**interface** *interface-id*]	（任意）すべてのマクロの説明または特定のインターフェイスの説明を表示します。
name *macro-name*	（任意）マクロ名で指定された 1 つのマクロに関する情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show parser macro** コマンドの出力の一部を示します。シスコのデフォルトのマクロの出力は、スイッチ プラットフォームおよびスイッチ上で動作するソフトウェア イメージによって異なります。

```
Switch# show parser macro
Total number of macros = 6
------------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

(テキスト出力は省略)

------------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

(テキスト出力は省略)
```

```
------------------------------------------------------------
Macro name : cisco-phone
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

(テキスト出力は省略)

------------------------------------------------------------
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

(テキスト出力は省略)

------------------------------------------------------------
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

(テキスト出力は省略)

------------------------------------------------------------
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

------------------------------------------------------------
```

次に **show parser macro name** コマンドの出力例を示します。

```
Switch# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

次に **show parser macro brief** コマンドの出力例を示します。

```
Switch# show parser macro brief
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
    customizable     : snmp
```

次に **show parser macro description** コマンドの出力例を示します。

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface    Macro Description(s)
-----------------------------------------------------------------
Gi0/1        standard-switch10
Gi0/2       this is test macro
-----------------------------------------------------------------
```

次に **show parser macro description interface** コマンドの出力例を示します。

```
Switch# show parser macro description interface gigabitethernet0/2
Interface    Macro Description
-----------------------------------------------------------------
Gi0/2      this is test macro
-----------------------------------------------------------------
```

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、追跡します。
macro description	インターフェイスに適用されるマクロ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、追跡します。
macro global description	スイッチに適用されるマクロの説明を追加します。
macro name	マクロを作成します。
show running-config	定義されたマクロを含む現在稼働中の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。

show policy-map

着信トラフィックの分類基準を定義する Quality of Service（QoS; サービス品質）ポリシー マップを表示するには、**show policy-map** ユーザ EXEC コマンドを使用します。ポリシー マップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。

show policy-map [*policy-map-name* [**class** *class-map-name*]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

policy-map-name	（任意）指定されたポリシーマップの名前を表示します。
class *class-map-name*	（任意）各クラスの QoS ポリシー アクションを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

（注）　**control-plane** および **interface** 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ていますが、サポートされていません。表示されている統計情報を無視します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show policy-map** コマンドの出力を示します。

```
Switch> show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
   set dscp 34
   police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
   set dscp 6
```

関連コマンド

コマンド	説明
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。

show port-security

特定の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するには、**show port-security** イネーブル EXEC コマンドを使用します。

show port-security [**interface** *interface-id*] [**address** | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスとしては、タイプ、モジュール、およびポート番号を含む物理ポートがあります。
address	（任意）すべてのポートまたは指定されたポートのセキュア MAC（メディア アクセス制御）アドレスをすべて表示します。
vlan	（任意）指定されたインターフェイス上の VLAN（仮想 LAN）すべてのポート セキュリティ設定を表示します。キーワードは、スイッチポート モードが **trunk** に設定されているインターフェイスでのみ表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

キーワードを指定しないでこのコマンドを入力すると、スイッチのすべてのセキュア ポートの管理ステータスおよび動作ステータスが出力されます。

interface-id を入力すると、インターフェイスのポート セキュリティ設定が表示されます。

address キーワードを指定してコマンドを入力すると、すべてのインターフェイスのセキュア MAC アドレス、および各セキュア アドレスのエージング情報が表示されます。

interface-id キーワードおよび **address** キーワードを指定してコマンドを入力すると、各セキュア アドレスのエージング情報を持ったインターフェイスの MAC アドレスがすべて表示されます。インターフェイス上でポート セキュリティがイネーブルでない場合も、このコマンドを使用して、そのインターフェイスの MAC アドレスをすべて表示することができます。

vlan キーワードを指定してコマンドを入力すると、インターフェイスの VLAN すべてに対するセキュア MAC アドレスの最大設定数および現在数が表示されます。オプションは、スイッチポート モードが **trunk** に設定されているインターフェイスでのみ表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**|exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show port-security** コマンドの出力を示します。

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
---------------------------------------------------------------------------
     Gi0/1         1               0             0            Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface** *interface-id* コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

次の例では、**show port-security address** コマンドの出力を示します。

```
Switch# show port-security address

Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi0/2       1
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface gigabitethernet0/2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/2 address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi0/2       1
------------------------------------------------------------------
Total Addresses: 1
```

次の例では、**show port-security interface** *interface-id* **vlan** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/2 vlan
Default maximum:not set, using 5120
VLAN  Maximum    Current
    5    default          1
   10    default         54
   11    default        101
   12    default        101
   13    default        201
   14    default        501
```

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

show sdm prefer

特定の機能に対するシステム リソースの割り当てを最大化するために使用可能な Switch Database Management（SDM）テンプレートに関する情報を表示するには、**show sdm prefer** イネーブル EXEC コマンドを使用します。

show sdm prefer [**default** | **qos**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

default	（任意）機能間でシステム リソースのバランスを取るテンプレートを表示します。
qos	（任意）Quality of Service（QoS; サービス品質）Access Control Entry（ACE; アクセス制御エントリ）用のシステム リソースを最大化するテンプレートを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

sdm prefer グローバル コンフィギュレーション コマンドを使用して SDM テンプレートを変更した場合には、設定を有効にするためにスイッチをリロードする必要があります。**reload** イネーブル EXEC コマンドを入力する前に **show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドは現在使用中のテンプレートおよびリロード後にアクティブになるテンプレートを表示します。

各テンプレートに表示される数字は、各機能リソースに対する概略の最大数を表します。実際の数値は、設定されている他の機能の数に依存します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show sdm prefer** コマンドの出力例を示します。

```
Switch# show sdm prefer default
 "default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                8K
  number of IPv4 IGMP groups:                     256
  number of IPv4/MAC qos aces:                    128
  number of IPv4/MAC security aces:               384
```

次の例では、**show sdm prefer qos** コマンドの出力例を示します。

```
Switch# show sdm prefer qos
 "qos" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                8K
  number of IPv4 IGMP groups:                     256
  number of IPv4/MAC qos aces:                    384
  number of IPv4/MAC security aces:               128
```

関連コマンド

コマンド	説明
sdm prefer	SDM テンプレートを最大化されたリソース量に設定します。

show setup express

Express Setup モードがスイッチでアクティブかどうかを表示するには、**show setup express** イネーブル EXEC コマンドを使用します。

show setup express [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例は、**show setup express** コマンドの出力を示しています。

```
Switch# show setup express
express setup mode is active
```

関連コマンド

コマンド	説明
setup express	Express Setup モードをイネーブルにします。

show spanning-tree

スパニングツリー ステート情報を表示するには、**show spanning-tree** ユーザ EXEC コマンドを使用します。

show spanning-tree [*bridge-group* | **active** [**detail**] | **backbonefast** | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration** [digest]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

bridge-group	（任意）ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。
active [**detail**]	（任意）アクティブ インターフェイスのスパニングツリー情報のみを表示します（イネーブル EXEC モードの場合のみ使用可能）。
backbonefast	（任意）スパニングツリー BackboneFast ステータスを表示します。
blockedports	（任意）ブロックされたポートの情報を表示します（イネーブル EXEC モードの場合のみ使用可能）。
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	（任意）このスイッチのステータスおよび設定を表示します（イネーブル EXEC モードの場合のみオプション キーワードが使用可能）。
detail [**active**]	（任意）インターフェイス情報の詳細サマリーを表示します（イネーブル EXEC モードの場合のみ **active** キーワードが使用可能）。
inconsistentports	（任意）矛盾するポートの情報を表示します（イネーブル EXEC モードの場合のみ使用可能）。
interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	（任意）指定されたインターフェイスのスパニングツリー情報を表示します（**portfast** および **state** 以外のオプションはイネーブル EXEC モードでのみすべて使用可能）。各インターフェイスは、スペースで区切って入力します。インターフェイスの範囲は入力できません。有効なインターフェイスとしては、物理ポート、VLAN（仮想 LAN）、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 チャネルは 1 ～ 6 です。

mst [**configuration** [**digest**]] [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	（任意）Multiple Spanning-Tree（MST）のリージョン設定およびステータスを表示します（イネーブル EXEC モードの場合のみ使用可能）。 キーワードの意味は次のとおりです。 • **digest —**（任意）現在の MST 設定識別子（MSTCI）に含まれる MD5 ダイジェストを表示します。標準スイッチ用と先行標準のスイッチ用の、2 つの独立したダイジェストが表示されます（イネーブル EXEC モードでのみ利用可能）。 IEEE 標準の実装のために用語が更新され、*txholdcount* フィールドが追加されました。 境界ポートに対して新しいマスター ロールが表示されます。 IEEE 標準ブリッジが先行標準の BPDU をポートから送信する場合には、単語 *pre-standard* または *Pre-STD* が表示されます。 ポートが先行標準の BPDU を送信するように設定されており、先行標準の BPDU をそのポートで受信していない場合には、単語 *pre-standard (config)* または *Pre-STD-Cf* が表示されます。 先行標準の BPDU を送信するように設定されていないポートで先行標準の BPDU を受信した場合には、単語 *pre-standard (rcvd)* または *Pre-STD-Rx* が表示されます。 ポートが転送ステートに戻るかまたは指定が終了する前に、指定ポートが不良指定情報を受信すると、*dispute* フラグが表示されます。 • *instance-id* **—** 単一のインスタンス ID、ハイフンで区切られた ID 範囲、またはカンマで区切られた一連の ID を指定できます。指定できる範囲は 1 ～ 4094 です。現在設定されているインスタンス数が表示されます。 • **interface** *interface-id* **—**（任意）有効なインターフェイスとしては、物理ポート、VLAN（仮想 LAN）、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 チャネルは 1 ～ 6 です。 • **detail —**（任意）インスタンスまたはインターフェイスの詳細情報を表示します。
pathcost method	（任意）デフォルトのパス コスト方式を表示します（イネーブル EXEC モードの場合のみ使用可能）。
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	（任意）ルート スイッチのステータスおよび設定を表示します（すべてのキーワードはイネーブル EXEC モードの場合のみ使用可能）。
summary [**totals**]	（任意）ポート状態のサマリー、またはスパニングツリー ステート セクションの総行数を表示します。単語 *IEEE Standard* は、スイッチで実行されている MST バージョンを示します。
uplinkfast	（任意）スパニングツリー UplinkFast ステータスを表示します。
vlan *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	（任意）指定された VLAN のスパニングツリー情報を表示します（キーワードの一部はイネーブル EXEC モードの場合のみ使用可能）。VLAN ID 番号によって特定される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。

| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	**digest** キーワードが追加され、新しい digest フィールドと transmit hold count フィールドが表示されます。

使用上の注意事項

vlan-id 変数を省略した場合は、すべての VLAN のスパニングツリー インスタンスにコマンドが適用されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show spanning-tree active** コマンドの出力を示します。

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0001.42e2.cdd0
              Cost        3038
              Port        24 (GigabitEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    49153  (priority 49152 sys-id-ext 1)
              Address     0003.fd63.9580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 3019      128.24   P2p
(テキスト出力は省略)
```

次の例では、**show spanning-tree detail** コマンドの出力を示します。

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled
```

```
 Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
(テキスト出力は省略)
```

次の例では、**show spanning-tree interface** *interface-id* コマンドの出力を示します。

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is enabled
BackboneFast         is enabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
(テキスト出力は省略)
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----------------------
Number of transitions via uplinkFast (all VLANs)            : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs)           : 0
Number of inferior BPDUs received (all VLANs)               : 0
Number of RLQ request PDUs received (all VLANs)             : 0
Number of RLQ response PDUs received (all VLANs)            : 0
Number of RLQ request PDUs sent (all VLANs)                 : 0
Number of RLQ response PDUs sent (all VLANs)                : 0
```

次の例では、**show spanning-tree mst configuration** コマンドの出力を示します。

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
-------------------------------
```

次の例では、**show spanning-tree mst interface** *interface-id* コマンドの出力を示します。

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

次の例では、**show spanning-tree mst 0** コマンドの出力を示します。

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
                      port    Gi0/1           path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
---------------------  ---- ----- --------- ---- --------------------------------
GigabitEthernet0/1     root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2     desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

関連コマンド

コマンド	説明
clear spanning-tree counters	スパニングツリーのカウンタをクリアします。
clear spanning-tree detected-protocols	プロトコル移行プロセスを再開します。
spanning-tree backbonefast	BackboneFast 機能をイネーブルにします。
spanning-tree bpdufilter	インターフェイスでの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree extend system-id	拡張システム ID 機能をイネーブルにします。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループガード機能をイネーブルにします。
spanning-tree link-type	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するように、デフォルト リンクタイプ設定を上書きします。
spanning-tree loopguard default	単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されないようにします。
spanning-tree mst configuration	MST リージョンを設定するための MST コンフィギュレーション モードを開始します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。

コマンド	説明
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニングツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU を廃棄してインターフェイス用に保持していた情報を期限切れにするまでの、MST リージョンでのホップ数を設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast対応インターフェイス上でBPDUフィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	リンクまたはスイッチに障害がある場合、またはスパニングツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。
spanning-tree vlan	VLAN 単位でスパニングツリーを設定します。

show storm-control

スイッチまたは指定されたインターフェイスのブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御の設定、またはストーム制御の履歴を表示するには、**show storm-control** ユーザ EXEC コマンドを使用します。

show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）タイプ、モジュール、およびポート番号を含む、物理ポートのインターフェイス ID です。
broadcast	（任意）ブロードキャスト ストーム スレッシュホールド設定を表示します。
multicast	（任意）マルチキャスト ストーム スレッシュホールド設定を表示します。
unicast	（任意）ユニキャスト ストーム スレッシュホールド設定を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

interface-id を入力すると、指定されたインターフェイスのストーム制御スレッシュホールドが表示されます。

interface-id を入力しない場合、スイッチ上のポートすべてのトラフィック タイプの設定が表示されます。

トラフィック タイプを指定しない場合は、ブロードキャスト ストーム制御の設定が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、キーワードを指定しない場合の **show storm-control** コマンドの出力の一部を示します。トラフィック タイプ キーワードを指定しないので、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control
Interface    Filter State   Upper        Lower      Current
---------    -------------  ----------   ---------  ---------
Gi0/1        Forwarding     20 pps       10 pps     5 pps
Gi0/2        Forwarding     50.00%       40.00%     0.00%
(テキスト出力は省略)
```

次の例では、特定のインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプ キーワードを指定しないので、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control gigabitethernet 0/1
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
```

表 2-27 に、**show storm-control** で表示されるフィールドの説明を示します。

表 2-27　show storm-control のフィールドの説明

フィールド	説明
Interface	インターフェイスの ID を表示します。
Filter State	フィルタのステータスを表示します。 • Blocking — ストーム制御はイネーブルであり、ストームが発生しています。 • Forwarding — ストーム制御はイネーブルであり、ストームは発生していません。 • Inactive — ストーム制御はディセーブルされています。
Upper	合計利用可能帯域に対する上昇抑制レベルのパーセント（%）をパケット / 秒またはビット / 秒で表示します。
Lower	合計利用可能帯域に対する下降抑制レベルのパーセント（%）をパケット / 秒またはビット / 秒で表示します。
Current	ブロードキャスト トラフィックまたは指定されたトラフィック タイプ（ブロードキャスト、マルチキャスト、またはユニキャスト）の帯域幅使用率を、利用可能な合計帯域幅に対するパーセントとして表示します。このフィールドは、ストーム制御がイネーブルの場合のみ有効です。

関連コマンド

コマンド	説明
storm-control	スイッチのブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御レベルを設定します。

show system mtu

グローバル Maximum Transmission Unit（MTU; 最大伝送ユニット）、またはスイッチの最大パケット サイズ設定を表示するには、**show system mtu** イネーブル EXEC コマンドを使用します。

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

system mtu または **system mtu jumbo** 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 MTU 設定を変更した場合、スイッチをリセットするまで新しい設定は有効になりません。

システム MTU は 10/100 Mbps で動作するポートを、システム ジャンボ MTU はギガビット ポートを、システム ルーティング MTU はルーテッド ポートを参照します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
```

関連コマンド

コマンド	説明
system mtu	ファスト イーサネット ポート、ギガビット イーサネット ポート、またはルーテッド ポートの MTU サイズを設定します。

show udld

すべてのポートまたは指定されたポートの UniDirectional Link Detection（UDLD; 単一方向リンク検出）管理ステータスおよび動作ステータスを表示するには、**show udld** イネーブル EXEC コマンドを使用します。

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイスの ID およびポート番号です。指定できるインターフェイスとして、物理ポートおよび VLAN（仮想 LAN）も含まれます。指定できる VLAN 範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

interface-id を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show udld** *interface-id* コマンドの出力を示します。次の例では、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを検出します。表 2-28 に、この例で使用されるフィールドの説明を示します。

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

表 2-28　show udld のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブル ステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼働しているかどうかを示す動作ステート
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	現在の UDLD ステート マシンのフェーズ。通常の双方向リンクの場合は、ほとんどの場合、ステート マシンはアドバタイズ フェーズです。
Message interval	ローカル デバイスからアドバタイズ メッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD が近接装置からのエコーを待機する期間（秒）
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間（秒）
Device ID	近接装置の ID
Current neighbor state	ネイバの現在のステート。ローカル デバイスおよび近接装置の両方で UDLD が通常どおり稼働している場合、ネイバ ステートおよびローカル ステートは双方向です。リンクがダウンしているか、またはネイバが UDLD 対応でない場合、キャッシュ エントリは表示されません。
Device name	装置名またはネイバのシステム シリアル番号。装置名が設定されていない、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバのポート ID
Neighbor echo 1 device	エコーの送信元であるネイバの装置名
Neighbor echo 1 port	エコーの送信元であるネイバのポート番号 ID
Message interval	ネイバがアドバタイズ メッセージを送信する速度（秒）
CDP device name	CDP デバイス名またはシステム シリアル番号。装置名が設定されていない、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。

関連コマンド

コマンド	説明
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにする、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	UDLD によるすべてのインターフェイス シャットダウンをリセットし、トラフィックが再び通過するのを許可します。

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するには、**show version** ユーザ EXEC コマンドを使用します。

show version [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show version** コマンドの出力を示します。

（注）　**show version** 出力には表示されていますが、*設定レジスタ* 情報はスイッチでサポートされていません。

```
Switch> show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(0.0.16)FX, CISCO
DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 17-May-05 01:43 by yenanh

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M), Version 12.2 [lqian-flo_pilsner 100]

 Switch uptime is 3 days, 20 hours, 8 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-0.0.16.FX.bin"

cisco WS-C2960-24TC-L (PowerPC405) processor with 61440K/4088K bytes of memory.
Processor board ID FHH0916001J
Last reset from power-on
Target IOS Version 12.2(25)FX
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:FC:FF:E8:80
Motherboard assembly number     : 73-9832-02
Motherboard serial number       : FHH0916001J
Motherboard revision number     : 01
System serial number            : FHH0916001J
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version              SW Image
------   -----  -----              ----------              ----------
*    1   26     WS-C2960-24TC-L    12.2(0.0.16)FX          C2960-LANBASE-M

Configuration register is 0xF
```

show vlan

スイッチ上のすべての設定済み VLAN（仮想 LAN）または特定の VLAN（VLAN ID または名前を指定した場合）のパラメータを表示するには、**show vlan** ユーザ EXEC コマンドを使用します。

show vlan [**brief** | **id** *vlan-id* **mtu** | **name** *vlan-name* | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

brief	（任意）VLAN ごとに VLAN 名、ステータス、およびポートを 1 行で表示します。
id *vlan-id*	（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。*vlan-id* の場合、指定できる範囲は 1 ～ 4094 です。
mtu	（任意）VLAN のリストと VLAN のポートに設定されている最小および Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズのリストを表示します。
name *vlan-name*	（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
remote-span	（任意）Remote SPAN（RSPAN; リモート SPAN）VLAN に関する情報を表示します。
summary	（任意）VLAN サマリー情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

（注）　**ifindex**、**internal usage**、および **private-vlan** 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ていますが、サポートされていません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に *yes* が表示されている場合、VLAN の各ポートに別々の MTU があり、大きな MTU を持つポートからそれより小さな MTU を持つポートへスイッチングされたパケットは廃棄される場合があります。VLAN に SVI がない場合、ハイフン（-）記号が SVI_MTU 列に表示されます。MTU-Mismatch 列に *yes* が表示されている場合、MiniMTU を持つポートと MaxMTU を持つポート名が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vlan** コマンドの出力を示します。表 2-29 に、表示されるフィールドの説明を示します。

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                Gi0/13, Gi0/14, Gi0/15, Gi0/16
(テキスト出力は省略)

2    VLAN0002                         active
3    VLAN0003                         active

(テキスト出力は省略)

1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0

(テキスト出力は省略)

1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

表 2-29　show vlan コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号
Name	VLAN の名前（設定されている場合）
Status	VLAN のステータス（アクティブまたは中断）
Ports	VLAN に属するポート
Type	VLAN のメディア タイプ
SAID	VLAN のセキュリティ アソシエーション ID
MTU	VLAN の MTU サイズ
Parent	親 VLAN（存在する場合）
RingNo	VLAN のリング番号（該当する場合）
BridgeNo	VLAN のブリッジ番号（該当する場合）
Stp	VLAN で使用される Spanning-Tree Protocol（STP; スパニングツリー プロトコル）タイプ
BrdgMode	この VLAN のブリッジング モード ― 可能な値は Source-Route Bridge（SRB; ソースルート ブリッジ）および Source-Route Transparent（SRT; ソースルート トランスペアレント）で、デフォルトは SRB です。
Trans1	トランスレーション ブリッジ 1

表 2-29　show vlan コマンドの出力フィールド（続き）

フィールド	説明
Trans2	トランスレーション ブリッジ 2
Remote SPAN VLANs	設定された RSPAN VLAN を特定します。
Primary/Secondary/ Type/Ports	–

次の例では、**show vlan summary** コマンドの出力を示します。

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 45
 Number of existing extended VLANs : 0
```

次の例では、**show vlan id** コマンドの出力を示します。

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi0/1, Gi0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

関連コマンド

コマンド	説明
switchport mode	ポートの VLAN（仮想 LAN）メンバーシップ モードを設定します。
vlan（グローバル コンフィギュレーション）	VLAN 1 ～ 4094 を設定できる場合、VLAN コンフィギュレーション モードをイネーブルにします。
vlan（VLAN コンフィギュレーション）	VLAN データベースの VLAN 特性を設定します。標準範囲 VLAN（VLAN ID 1 ～ 1005）の場合のみ使用できます。先行ゼロは入力しないでください。

show vmps

VLAN Query Protocol（VQP）バージョン、再確認インターバル、再試行回数、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）の IP アドレス、および現在のサーバやプライマリ サーバを表示するには、キーワードを指定しないで **show vmps** イネーブル EXEC コマンドを使用します。**statistics** キーワードを指定すると、クライアント側の統計情報が表示されます。

show vmps [**statistics**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

statistics	（任意）VQP のクライアント側統計情報およびカウンタを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vmps** コマンドの出力を示します。

```
Switch> show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
---------------------
VMPS Action:          other
```

次の例では、**show vmps statistics** コマンドの出力を示します。表 2-30 に、この例で表示される各フィールドの説明を示します。

```
Switch> show vmps statistics
VMPS Client Statistics
----------------------
VQP  Queries:               0
VQP  Responses:             0
VMPS Changes:               0
VQP  Shutdowns:             0
VQP  Denied:                0
VQP  Wrong Domain:          0
VQP  Wrong Version:         0
VQP  Insufficient Resource: 0
```

表 2-30　show vmps statistics のフィールドの説明

フィールド	説明
VQP Queries	クライアントから VMPS に送信されるクエリー数
VQP Responses	VMPS からクライアントに送信される応答数
VMPS Changes	サーバ間で VMPS を変更した回数
VQP Shutdowns	ポートをシャットダウンするために VMPS が応答を送信した回数。クライアントはポートをディセーブルにし、このポート上のすべてのダイナミック アドレスをアドレス テーブルから削除します。接続を復元するには、ポートを再び管理上のイネーブル状態にする必要があります。
VQP Denied	VMPS がセキュリティ上の理由からクライアント要求を拒否した回数。VMPS 応答がアドレスを拒否した場合、このアドレスではフレームはワークステーションへ転送されず、またはワークステーションから転送されません（VLAN[仮想 LAN] にポートが割り当てられている場合、ブロードキャストまたはマルチキャスト フレームはワークステーションに転送されます）。クライアントは拒否されたアドレスをブロック済みアドレスとしてアドレス テーブルに保管します。これにより、このワークステーションから受信した各新規パケットに対するクエリーが、これ以上 VMP に送信されなくなります。エージング タイム内に、このワークステーションからこのポートに新規パケットが着信しない場合、クライアントはアドレスを期限切れにします。
VQP Wrong Domain	要求内の管理ドメインが VMPS の管理ドメインと一致しない回数。ポートの従来の VLAN 割り当ては変更されません。この応答は、サーバおよびクライアントに同じ VTP 管理ドメインが設定されていないことを意味します。
VQP Wrong Version	クエリー パケットのバージョン フィールドに、VMPS でサポートされているバージョンよりも大きな値が格納されている回数。ポートの VLAN 割り当ては変更されません。スイッチは VMPS バージョン 1 要求のみを送信します。
VQP Insufficient Resource	リソースのアベイラビリティに問題があるために、VMPS が要求に応答できない回数。再試行制限に達していない場合、クライアントはサーバごとの再試行回数に達したかどうかに応じて、同じサーバまたは次の代替サーバに要求を再送信します。

関連コマンド

コマンド	説明
clear vmps statistics	VQP クライアントに保持されている統計情報を消去します。
vmps reconfirm（イネーブル EXEC）	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。
vmps retry	VQP クライアントのサーバごとの再試行回数を設定します。
vmps server	プライマリ VMPS および最大で 3 台のセカンダリ サーバを設定します。

show vtp

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）の管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、**show vtp** ユーザ EXEC コマンドを使用します。

show vtp {**counters** | **password** | **status**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

counters	スイッチの VTP 統計情報を表示します。
password	設定された VTP パスワードを表示します。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vtp counters** コマンドの出力を示します。表 2-31 に、表示される各フィールドの説明を示します。

```
Switch> show vtp counters

VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa0/47            0                0                0
Fa0/48            0                0                0
Gi0/1             0                0                0
Gi0/2             0                0                0
```

表 2-31　show vtp counters のフィールドの説明

フィールド	説明
Summary advertisements received	トランク ポート上でこのスイッチが受信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメインの名前、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements received	トランク ポート上でこのスイッチが受信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つまたは複数の VLAN に関する情報がすべて含まれています。
Request advertisements received	トランク ポート上でこのスイッチが受信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Summary advertisements transmitted	トランク ポート上でこのスイッチが送信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメインの名前、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements transmitted	トランク ポート上でこのスイッチが送信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つまたは複数の VLAN に関する情報がすべて含まれています。
Request advertisements transmitted	トランク ポート上でこのスイッチが送信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Number of configuration revision errors	リビジョン エラーの数 新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、スイッチのコンフィギュレーション リビジョン番号が増加します。 リビジョン番号がスイッチのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズをスイッチが受信すると、リビジョン エラーが増加します。このエラーは、2 つのスイッチの VTP パスワードが異なるか、またはスイッチの設定が異なることを意味します。 これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期化されなくなることがあります。
Number of configuration digest errors	MD5 ダイジェスト エラーの数 サマリー パケット内の MD5 ダイジェストと、スイッチで計算された受信済みアドバタイズの MD5 ダイジェストが一致しない場合は、ダイジェスト エラーが増加します。このエラーは、通常、2 つのスイッチの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのスイッチで VTP パスワードが同じになるようにします。 これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなることがあります。

表 2-31　show vtp counters のフィールドの説明（続き）

フィールド	説明
Number of V1 summary errors	バージョン 1 エラーの数 VTP V2 モードのスイッチが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリー エラーが増加します。これらのエラーは、少なくとも 1 つの近接スイッチ上で VTP バージョン 1 が稼働しているか、または V2 モードがディセーブルの状態で VTP バージョン 2 が稼働していることを意味します。この問題を解決するには、VTP V2 モードのスイッチの設定をディセーブルに変更します。
Join Transmitted	トランク上で送信された VTP プルーニング メッセージの数
Join Received	トランク上で受信された VTP プルーニング メッセージの数
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリー メッセージの数

次の例では、**show vtp status** コマンドの出力を示します。表 2-32 に、表示される各フィールドの説明を示します。

```
Switch> show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Transparent
VTP Domain Name                 : shared_testbed1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

表 2-32　show vtp status のフィールドの説明

フィールド	説明
VTP Version	スイッチ上で稼働している VTP バージョンを表示します。デフォルトでは、スイッチはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
Configuration Revision	このスイッチの現在のコンフィギュレーション リビジョン番号
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数
Number of Existing VLANs	既存の VLAN 数

表 2-32　show vtp status のフィールドの説明（続き）

フィールド	説明
VTP Operating Mode	VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。 サーバ — VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチで VLAN を設定することができます。このスイッチを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM（不揮発性 RAM）から復元できます。デフォルトでは、すべてのスイッチが VTP サーバです。 （注）　スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバ モードに戻ることができない場合、スイッチは VTP サーバ モードから VTP クライアント モードに自動的に移行します。 クライアント — VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN コンフィギュレーションを格納するために必要な不揮発性ストレージがありません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。 トランスペアレント — VTP トランスペアレント モードのスイッチは、VTP に対してディセーブルであり、アドバタイズの送信や、他のデバイスから送信されたアドバタイズの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定にも影響しません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。
VTP Domain Name	スイッチの管理ドメインを特定する名前
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワーク装置にアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されます。
VTP V2 Mode	VTP バージョン 2 モードがイネーブルかどうかを表示します。すべての VTP バージョン 2 スイッチは、デフォルトでバージョン 1 モードで動作します。各 VTP スイッチは他のすべての VTP 装置の機能を自動的に検出します。VTP デバイス ネットワーク内のすべての VTP スイッチがバージョン 2 モードで動作可能な場合のみ、ネットワークをバージョン 2 に設定してください。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
MD5 Digest	VTP コンフィギュレーションの 16 バイト チェックサム
Configuration Last Modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったスイッチの IP アドレスを表示します。

関連コマンド

コマンド	説明
clear vtp counters	VTP およびプルーニング カウンタを消去します。
vtp（グローバル コンフィギュレーション）	VTP のファイル名、インターフェイス名、ドメイン名、およびモードを設定します。
vtp（VLAN コンフィギュレーション）	VTP のドメイン名、パスワード、プルーニング、およびモードを設定します。

shutdown

インターフェイスをイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドを使用します。ディセーブルであるインターフェイスを再起動する場合は、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートはイネーブルです（シャットダウンしません）。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

shutdown コマンドを入力すると、ポートは転送を停止します。ポートをイネーブルにするには、**no shutdown** コマンドを使用します。

削除、中断、またはシャットダウンされた VLAN（仮想 LAN）に割り当てられているスタティック アクセス ポートに **no shutdown** コマンドを使用しても、無効です。ポートを再びイネーブルにするには、まずポートをアクティブ VLAN のメンバーにする必要があります。

shutdown コマンドは指定されたインターフェイスの機能すべてをディセーブルにします。

このコマンドもインターフェイスを利用できなくします。**show interfaces** イネーブル EXEC コマンドは、インターフェイスがディセーブルかどうかを表示します。シャットダウンしたインターフェイスは、管理上のダウン状態と表示されます。

例

次の例では、ポートをディセーブルにし、再びイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

設定を確認するには、**show interfaces** イネーブル 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	すべてのインターフェイスまたは特定のインターフェイス固有の統計情報を表示します。

shutdown vlan

指定された VLAN（仮想 LAN）のローカル トラフィックをシャットダウン（中断）するには、**shutdown 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。VLAN のローカル トラフィックを再起動するには、このコマンドの **no** 形式を使用します。

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

構文の説明

vlan-id	ローカルにシャットダウンする VLAN の ID です。指定できる範囲は 2 ～ 1001 です。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）環境のデフォルト VLAN として定義された VLAN、および拡張範囲 VLAN（指定範囲が 1005 を超える VLAN）は、シャットダウンできません。デフォルト VLAN は、1 および 1002 ～ 1005 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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

shutdown vlan コマンドは、VTP データベース内の VLAN 情報を変更しません。このコマンドはローカル トラフィックをシャットダウンしますが、スイッチは VTP 情報をアドバタイズし続けます。

例

次の例では、VLAN 2 のトラフィックをシャットダウンする方法を示します。

```
Switch(config)# shutdown vlan 2
```

設定を確認するには、**show vlan** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
shutdown（config-vlan モード）	config-vlan モード（**vlan** *vlan-id* グローバル コンフィギュレーション コマンドで開始）の場合に、VLAN のローカル トラフィックをシャットダウンします。
vlan database	VLAN コンフィギュレーション モードを開始します。

snmp-server enable traps

さまざまなトラップの SNMP（簡易ネットワーク管理プロトコル）通知、または情報要求を Network Management System（NMS; ネットワーク管理システム）に送信するには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用します。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。

snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** | **hsrp** | **ipmulticast** | **mac-notification** | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

no snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** | **hsrp** | **ipmulticast** | **mac-notification** | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate**] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

構文の説明

bridge [**newroot**] [**topologychange**]	（任意）STP ブリッジ MIB トラップを生成します。キーワードの意味は次のとおりです。 • **newroot —**（任意）SNMP STP Bridge MIB の新しいルート トラップをイネーブルにします。 • **topologychange —**（任意）SNMP STP Bridge MIB のトポロジー変更トラップをイネーブルにします。
cluster	（任意）クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
entity	（任意）SNMP エンティティ トラップをイネーブルにします。
envmon [**fan**	**shutdown**	**status**	**supply**	**temperature**]	（任意）SNMP 環境トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **fan —**（任意）ファン トラップをイネーブルにします。 • **shutdown —**（任意）環境モニタ シャットダウン トラップをイネーブルにします。 • **status —**（任意）SNMP 環境ステータス変更トラップをイネーブルにします。 • **supply —**（任意）環境モニタ電源トラップをイネーブルにします。 • **temperature —**（任意）環境モニタ温度トラップをイネーブルにします。
flash	（任意）SNMP FLASH 通知をイネーブルにします。
hsrp	（任意）Hot Standby Router Protocol（HSRP）トラップをイネーブルにします。
ipmulticast	（任意）IP マルチキャスト ルーティング トラップをイネーブルにします。
mac-notification	（任意）MAC（メディア アクセス制御）アドレス通知トラップをイネーブルにします。

msdp	（任意）Multicast Source Discovery Protocol（MSDP）トラップをイネーブルにします。
ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	（任意）Open Shortest Path First（OSPF）トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **cisco-specific —**（任意）Cisco 固有のトラップをイネーブルにします。 • **errors —**（任意）エラー トラップをイネーブルにします。 • **lsa —**（任意）Link-State Advertisement（LSA; リンク ステート アドバタイズ）トラップをイネーブルにします。 • **rate-limit —**（任意）レート制限トラップをイネーブルにします。 • **retransmit —**（任意）パケット再送トラップをイネーブルにします。 • **state-change —**（任意）ステート変更トラップをイネーブルにします。
pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	（任意）Protocol-Independent Multicast（PIM）トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **invalid-pim-message —**（任意）無効な PIM メッセージ トラップをイネーブルにします。 • **neighbor-change —**（任意）PIM ネイバ変更トラップをイネーブルにします。 • **rp-mapping-change —**（任意）Rendezvous Point（RP）マッピング変更トラップをイネーブルにします。
port-security [**trap-rate** *value*]	（任意）ポート セキュリティ トラップをイネーブルにします。1 秒間に送信するポート セキュリティ トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
rtr	（任意）SNMP Response Time Reporter トラップをイネーブルにします。
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	（任意）SNMP トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **authentication —**（任意）認証トラップをイネーブルにします。 • **coldstart —**（任意）コールド スタート トラップをイネーブルにします。 • **linkdown —**（任意）リンクダウン トラップをイネーブルにします。 • **linkup —**（任意）リンクアップ トラップをイネーブルにします。 • **warmstart —**（任意）ウォーム スタート トラップをイネーブルにします。
storm-control trap-rate *value*	（任意）ストーム制御トラップをイネーブルにします。1 秒間に送信するストーム制御トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。

stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **inconsistency —**（任意）SNMP STPX MIB Inconsistency Update トラップをイネーブルにします。 • **root-inconsistency —**（任意）SNMP STPX MIB Root Inconsistency Update トラップをイネーブルにします。 • **loop-inconsistency —**（任意）SNMP STPX MIB Loop Inconsistency Update トラップをイネーブルにします。
syslog	（任意）SNMP Syslog トラップをイネーブルにします。
tty	（任意）TCP 接続トラップを送信します。デフォルトではイネーブルです。
vlan-membership	（任意）SNMP VLAN（仮想 LAN）メンバーシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN 削除トラップをイネーブルにします。
vtp	（任意）VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）トラップをイネーブルにします。

（注） **cpu** [**threshold**]、**insertion**、および **removal** 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ていますが、サポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

snmp-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、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

snmp-server enable traps コマンドは、トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにします。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次の例では、NMS に VTP トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps vtp
```

設定を確認するには、**show vtp status** または **show running-config** イネーブル 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。
snmp-server host	SNMP トラップを受信するホストを指定します。

snmp-server host

SNMP（簡易ネットワーク管理プロトコル）通知処理の受信側（ホスト）を指定するには、**snmp-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。指定されたホ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。

snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth**| **priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}] [**vrf** *vrf-instance*] *community-string*

構文の説明

host-addr	ホストのインターネット アドレスまたは名前（ターゲットとなる受信側）です。
udp-port *port*	（任意）トラップを受信するホストの User Datagram Protocol（UDP）ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンです。 次のキーワードがサポートされています。 **1 —** SNMPv1 です。情報の場合は、このオプションを使用できません。 **2c —** SNMPv2C です。 **3 —** SNMPv3 です。バージョン 3 キーワードのあとに、次に示すオプション キーワードを指定できます。 • **auth**（任意）— Message Digest 5（MD5）および Secure Hash Algorithm（SHA）によるパケット認証が可能です。 • **noauth**（デフォルト）— noAuthNoPriv というセキュリティ レベルです。[**auth** | **noauth** | **priv**] キーワードが指定されていない場合は、これがデフォルトです。 • **priv**（任意）— Data Encryption Standard（DES; データ暗号化規格）によるパケット暗号化（*privacy* ともいう）をイネーブルにします。 （注） **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ利用できます。
vrf *vrf-instance*	（任意）Virtual Private Network（VPN; 仮想私設網）ルーティング インスタンスとホスト名です。
community-string	通知処理によって送信されるパスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。

notification-type	（任意）ホストに送信される通知のタイプです。タイプを指定しない場合、すべての通知が送信されます。通知タイプには、1 つまたは複数のキーワードを指定できます。 • **bridge —** （任意）SNMP Spanning-Tree Protocol（STP; スパニングツリー プロトコル）ブリッジ MIB トラップを送信します。 • **cluster —** クラスタ メンバー ステータス トラップを送信します。 • **config —** SNMP 設定トラップを送信します。 • **copy-config —** SNMP コピー設定トラップを送信します。 • **entity —** SNMP エンティティ トラップを送信します。 • **envmon —** SNMP 環境モニタ トラップを送信します。 • **flash —** SNMP FLASH 通知を送信します。 • **hsrp**SNMP Hot Standby Router Protocol（HSRP）トラップを送信します。 • **ipmulticast**SNMP IP マルチキャスト ルーティング トラップを送信します。 • **mac-notification**SNMP MAC 通知トラップを送信します。 • **msdp**SNMP MSDP トラップを送信します。 • **ospf**OSPF トラップを送信します。 • **pim**SNMP PIM トラップを送信します。 • **port-security**SNMP ポート セキュリティ トラップを送信します。 • **rtr**SNMP Response Time Reporter トラップを送信します。 • **snmp**SNMP タイプ トラップを送信します。 • **storm-control**SNMP ストーム制御トラップを送信します。 • **stpx**SNMP STP 拡張 MIB トラップを送信します。 • **syslog**SNMP Syslog トラップを送信します。 • **tty**TCP 接続トラップを送信します。 • **udp-port** *port* **—** トラップを受信するホストの UDP ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。 • **vlan-membership**SNMP VLAN メンバーシップ トラップを送信します。 • **vlancreate**SNMP VLAN 作成トラップを送信します。 • **vlandelete**SNMP VLAN 削除トラップを送信します。 • **vtp**VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）トラップを送信します。

（注）　**cpu** および **fru-ctrl** 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。

デフォルト

このコマンドは、デフォルトではディセーブルです。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップ タイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで **noauth**（noAuthNoPriv）セキュリティ レベルになります。

コマンド モード　グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

SNMP 通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側は、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信した SNMP エンティティは、SNMP 応答 PDU を使用してメッセージに確認応答します。送信側が応答を受信しなかった場合は、再度情報要求を送信できます。したがって、情報が目的の宛先に到達する可能性が高まります。

ただし、情報はエージェントおよびネットワークのリソースを余計に消費します。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は 1 回限りですが、情報は数回にわたって再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するようにスイッチを設定するには、少なくとも 1 つの **snmp-server host** コマンドを入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合は、ホストに対してすべてのトラップ タイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。ホストごとのコマンドでは、複数の通知タイプを指定することができます。

ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、あとのコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドのみが有効です。たとえば、ホストに **snmp-server host inform** を入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番めのコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。**snmp-server enable traps** コマンドは、グローバルに送信される SNMP 通知を指定します。1 つのホストが大部分の通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドおよび **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブル化されます。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング *comaccess* を設定し、このストリングによる、アクセス リスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

次の例では、*myhost.cisco.com* という名前で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、*comaccess* として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ　ストリング　*public*　を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

設定を確認するには、**show running-config** イネーブル 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。
snmp-server enable traps	各トラップ タイプ、または情報要求の SNMP 通知をイネーブルにします。

snmp trap mac-notification

特定のレイヤ 2 インターフェイスの SNMP（簡易ネットワーク管理プロトコル）MAC（メディアアクセス制御）アドレス通知トラップをイネーブルにするには、**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。

snmp trap mac-notification {**added** | **removed**}

no snmp trap mac-notification {**added** | **removed**}

構文の説明

added	このインターフェイスに MAC アドレスが追加されると、MAC 通知トラップをイネーブルにします。
removed	このインターフェイスから MAC アドレスが削除されると、MAC 通知トラップをイネーブルにします。

デフォルト

デフォルトでは、アドレス追加とアドレス削除のトラップはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

snmp trap mac-notification コマンドを使用して特定のインターフェイスの通知トラップをイネーブルにできますが、トラップが生成されるのは、**snmp-server enable traps mac-notification** および **mac address-table notification** グローバル コンフィギュレーション コマンドをイネーブルにした場合のみです。

例

次の例では、ポートに MAC アドレスを追加した場合に、MAC 通知トラップをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

設定を確認するには、**show mac address-table notification interface** イネーブル 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 notification	MAC アドレス通知グローバル カウンタをクリアします。
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 address-table notification	**interface** キーワードが追加された場合に、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。

spanning-tree backbonefast

BackboneFast 機能をイネーブルにするには、**spanning-tree backbonefast** 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場合は、このコマンドの **no** 形式を使用します。

spanning-tree backbonefast

no spanning-tree backbonefast

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

BackboneFast はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

BackboneFast 機能は、Rapid PVST+ または Multiple Spanning-Tree（MST）モード用に設定できますが、スパニング ツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

スイッチのルート ポートまたはブロックされたポートが、指定されたスイッチから不良 Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル ユニット）を受信すると、BackboneFast が開始します。不良 BPDU は、1 台のスイッチをルート ブリッジと指定スイッチの両方として識別します。スイッチが不良 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（*間接* リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。ルート スイッチへの代替パスがある場合に BackboneFast を使用すると、不良 BPDU を受信するインターフェイスの最大エージング タイムが期限切れになり、ブロックされた ポートをただちにリスニング ステートに移行できます。そのあと、BackboneFast はインターフェイスをフォワーディング ステートに移行させます。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。

間接リンク障害を検出できるようにしたり、スパニングツリーの再認識をより短時間で開始するには、サポートされるすべてのスイッチで BackboneFast をイネーブルにしてください。

例

次の例では、スイッチ上で BackboneFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree backbonefast
```

設定を確認するには、**show spanning-tree summary** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。

spanning-tree bpdufilter

インターフェイスでの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の送受信を禁止するには、**spanning-tree bpdufilter** 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。

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

構文の説明

disable	指定されたインターフェイス上で BPDU フィルタリングをディセーブルにします。
enable	指定されたインターフェイス上で BPDU フィルタリングをイネーブルにします。

デフォルト

BPDU フィルタリングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、BPDU フィルタリング機能をイネーブルにできます。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdufilter default** 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。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdufilter** 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、ポート上で BPDU フィルタリング機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree bpduguard

Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信したインターフェイスを errdisable ステートにするには、**spanning-tree bpduguard** 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。

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

構文の説明

disable	指定されたインターフェイス上で BPDU ガードをディセーブルにします。
enable	指定されたインターフェイス上で BPDU ガードをイネーブルにします。

デフォルト

BPDU ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

手動でインターフェイスを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でインターフェイスがスパニングツリー トポロジーに追加されないようにするには、BPDU ガード機能を使用します。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、BPDU ガード機能をイネーブルにできます。

すべての PortFast 対応インターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** 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。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard** 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、ポート上で BPDU ガード機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree cost

スパニングツリー計算用のパス コストを設定するには、**spanning-tree cost** 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。ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。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。

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

構文の説明

vlan *vlan-id*	（任意）スパニングツリー インスタンスに関連付けられた VLAN（仮想 LAN）範囲です。VLAN ID 番号によって特定される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
cost	パス コスト。パス コストの範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mbps — 4
- 100 Mbps — 19
- 10 Mbps — 100

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

cost を設定する場合は、値が大きいほどコストが高くなります。

spanning-tree vlan *vlan-id* **cost** *cost* コマンドと **spanning-tree cost** *cost* コマンドの両方でインターフェイスを設定すると、**spanning-tree vlan** *vlan-id* **cost** *cost* コマンドが有効になります。

例

次の例では、ポートでパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ～ 15、20 でパス コストを 300 に設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

設定を確認するには、**show spanning-tree interface** *interface-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree etherchannel guard misconfig

スイッチが EtherChannel の設定矛盾を検出した場合にエラー メッセージを表示するには、**spanning-tree etherchannel guard misconfig** 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。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。

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

EtherChannel ガードは、スイッチでイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチが EtherChannel の設定矛盾を検出した場合、次のエラー メッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

EtherChannel の設定を誤ったスイッチ ポートを表示するには、**show interfaces status err-disabled** イネーブル EXEC コマンドを使用します。リモート デバイスで EtherChannel の設定を確認するには、リモート デバイスの **show etherchannel summary** イネーブル EXEC コマンドを使用します。

EtherChannel の設定矛盾によりポートが errdisable ステートの場合は、**errdisable recovery cause channel-misconfig** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動で再度イネーブルにすることができます。

例

次の例では、EtherChannel 設定矛盾ガード機能をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

設定を確認するには、**show spanning-tree summary** イネーブル 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 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。
show etherchannel summary	各チャネル グループのサマリーを 1 行として、チャネルの EtherChannel 情報を表示します。
show interfaces status err-disabled	errdisable ステートのインターフェイスが表示されます。

spanning-tree extend system-id

拡張システム ID 機能をイネーブルにするには、**spanning-tree extend system-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。

spanning-tree extend system-id

（注）　このコマンドの **no** バージョンは、コマンドラインのヘルプ ストリングに表示されていますが、サポートされていません。拡張システム ID 機能をディセーブルにすることはできません。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

拡張システム ID はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチは、IEEE 802.1t スパニングツリー拡張をサポートします。以前スイッチ プライオリティに使用されたビットの一部は現在、拡張システム ID（Per-VLAN Spanning-Tree Plus [PVST+] と Rapid PVST+ の VLAN［仮想 LAN］）識別子、または Multiple Spanning-Tree [MST] のインスタンス識別子）に使用します。

スパニングツリーは、ブリッジ ID が VLAN または MST インスタンスごとに一意となるようにするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC（メディア アクセス制御）アドレスを使用しています。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。詳細については、「spanning-tree mst root」および「spanning-tree vlan」を参照してください。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree guard

選択されたインターフェイスに関連付けられたすべての VLAN（仮想 LAN）上で、ルート ガードまたはループ ガードをイネーブルにするには、**spanning-tree guard** 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。ルート ガードは、スパニングツリー ルート ポートまたはスイッチのルートへのパスとなることができるインターフェイスを制限します。ループ ガードは、障害によって単一方向リンクが作成された場合に、代替ポートまたはルート ポートが指定ポートにならないようにします。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。

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

構文の説明

loop	ループ ガードをイネーブルにします。
none	ルート ガードまたはループ ガードをディセーブルにします。
root	ルート ガードをイネーブルにします。

デフォルト

ルート ガードはディセーブルです。

ループガードは、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドに従って設定されます（グローバルにディセーブル化）。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、ルート ガードまたはループ ガードをイネーブルにできます。

ルート ガードがイネーブルの場合に、スパニングツリーを計算すると、インターフェイスがルート ポートとして選択され、root-inconsistent（ブロック）ステートに移行します。これにより、カスタマーのスイッチがルート スイッチになったり、ルートへのパスになることはなくなります。ルート ポートは、スイッチからルート スイッチまでの最適パスを提供します。

no spanning-tree guard または **no spanning-tree guard none** コマンドを入力すると、ルート ガードは選択されたインターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが root-inconsistent（ブロック）ステートの場合、インターフェイスはリスニング ステートに自動的に移行します。

UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）になり、フォワーディング ステートに移行できなくなります。スイッチが Rapid PVST+ モードまたは MST モードで稼働している場合は、UplinkFast 機能を使用できません。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートは指定ポートになることがなく、スパニングツリーはルートポートまたは代替ポートで Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を送信しません。スイッチが MST モードで動作している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ルート ガードまたはループ ガードをディセーブルにする場合は、**spanning-tree guard none** 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。ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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、指定されたポートに関連付けられたすべての VLAN で、ルート ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

次の例では、指定されたポートに関連付けられたすべての VLAN で、ループ ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree loopguard default	単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されないようにします。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree link-type

インターフェイスのデュプレックス モードによって決まるデフォルトのリンクタイプ設定を上書きし、Rapid Spanning-Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）がフォワーディング ステートに移行できるようにするには、**spanning-tree link-type** 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。

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

構文の説明

point-to-point	インターフェイスのリンク タイプがポイントツーポイントであることを指定します。
shared	インターフェイスのリンク タイプが共有であることを指定します。

デフォルト

スイッチは、デュプレックス モードからインターフェイスのリンク タイプを取得します。つまり、全二重インターフェイスはポイントツーポイント リンクであるとみなされ、半二重インターフェイスは共有リンクであるとみなされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

リンク タイプのデフォルト設定を上書きするには、**spanning-tree link-type** コマンドを使用します。たとえば、半二重リンクは、Multiple Spanning-Tree Protocol（MSTP）または Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルが稼働し高速移行がイネーブルであるリモート スイッチの 1 つのインターフェイスに、ポイントツーポイントで物理的に接続できます。

例

次の例では、（デュプレックスの設定に関係なく）リンク タイプを共有に指定し、フォワーディング ステートへの高速移行を禁止する方法を示します。

```
Switch(config-if)# spanning-tree link-type shared
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* または **show spanning-tree interface** *interface-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
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（強制的に近接スイッチと再度ネゴシエートさせる）します。
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー ステート情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。

spanning-tree loopguard default

代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぐには、**spanning-tree loopguard default** 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。

spanning-tree loopguard default

no spanning-tree loopguard default

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ループ ガードはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、ループ ガード機能をイネーブルにできます。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートは指定ポートになることがなく、スパニングツリーはルートポートまたは代替ポートで Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を送信しません。スイッチが MST モードで動作している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ループ ガードは、スパニングツリーがポイントツーポイントとみなすインターフェイス上でのみ動作します。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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、ループ ガードをグローバルにイネーブルにします。

```
Switch(config)# spanning-tree loopguard default
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree guard loop	指定したインターフェイスに関連付けられたすべての VLAN で、ループ ガード機能をイネーブルにします。

spanning-tree mode

スイッチ上で Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、または Multiple Spanning-Tree（MST）をイネーブルにするには、**spanning-tree mode** 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。

spanning-tree mode {**mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

構文の説明

mst	（IEEE 802.1s および IEEE 802.1w に基づき）MST、および Rapid Spanning-Tree Protocol（RSTP）をイネーブルにします。
pvst	（IEEE 802.1D に基づき）PVST+ をイネーブルにします。
rapid-pvst	（IEEE 802.1w に基づき）Rapid PVST+ をイネーブルにします。

デフォルト

デフォルト モードは PVST+ です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチは PVST+、Rapid PVST+、および MSTP をサポートしますが、複数のモードを同時にアクティブにすることはできません。すべての VLAN（仮想 LAN）は、PVST+、Rapid PVST+、または MSTP を稼働します。

MST モードをイネーブルにした場合、RSTP は自動的にイネーブルになります。

注意　スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが以前のモードのために停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。

例

次の例では、スイッチ上で MST と RSTP をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode mst
```

次の例では、スイッチ上で Rapid PVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode rapid-pvst
```

設定を確認するには、**show running-config** イネーブル 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。

spanning-tree mst configuration

Multiple Spanning-Tree（MST）リージョンを設定する場合に使用する MST コンフィギュレーション モードを開始するには、**spanning-tree mst configuration** 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。

spanning-tree mst configuration

no spanning-tree mst configuration

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべての VLAN（仮想 LAN）が Common and Internal Spanning-Tree（CIST）インスタンス（インスタンス 0）にマッピングされます。

デフォルト名は空の文字列です。

リビジョン番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上の注意事項

spanning-tree mst configuration コマンドは、MST コンフィギュレーション モードを開始します。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。

- **abort**：構成変更を適用しないで、MST リージョン コンフィギュレーション モードを終了します。
- **exit**：MST リージョン コンフィギュレーション モードを終了し、すべての構成変更を適用します。
- **instance** *instance-id* **vlan** *vlan-range*：VLAN を MST インスタンスにマッピングします。*instance-id* に指定できる範囲は 1 ～ 4094 です。指定できる *vlan-range* の範囲は 1 ～ 4094 です。VLAN ID 番号によって特定される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。
- **name** *name*：構成名を設定します。*name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
- **no**：**instance**、**name**、および **revision** コマンドを無視するか、またはデフォルト設定に戻します。
- **private-vlan**：このコマンドは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。
- **revision** *version*：構成のリビジョン番号を設定します。指定できる範囲は 0 ～ 65535 です。
- **show** [**current** | **pending**]：現在の、または保留中の MST リージョン構成を表示します。

MST モードでは、スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピングできる VLAN 数は制限されていません。

VLAN を MST インスタンスにマッピングすると、マッピングが増加し、コマンドで指定された VLAN はマッピングされていた VLAN に追加、または VLAN から削除されます。範囲を指定する場合はハイフンを使用します。たとえば、**instance 1 vlan 1-63** は、MST インスタンス 1 に VLAN 1 ～ 63 をマッピングします。列挙して指定する場合はカンマを使用します。たとえば、**instance 1 vlan 10, 20, 30** は、MST インスタンス 1 に VLAN 10、20、および 30 をマッピングします。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、CIST インスタンス（インスタンス 0）にマッピングされます。このマッピングは、このコマンドの **no** 形式では解除できません。

2 台以上のスイッチが同一 MST リージョン内に存在するには、同じ VLAN マッピング、同じ構成リビジョン番号、および同じ名前が設定されている必要があります。

例

次の例では、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付け、構成リビジョンを 1 に設定し、変更確認前の構成を表示し、変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

次の例では、インスタンス 2 にすでにマッピングされている VLAN があれば、そこに VLAN 1 ～ 100 を追加し、インスタンス 2 にマッピングされていた VLAN 40 ～ 60 を CIST インスタンスに移動し、インスタンス 10 に VLAN 10 を追加し、インスタンス 2 にマッピングされたすべての VLAN を削除し、それらを CIST インスタンスにマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

設定を確認するには、**show pending** MST コンフィギュレーション コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst configuration	MST リージョンの設定を表示します。

spanning-tree mst cost

Multiple Spanning-Tree（MST）計算用のパス コストを設定するには、**spanning-tree mst cost** 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。ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。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。

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

構文の説明

instance-id	スパニングツリー インスタンス範囲。単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
cost	パス コストの範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mbps — 20000
- 100 Mbps — 200000
- 10 Mbps — 2000000

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上の注意事項

cost を設定する場合は、値が大きいほどコストが高くなります。

例

次の例では、インスタンス 2、およびインスタンス 4 に関連付けられたポートにパス コストとして 250 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst forward-time

すべての Multiple Spanning-Tree（MST）インスタンスに転送遅延時間を設定するには、**spanning-tree mst forward-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。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。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。

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

構文の説明

seconds	リスニングおよびラーニング ステートの期間です。指定できる範囲は 4 ～ 30 秒です。

デフォルト

デフォルト値は 15 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

spanning-tree mst forward-time コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての MST インスタンスについて、スパニングツリーの転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst forward-time 18
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージから送信される hello Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の間隔を設定します。
spanning-tree mst max-age	スパニングツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU が廃棄されるまでのリージョンのホップ数を設定します。

spanning-tree mst hello-time

ルート スイッチ コンフィギュレーション メッセージから送信される hello Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の間隔を設定するには、**spanning-tree mst hello-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。

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

構文の説明

seconds	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔です。指定できる範囲は 1 ～ 10 秒です。

デフォルト

デフォルト値は 2 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

spanning-tree mst max-age seconds グローバル コンフィギュレーション コマンドを設定したあとに、指定されたインターバル内でルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジーを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst hello-time コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての MST インスタンスについて、スパニングツリーの hello タイムを 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst hello-time 3
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst max-age	スパニングツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU が廃棄されるまでのリージョンのホップ数を設定します。

spanning-tree mst max-age

スパニングツリーがルート スイッチから受信するメッセージの間隔を設定するには、**spanning-tree mst max-age** 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。スイッチがこの期間内にルート スイッチから Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）メッセージを受信しない場合は、スパニングツリー トポロジーが再計算されます。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。

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

構文の説明

seconds	スパニングツリーがルート スイッチからメッセージを受信する間隔です。指定できる範囲は 6 ～ 40 秒です。

デフォルト

デフォルト値は 20 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

spanning-tree mst max-age seconds グローバル コンフィギュレーション コマンドを設定したあとに、指定されたインターバル内でルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジーを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst max-age コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニングツリーの有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-age 30
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-hops	BPDU が廃棄されるまでのリージョンのホップ数を設定します。

spanning-tree mst max-hops

Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）が廃棄され、インターフェイスに保持された情報が期限切れになるまでの、リージョンのホップ数を設定するには、**spanning-tree mst max-hops** 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。

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

構文の説明

hop-count	BPDU が廃棄されるまでのリージョンのホップ数です。指定できるホップ数は 1 ～ 255 です。

デフォルト

デフォルトのホップ数は 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*hop-count* の範囲が 1 ～ 255 に変更されました。

使用上の注意事項

インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。スイッチは、BPDU を受信すると、受信した残りのホップ カウントを 1 つ減らして、生成する M レコードの残りのホップ カウントとしてこの値を伝播します。ホップ カウントが 0 になると、スイッチは BPDU を廃棄して、インターフェイスに保持された情報を期限切れにします。

spanning-tree mst max-hops コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニングツリーの最大ホップ数を 10 に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-hops 10
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニングツリーがルート スイッチからメッセージを受信する間隔を指定します。

spanning-tree mst port-priority

インターフェイスのプライオリティを設定するには、**spanning-tree mst 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。ループが発生した場合、Multiple Spanning-Tree Protocol（MSTP）はフォワーディング ステートに設定するインターフェイスを判別できます。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。

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

構文の説明

instance-id	スパニングツリー インスタンス範囲。単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
priority	指定できる範囲は 0 ～ 240 で、16 ずつ増加します。有効なプライオリティ値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上の注意事項

最初に選択させたいインターフェイスには高いプライオリティ（小さい数値）を与え、最後に選択させたいインターフェイスには低いプライオリティ（大きい数値）を与えます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、Multiple Spanning-Tree（MST）はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

例

次の例では、ループが発生した場合に、スパニングツリー インスタンス 20 および 22 に関連付けられたインターフェイスがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst pre-standard

先行標準の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）のみを送信するようにポートを設定するには、**spanning-tree mst pre-standard** 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。

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト状態は、先行標準のネイバの自動検出です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

ポートは先行標準の BPDU と標準 BPDU の両方を受け付けます。ネイバ タイプが不一致の場合は、Common and Internal Spanning Tree（CIST）のみがこのインターフェイスで実行されます。

（注）　スイッチのポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** 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*必要があります*。先行標準の BPDU のみを送信するようにポートを設定しないと、Multiple STP（MSTP）のパフォーマンスが次第に低下する可能性があります。

先行標準のネイバを自動検出するようにポートが設定されている場合は、**show spanning-tree mst** コマンドの結果に *prestandard* フラグが必ず表示されます。

例

次の例では、先行標準の BPDU のみを送信するようにポートを設定する方法を示します。

```
Switch(config-if)# spanning-tree mst pre-standard
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	指定されたインターフェイスの、*prestandard* フラグを含む Multiple Spanning-Tree（MST）情報を表示します。

spanning-tree mst priority

指定されたスパニングツリー インスタンスのスイッチ プライオリティを設定するには、**spanning-tree mst 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。

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

構文の説明

instance-id	スパニングツリー インスタンス範囲。単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 で、4096 ずつ増加します。有効なプライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

例

次の例では、Multiple Spanning-Tree（MST）インスタンス 20 ～ 21 のスパニングツリー プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

設定を確認するには、**show spanning-tree** mst *instance-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。

spanning-tree mst root

ネットワークの直径に基づいて、Multiple Spanning-Tree（MST）ルート スイッチ プライオリティおよびタイマーを設定するには、**spanning-tree mst root** 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。

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

構文の説明

instance-id	スパニングツリー インスタンス範囲。単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
root primary	このスイッチを強制的にルート スイッチに設定します。
root secondary	プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 に対してのみ使用できます。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージから送信される hello Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。

デフォルト

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

hello タイムは 2 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上の注意事項

spanning-tree mst *instance-id* **root** コマンドは、バックボーン スイッチでのみ使用してください。

spanning-tree mst *instance-id* **root** コマンドを入力すると、ソフトウェアはこのスイッチをスパニングツリー インスタンスのルートに設定できるように、十分高いプライオリティを設定しようとします。拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定されたインスタンスのルートになる場合です。指定インスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree mst *instance-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチ プライオリティをデフォルト値（32768）から 28672 に変更します。ルート スイッチに障害が発生した場合は、このスイッチが次のルート スイッチになります（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用していて、ルート スイッチになる可能性が低い場合）。

例

次の例では、スイッチをインスタンス 10 のルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

次の例では、スイッチをインスタンス 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree mst** *instance-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニングツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU が廃棄されるまでのリージョンのホップ数を設定します。

spanning-tree port-priority

インターフェイスのプライオリティを設定するには、**spanning-tree 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。ループが発生した場合、スパニングツリーはフォワーディング ステートにするインターフェイスを判別できます。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。

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

構文の説明

vlan *vlan-id*	（任意）スパニングツリー インスタンスに関連付けられた VLAN（仮想 LAN）範囲です。VLAN ID 番号によって特定される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
priority	指定できる範囲は 0 ～ 240 で、16 ずつ増加します。有効なプライオリティ値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

変数 *vlan-id* を省略した場合、このコマンドは VLAN 1 に関連付けられたスパニングツリー インスタンスに適用されます。

インターフェイスが割り当てられていない VLAN にも、プライオリティを設定できます。このインターフェイスを VLAN に割り当てると、設定が有効になります。

spanning-tree vlan *vlan-id* **port-priority** *priority* コマンドおよび **spanning-tree port-priority** *priority* コマンド両方でインターフェイスを設定する場合、**spanning-tree vlan** *vlan-id* **port-priority** *priority* コマンドが有効になります。

例

次の例では、ループが発生した場合にポートがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

次の例では、VLAN 20 ～ 25 でポート プライオリティ値を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

設定を確認するには、**show spanning-tree interface** *interface-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree portfast（グローバル コンフィギュレーション）

PortFast 対応インターフェイス上で Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）、および BPDU ガード機能をグローバルにイネーブルにしたり、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast** 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。BPDU フィルタリング機能を使用すると、スイッチ インターフェイスでの BPDU の送受信を禁止することができます。BPDU ガード機能は、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。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。

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

構文の説明

bpdufilter default	PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにし、エンド ステーションに接続されたスイッチ インターフェイスでの BPDU の送受信を禁止します。
bpduguard default	PortFast 対応インターフェイス上で BPDU ガード機能をグローバルにイネーブルにし、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。
default	すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。

デフォルト

BPDU フィルタリング、BPDU ガード、および PortFast 機能は、個別に設定しないかぎり、すべてのインターフェイス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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、これらの機能をイネーブルにできます。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドは、PortFast 対応インターフェイス（PortFast 動作ステートのインターフェイス）上で BPDU フィルタリングをグローバルにイネーブルにします。ただし、リンクが確立してからスイッチが発信 BPDU のフィル

タリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチ インターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpufilter** インターフェイス コンフィギュレーション コマンドを使用します。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドは、PortFast 動作ステートのインターフェイス上で BPDU ガードをグローバルにイネーブルにします。有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていない装置の接続などのような無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは errdisable ステートになります。手動でインターフェイスを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpuguard** 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。

すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast default** 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。PortFast は、エンド ステーションに接続するインターフェイスに限って設定します。そうしないと、偶発的なトポロジー ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。リンクがアップすると、PortFast 対応インターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパニングツリーフォワーディング ステートに移行します。

spanning-tree portfast default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast** 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。**no spanning-tree portfast default** 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、**spanning-tree portfast** 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を個別に設定した場合を除き、すべてのインターフェイス上で PortFast をディセーブルにすることができます。

例　次の例では、BPDU フィルタリング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)# spanning-tree portfast bpdufilter default
```

次の例では、BPDU ガード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)# spanning-tree portfast bpduguard default
```

次の例では、すべての非トランク インターフェイス上で PortFast 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)# spanning-tree portfast default
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree bpdufilter	インターフェイスが BPDU を送受信しないようにします。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。

spanning-tree portfast（インターフェイス コンフィギュレーション）

関連しているすべての VLAN（仮想 LAN）内のインターフェイス上で PortFast 機能をイネーブルにするには、**spanning-tree portfast** 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。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。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。

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

構文の説明

disable	（任意）指定されたインターフェイスの PortFast 機能をディセーブルにします。
trunk	（任意）トランキング インターフェイスの PortFast 機能をイネーブルにします。

デフォルト

すべてのインターフェイスで PortFast 機能はディセーブルですが、ダイナミック アクセス ポートでは自動的にイネーブルになります。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

この機能は、エンド ステーションに接続するインターフェイスに限って使用します。そうしないと、偶発的なトポロジー ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** 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必要があります。**spanning-tree portfast** コマンドは、トランク ポートではサポートされません。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼働している場合は、その機能をイネーブルにできます。

この機能はインターフェイス上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行されます。

spanning-tree portfast default 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、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにできます。ただし、**spanning-tree portfast** 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、グローバル設定を上書きすることができます。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast disable** 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、トランク インターフェイス以外のインターフェイス上で PortFast 機能をイネーブルにできます。

例

次の例では、特定のポート上で PortFast 機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

設定を確認するには、**show running-config** イネーブル 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。
spanning-tree bpdufilter	インターフェイスでの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。

spanning-tree transmit hold-count

毎秒送信される Bridge Protocol Data Unit（BPDU）の数を設定するには、**spanning-tree transmit hold-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。

spanning-tree transmit hold-count [*value*]

no spanning-tree transmit hold-count [*value*]

構文の説明

value	（任意）毎秒送信される BPDU の数。指定できる範囲は 1 ～ 20 です。

デフォルト

デフォルト値は 6 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上の注意事項

transmit hold-count 値を増やすと、スイッチが rapid-per-VLAN Spanning-Tree plus（rapid-PVST+）モードの場合に CPU 利用率に重大な影響が生じる場合があります。この値を減らすと、収束が遅くなります。デフォルト設定の使用を推奨します。

例

次の例では、transmit hold-count を 8 に設定する方法を示します。

```
Switch(config)# spanning-tree transmit hold-count 8
```

設定を確認するには、**show spanning-tree mst** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	transmit hold-count を含む、Multiple Spanning-Tree（MST）リージョン設定およびステータスを表示します。

spanning-tree uplinkfast

リンクやスイッチに障害が発生した場合、またはスパニングツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにするには、**spanning-tree uplinkfast** 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。

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

構文の説明

max-update-rate *pkts-per-second*	（任意）更新パケットを送信するときの 1 秒間のパケット数です。指定できる範囲は 0 ～ 32000 です。

デフォルト

UplinkFast はディセーブルです。

更新速度は 150 パケット / 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドは、アクセス スイッチ上だけで使用します。

UplinkFast 機能は、Rapid PVST+ または Multiple Spanning-Tree（MST）モード用に設定できますが、スパニング ツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになり、VLAN（仮想 LAN）単位でイネーブルにすることはできません。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されます。UplinkFast をイネーブルにする、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、全 VLAN のスイッチ プライオリティと全インターフェイスのパス コストがデフォルト値に設定されます。

ルート ポートに障害が発生していることがスパニングツリーで検出されると、UplinkFast はスイッチをただちに代替ルート ポートに変更して、新しいルート ポートを直接フォワーディング ステートに移行させます。この間、トポロジー変更通知が送信されます。

UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）になり、フォワーディング ステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパニングツリー トポロジーのコンバージェンスに要する時間が長くなります。

例

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree uplinkfast
```

設定を確認するには、**show spanning-tree summary** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。
spanning-tree vlan root primary	このスイッチを強制的にルート スイッチに設定します。

spanning-tree vlan

VLAN（仮想 LAN）単位でスパニングツリーを設定するには、**spanning-tree 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。

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

構文の説明

vlan-id	スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号によって特定される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
forward-time *seconds*	（任意）指定したスパニングツリー インスタンスの転送遅延時間を設定します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。指定できる範囲は 4 ～ 30 秒です。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージから送信される hello Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。
max-age *seconds*	（任意）スパニングツリーがルート スイッチからメッセージを受信する間隔を設定します。スイッチがこの期間内にルート スイッチから BPDU メッセージを受信しない場合は、スパニングツリー トポロジーが再計算されます。指定できる範囲は 6 ～ 40 秒です。
priority *priority*	（任意）指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、このスイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 で、4096 ずつ増加します。有効なプライオリティ値は、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。
root primary	（任意）このスイッチを強制的にルート スイッチに設定します。
root secondary	（任意）プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。

デフォルト

すべての VLAN でスパニングツリーがイネーブルです。

転送遅延時間は 15 秒です。

hello タイムは 2 秒です。

有効期限は 20 秒です。

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

コマンド モード　グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

STP をディセーブルにすると、VLAN はスパニングツリー トポロジーへの参加を停止します。管理上のダウン状態のインターフェイスは、ダウン状態のままです。受信された BPDU は、他のマルチキャスト フレームと同様に転送されます。STP がディセーブルの場合、VLAN はループを検出や禁止を行いません。

現在アクティブでない VLAN 上で STP をディセーブルにしたり、変更を確認するには、**show running-config** または **show spanning-tree vlan** *vlan-id* イネーブル EXEC コマンドを使用します。設定は、VLAN がアクティブである場合に有効となります。

STP をディセーブルにするか、再びイネーブルにすると、ディセーブルまたはイネーブルにする VLAN 範囲を指定できます。

VLAN をディセーブルにしてからイネーブルにした場合、その VLAN に割り当てられていたすべての VLAN は引き続きメンバーとなります。ただし、すべてのスパニングツリー ブリッジ パラメータは元の設定（VLAN がディセーブルになる直前の設定）に戻ります。

インターフェイスが割り当てられていない VLAN 上で、スパニングツリー オプションをイネーブルにすることができます。インターフェイスに設定を割り当てると、設定が有効になります。

max-age *seconds* を設定すると、指定されたインターバル内にスイッチがルート スイッチから BPDU を受信しなかった場合に、スパニングツリー トポロジーが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree vlan *vlan-id* **root** コマンドは、バックボーン スイッチでのみ使用してください。

spanning-tree vlan *vlan-id* **root** コマンドを入力すると、ソフトウェアは各 VLAN の現在のルート スイッチのスイッチ プライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定された VLAN のルートになる場合です。指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree vlan *vlan-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチ プライオリティをデフォルト値（32768）から 28672 に変更します。ルート スイッチに障害が発生した場合は、このスイッチが次のルート スイッチになります（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用していて、ルート スイッチになる可能性が低い場合）。

例

次の例では、VLAN 5 上で STP をディセーブルにする方法を示します。

```
Switch(config)# no spanning-tree vlan 5
```

設定を確認するには、**show spanning-tree** イネーブル EXEC コマンドを入力します。このインスタンスのリストに、VLAN 5 は表示されません。

次の例では、VLAN 20 と VLAN 25 のスパニングツリーについて、転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

次の例では、VLAN 20 ～ 24 のスパニングツリーについて、hello 遅延時間を 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

次の例では、VLAN 20 のスパニングツリーについて、有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

次の例では、スパニングツリー インスタンス 100 およびインスタンス 105 ～ 108 の **max-age** パラメータをデフォルト値に戻す方法を示します。

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

次の例では、VLAN 20 のスパニングツリーについて、プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

次の例では、スイッチを VLAN 10 のルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

次の例では、スイッチを VLAN 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree vlan** *vlan-id* イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree vlan	スパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループガード機能をイネーブルにします。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにし、新しいルート ポートを短時間で選択できるようにします。

speed

ポート速度を 10/100 Mbps または 10/100/1000 Mbps に指定するには、**speed** 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** 形式または **default** 形式を使用します。

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

構文の説明

10	ポートは 10 Mbps で稼働します。
100	ポートは 100 Mbps で稼働します。
1000	ポートは 1000 Mbps で稼働します。このオプションは、10/100/1000 Mbps ポートでのみ有効で表示されます。
auto	ポートは、リンクの相手側のポートの動作速度を自動的に検出します。**10**、**100**、または **1000** キーワードとともに **auto** キーワードを使用すると、ポートは指定の速度で自動ネゴシエートします。
nonegotiate	自動ネゴシエーションがディセーブルにされており、ポートは 1000 Mbps で稼働します。

デフォルト

デフォルトは **auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

SFP モジュール ポートが自動ネゴシエーションをサポートしてないデバイスに接続されている場合、ネゴシエートしないように（**nonegotiate**）速度を設定できます。

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。

ラインの両端が自動ネゴシエーションをサポートする場合、デフォルト自動ネゴシエーション設定を推奨します。インターフェイス 1 つが自動ネゴシエーションをサポートし、相手側がサポートしない場合、サポート側は **auto** 設定を使用しますが、相手側にデュプレックスおよび速度を設定します。

注意　インターフェイス速度とデュプレックス モード コンフィギュレーションを変更すると、インターフェイスをシャットダウンし、再設定中に再度イネーブルにする場合があります。

スイッチ速度とデュプレックス パラメータの設定については、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。

例

次の例では、ポートの速度を 100 Mbps に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

次の例では、10 Mbps でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

次の例では、10 Mbps または 100 Mbps でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

設定を確認するには、**show interfaces** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
duplex	デュプレックス モードの動作を指定します。
show interfaces	すべてのインターフェイスまたは特定のインターフェイス固有の統計情報を表示します。

srr-queue bandwidth limit

ポートでの最大出力を制限するには、**srr-queue bandwidth 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。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。

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

構文の説明

weight1	制限されるポート速度のパーセント。指定できる範囲は 10 ～ 90 です。

デフォルト

ポートはレート制限されてなく、100% に設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ハードウェアはライン レートが 6 つずつ増加するよう調整しているので、この値は正確ではありません。

（注）　出力キュー　デフォルト設定は、たいていの場合に適します。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 Quality of Service（QoS; サービス品質）ソリューションを満たさない場合のみ、設定を変更することができます。

例

次の例では、ポートを 800 Mbps に制限する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** イネーブル 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 srr-queue output cos-map	Class of Service（CoS; サービス クラス）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Services Code Point（DSCP）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッシュホールドを設定し、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	キューセットに対するポートをマッピングします。
show mls qos interface queueing	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出力キュー 4 つで帯域幅をシェーピングします。
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出力キュー 4 つで帯域幅を共有します。

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出力キュー 4 つで帯域幅をシェーピングするには、**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。

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

構文の説明

weight1 weight2 weight3 weight4	シェーピングされるポートのパーセントを判別する重みを指定します。インバース比（1/*weight*）は、このキューのシェーピング帯域幅を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。

デフォルト

重み 1 は 25、重み 2、重み 3、および重み 4 は 0 に設定されています。このキューは共有モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

shaped モードでは、キューは帯域幅のパーセントとして保証され、この量にレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を越えて使用できません。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにするために、シェーピングを使用します。

shaped モードは、shared モードを無効にします。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは shared モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューをシェーピングと共有両方に設定する場合、最小のキューをシェーピングに設定します。

（注） 出力キュー　デフォルト設定は、たいていの場合に適します。出力キューに関して深く理解し、この設定が QoS ソリューションを満たさない場合のみ、設定を変更する必要があります。

例

次の例では、同じポートのキューをシェーピングと共有両方に設定する方法を示します。キュー 2、3、4 の重み比が 0 に設定されているので、キューは shared モードで動作します。キューの帯域幅の重みは 1/8、12.5% です。キュー 1 は、この帯域幅で保証され制限されています。他のキューにトラフィックがなくアイドルであっても、他のキューにスロットを拡張しません。キュー 2、3、4 は shared モードで、キュー 1 の設定は無視されます。shared モードのキューに割り当てられた帯域幅比は、4/（4+4+4）、33% です。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** イネーブル 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 srr-queue output cos-map	Class of Service（CoS; サービス クラス）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Services Code Point（DSCP）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッシュホールドを設定し、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。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対するポートをマッピングします。
show mls qos interface queueing	QoS 情報を表示します。
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出力キュー 4 つで帯域幅を共有します。

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出力キュー 4 つで帯域幅を共有するには、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドスイッチを使用します。重み比は、Shaped Round Robin（SRR）スケジューラが各キューからパケットを取り出す周波数比です。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。

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

構文の説明

weight1 weight2 weight3 weight4	*weight1*、*weight2*、*weight3*、および *weight4* は、SRR スケジューラがパケットを取り出す周波数比を指定します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。

デフォルト

重み 1、重み 2、重み 3、および重み 4 は 25（帯域幅の 1/4 が各キューに割り当てられています）です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

各重みの絶対値は意味がないので、パラメータ比だけを使用します。

shared モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは SRR shared モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューをシェーピングと共有両方に設定する場合、最小のキューをシェーピングに設定します。

（注）　出力キュー　デフォルト設定は、たいていの場合に適します。出力キューに関して深く理解し、この設定が QoS ソリューションを満たさない場合のみ、設定を変更する必要があります。

例

次の例では、出力ポートで稼働する SRR スケジューラの重みの比を設定する方法を示します。キュー 4 つを使用します。shared モードの各キューに割り当てられた帯域幅は、1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、4/（1+2+3+4）で、キュー 1、2、3、4 ごとに 10%、20%、30%、40% です。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** イネーブル 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 srr-queue output cos-map	Class of Service（CoS; サービス クラス）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Services Code Point（DSCP）値を出力キュー、またはキューとスレッシュホールド ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD; 重み付きテール廃棄）スレッシュホールドを設定し、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。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対するポートをマッピングします。
show mls qos interface queueing	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出力キュー 4 つで帯域幅をシェーピングします。

storm-control

インターフェイスでブロードキャスト、マルチキャスト、またはユニキャス ストーム制御をイネーブルにして、スレッシュホールドを設定するには、**storm-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。

storm-control {{**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

構文の説明

broadcast	インターフェイスのブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイスのマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイスのユニキャスト ストーム制御をイネーブルにします。
level *level* [*level-low*]	上昇および下降の抑制レベルをポートの合計帯域に対するパーセント（%）で指定します。 • *level* — 上昇抑制レベル。小数第 2 位まで指定できます。指定できる範囲は 0.00 ～ 100.00 です。*level* に指定した値に達すると、ストーム パケットのフラッディングをブロックします。 • *level-low* —（任意）下降抑制レベル。小数第 2 位まで指定できます。指定できる範囲は 0.00 ～ 100.00 です。この値は、上昇抑制レベル以下である必要があります。下降抑制レベルを設定しない場合は、上昇抑制レベルに設定されます。
level bps *bps* [*bps-low*]	ポートでのトラフィックの受信時における上昇および下降の抑制レベルをビット / 秒で指定します。 • *bps* — 上昇抑制レベル。小数第 1 位まで指定できます。指定できる範囲は 0.0 ～ 10000000000.0 です。*bps* に指定した値に達すると、ストーム パケットのフラッディングをブロックします。 • *bps-low* —（任意）下降抑制レベル。小数第 1 位まで指定できます。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は、上昇抑制レベル以下である必要があります。 大きな数のスレッシュホールドには、k、m、g などの単位を使用できます。
level pps *pps* [*pps-low*]	ポートでのトラフィックの受信時における上昇および下降の抑制レベルをパケット / 秒で指定します。 • *pps* — 上昇抑制レベル。小数第 1 位まで指定できます。指定できる範囲は 0.0 ～ 10000000000.0 です。*pps* に指定した値に達すると、ストーム パケットのフラッディングをブロックします。 • *pps-low* —（任意）下降抑制レベル。小数第 1 位まで指定できます。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は、上昇抑制レベル以下である必要があります。 大きな数のスレッシュホールドには、k、m、g などの単位を使用できます。

action {**shutdown** | **trap**}	ポートでストームが発生した場合に実行するアクション。デフォルトのアクションでは、トラフィックをフィルタリングして、Simple Network Management Protocol（SNMP）トラップを送信しません。 キーワードの意味は次のとおりです。 • **shutdown —** ストームの間、ポートをディセーブルにします。 • **trap —** ストームの発生時に SNMP トラップを送信します。

デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルトのアクションでは、トラフィックをフィルタリングして、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ストーム制御は、物理ポートでだけサポートされています。ストーム制御は、CLI（コマンドライン インターフェイス）では利用できますが、EtherChannel ポート チャネルではサポートされていません。

ストーム制御抑制レベルは、トラフィック受信時におけるポートの合計帯域に対するパーセント（%）としてパケット / 秒単位で、あるいはトラフィック受信時レートとしてビット / 秒単位で入力できます。

合計帯域のパーセント（%）で指定する場合、抑制値 100% は、指定されたトラフィック タイプを制限しないことを示します。**level 0 0** という値は、ポート上のブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがすべてブロックされることを示します。ストーム制御がイネーブルになるのは、上昇抑制レベルが 100% 未満の場合だけです。他のストーム制御設定を指定しない場合、デフォルトのアクションでは、ストームの原因となるトラフィックをフィルタリングし、SNMP トラップを送信しません。

（注） マルチキャスト　トラフィックのストーム制御スレッシュホールドに達した場合、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）および Cisco Discovery Protocol（CDP）フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。

trap および **shutdown** オプションは、それぞれ独立して機能します。

パケット ストームが検出されたときにシャットダウンとして実行されるアクションを設定する（ストーム時にポートが errdisabled ステートになる）場合、インターフェイスをこのステートから解除するには、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、アクションを **trap** として設定します（ストームの検出時にスイッチはトラップを送出します）。

ストームの発生時のアクションがトラフィックのフィルタリングの場合で、下降抑制レベルを指定しないとき、スイッチは、トラフィック レートが上昇抑制レベルより低下するまですべてのトラフィックをブロックします。下降抑制レベルを指定した場合、スイッチは、トラフィック レートが下降抑制レベルより低下するまでトラフィックをブロックします。

ブロードキャスト ストームの発生時のアクションがトラフィックのフィルタリングの場合、スイッチは、ブロードキャスト トラフィックだけをブロックします。

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

次の例は、75.5% の上昇抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示しています。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例は、ポートでのユニキャスト ストーム制御をイネーブルにして、87% の上昇抑制レベルと 65% の下降抑制レベルを設定する方法を示しています。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例は、ポートでのマルチキャスト ストーム制御をイネーブルにして、2000 パケット / 秒の上昇抑制レベルと 1000 パケット / 秒の下降抑制レベルを設定する方法を示しています。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例は、ポートで **shutdown** アクションをイネーブルにする方法を示しています。

```
Switch(config-if)# storm-control action shutdown
```

設定を確認するには、**show storm-control** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show storm-control	すべてのインターフェイスまたは特定のインターフェイス上のブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御の設定を表示します。

switchport access

ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定するには、**switchport access** 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。スイッチポート モードが **access** に設定されている場合、ポートは指定された VLAN（仮想 LAN）のメンバーとして動作します。**dynamic** として設定されているポートは、受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。アクセス モードをスイッチのデフォルト VLAN 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。

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

構文の説明

vlan *vlan-id*	インターフェイスをアクセス モード VLAN の VLAN ID を持ったスタティック アクセス ポートとして設定します。指定できる範囲は 1 ～ 4094 です。
vlan dynamic	VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）プロトコルによってアクセス モード VLAN が決まるように指定します。ポートに接続されたホスト（複数可）の送信元 MAC（メディア アクセス制御）アドレスに基づいて、ポートが VLAN に割り当てられます。スイッチは受信された新しい MAC アドレスをすべて VMPS サーバに送信して、ダイナミック アクセス ポートに割り当てる VLAN の名前を取得します。ポートにすでに VLAN が割り当てられていて、送信元が VMPS によって承認されている場合、スイッチはパケットを該当する VLAN に転送します。

デフォルト

デフォルト アクセスVLANおよびトランク インターフェイス ネイティブVLANは、プラットフォームまたはインターフェイス ハードウェアに対応するデフォルト VLAN です。

最初はダイナミック アクセス ポートはどの VLAN にも属さず、受信したパケットに基づいて割り当てを受信します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

no switchport access コマンドは、アクセス モード VLAN を装置のデフォルト VLAN にリセットします。

switchport access vlan コマンドを有効にするには、ポートをアクセス モードにする必要があります。

アクセス ポートを割り当てることができるのは、1 つの VLAN のみです。

ポートをダイナミックとして設定するには、事前に VMPS サーバ（Catalyst 6000 シリーズ スイッチなど）を設定する必要があります。

ダイナミック アクセス ポートには、次の制限事項が適用されます。

- ソフトウェアは、Catalyst 6000 シリーズ スイッチなどの VLAN Query Protocol（VQP; VLAN クエリー プロトコル）をクエリーできる VQP クライアントを実装します。Catalyst 2960 スイッチは、VMPS サーバではありません。ポートをダイナミックとして設定するには、事前に VMPS サーバを設定する必要があります。

- ダイナミック アクセス ポートは、エンド ステーションを制御する場合のみ使用します。ブリッジング プロトコルを使用するスイッチまたはルータにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。
- STP がダイナミック アクセス ポートを STP ブロッキング ステートにしないように、ネットワークを設定します。ダイナミック アクセス ポートでは、PortFast 機能が自動的にイネーブルになります。
- ダイナミック アクセス ポートは、1 つの VLAN にのみ属することができ、VLAN タギングは使用しません。
- ダイナミック アクセス ポートを次のように設定することはできません。
  - EtherChannel ポート グループのメンバー（ダイナミック アクセス ポートは、他のダイナミック ポートを含めて、他のポートとグループ化できません）
  - スタティック アドレス エントリ内の送信元または宛先ポート
  - モニタ ポート

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスがデフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Switch(config-if)# switchport access vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN（仮想 LAN）メンバーシップ モードを設定します。

switchport backup interface

互いにバックアップを提供するインターフェイスのペアである Flex Link を設定するには、レイヤ 2 インターフェイスで **switchport backup interface** 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。Flex Link コンフィギュレーションを削除する場合は、このコマンドの **no** 形式を使用します。

switchport backup interface {*interface-id*}

no switchport backup

構文の説明

interface-id	設定されるインターフェイスへのバックアップ リンクとして機能するレイヤ 2 インターフェイスを指定します。このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 6 です。

（注） VLAN（仮想 LAN）インターフェイスは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。

デフォルト

デフォルトは、Flex Link が定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

Flex Link を設定すると、1 つのリンクがプライマリ インターフェイスとして機能してトラフィックを転送し、もう一方のインターフェイスがスタンバイ モードになり、プライマリ リンクがシャットダウンされた場合に転送を開始できるように準備されます。設定されるインターフェイスはアクティブ リンクと呼ばれ、指定されたインターフェイスをバックアップ リンクとして識別されます。この機能は Spanning Tree Protocol（STP; スパニングツリー プロトコル）の代わりに提供され、ユーザが STP をオフにしても基本的なリンク冗長性を維持できます。

- このコマンドは、レイヤ 2 インターフェイスに対してのみ使用可能です。
- アクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つのアクティブ リンクに対してのみバックアップ リンクになれます。アクティブ リンクは別の FLex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ（たとえばファスト イーサネットやギガビット イーサネット）でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を引き継いだ場合にループが発生したり動作が変更したりしないように、両方の FLex Link を似たような特性で設定する必要があります。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルと物理インターフェイスを Flex Link として設定でき、ポート チャネルまたは物理インターフェイスをプライマリ リンクにできます。

- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN（仮想 LAN）で STP に参加しません。STP が動作していない場合、設定されているトポロジーでループが発生していないことを確認してください。

例

次に、2 つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
```

設定を確認するには、**show interfaces switchport** backup イネーブル 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 [*interface-id*] **switchport backup**	スイッチまたは指定されているインターフェイスに設定されている Flex Link とそのステータスを表示します。

switchport block

未知のマルチキャストまたはユニキャスト パケットが転送されるのを防ぐには、**switchport block** 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。未知のマルチキャストまたはユニキャスト パケットを転送する場合は、このコマンドの **no** 形式を使用します。

switchport block {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

構文の説明

multicast	未知のマルチキャスト トラフィックをブロックするように指定します。
unicast	未知のユニキャスト トラフィックをブロックするように指定します。

デフォルト

未知のマルチキャストおよびユニキャスト トラフィックはブロックされません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

デフォルトでは、未知の MAC（メディア アクセス制御）アドレス内のすべてのトラフィックは、すべてのポートに送信されます。保護ポートまたは保護されていないポート上で、未知のマルチキャストまたはユニキャスト トラフィックをブロックできます。保護ポートで、未知のマルチキャストまたはユニキャスト トラフィックがブロックされていない場合、セキュリティ問題となります。

未知のマルチキャストまたはユニキャスト トラフィックのブロッキングは、保護ポートで自動的にイネーブルにならないので、明示的に設定する必要があります。

パケットのブロッキングの詳細については、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、インターフェイスで未知のマルチキャスト トラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block multicast
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。

switchport host

ホスト接続のポートを最適化するには、**switchport host** 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。このコマンドの **no** 形式は、システムに影響を与えません。

switchport host

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ホスト接続用に最適化されていないポートのデフォルトです。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ホスト接続のためポートを最適化するには、**switchport host** コマンドでアクセスするスイッチ ポート モードを設定し、スパニングツリー PortFast をイネーブルにし、チャネル グルーピングをディセーブルにします。エンド ステーション 1 つのみが、この設定を受け入れます。

スパニングツリー PortFast はイネーブルなので、**switchport host** コマンドを単一ホストと接続するポートにだけ入力します。その他のスイッチ、ハブ、コンセントレータ、またはブリッジと fast-start ポートを接続すると、一時的にスパニングツリー ループが発生することがあります。

switchport host コマンドをイネーブルにすると、パケット転送を開始するのにかかる時間が短縮されます。

例

次の例では、ホスト接続のポート コンフィギュレーションを最適化する方法を示します。

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 switchport	スイッチポート モードなど、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。

switchport mode

ポートの VLAN（仮想 LAN）メンバーシップ モードを設定するには、**switchport 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。モードをデバイスの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。

switchport mode {**access** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode {**access** | **dynamic** | **trunk**}

構文の説明

access	アクセス モード（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）を設定します。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN のみです。
dynamic auto	インターフェイス トランキング モード ダイナミック パラメータに auto を指定すると、インターフェイスがリンクをトランク リンクに変換します。これは、デフォルト スイッチポート モードです。
dynamic desirable	インターフェイス トランキング モード ダイナミック パラメータに desirable を指定すると、インターフェイスがリンクをトランク リンクにアクティブに変換します。
trunk	無条件にポートをトランクに設定します。ポートは VLAN レイヤ 2 インターフェイスをトランキングします。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2 つのスイッチ間、スイッチとルータ間のポイントツーポイント リンクです。

デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して、適切なモードでポートを設定した場合のみです。スタティックアクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定のみです。

access モードを入力した場合、インターフェイスはパラメータ非トランキング モードになり、近接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを入力した場合、インターフェイスはパーマネント トランキング モードになり、接続先のインターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを入力した場合に、近接インターフェイスが **trunk** または **desirable** モードに設定されると、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを入力した場合に、近接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されると、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルである Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）によって管理されます。ただし、一部のインターネットワーキング装置では DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この事態を避けるには、DTP をサポートしない装置に接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクでトランキングを行わない場合は、**switchport mode access** 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、トランキングをディセーブルにします。
- DTP　をサポートしていない装置でトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** 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、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセス ポート とトランク ポートは、同時に指定できません。

IEEE 802.1x 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1x を **dynamic auto** または **dynamic desirable** に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 対応ポートを **dynamic auto** または **dynamic desirable** ポートに変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 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。

例

次の例では、ポートをアクセス モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport access	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport trunk	インターフェイスがトランキング モードである場合のトランク特性を設定します。

switchport nonegotiate

switchport nonegotiate インターフェイス コンフィギュレーション コマンドは、レイヤ 2 インターフェイス上で Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）ネゴシエーション パケットが送信されないように指定します。スイッチは、このインターフェイス上で DTP ネゴシエーションを行いません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate

no switchport nonegotiate

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

nonegotiate ステータスを解除するには、**switchport nonegotiate** コマンドの **no** 形式を使用します。

このコマンドが有効なのは、インターフェイス スイッチング モードがアクセスまたはトランク（**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定）の場合のみです。**dynamic**（**auto** または **desirable**）モードでこのコマンドを実行しようとすると、エラーが戻されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。**mode** パラメータ（access または trunk）に基づいて、装置はトランキングしたり、しなかったりします。

- これらのリンクでトランキングを行わない場合は、**switchport mode access** 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、トランキングをディセーブルにします。

- DTP をサポートしていない装置でのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** 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、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

例

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、（mode の設定に応じて）トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport nonegotiate
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN（仮想 LAN）メンバーシップ モードを設定します。

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するには、キーワードを指定しないで **switchport 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。キーワードを指定すると、セキュア MAC（メディア アクセス制御）アドレス、スティッキ MAC アドレス ラーニング、セキュア MAC アドレスの最大数、または違反モードが設定されます。ポート セキュリティをディセーブルするか、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

no switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

構文の説明

aging	（任意）**switchport port-security aging** コマンドを参照してください。
mac-address *mac-address*	（任意）48 ビット MAC アドレスを入力して、インターフェイスのセキュア MAC アドレスを指定します。設定された最大値まで、セキュア MAC アドレスを追加することができます。
vlan *vlan-id*	（任意）トランク ポートでのみ、VLAN（仮想 LAN）ID および MAC アドレスを指定します。VLAN ID が指定されていない場合、ネイティブ VLAN を使用します。
vlan access	（任意）アクセス ポートでのみ、VLAN（仮想 LAN）をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでのみ、VLAN（仮想 LAN）を音声 VLAN として指定します。 （注）　**voice** キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合のみ利用可能です。
mac-address sticky [*mac-address*]	（任意）**mac-address sticky** キーワードのみを入力して、インターフェイスの *sticky learning* をイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習されたすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。 （任意）スティッキ セキュア MAC アドレスを指定するには、*mac-address* を入力します。
maximum *value*	（任意）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。スイッチで設定できるセキュア MAC アドレスの最大数は、システムで許可された利用可能な MAC アドレスの最大数によって設定されます。詳細については、**sdm prefer** 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。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他セキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。 デフォルト設定は 1 です。

vlan [*vlan-list*]	（任意）トランク ポートでは、VLAN のセキュア MAC アドレスの最大数を設定できます。**vlan** キーワードを入力しない場合、デフォルト値を使用します。 • **vlan —** VLAN ごとの最大値を設定します。 • **vlan** *vlan-list* **—** ハイフンで区切られた VLAN 範囲の、またはカンマで区切られた一連の VLAN 上の、VLAN ごとの最大値を設定します。VLAN が指定されていない場合、VLAN ごとの最大値を使用します。
violation	（任意）セキュリティ違反モード、またはポート セキュリティに違反した場合の対処法を設定します。デフォルトは **shutdown** です。
protect	セキュリティ違反保護モードを設定します。このモードでポート セキュア MAC アドレス数がポートで許可された最大制限数に達した場合、最大値を下回るか、または最大許容アドレス数を増やすのに十分なセキュア MAC アドレス数を削除するまで、未知の送信元アドレスを持ったパケットが削除されます。セキュリティ違反が起こっても、ユーザには通知されません。 **（注）** トランク　ポート上で保護モードを設定することは推奨しません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。
restrict	セキュリティ違反制限モードを設定します。このモードでは、セキュア MAC アドレス数がポートで許可された制限に達した場合、十分な数のセキュア MAC アドレスを削除するか、または最大許容アドレス数を増やすまで、未知の送信元アドレスを持ったパケットが削除されます。SNMP トラップ 1 つが送信され、Syslog メッセージがログされ、violation カウンタが増加します。
shutdown	セキュリティ違反シャットダウン モードを設定します。このモードでは、違反が発生しポート LED がオフになった場合、インターフェイスは errdisable になります。SNMP トラップ 1 つが送信され、Syslog メッセージがログされ、violation カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動で再度イネーブルにすることができます。

デフォルト

ポート セキュリティをディセーブルするデフォルトです。

セキュリティがイネーブルでキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数が 1 になります。

デフォルトの違反モードは、**shutdown** です。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア　ポートはアクセス　ポートまたはトランク　ポートになることができますが、ダイナミック アクセス ポートにはなれません。
- セキュア ポートは保護ポートにはなれません。
- セキュア ポートを Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN ポートで設定されたインターフェイスでポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に、アクセス VLAN の最大セキュア アドレス許容数を加算して設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが最大で 2 つ必要です。Cisco IP Phone アドレスは音声 VLAN で学習されます。また、アクセス VLAN でも学習される場合があります。PC を Cisco IP Phone に接続するには、追加の MAC アドレスが必要です。
- 音声 VLAN は、アクセス ポートでのみサポートされ、トランク ポートではサポートされません。
- インターフェイスにセキュア アドレス最大値を入力した場合、新規の値が前回の値より大きいと、新規の値が前回の設定値を無効にします。新規の値が前回の値より小さくて、インターフェイスで設定されたセキュア アドレス数が新規の値を越えた場合、コマンドが拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

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

音声 VLAN ポート上でポート セキュリティをイネーブルにした場合、および IP Phone に接続された PC が存在する場合は、ポート上で許可される最大セキュア アドレス数を 1 より大きい値に設定する必要があります。

セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再度イネーブルにすることができます。

アドレス最大値を 1 に設定し、接続されている装置の MAC アドレスを設定すると、装置はポートの帯域幅をフルに利用できます。

インターフェイスにセキュア アドレス最大値を入力すると、次のとおりになります。

- 新規の値が前回の値より大きいと、新規の値が前回の設定値を無効にします。
- 新規の値が前回の値より小さくて、インターフェイスで設定されたセキュア アドレス数が新規の値を越えた場合、コマンドが拒否されます。

スティッキ セキュア MAC アドレスには次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスでスティッキ ラーニングをイネーブルにした場合、インターフェイスはスティッキ ラーニングをイネーブルする前に動的に学習されたアドレスなど、ダイナミック セキュア MAC アドレスすべてをスティッキ セキュア MAC アドレスに変換し、スティッキ セキュア MAC アドレスすべてを実行コンフィギュレーションに追加します。

- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ ラーニングをディセーブルする、または実行コンフィギュレーションを削除する場合、スティッキ セキュア MAC アドレスの一部は実行コンフィギュレーションのままですが、アドレス テーブルから削除されます。削除されたアドレスは動的に再設定され、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスを設定する場合、アドレスはアドレス テーブルと実行コンフィギュレーションに追加されますポート セキュリティをディセーブルした場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに保持されます。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。スティッキ ラーニングをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキ ラーニングをディセーブルにして **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラー メッセージが表示されスティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されません。

例

次の例では、1 つのポートでポート セキュリティをイネーブルにする方法と、セキュア アドレスの最大数を 5 に設定する方法を示します。Violation モードはデフォルトで、セキュア MAC アドレスは設定されません。

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

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

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

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

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

設定を確認するには、**show port-security** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
show port-security address	スイッチで設定されるセキュア アドレスをすべて表示します。
show port-security interface *interface-id*	スイッチまたは特定のインターフェイスのポート セキュリティ設定を表示します。

switchport port-security aging

セキュア アドレス エントリのエージング タイムおよびタイプを設定したり、特定のポートのセキュア アドレスのエージング動作を変更するには、**switchport port-security aging** 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 セキュリティのエージングをディセーブルにするか、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

no switchport port-security aging {**static** | **time** | **type**}

構文の説明

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

デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルト期間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

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

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

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

セキュア アドレスのアクセス制限を解除するには、セキュア アドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュア アドレスのエージングをディセーブルにします。

例

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを非アクティビティ、エージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

関連コマンド

コマンド	説明
show port-security	ポートに定義されたポート セキュリティ設定を表示します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC（メディア アクセス制御）アドレスを設定します。

switchport priority extend

着信したタグなしフレームのポート プライオリティ、または指定されたポートに接続された IP Phone が受信するフレームのプライオリティを設定するには、**switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {**cos** *value* | **trust**}

no switchport priority extend

構文の説明

cos *value*	PC から受信した、または特定の Class of Service（CoS; サービス クラス）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は、0 ～ 7 です。7 は最高位のプライオリティです。デフォルト値は 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

デフォルト

ポートで受信したタグのないフレームについて、デフォルト ポート プライオリティは、CoS 値 0 に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

音声 VLAN（仮想 LAN）をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol（CDP）パケットを送信し、Cisco IP Phone のアクセス ポートに接続する装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone にコンフィギュレーションを送信するには、Cisco IP Phone に接続するスイッチ ポートの CDP をイネーブルする必要があります（デフォルトにより、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです）。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの Quality of Service（QoS; サービス品質）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドをに入力して、信頼するポート信頼状態を設定することを推奨します。

例

次の例では、受信された IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport priority extend trust
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport voice vlan	ポートに音声 VLAN を設定します。

switchport protected

同じスイッチ上の保護ポートから、レイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離するには、**switchport protected** 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。ポートで保護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。

switchport protected

no switchport protected

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

保護ポートは定義されていません。すべてのポートが保護されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

スイッチポート保護機能はスイッチに対してローカルです。同じスイッチ上の保護ポート間の通信は、レイヤ 3 デバイスを通してのみ行うことができます。異なるスイッチ上の保護ポート間の通信を禁止するには、各スイッチの保護ポートに一意の VLAN（仮想 LAN）を設定し、スイッチ間にトランク リンクを設定する必要があります。保護ポートはセキュア ポートとは異なります。

保護ポートは、他の保護ポートに（ユニキャスト、マルチキャスト、またはブロードキャスト）トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックのみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。

モニタするポートおよびモニタされるポートの両方が保護ポートの場合、ポート モニタリングは機能しません。

例

次の例では、インターフェイス上で保護ポートをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport block	インターフェイス上で未知のユニキャストまたは未知のマルチキャスト トラフィックを防ぎます。

switchport trunk

インターフェイスがトランキング モードの場合に、トランクの特性を設定するには、**switchport trunk** 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。トランキング特性をデフォルトにリセットする場合は、このコマンドの **no** 形式を使用します。

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **native vlan** | {**pruning vlan**}

構文の説明

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可 VLAN（仮想 LAN）のリストを設定します。次の *vlan-list* 形式を参照してください。**none** キーワードは無効です。デフォルトは **all** です。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングが適格である VLAN のリストを設定します。**all** キーワードは無効です。

vlan-list 形式は、**all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [**,***vlan-atom...*] です。

- **all** は 1 ～ 4094 の VLAN すべてを指定します。リストの VLAN すべてを同時に設定するのを許可しないコマンドでは、このキーワードを使用できません。
- **none** — 空のリストを意味します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** — 現在設定されている VLAN リストを置き換えないで、定義済み VLAN リストを追加します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN（1005 を越える VLAN ID）を使用できます。

（注）　許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストは追加できません。

連続しない VLAN ID はカンマで区切ります。ID 範囲を指定するには、ハイフンを使用します。

- **remove** — 現在設定されている VLAN リストを置き換えないで、リストから定義済み VLAN リストを削除します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。

（注）　許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

連続しない VLAN ID はカンマで区切ります。ID 範囲を指定するには、ハイフンを使用します。

- **except** — 定義済み VLAN リストを以外の、計算する必要がある VLAN を示します（指定した VLAN を除く VLAN が追加されます）。有効な ID は 1 ～ 1005 です。連続しない VLAN ID はカンマで区切ります。ID 範囲を指定するには、ハイフンを使用します。
- *vlan-atom* は、1 ～ 4094 の 1 つの VLAN 番号、または 2 つの VLAN 番号で示された連続した VLAN 範囲（低い番号を先にして、ハイフンで区切られた）のいずれかです。

デフォルト

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。

すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

ネイティブ VLAN：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブ モード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニングツリー ループまたはストームの危険性を減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol [CDP]、Port Aggregation Protocol［PAgP; ポート集約プロトコル］、Link Aggregation Control Protocol [LACP]、DTP、および VLAN 1 の VLAN Trunking Protocol [VTP; VLAN トランキング プロトコル]）を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルト リスト（すべての VLAN を許可）にリセットします。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

例

次の例では、VLAN 3 を、すべてのタグなしトラフィックを送信するデフォルト ポートに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN（仮想 LAN）メンバーシップ モードを設定します。

switchport voice vlan

ポートに音声 VLAN（仮想 LAN）を設定するには、**switchport voice 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。

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}

no switchport voice vlan

構文の説明

vlan-id	音声トラフィックに使用する VLAN を指定します。指定できる範囲は 1 ～ 4094 です。デフォルトでは、IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	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。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	IP Phone に、音声 VLAN に関する指示はしません。電話キー パッドから入力された設定を使用します。
untagged	タグなし音声トラフィックを送信するように電話を設定します。電話のデフォルト設定です。

デフォルト

デフォルトでは、スイッチは電話を自動設定しません（**none**）。

デフォルトでは、電話はフレームにタグを付けません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

設定情報を電話に送信するには、スイッチの Cisco IP Phone に接続しているスイッチポートで Cisco Discovery Protocol（CDP）をイネーブルにします。デフォルトにより、CDP はインターフェイスでグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの Quality of Service（QoS; サービス品質）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するポート信頼状態を設定することを推奨します。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを特定の VLAN ID タグ付きで転送します。スイッチは IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1q、**none**、または **untagged** を選択した場合、スイッチは指定された音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 IP precedence 値を伝送します。音声トラフィックのデフォルト値は 5 です。

音声 VLAN で設定された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場合は、ポートの最大セキュア アドレス許容数を 2 以上に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC（メディア アクセス制御）アドレスが 2 つ必要です。アクセス VLAN 用に 1 つ、音声 VLAN 用にもう 1 つです。PC を IP Phone に接続するには、追加の MAC アドレスが必要です。

アクセス VLAN で任意のポート セキュリティ タイプがイネーブルされた場合、音声 VLAN でダイナミック ポート セキュリティは自動的にイネーブルになります。

音声 VLAN では、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

例

次の例では、VLAN 2 をポート用音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport voice vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** イネーブル 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 *interface-id* **switchport**	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport priority extend	指定されたポートに接続されたデバイスが、着信ポートで受信したプライオリティ トラフィックを処理する方法を指定します。

system mtu

パケットの最大サイズ、またはギガビット イーサネット ポートあるいはファスト イーサネット（10/100）ポートの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを設定するには、**system mtu** 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。グローバル MTU 値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system mtu {*bytes* | **jumbo** *bytes*}

no system mtu

構文の説明

bytes	10 Mbps または 100 Mbps のポートのシステム MTU を設定します。指定できる範囲は 1500 ～ 1998 バイトです。これは 10/100 Mbps イーサネット スイッチ ポートで受信される最大 MTU です。
jumbo *bytes*	1000 Mbps 以上で動作するギガビット イーサネット ポートのシステム ジャンボ MTU を設定します。指定できる範囲は 1500 ～ 9000 バイトです。これはギガビット イーサネット ポートの物理ポートで受信される最大 MTU です。

デフォルト

すべてのポートのデフォルトの MTU サイズは 1500 バイトです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンドを使用してシステム MTU またはジャンボ MTU サイズを変更する場合、新しい設定を有効にするにはスイッチをリセットする必要があります。

1000 Mbps で動作するギガビット イーサネット ポートは **system mtu** コマンドによる影響を受けません。10/100 Mbps ポートは **system mtu jumbo** コマンドによる影響を受けません。

指定されたスイッチ タイプの許容範囲外の値を入力すると、値が拒否されます。

（注） このスイッチはインターフェイス単位での MTU 設定をサポートしません。

スイッチの CPU で受信できるフレーム サイズは、**system mtu** コマンドで入力した値に関係なく、1998 バイトに制限されています。転送またはルーティングされるフレームは通常、CPU では受信されませんが、一部のパケット（制御トラフィック、SNMP、Telnet、およびルーティング プロトコルなど）は CPU に送られます。

スイッチはパケットのフラグメント化を行わないため、*出力*インターフェイスでサポートされているパケット サイズより大きなパケットは廃棄されます。

たとえば、**system mtu** 値が 1998 バイトであり、**system mtu jumbo** 値が 5000 バイトの場合には、1000 Mbps で動作するインターフェイスでは 5000 バイトまでのパケットを受信できます。ただし、1000 Mbps で動作するインターフェイスでは 1998 バイトを超えるパケットを受信できますが、その宛先インターフェイスが 10 または 100 Mbps で動作している場合には、パケットは廃棄されます。

例

次の例では、1000 Mbps 以上で動作するギガビット イーサネット ポートのジャンボ パケット サイズを 1800 バイトに設定する方法を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show system mtu** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show system mtu	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 ポートに設定されたパケット サイズを表示します。

test cable-diagnostics tdr

インターフェイスで Time Domain Reflector（TDR）機能を実行するには、**test cable-diagnostics tdr** イネーブル EXEC コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDR を実行するインターフェイスを指定します。

デフォルト

デフォルトはありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

TDR は、10/100 および 10/100/1000 の銅線のイーサネット ポートでのみサポートされます。SFP モジュール ポートではサポートされません。TDR 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。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行したあと、結果を表示するには **show cable-diagnostics tdr interface** *interface-id* イネーブル EXEC コマンドを使用します。

例

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

インターフェイスのリンク ステータスがアップ状態で速度が 10 または 100 Mbps である場合、**test cable-diagnostics tdr interface** *interface-id* コマンドを入力すると次のメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連コマンド

コマンド	説明
show cable-diagnostics tdr	TDR 結果が表示されます。

traceroute mac

指定された送信元 MAC（メディア アクセス制御）アドレスから指定された宛先 MAC アドレスまでパケットがたどるレイヤ 2 パスを表示するには、**traceroute mac** イネーブル EXEC コマンドを使用します。

traceroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

構文の説明

interface *interface-id*	（任意）送信元または宛先スイッチのインターフェイスを指定します。
source-mac-address	送信元スイッチの MAC アドレスを 16 進数で指定します。
destination-mac-address	宛先スイッチの MAC アドレスを 16 進数で指定します。
vlan *vlan-id*	（任意）送信元スイッチから宛先スイッチへとパケットがたどるレイヤ 2 パスをトレースする VLAN（仮想 LAN）を指定します。指定できる VLAN（仮想 LAN）ID は、1 ～ 4094 です。
detail	（任意）詳細情報を指定します。

デフォルト

デフォルトはありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

レイヤ 2 traceroute を正常に機能させるには、ネットワークのスイッチで Cisco Discovery Protocol（CDP）をイネーブルにする必要があります。CDP をディセーブルにしないでください。

スイッチが、レイヤ 2 traceroute をサポートしていない装置をレイヤ 2 パスで検出した場合、スイッチはレイヤ 2 トレース クエリーを送信し続け、タイム アウトにします。

このパスで特定されるホップの最大数は 10 です。

レイヤ 2 traceroute は、ユニキャスト トラフィックのみをサポートします。マルチキャスト送信元または宛先 MAC アドレスを指定する場合、物理パスは特定されず、エラー メッセージが表示されます。

指定された送信元および宛先アドレスが同じ VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。別の VLAN に属する送信元および宛先アドレスを指定する場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合、送信元または宛先 MAC アドレスが属する VLAN を指定する必要があります。VLAN を指定しない場合、パスは特定されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバがポートで検出される）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能はトークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定して、レイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用して、レイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
C-12T/2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5/WS-C2950G-24-EI/2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1/WS-C3550-12G/2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2/WS-C3550-24/2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先スイッチのインターフェイスを指定して、レイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface
fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、スイッチが送信元スイッチに接続していない場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C2960-12T] (2.2.5.5)
con5/WS-C2960-12T/2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1/WS-C3550-12G/2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2/WS-C3550-24/2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、スイッチが送信元 MAC アドレスの宛先ポートを見つけられない場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

次の例では、送信元および宛先装置が別の VLAN に存在する場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先スイッチが複数の VLAN に属する場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
traceroute mac ip	指定された送信元 IP アドレスまたはホスト名から指定された宛先 IP アドレスまたはホスト名までパケットがたどるレイヤ 2 パスを表示します。

traceroute mac ip

指定された送信元 IP アドレスまたはホスト名から指定された宛先 IP アドレスまたはホスト名までパケットがたどるレイヤ 2 パスを表示するには、**traceroute mac ip** イネーブル EXEC コマンドを使用します。

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

構文の説明

source-ip-address	送信元スイッチの IP アドレスをドット付き 10 進表記の 32 ビットとして指定します。
destination-ip-address	宛先スイッチの IP アドレスをドット付き 10 進表記の 32 ビットとして指定します。
source-hostname	送信元スイッチの IP ホスト名を指定します。
destination-hostname	宛先スイッチの IP ホスト名を指定します。
detail	（任意）詳細情報を指定します。

デフォルト

デフォルトはありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

レイヤ 2 traceroute を正常に機能させるには、ネットワークのスイッチで Cisco Discovery Protocol（CDP）をイネーブルにする必要があります。CDP をディセーブルにしないでください。

スイッチが、レイヤ 2 traceroute をサポートしていない装置をレイヤ 2 パスで検出した場合、スイッチはレイヤ 2 トレース クエリーを送信し続け、タイム アウトにします。

このパスで特定されるホップの最大数は 10 です。

指定された送信元および宛先 IP アドレスが同じサブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、IP アドレスと対応する MAC（メディア アクセス制御）アドレスおよび VLAN（仮想 LAN）ID を関連付けるために、スイッチは Address Resolution Protocol（ARP）を使用します。

- 指定された IP アドレスの ARP エントリが存在する場合、スイッチは関連 MAC アドレスを使用して物理パスを特定します。
- ARP エントリが存在しない場合、スイッチは ARP クエリーを送信して IP アドレスを解決しようとします。IP アドレスが同じサブネットに存在する必要があります。IP アドレスが解決されていない場合、パスは特定されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバがポートで検出される）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能はトークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用し、送信元および宛先 IP アドレスを指定して、レイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6/WS-2960-12T/2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5/WS-C2950G-24-EI/2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1/WS-C3550-12G/2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2/WS-C3550-24/2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定して、レイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 パスを示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
rmon collection stats	指定された送信元 MAC アドレスから指定された宛先 MAC アドレスでパケットがたどるレイヤ 2 パスを表示します。

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 コマンドにより分類されたトラフィックの信頼状態を定義するには、**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。

trust [**cos** | **dscp** | **ip-precedence**]

no trust [**cos** | **dscp** | **ip-precedence**]

構文の説明

cos	（任意）パケットの Class of Service（CoS; サービス クラス）値を使用することにより、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 デフォルト CoS 値が使用されます。
dscp	（任意）パケットの Differentiated Services Code Point（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）を使用することにより、入力パケットを分類します。非 IP パケットでは、パケットにタグが付いている場合、パケット CoS 値が使用されます。パケットにタグが付いていない場合、デフォルト ポート CoS 値を使用して CoS を DSCP にマッピングします。
ip-precedence	（任意）パケット 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）を使用することにより、入力パケットを分類します。非 IP パケットでは、パケットにタグが付いている場合、パケット CoS 値が使用されます。パケットにタグが付いていない場合、ポートのデフォルト CoS 値を使用して CoS を DSCP にマッピングします。

デフォルト

アクションは信頼されていません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

特定のトラフィックの Quality of Service（QoS; サービス品質）の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、ある DSCP 値を持った着信トラフィックが信頼されます。着信トラフィックの DSCP 値と一致し、信頼できるクラス マップを設定できます。

このコマンドで設定された信頼値は、**mls qos trust** インターフェイス コンフィギュレーション コマンドで設定された信頼値より優先されます。

同じポリシー マップ内では、**trust** コマンドと **set** ポリシーマップ クラス コンフィギュレーション コマンドと同時に指定できません。

trust cos を指定する場合、パケットに DSCP 値を生成するために、QoS は受信またはデフォルト ポート CoS 値、および CoS/DSCP マップを使用します。

trust dscp を指定する場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用します。タグなしの非 IP パケットでは、QoS はデフォルト ポート CoS 値を使用します。どちらの場合でも、パケットの DSCP 値は CoS/DSCP マップから取得します。

trust ip-precedence を指定する場合、QoS は入力パケットから IP precedence 値と IP precedence/DSCP マップを使用します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用します。タグなしの非 IP パケットでは、QoS はデフォルト ポート CoS 値を使用します。どちらの場合でも、パケットの DSCP は CoS/DSCP マップから取得します。

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。イネーブル EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、*class1* で分類されたトラフィックの着信 DSCP 値を信頼するため、ポート信頼状態を定義する方法を示します。

```
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 policed-dscp-transmit
Switch(config-pmap-c)# exit
```

設定を確認するには、**show policy-map** イネーブル 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。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定することができるポリシー マップを作成または変更します。
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	QoS ポリシー マップを表示します。

udld

UniDirectional Link Detection（UDLD; 単一方向リンク検出）でアグレッシブ モードまたはノーマル モードをイネーブルにし、設定可能なメッセージ タイマーを設定するには、**udld** 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。すべての光ファイバ ポートでアグレッシブ モードまたはノーマル モードの UDLD 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。

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

構文の説明

aggressive	すべての光ファイバ インターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバ インターフェイスにおいて、ノーマル モードで UDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズ フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 7 ～ 90 秒です。

デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 60 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

UDLD は、ノーマル（デフォルト）モードおよびアグレッシブ モードをサポートします。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードおよびアグレッシブ モードの詳細については、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「Understanding UDLD」の章を参照してください。

プローブ パケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷のトレードオフを行っていることになります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバ インターフェイスだけです。他のインターフェイス タイプで UDLD をイネーブルにする場合は、**udld** 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。

次のコマンドを使用して、UDLD によってシャットダウンされたインターフェイスをリセットできます。

- **udld reset** イネーブル EXEC コマンド **—** UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド

- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力 — グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port** または **udld port aggressive** 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 — 指定されたインターフェイスの UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド — 自動的に UDLD errdisable ステートから回復します。

例

次の例では、すべての光ファイバ インターフェイスで UDLD をイネーブルにする方法を示します。

```
Switch(config)# udld enable
```

設定を確認するには、**show udld** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show udld	すべてのポートまたは指定されたポートの UDLD 管理ステータスおよび動作ステータスを表示します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	UDLD によるすべてのインターフェイスのシャットダウンをリセットし、トラフィックが再び通過することを許可します。

udld port

個々のインターフェイスで UniDirectional Link Detection（UDLD; 単一方向リンク検出）をイネーブルにするか、光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルにされるのを防ぐには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻したり、非光ファイバ ポートで入力された場合に UDLD をディセーブルしたりする場合は、このコマンドの **no** 形式を使用します。

udld port [**aggressive**]

no udld port [**aggressive**]

構文の説明

aggressive	指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

デフォルト

光ファイバ インターフェイスでは、UDLD はイネーブル、アグレッシブ モード、ディセーブルのいずれでもありません。このため、光ファイバ インターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに従い UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートは単一方向リンクを検出できません。

UDLD は、ノーマル（デフォルト）モードおよびアグレッシブ モードをサポートします。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードおよびアグレッシブ モードの詳細については、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 UDLD」を参照してください。

ノーマル モードで UDLD をイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。アグレッシブ モードで UDLD をイネーブルにするには、**udld port aggressive** 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。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を無効にする場合は、光ファイバ ポートで **udld port aggressive** コマンドを使用します。設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no** 形式を使用します。

次のコマンドを使用して、UDLD によってシャットダウンされたインターフェイスをリセットできます。

- **udld reset** イネーブル EXEC コマンド — UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力 — グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port** または **udld port aggressive** 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 — 指定されたインターフェイスの UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド — 自動的に UDLD errdisable ステートから回復します。

例

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定にもかかわらず、光ファイバ上で UDLD をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld** *interface* イネーブル 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。
show udld	すべてのポートまたは指定されたポートの UDLD 管理ステータスおよび動作ステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにする、または設定可能なメッセージ タイマーの時間を設定します。
udld reset	UDLD によるすべてのインターフェイスのシャットダウンをリセットし、トラフィックが再び通過することを許可します。

udld reset

UniDirectional Link Detection（UDLD; 単一方向リンク検出）によりディセーブルになったインターフェイスをすべてリセットし、トラフィックの転送を再び許可するには、**udld reset** イネーブル EXEC コマンドを使用します（イネーブルの場合には、スパニングツリー、Port Aggregation Protocol［PAgP; ポート集約プロトコル］、Dynamic Trunking Protocol [DTP] などの他の機能が有効になります）。

udld reset

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

インターフェイスの設定で、UDLD がまだイネーブルである場合、これらのポートは再び UDLD の稼働を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

例

次の例では、UDLD によりディセーブルになったインターフェイスをすべてリセットする方法を示します。

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

設定を確認するには、**show udld** イネーブル 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。
show udld	すべてのポートまたは指定されたポートの UDLD 管理ステータスおよび動作ステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにする、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。

vlan（グローバル コンフィギュレーション）

VLAN（仮想 LAN）を追加して、config-vlan モードを開始するには、**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。VLAN を削除する場合は、このコマンドの **no** 形式を使用します。標準範囲 VLAN（VLAN ID 1 ～ 1005）の設定情報は、常に VLAN データベースに保存されます。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）モードがトランスペアレントな場合は、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成することができます。すると、VTP モード、ドメイン名、および VLAN 設定は、スイッチの実行コンフィギュレーション ファイルに保存されます。**copy running-config startup-config** イネーブル EXEC コマンドを使用すれば、設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存することができます。

vlan *vlan-id*

no vlan vlan-*id*

構文の説明

vlan-id	追加および設定する VLAN の ID。*vlan-id* では、指定できる範囲は 1 ～ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力することができます。

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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を追加するには、**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ください。拡張範囲で VLAN を設定する前に、**vtp transparent** グローバル コンフィギュレーション コマンドまたは VLAN 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 VTP トランスペアレント モードにします。拡張範囲 VLAN は、VTP によって学習されず、VLAN データベースにも追加されませんが、VTP モードがトランスペアレントである場合には、VTP モード、ドメイン名、およびすべての VLAN 設定は、実行コンフィギュレーションに保存され、これをスイッチ スタートアップ コンフィギュレーション ファイルに保存することもできます。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、設定は次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードがトランスペアレントであり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- VTP モードがサーバの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN の VTP モードおよび VTP 設定には VLAN データベース情報が使用されます。

スイッチが VLAN トランスペアレント モードでない場合に拡張範囲 VLAN を作成しようとすると、VLAN は拒否され、エラー メッセージが表示されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、config-vlan モードを開始することができません。

vlan コマンドを VLAN ID とともに入力すると、config-vlan モードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更することができます。指定された VLAN は、config-vlan モードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。

次のコンフィギュレーション コマンドが config-vlan モードで利用できます。このコマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

（注）　すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされている VLAN コンフィギュレーション コマンドは、**mtu** *mtu-size* および **remote-span** です。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。

- **are** *are-number* : この VLAN の ARE（全ルート エクスプローラ）ホップの最大数を定義します。このキーワードは TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルトは 7 です。値が入力されない場合、最大数は 0 であるとみなされます。
- **backupcrf** : バックアップ CRF モードを指定します。このキーワードは、Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN だけに適用されます。
  - **enable** は、この VLAN のバックアップ CRF モードをイネーブルにします。
  - **disable** は、この VLAN のバックアップ CRF モードをディセーブルにします（デフォルト）。
- **bridge** {*bridge-number* | **type**} : 論理分散ソース ルーティング ブリッジ、すなわち、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0 ～ 15 です。デフォルトのブリッジ番号は、FDDI-NET、TrBRF、およびトークンリング NET VLAN では 0（ソース ルーティング ブリッジなし）です。**type** キーワードは、TrCRF VLAN にだけ適用され、次のうちのどちらかです。
  - **srb**（source-route bridge［SRB; ソースルート ブリッジ］）
  - **srt**（Source-Route Transparent［SRT; ソースルート トランスペアレント］）ブリッジング VLAN
- **exit** : 変更を適用し、VLAN データベース リビジョン番号（VLAN 1 ～ 1005 のみ）を増分し、config-vlan モードを終了します。
- **media** : VLAN メディア タイプを定義します。様々なメディア タイプで有効なコマンドおよび構文については、表 2-33 を参照してください。

（注）　スイッチがサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別のスイッチに対する VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）グローバル アドバタイズに限って設定します。これらの VLAN はローカルに停止されます。

  - **ethernet** は、イーサネット メディア タイプです（デフォルト）。
  - **fddi** は、FDDI メディア タイプです。
  - **fd-net** は、FDDI Network Entity Title（NET）メディア タイプです。
  - **tokenring** は、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v 2 モードがイネーブルの場合は TrCRF です。
  - **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
- **mtu** *mtu-size* : Maximum Transmission Unit（MTU; 最大伝送ユニット）（バイト単位のパケット サイズ）を指定します。指定できる範囲は 1500 ～ 18190 です。デフォルトは 1500 バイトです。

- **name** *vlan-name*：管理ドメイン内で一意である 1 ～ 32 文字の ASCII 文字列で VLAN を命名します。デフォルトは *VLANxxxx* です。ここで、*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。
- **no**：コマンドを無効にし、デフォルト設定に戻します。
- **parent** *parent-vlan-id*：既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定します。このパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときに必要です。指定できる番号は 0 ～ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0（親 VLAN なし）です。トークンリングおよび TrCRF VLAN では、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
- **remote-span**：VLAN を Remote SPAN（RSPAN）VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN が削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも無効となります。VTP がイネーブルの場合、新規の RSPAN VLAN は 1024 より低い VLAN ID の VTP により伝播されます。VLAN ではラーニングはディセーブルです。詳細は、**remote-span** コマンドを参照してください。
- **ring** *ring-number*：FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる値は、1 ～ 4095 です。トークンリング VLAN のデフォルトは 0 です。FDDI VLAN については、デフォルトはありません。
- **said** *said-value*：IEEE 802.10 に記載されている Security Association Identifier（SAID）を指定します。指定できる値は、1 ～ 4294967294 です。この値は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。
- **shutdown**：VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、config-vlan モードを終了したときに有効になります。
- **state**：VLAN ステートを指定します。
  - **active** は、VLAN が稼働中であることを意味します（デフォルト）。
  - **suspend** は、VLAN が停止していることを意味します。停止している VLAN はパケットを通過させません。
- **ste** *ste-number*：STE（スパニングツリー エクスプローラ）ホップの最大数を定義します。このキーワードは、Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。
- **stp type**：FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを定義します。FDDI-NET VLAN の場合、デフォルトの STP タイプは **ieee** です。トークンリング NET VLAN の場合、デフォルトの STP タイプは **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。
  - SRT ブリッジングを実行している IEEE イーサネット STP の場合は **ieee**
  - SRB を実行している IBM STP の場合は、**ibm**
  - SRT ブリッジング（IEEE）および SRB（IBM）の組み合わせを実行している STP の場合は、**auto**
- **tb-vlan1** *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id*：この VLAN がトランスレーショナル ブリッジングを行っている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる値は、0 ～ 1005 です。値が指定されないと、0（トランスレーショナル ブリッジングなし）とみなされます。

表 2-33　様々なメディア タイプで指定できるコマンドと構文

メディア タイプ	指定できる構文
イーサネット	**name** *vlan-name*、**media ethernet**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、***remote-span***、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*、**media fddi**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**ring** *ring-number*、**parent** *parent-vlan-id*、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*

表 2-33　様々なメディア タイプで指定できるコマンドと構文（続き）

メディア タイプ	指定できる構文
FDDI-NET	**name** *vlan-name*、**media fd-net**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**bridge** *bridge-number*、**stp type** {**ieee** | **ibm** | **auto**}、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id* VTP v2 モードがディセーブルの場合、**stp type** を **auto** に設定しないでください。
トークンリング	VTP v1 モードがイネーブルの場合 **name** *vlan-name*, **media tokenring, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）	VTP v2 モードがイネーブルの場合 **name** *vlan-name*、**media tokenring**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**ring** *ring-number*、**parent** *parent-vlan-id*、**bridge type** {**srb** | **srt**}、**are** *are-number*、**ste** *ste-number*、**backupcrf** {**enable** | **disable**}、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
トークンリング NET	VTP v1 モードがイネーブルの場合 **name** *vlan-name*, **media tr-net**、**state** {**suspend** | **active**}, **said** *said-value*、**mtu** *mtu-size*、**bridge** *bridge-number*、**stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）	VTP v2 モードがイネーブルの場合 **name** *vlan-name*, **media tr-net, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

表 2-34 では、VLAN の設定規則を説明します。

表 2-34　VLAN 設定規則

設定	規則
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしておかないでください。 TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1 つのバックアップ Concentrator Relay Function（CRF; コンセントレータ リレー機能）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしておかないでください。

表 2-34　VLAN 設定規則（続き）

設定	規則
VTP v1 モードがイネーブルの場合	VLAN の STP タイプを auto に設定しないでください。 この規則は、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つにもとの VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）もとの VLAN とは異なったメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なったメディア タイプである必要があります。

例

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには *VLANxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。デフォルトの **media** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの *said-value* 変数は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、**stp-type** オプションは **ieee** です。**exit** config-vlan コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何もしません。

次の例では、すべての特性がデフォルトである VLAN を新規作成し、config-vlan モードを開始する方法を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

次の例では、すべての特性がデフォルトである拡張範囲 VLAN を新規作成し、config-vlan モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する方法を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

設定を確認するには、**show vlan** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または管理ドメイン内の 1 つの VLAN（VLAN ID または名前が指定されている場合）のパラメータを表示します。
vlan（VLAN コンフィギュレーション）	標準範囲 VLAN を VLAN データベースに設定します。

vlan（VLAN コンフィギュレーション）

VLAN（仮想 LAN）データベースに標準範囲 VLAN（VLAN ID 1 ～ 1005）の VLAN 特性を設定するには、**vlan** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** イネーブル EXEC コマンドを入力します。VLAN 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。設定された特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。

vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* |
type {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** mtu-size]
[**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*]
[**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}]
[**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id]*

no vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* |
type {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** *mtu-size*]
[**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*]
[**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}]
[**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は、このコマンドでは追加したり変更したりすることはできません。拡張範囲 VLAN を追加する場合は、**vlan（グローバル コンフィギュレーション）**コマンドで config-vlan モードを開始します。

（注） スイッチがサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別のスイッチに対する VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）グローバル アドバタイズに限って設定します。これらの VLAN はローカルに停止されます。

構文の説明

vlan-id	設定された VLAN の ID。指定できる値は、1 ～ 1005 です。この値は、管理ドメイン内で一意である必要があります。先行ゼロは入力しないでください。
are *are-number*	（任意）この VLAN の ARE（全ルート エクスプローラ）ホップの最大数を指定します。このキーワードは、Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。値が入力されない場合、最大数は 0 であるとみなされます。

backupcrf {**enable** | **disable**}	（任意）バックアップ CRF モードを指定します。このキーワードは、Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN だけに適用されます。 • **enable** は、この VLAN のバックアップ CRF モードをイネーブルにします。 • **disable** は、この VLAN のバックアップ CRF モードをディセーブルにします。
bridge *bridge-number* | **type** {**srb** | **srt**}	（任意）論理分散ソース ルーティング ブリッジ、すなわち FDDI-NET、トークンリング NET、および Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。 指定できる範囲は 0 ～ 15 です。 **type** キーワードは、TrCRF VLAN にだけ適用され、次のうちの 1 つです。 • **srb**（source-route bridge [SRB; ソースルート ブリッジ]） • **srt**（Source-Route Transparent [SRT; ソースルート トランスペアレント]）ブリッジング VLAN
media {**ethernet** | **fddi** | **fd-net** | **tokenring** | **tr-net**}	（任意）VLAN メディア タイプを指定します。表 2-35 に各メディア タイプで指定できる構文を表示します。 • **ethernet** は、イーサネット メディア タイプです（デフォルト）。 • **fddi** は、FDDI メディア タイプです。 • **fd-net** は、FDDI Network Entity Title（NET）メディア タイプです。 • **tokenring** は、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v2 モードがイネーブルの場合は TrCRF です。 • **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
mtu *mtu-size*	（任意）Maximum Transmission Unit（MTU; 最大伝送ユニット）（バイト単位のパケットサイズ）を指定します。指定できる範囲は 1500 ～ 18190 です。
name *vlan-name*	（任意）管理ドメイン内で一意である 1 ～ 32 文字の ASCII 文字列で VLAN 名を指定します。
parent *parent-vlan-id*	（任意）既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定します。このパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときに必要です。指定できる範囲は 0 ～ 1005 です。
ring *ring-number*	（任意）FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ～ 4095 です。
said *said-value*	（任意）IEEE 802.10 に記載されている Security Association Identifier（SAID）を指定します。指定できる値は、1 ～ 4294967294 です。この値は、管理ドメイン内で一意である必要があります。
state {**suspend** | **active**}	（任意）VLAN ステートを指定します。 • **active** である場合、VLAN は稼働中です。 • **suspend** の場合、VLAN は停止しています。停止している VLAN はパケットを通過させません。

ste *ste-number*	（任意）STE（スパニングツリー エクスプローラ）ホップの最大数を指定します。このキーワードは、Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。
stp type {**ieee** | **ibm** | **auto**}	（任意）FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを指定します。 • SRT ブリッジングを実行している IEEE イーサネット STP の場合は **ieee** • SRB を実行している IBM STP の場合は、**ibm** • SRT ブリッジング（IEEE）および SRB（IBM）の組み合わせを実行している STP の場合は、**auto**
tb-vlan1 *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id*	（任意）この VLAN がトランスレーショナル ブリッジングを行っている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる値は、0 ～ 1005 です。値が指定されないと、0 とみなされます。

表 2-35 に、様々なメディア タイプで指定できる構文オプションを示します。

表 2-35　様々なメディア タイプで指定できる構文

メディア タイプ	指定できる構文
イーサネット	**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI	**vlan** *vlan-id* [**name** *vlan-name*] **media fddi** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI-NET	**vlan** *vlan-id* [**name** *vlan-name*] **media fd-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*] VTP v2 モードがディセーブルの場合、**stp type** を **auto** に設定しないでください。
トークンリング	VTP v1 モードがイネーブルの場合 **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）	VTP v2 モードがイネーブルの場合 **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**bridge type** {**srb** | **srt**}] [**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
トークンリング NET	VTP v1 モードがイネーブルの場合 **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

表 2-35　様々なメディア タイプで指定できる構文（続き）

メディア タイプ	指定できる構文
Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）	VTP v2 モードがイネーブルの場合 **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

表 2-36 では、VLAN の設定規則を説明します。

表 2-36　VLAN 設定規則

設定	規則
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしておかないでください。 TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1 つのバックアップ Concentrator Relay Function（CRF; コンセントレータ リレー機能）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしておかないでください。
VTP v1 モードがイネーブルの場合	VLAN の STP タイプを auto に設定しないでください。 この規則は、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つにもとの VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）もとの VLAN とは異なったメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なったメディア タイプである必要があります。

デフォルト

ARE 値は 7 です。

バックアップ CRF はディセーブルです。

FDDI-NET、TrBRF、およびトークンリング NET VLAN については、ブリッジ番号は 0（ソース ルーティング ブリッジなし）です。

media タイプは **ethernet** です。

デフォルトの *mtu-size* は 1500 バイトです。

vlan-name 変数は *VLANxxxx* です。ここで、*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。

親 VLAN ID は、FDDI およびトークンリング VLAN では 0（親 VLAN なし）です。TrCRF VLAN では、親 VLAN ID を指定する必要があります。トークンリングおよび TrCRF VLAN では、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。

トークンリング VLAN の *ring-number* は 0 です。FDDI VLAN の場合は、デフォルトはありません。

said-value は、100000 に VLAN ID 番号を加算した値です。

ステートは **active** です。

STE 値は 7 です。

STP タイプは、FDDI-NET では **ieee**、トークンリング NET VLAN では **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。

tb-vlan1-id および *tb-vlan2-id* 変数は 0（トランスレーショナル ブリッジングなし）です。

コマンド モード

VLAN コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

このコマンド モードが利用できるのは、標準範囲 VLAN（VLAN ID 1 ～ 1005）を設定する場合に限ります。

（注） 拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定する場合は、**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ください。

VTP の設定は常に VLAN データベースに保存されます。VTP モードがトランスペアレントの場合、VTP 設定は、VTP モードおよびドメイン名とともにスイッチの実行コンフィギュレーション ファイルにも保存されます。**copy running-config startup-config** イネーブル EXEC コマンドを使用すれば、これをスイッチ スタートアップ コンフィギュレーション ファイルに保存することができます。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存してスイッチを再起動した場合、設定は次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードがトランスペアレントであり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- VTP モードがサーバである場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN の VTP モードおよび VTP 設定には VLAN データベース情報が使用されます。

no vlan コマンドを使用した結果は次のとおりです。

- **no vlan** *vlan-id* 形式を使用すると、VLAN は削除されます。VLAN を削除すると、削除された VLAN を参照する他の親 VLAN およびトランスレーショナル ブリッジング パラメータは自動的に 0 にリセットされます。
- **no vlan** *vlan-id* **bridge** 形式を使用すると、VLAN ソース ルーティング ブリッジ番号はデフォルトの 0 に戻ります。**vlan** *vlan-id* **bridge** コマンドは、FDDI-NET およびトークンリング NET VLAN でのみ使用され、他の VLAN タイプでは無視されます。
- **no vlan** *vlan-id* **media** 形式を使用すると、メディア タイプはデフォルト（**ethernet**）に戻ります。VLAN メディア タイプ（**no** 形式を含む）を変更すると、（そのコマンドに **mtu** キーワードも存在しない場合）VLAN MTU はそのタイプのデフォルトの MTU にリセットされます。また、VLAN の親 VLAN およびトランスレーショナル ブリッジング VLAN も（そのコマンドに **parent**、**tb-vlan1**、または **tb-vlan2** が存在しない場合）デフォルトにリセットされます。
- **no vlan** *vlan-id* **mtu** 形式を使用すると、VLAN MTU は適用可能な VLAN メディア タイプのデフォルトに戻ります。**media** キーワードを使用しても MTU を変更することができます。
- **no vlan** *vlan-id* **name** *vlan-name* 形式を使用すると、VLAN 名はデフォルト名に戻ります（*VLANxxxx*、ここで *xxxx* は VLAN ID 番号に等しい 4 桁の数字［先行ゼロを含む］です）。
- **no vlan** *vlan-id* **parent** 形式を使用すると、親 VLAN はデフォルト（0）に戻ります。親 VLAN が削除された場合、または **media** キーワードによって VLAN タイプまたは親 VLAN の VLAN タイプが変更された場合、親 VLAN はデフォルトにリセットされます。
- **no vlan** *vlan-id* **ring** 形式を使用すると、VLAN 論理リング番号はデフォルト（0）に戻ります。
- **no vlan** *vlan-id* **said** 形式を使用すると、VLAN SAID はデフォルト（100000 に VLAN ID を加算した値）に戻ります。
- **no vlan** *vlan-id* **state** 形式を使用すると、VLAN ステートはデフォルト（**active**）に戻ります。
- **no vlan** *vlan-id* **stp type** 形式を使用すると、VLAN スパニングツリー タイプはデフォルト（**ieee**）に戻ります。
- **no vlan** *vlan-id* **tb-vlan1** または **no vlan** *vlan-id* **tb-vlan2** 形式を使用すると、1 つまたは複数の VLAN トランスレーショナル ブリッジ VLAN はデフォルト（0）に戻ります。トランスレーショナル ブリッジ VLAN は、影響を受ける VLAN とは異なった VLAN タイプである必要があります。2 つ指定した場合には、この 2 つが互いに異なった VLAN タイプである必要があります。トランスレーショナル ブリッジ VLAN が削除された場合、**media** キーワードにより VLAN タイプが変更された場合、または **media** キーワードにより対応するトランスレーション ブリッジ VLAN の VLAN タイプが変更された場合、トランスレーショナル ブリッジ VLAN はデフォルトに戻ります。

例

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには *VLANxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。デフォルトの **media** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの *said-value* 変数は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、**stp-type** オプションは **ieee** です。**exit** または **apply** vlan コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何もしません。

```
Switch(vlan)# vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

次の例では、名前および MTU サイズを変更することにより既存の VLAN を変更する方法を示します。

```
Switch(vlan)# no vlan name engineering mtu 1200
```

設定を確認するには、**show vlan** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または管理ドメイン内の 1 つの VLAN（VLAN ID または名前が指定されている場合）のパラメータを表示します。
vlan（グローバル コンフィギュレーション）	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vlan database

VLAN（仮想 LAN）コンフィギュレーション モードを開始するには、**vlan database** イネーブル EXEC コマンドを使用します。このモードから、標準範囲 VLAN の VLAN 設定の追加、削除、および変更を行い、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を使用してこれらの変更をグローバルに伝播することができます。設定情報は、VLAN データベースに保存されます。

vlan database

（注）　VLAN コンフィギュレーション モードが有効なのは、VLAN ID 1 ～ 1005 だけです。

構文の説明

このコマンドには、引数またはキーワードはありません。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VLAN データベース コンフィギュレーション コマンドを使用することにより、VLAN 1 ～ 1005 を設定することができます。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定するには、**vlan（グローバル コンフィギュレーション）**コマンドで config-vlan モードを開始します。また、**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 ID 1 ～ 1005 を設定することもできます。

VLAN コンフィギュレーション モードからイネーブル EXEC モードに戻る場合は、**exit** コマンドを入力します。

（注）　このコマンド モードはセッション指向であるため、他のモードとは異なっています。VLAN パラメータを追加、削除、または変更した場合、**apply** または **exit** コマンドを入力してセッションを終了するまでその変更は適用されません。変更が適用されると、VTP コンフィギュレーション バージョンは増分されます。**abort** を入力して変更を VTP データベースに適用しないこともできます。

VLAN コンフィギュレーション モードに入ると、VLAN データベースにアクセスして、次のコマンドで変更を行うことができます。

- **vlan**：サブコマンドにアクセスして、1 つの VLAN と関連付けられた値を追加、削除、または変更します。詳細は、**vlan（VLAN コンフィギュレーション）**コマンドを参照してください。
- **vtp**：サブコマンドにアクセスして、VTP 管理機能を実行します。詳細は、**vtp（VLAN コンフィギュレーション）**コマンドを参照してください。

VLAN または VTP パラメータを変更した場合、次の編集バッファ処理コマンドを使用することができます。

- **abort**：変更を適用せずにこのモードを終了します。VLAN コンフィギュレーション モードを開始する前に稼働していた VLAN 設定を使用し続けます。

- **apply**：現在の変更を VLAN データベースに適用し、データベース コンフィギュレーション リビジョン番号を増分し、管理ドメイン全体にこれを伝播し、VLAN コンフィギュレーション モードに残ります。

（注）　スイッチが VTP クライアント モードである場合にはこのコマンドを使用することはできません。

- **exit**：すべてのコンフィギュレーション変更を VLAN データベースに適用し、データベース コンフィギュレーション番号を増分し、管理ドメイン全体にこれを伝播し、イネーブル EXEC モードに戻ります。
- **no**：コマンドを無効にするか、デフォルトに設定します。指定できる値は **vlan** および **vtp** です。
- **reset**：VLAN データベースに対して実行しようとした変更を破棄し、設定しようとしたデータベースをスイッチ上で実施されている VLAN データベースにリセットし、VLAN コンフィギュレーション モードに残ります。
- **show**：VLAN データベース情報を表示します。
- **show changes** [*vlan-id*]：すべての標準範囲 VLAN ID（1 ～ 1005）または指定された VLAN ID（1 ～ 1005）について、スイッチ上の VLAN データベースと設定しようとしている VLAN データベース間の相違を表示します。
- **show current** [*vlan-id*]：スイッチ上または選択された VLAN（1 ～ 1005）上の VLAN データベースを表示します。
- **show proposed** [*vlan-id*]：設定しようとしている VLAN データベースまたは設定しようとしているデータベースから選択された VLAN（1 ～ 1005）を表示します。設定しようとしている VLAN データベースは、**exit** または **apply** VLAN コンフィギュレーション コマンドを使用するまで実行コンフィギュレーショではありません。

show vlan イネーブル EXEC コマンドを入力すると、VLAN データベース変更が行われたのか、それとも打ち切られたのかを確認することができます。出力は、**show** VLAN データベース コンフィギュレーション コマンドの出力とは異なっています。

例

次の例では、イネーブル EXEC モードから VLAN コンフィギュレーション モードを開始して、VLAN データベース情報を表示する方法を示します。

```
Switch# vlan database
Switch(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500

VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

(テキスト出力は省略)
```

次に **show changes** コマンドの出力例を示します。

```
Switch(vlan)# show changes

DELETED:
  VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

次の例では、現在のデータベースの VLAN 7 と設定しようとしているデータベースとの相違を表示する方法を示します。

```
Switch(vlan)# show changes 7

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

次に **show current 20** コマンドの出力例を示します。現在のデータベースの VLAN 20 だけが表示されます。

```
Switch(vlan)# show current 20
VLAN ISL Id: 20
    Name: VLAN0020
    Media Type: Ethernet
    VLAN 802.10 Id: 100020
    State: Operational
    MTU: 1500
```

関連コマンド

コマンド	説明
show vlan	管理ドメイン内のすべての設定された VLAN のパラメータを表示します。
shutdown vlan	指定された VLAN でローカル トラフィックをシャットダウン（停止）します。
vlan（グローバル コンフィギュレーション）	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vmps reconfirm（イネーブル EXEC）

ただちに VLAN Query Protocol（VQP）クエリーを送信して、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）でのすべてのダイナミック VLAN（仮想 LAN）割り当てを再確認するには、**vmps reconfirm** イネーブル EXEC コマンドを使用します。

vmps reconfirm

構文の説明

このコマンドには、引数またはキーワードはありません。

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

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VQP クエリーを VMPS へただちに送信する方法を示します。

```
Switch# vmps reconfirm
```

show vmps イネーブル EXEC コマンドを入力して、Reconfirmation Status セクションの VMPS Action 列を調べることにより、設定を確認することができます。**show vmps** コマンドは、再確認タイマー切れまたは **vmps reconfirm** コマンドの入力のいずれかにより最後に割り当てが再確認された結果を表示します。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（グローバル コンフィギュレーション）	VQP クライアントの再確認間隔を変更します。

vmps reconfirm（グローバル コンフィギュレーション）

VLAN Query Protocol（VQP）クライアントの再確認間隔を変更するには、**vmps reconfirm** 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。

vmps reconfirm *interval*

no vmps reconfirm

構文の説明

interval	ダイナミック VLAN（仮想 LAN）割り当てを再確認するための VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）への VQP クライアント クエリーの再確認間隔。指定できる範囲は 1 ～ 120 分です。

デフォルト

デフォルトの再確認間隔は 60 分です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VQP クライアントが 20 分ごとにダイナミック VLAN エントリを再確認するように設定する方法を示します。

```
Switch(config)# vmps reconfirm 20
```

show vmps イネーブル EXEC コマンドを入力して、Reconfirm Interval 列を調べることにより、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 vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（イネーブル EXEC）	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。

vmps retry

VLAN Query Protocol（VQP）クライアントのサーバごとの再試行回数を設定するには、**vmps retry** 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。

vmps retry *count*

no vmps retry

構文の説明

count	リストの次のサーバに照会する前にクライアントが VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）と通信しようとした回数。指定できる範囲は 1 ～ 10 です。

デフォルト

デフォルトの再試行回数は 3 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、再試行回数を 7 に設定する方法を示します。

```
Switch(config)# vmps retry 7
```

show vmps イネーブル EXEC コマンドを入力して、Server Retry Count 列を調べることにより、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 vmps	VQP および VMPS 情報を表示します。

vmps server

プライマリ VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）および最大 3 つまでのセカンダリ サーバを設定するには、**vmps server** 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。VMPS サーバを削除する場合は、このコマンドの **no** 形式を使用します。

vmps server *ipaddress* [**primary**]

no vmps server [*ipaddress*]

構文の説明

ipaddress	プライマリおよびセカンダリ VMPS サーバの IP アドレスまたはホスト名。ホスト名を指定した場合には、Domain Name System（DNS; ドメイン ネーム システム）サーバを設定してください。
primary	(任意)プライマリとセカンダリのどちらの VMPS サーバを設定するのかを決定します。

デフォルト

プライマリまたはセカンダリ VMPS サーバは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

primary が入力されているかどうかに関わらず、最初に入力されたサーバは自動的にプライマリ サーバとして選択されます。最初のサーバ アドレスは、次のコマンドで **primary** を使用することにより無効にすることができます。

クラスタ コンフィギュレーションのメンバー スイッチに IP アドレスがない場合、クラスタはそのメンバー スイッチに設定された VMPS サーバを使用しません。その代わり、クラスタはコマンド スイッチの VMPS サーバを使用し、コマンド スイッチは VMPS 要求のプロキシとなります。VMPS サーバは、クラスタを単一スイッチとして扱い、コマンド スイッチの IP アドレスを使用して要求に応答します。

ipaddress を指定せずに **no** 形式を使用すると、すべての設定されたサーバが削除されます。ダイナミック アクセス ポートが存在するときにすべてのサーバを削除すると、スイッチは、VMPS に照会することができないため、これらのポートの新しい送信元からのパケットを転送することができません。

例

次の例では、IP アドレス 191.10.49.20 をプライマリ VMPS サーバとして設定する方法を示します。IP アドレス 191.10.49.21 および 191.10.49.22 のサーバは、セカンダリ サーバとして設定されます。

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

次の例では、IP アドレス 191.10.49.21 のサーバを削除する方法を示します。

```
Switch(config)# no vmps server 191.10.49.21
```

show vmps イネーブル EXEC コマンドを入力して、VMPS Domain Server 列を調べることにより、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 vmps	VQP および VMPS 情報を表示します。

vtp（グローバル コンフィギュレーション）

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）コンフィギュレーション特性を設定または変更するには、**vtp** 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。設定を削除したり、デフォルト設定に戻したりする場合は、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** | **password** | **pruning** | **version**}

構文の説明

domain *domain-name*	VTP ドメイン名をスイッチの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名は大文字と小文字を区別します。
file *filename*	VTP VLAN（仮想 LAN）設定が保存されている Cisco IOS ファイル システム ファイルを指定します。
interface *name*	この装置で更新された VTP ID を提供するインターフェイスの名前を指定します。
only	（任意）このインターフェイスの IP アドレスを VTP IP アップデータとして使用します。
mode	VTP 装置モードを client、server、または transparent と指定します。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信することができますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチでは VLAN を設定することができます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復することができます。
transparent	スイッチを VTP トランスペアレント モードにします。VTP トランスペアレント モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。 VTP モードがトランスペアレントである場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** イネーブル EXEC コマンドを入力します。

password *password*	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードは大文字と小文字を区別します。
pruning	スイッチ上で VTP プルーニングをイネーブルに設定します。
version *number*	VTP バージョンをバージョン 1 またはバージョン 2 に設定します。

デフォルト

デフォルトのファイル名は *flash:vlan.dat* **です。**

デフォルト モードはサーバ モードです。

ドメイン名またはパスワードは定義されません。

パスワードは設定されません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 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

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VTP モード、VTP ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードがトランスペアレントであり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ VTP モードがサーバ モードの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VTP および VLAN 設定は、VLAN データベース情報によって選択され、1005 を超える VLAN は、スイッチ コンフィギュレーション ファイルから設定されます。

新規データベースをロードするのに **vtp file** *filename* を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じてもスイッチは VTP アドバタイズを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信したあと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出したあと、NVRAM（不揮発性 RAM）をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、スイッチを VTP サーバ モードに戻すことができます。
- **vtp mode server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを戻さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバの設定を複製します。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたはトランスペアレント モードである場合、スイッチの設定は変更されません。
- トランスペアレント モードのスイッチは、VTP に参加しません。トランスペアレント モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードのスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチを非パスワード ステートに戻す場合は、このコマンドの **no vtp password** 形式を使用します。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ～ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2（v2）モード ステートのトグリングを行うと、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP 装置の機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するよう設定する必要があります。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。

- Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）または Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

例

次の例では、VTP コンフィギュレーション メモリのファイル名を *vtpfilename* に変更する方法を示します。

```
Switch(config)# vtp file vtpfilename
```

次の例では、装置メモリのファイル名をクリアする方法を示します。

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、この装置の VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP トランスペアレント モードにする方法を示します。

```
Switch(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Switch(config)# vtp version 2
```

設定を確認するには、**show vtp status** イネーブル 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 status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
vtp（VLAN コンフィギュレーション）	VTP のドメイン名、パスワード、プルーニング、バージョン、およびモードを設定します。

vtp（VLAN コンフィギュレーション）

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）特性を設定するには、**vtp** VLAN（仮想 LAN）コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** イネーブル EXEC コマンドを入力します。デフォルト設定に戻したり、特性をディセーブルにしたり、パスワード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。

vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}

no vtp {**client** | **password** | **pruning** | **transparent** | **v2-mode**}

構文の説明

domain *domain-name*	スイッチの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定することにより、VTP ドメイン名を設定します。ドメイン名は大文字と小文字を区別します。
password *password*	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードは大文字と小文字を区別します。
pruning	VTP 管理ドメインでプルーニングをイネーブルにします。VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
v2-mode	管理ドメインで VTP バージョン 2 をイネーブルにします。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信することができますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチで VLAN を設定することができます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復することができます。
transparent	スイッチを VTP トランスペアレント モードにします。VTP トランスペアレント モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。

デフォルト

デフォルト モードはサーバ モードです。

ドメイン名は定義されません。

パスワードは設定されません。

プルーニングはディセーブルです。

VTP バージョン 2（v2 モード）はディセーブルです。

コマンド モード　VLAN コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上の注意事項

VTP モードがトランスペアレントである場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** イネーブル EXEC コマンドを入力します。

VTP モードを設定するときには、次の注意事項に従ってください。

- スイッチを VTP サーバ モードに戻すには、このコマンドの **no vtp client** および **no vtp transparent** 形式を使用します。
- **vtp server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを戻さないことを除けば、**no vtp client** または **no vtp transparent** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバの設定を複製します。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたはトランスペアレント モードである場合、スイッチの設定は変更されません。
- トランスペアレント モードのスイッチは、VTP に参加しません。トランスペアレント モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードにあるスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 設定を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。

（注）　VTP コンフィギュレーション モードの VTP 設定は、適用されたときに VLAN データベースに保存されます。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じてもスイッチは VTP アドバタイズを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信したあと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出したあと、NVRAM（不揮発性 RAM）をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。

- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチを非パスワード ステートに戻す場合は、このコマンドの **no vtp password** 形式を使用します。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP サーバでプルーニングをイネーブルにすると、プルーニングは管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョン 2（v2 モード）をイネーブルにする場合には、次の注意事項に従ってください。

- バージョン 2（v2 モード）ステートのトグリングを行うと、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP 装置の機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するよう設定する必要があります（**no vtp v2-mode**）。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、または Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）や Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN メディア タイプを設定している場合には、VTP バージョン 2（**v2-mode**）をイネーブルにしてください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。

例

次の例では、スイッチを VTP トランスペアレント モードにする方法を示します。

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

次の例では、設定しようとしている新規 VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

次の例では、設定しようとしている新規 VLAN データベースで v2 モードをイネーブルにする方法を示します。

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

設定を確認するには、**show vtp status** イネーブル 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 status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーニング適格リストを設定します。
vtp（グローバル コンフィギュレーション）	VTP ファイル名、インターフェイス、ドメイン名、およびモードを設定します。