



Catalyst 3750 スイッチ Cisco IOS コマンド

aaa accounting dot1x

Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントティング) をイネーブルにし、特定のアカウントティング方式を回線単位またはインターフェイス単位で定義する IEEE (米国電気電子学会) 802.1x セッションの方式リストを作成するには、**aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x アカウントティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

シンタックスの説明

name	サーバグループ名。これは、 broadcast group および group キーワードのあとに入力する場合、オプションになります。
default	次に続くアカウントティング方式を、アカウントティングサービスのデフォルトのリストとして使用します。
start-stop	プロセスの開始時に開始アカウントティング通知を、プロセスの終了時に停止アカウントティング通知を送信します。開始アカウントティング記録が、バックグラウンドで送信されます。アカウントティングサーバで開始アカウントティング通知が受信されたかどうかに関わらず、要求されたユーザのプロセスが開始します。
broadcast	アカウントティング記録を複数の AAA サーバに送信できるようにし、各グループの最初のサーバにアカウントティング記録を送信します。最初のサーバが使用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。

group	アカウントリングサービスに使用され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 — すべての RADIUS ホストのリスト • tacacs+ — すべての Terminal Access Controller Access Control System Plus (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、オプションになります。オプション以外の group キーワードも入力できます。
radius	(任意) RADIUS 許可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(20)SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、RADIUS サーバへのアクセスが必要です。

インターフェイス上で IEEE 802.1x RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

例

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

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



(注)

RADIUS 認証サーバは、AAA クライアントからの更新またはウォッチドッグパケットを受け取り、ログするよう適切に設定される必要があります。

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1x を実行中のインターフェイスで使用する 1 つまたは複数の AAA 方式を指定します。
aaa new-model	AAA アクセス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	定期的な再認証をイネーブルまたはディセーブルにします。
dot1x timeout reauth-period	再認証の試行間隔 (秒) を指定します。

aaa authentication dot1x

IEEE（米国電気電子学会）802.1x に準拠するポートで使用する Authentication, Authorization, Accounting（AAA; 認証、許可、アカウントティング）方式を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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には、このコマンドの **no** 形式を使用します。

```
aaa authentication dot1x {default} method1
```

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

シンタックスの説明

default	この引数のあとに指定した認証方式を、ユーザ ログイン時のデフォルトの方式として使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、 group radius キーワードを入力します。



(注)

他のキーワードがコマンドラインのヘルプ スtring に表示されていますが、**default** および **group radius** キーワードだけがサポートされます。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

method 引数は、認証アルゴリズムがクライアントによって提供されたパスワードを確認するために試行する方式を、試行する順序で指定します。実際に IEEE 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。

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

設定された認証方式のリストを表示するには、**show running-config** 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 に準拠している認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返された場合、ユーザがネットワークへアクセスすることは許可されません。

```
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。

action

VLAN（仮想 LAN）のアクセス マップのエントリに対してアクションを設定するには、スイッチ スタックまたはスタンドアロンスイッチ上で **action** アクセスマップ コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

action {drop | forward}

no action

シンタックスの説明

drop	指定の条件に一致した場合、パケットを廃棄します。
forward	指定の条件に一致した場合、パケットを転送します。

デフォルト

デフォルトのアクションは、パケットを転送する設定です。

コマンドモード

アクセスマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

アクションに **drop** を指定した場合、**match** コマンドにおける Access Control List (ACL; アクセス制御リスト) 名の設定を含め、アクセス マップを定義してから VLAN に適用する必要があります。アクセス マップを定義しない場合、すべてのパケットは廃棄されます。

アクセスマップ コンフィギュレーション モードで、VLAN マッピングの一致条件を定義するには、**match** アクセス マップ コンフィギュレーション コマンドを使用します。パケットが条件に一致した場合に発生するアクションを設定するには、**action** コマンドを使用します。

drop および **forward** のパラメータは、このコマンドの **no** 形式では使用されません。

例

次の例では、VLAN アクセス マップ *vmap4* を識別し、VLAN 5 および VLAN 6 に適用することで、アクセス リスト *al2* に定義されたパケット一致条件と一致した場合、VLAN の IP パケットを転送させています。

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

設定を確認するには、**show vlan access-map** 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
access-list {deny permit}	標準番号付き Access Control List (ACL; アクセス制御リスト) 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	名前付きアクセス リストを作成します。構文情報については、 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands を選択してください。
mac access-list extended	名前付き MAC (メディア アクセス制御) アドレス アクセス リストを作成します。
match (アクセスマップ コンフィギュレーション)	VLAN マップの一致条件を定義します。
show vlan access-map	スイッチ上に作成されている VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

archive copy-sw

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

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

シンタックスの説明

/destination-system destination-stack- member-number	(任意) 実行イメージのコピー先のスタック メンバー番号。指定できる範囲は、1 ～ 9 です。
/force-reload	(任意) ソフトウェア イメージのダウンロードが成功したあと、無条件にシステムのリロードを強制します。
/leave-old-sw	(任意) ダウンロードが成功したあと、古いソフトウェア バージョンを保存します。
/no-set-boot	(任意) 新しいソフトウェア イメージのダウンロードが成功したあと、BOOT 環境変数の設定は新しいソフトウェア イメージを示すように変更されません。
/overwrite	(任意) ダウンロードされたソフトウェア イメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	(任意) 変更された設定が保存されていない場合を除き、イメージをダウンロードしたあとでシステムをリロードします。
/safe	(任意) 現在のソフトウェア イメージを保存します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。
source-stack-member- number	実行イメージのコピー元のスタック メンバー番号。指定できる範囲は、1 ～ 9 です。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

現行のソフトウェア イメージは、コピーされたイメージで上書きされません。

ソフトウェア イメージと HTML ファイルの両方がコピーされます。

新しいイメージは flash: ファイル システムにコピーされます。

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

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



(注)

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

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

/destination-system destination-stack-member-number のコマンド オプション繰り返すことで、イメージのコピー先に複数のスタック メンバーを指定し、各スタック メンバーをアップグレードできます。**destination-stack-member-number** を指定しない場合、デフォルト設定で、実行中のイメージ ファイルがすべてのスタック メンバーにコピーされます。

/safe または **/leave-old-sw** オプションを使用した場合に、十分なフラッシュ メモリがないと、新しいイメージのコピーに失敗する場合があります。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合にエラーが発生します。

/leave-old-sw オプションを使用したために、新しいイメージをコピーしても古いイメージ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できます。詳細は、「**delete**」(p.2-73) を参照してください。

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

/overwrite オプションなしでこのコマンドを指定する場合、新しいイメージが、スイッチ フラッシュ デバイスのイメージまたはスタック メンバーで実行中のものと同じではないことが、アルゴリズムによって確認されます。イメージが同じである場合には、コピーは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがコピーされます。

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

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

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

これらのオプションの前に **source-stack-member-number** オプションを入力する場合、**archive copy-sw source-stack-member-number** コマンドしか入力できません。

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

- 実行イメージをスタック メンバーから別のスタック メンバーにコピーして、2 つめのスタック メンバーのフラッシュ メモリのソフトウェア イメージ (すでに存在する場合) をコピーしたイメージで上書きするには、**archive copy-sw/destination destination-stack-member-number / overwrite source-stack-member-number** コマンドを入力します。

- 実行イメージをスタック メンバーから別のスタック メンバーにコピーして、現在のソフトウェア イメージを維持しながらイメージのコピー後にシステムをリロードするには、**archive copy-sw/destination destination-stack-member-number/safe/reload source-stack-member-number** コマンドを入力します。

例

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

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

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

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

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

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

関連コマンド

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

archive download-sw

新しいイメージを Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバからスイッチまたはスイッチ スタックにダウンロードして、既存のイメージを上書きまたは保存するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 | /no-version-check
|/destination-system stack-member-number |/only-system-type system-type | /overwrite | /reload |
/safe} source-url
```

シンタックスの説明

/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、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、組み込み型デバイス 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た場合にだけ削除されます。
/leave-old-sw	ダウンロードが成功したあと、古いソフトウェア バージョンを保存します。
/no-set-boot	新しいソフトウェア イメージのダウンロードが成功したあと、BOOT 環境変数の設定は新しいソフトウェア イメージを示すように変更されません。
/no-version-check	イメージ上、およびスイッチ スタック上のスタック プロトコルのバージョンの互換性を確認せずに、ソフトウェア イメージをダウンロードします。
/destination-system stack-member-number	アップグレードする特定のスタック メンバーを指定します。指定できる範囲は、1 ～ 9 です。
/only-system-type system-type	アップグレードする特定のシステム タイプを指定します。指定できる範囲は 0 ～ FFFFFFFF です。
/overwrite	ダウンロードされたソフトウェア 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	変更された設定が保存されていない場合を除き、イメージのダウンロードに成功した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までは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。

<i>source-url</i>	ローカル ファイル システムまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。 • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文 flash: スタック メンバー上のローカル フラッシュ ファイル システムの構文 flash member number: • 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 • TFTP の構文 tftp:[[/location]/directory]/image-name.tar <i>image-name.tar</i> は、スイッチにダウンロードし、インストールするソフトウェア イメージです。

デフォルト

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

ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。

新しいイメージは **flash:** ファイル システムにダウンロードされます。

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

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

イメージのスタック プロトコルの互換性は、ダウンロードする場合にスイッチ スタックのバージョンで確認されます。

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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	http および https キーワードが追加されました。

使用上のガイドライン

/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** オプションを使用した場合に、十分なフラッシュ メモリがないと、新しいイメージのダウンロードに失敗する場合があります。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合にエラーが発生します。

/leave-old-sw オプションを使用したために、新しいイメージをダウンロードしても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できます。詳細は、「**delete**」(p.2-73) を参照してください。

スイッチ スタックの既存のバージョンとは異なるスタック プロトコルのバージョンのイメージをダウンロードする場合、**/no-version-check** オプションを使用します。このオプションを使用する場合には **/destination-system** オプションを使用し、イメージでアップグレードする特定のスタック メンバーを指定してください。



(注)

/no-version-check オプションの使用には注意が必要です。同一のスイッチ スタックにするためには、スタック マスターを含め、すべてのスタック メンバーは、スタック プロトコルのバージョンを同一にする必要があります。このオプションを指定することで、イメージをダウンロードする場合のスタック プロトコルのバージョンと、スイッチ スタックのバージョンの互換性の最初の確認をスキップできます。

/destination-system のコマンドオプション繰り返すことで、複数のスタック メンバーを指定し、アップグレードできます。

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

/overwrite オプションなしでこのコマンドを指定する場合、ダウンロード アルゴリズムは、新しいイメージが、スイッチ フラッシュ デバイスのイメージ、またはスタック メンバーで実行中のものと同じではないことを確認します。イメージが同じである場合には、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** 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、スイッチ上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、ダウンロードが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
```

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

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

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の 1 つまたは複数のスタック メンバー上のフラッシュ メモリにコピーします。
archive tar	tar ファイルの作成、tar ファイル内のファイルを一覧表示、tar ファイルからのファイル抽出を行います。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。
delete	フラッシュ メモリ デバイスのファイルまたはディレクトリを削除します。

archive tar

tar ファイルの作成、tar ファイル内のファイル一覧表示、tar ファイルからのファイル抽出を実行するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**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...]}
```

シンタックスの説明

/create destination-url
flash:/file-url

ローカル ファイル システムまたはネットワーク ファイル システムに新しい tar ファイルを作成します。

destination-url には、ローカル ファイル システムまたはネットワーク ファイル システムの宛先 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（ファイル転送プロトコル）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
rnp:[[/username@location]/directory]/tar-filename.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]/tar-filename.tar

tar-filename.tar は、作成する tar ファイルです。

flash:/file-url には、新しい tar ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。

送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

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

デフォルト 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
イメージ名では、大文字と小文字が区別されます。

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 にある 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 *c3750-ipservices-tar.12-25.SEB* ファイルの内容を表示する方法を示します。tar ファイルの内容は画面に表示されます。

```
Switch# archive tar/table flash:c3750-ipservices-12-25.SEB.tar
info (219 bytes)

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

次の例では、*c3750-ipservices-12-25.SEB/html* のディレクトリとその内容のみを表示する方法を示します。

```
Switch# archive tar/table flash:c3750-ipservices-12-25.SEB.tar
c3750-ipservices-12-25/html
c3750-ipservices-mz.12-25.SEB/html/ (directory)
c3750-ipservices-mz.12-25.SEB/html/const.htm (556 bytes)
c3750-ipservices-mz.12-25.SEB/html/xhome.htm (9373 bytes)
c3750-ipservices-mz.12-25.SEB/html/menu.css (1654 bytes)
(テキスト出力は省略)
```

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

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

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の1つまたは複数のスタック メンバー上のフラッシュ メモリにコピーします。
archive download-sw	新しいイメージを 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、スイッチ スタックまたはスタンドアロン スイッチ上で **archive upload-sw** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明

/source-system-num <i>stack member number</i>	アップロードするイメージを持った特定のスタック メンバーを指定します。
/version <i>version_string</i>	(任意) アップロードするイメージの特定のバージョンを、文字列で指定します。
<i>destination-url</i>	ローカル ファイル システムまたはネットワーク ファイル システムの宛先 URL エイリアス。次のオプションがサポートされています。 - スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文 flash: スタック メンバー上のローカル フラッシュ ファイル システムの構文 flash member number: - 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 rnp:[[/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 <i>image-name.tar</i> 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 システムから現在の実行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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

アップロード機能を利用できるのは、組み込み型デバイス マネージャに関連する HTML ファイルが既存イメージでインストールされている場合に限られます。

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

イメージ名では、大文字と小文字が区別されます。

例

次の例では、スタック メンバー 6 で現在実行中のイメージを、172.20.140.2 の TFTP サーバへアップロードする方法を示します。

```
Switch# archive upload-sw/source-system-num 6 tftp://172.20.140.2/test-image.tar
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバーのフラッシュ メモリから実行イメージを、別の 1 つまたは複数のスタック メンバー上のフラッシュ メモリにコピーします。
archive download-sw	新しいイメージをスイッチにダウンロードします。
archive tar	tar ファイルの作成、tar ファイル内のファイルを一覧表示、tar ファイルからのファイル抽出を行います。

arp access-list

Address Resolution Protocol (ARP; アドレス解決プロトコル) Access Control List (ACL; アクセス制御リスト) を定義する、または以前定義したリストの最後にコマンドを追加するには、スイッチ スタックまたはスタンドアロンスイッチ上で **arp access-list** グローバル コンフィギュレーション コマンドを使用します。指定の ARP アクセス リストを削除する場合は、このコマンドの **no** 形式を使用します。

arp access-list *acl-name*

no arp access-list *acl-name*

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

<i>acl-name</i>	ACL 名

デフォルト

ARP アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

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

- **default** : コマンドをデフォルト設定に戻します。
- **deny** : 拒否するパケットを指定します。詳細は、「[deny \(ARP アクセスリスト コンフィギュレーション\)](#)」(p.2-74) を参照してください。
- **exit** : ARP アクセスリスト コンフィギュレーション モードを終了します。
- **no** : コマンドを無効にする、またはデフォルト設定に戻します。
- **permit** : 転送するパケットを指定します。詳細は、「[permit \(ARP アクセスリスト コンフィギュレーション\)](#)」(p.2-271) を参照してください。

指定された一致条件に基づいた ARP パケットを転送および廃棄するには、**permit** および **deny** アクセスリスト コンフィギュレーション コマンドを使用します。

ARP ACL が定義されている場合、これを VLAN (仮想 LAN) に適用するには、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用します。IP から MAC (メディア アクセス制御) へのアドレス バインディングだけを含む ARP パケットは、ACL と照合されます。その他のすべてのタイプのパケットは、検証されずに入力 VLAN にブリッジされます。ACL がパケットを許可すると、スイッチがこれを転送します。明示的な拒否ステートメントにより ACL がパケットを拒否した場合、スイッチはこのパケットを廃棄します。暗黙的な拒否ステートメントにより ACL がパケットを拒否した場合、スイッチはパケットを Dynamic Host Configuration Protocol (DHCP) バインディングのリストと照合します (ACL がスタティック でない場合のみ。スタティックの場合は、パケットはバインディングと照合されません)。

例

次の例では、ARP アクセス リストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd: を使用して、ホストからの ARP 要求および ARP 応答の両方を許可する方法を示します。

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

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

auto qos voip

Quality of Service (QoS; サービス品質) ドメイン内の Voice over IP (VoIP) に対し、QoS を自動的に設定するには、スイッチスタックまたはスタンドアロンスイッチ上で **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]
```

シンタックスの説明

cisco-phone	このポートが Cisco IP Phone に接続されていると識別し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルを信頼できるのは、IP Phone が検知される場合に限りです。このキーワードは、10 ギガビットイーサネット インターフェイスではサポートされません。
cisco-softphone	このポートが Cisco SoftPhone を実行している装置に接続されていると識別し、自動的に VoIP の QoS を設定します。このキーワードは、10 ギガビットイーサネット インターフェイスではサポートされません。
trust	このポートが信頼性のあるスイッチまたはルータに接続されていると識別し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルは信頼できます。ルーティングされないポートの場合、着信パケットの Class of Service (CoS; サービス クラス) 値が信頼できます。ルーテッドポートの場合、着信パケットの DSCP 値が信頼できます。

デフォルト

Auto-QoS は、ポート上でディセーブルに設定されています。

Auto-QoS がイネーブルの場合、Auto-QoS は入力パケット ラベルを使用して、表 2-1 に示すようなトラフィックの分類、パケット ラベルの割り当て、および入力キューと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 制御 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、入力キューに対して生成された Auto-QoS の設定を示します。

表 2-2 入力キューに対する Auto-QoS の設定

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

1. SRR = Shaped Round Robin (シェイプドラウンドロビン)。入力キューは共有モードのみサポートします。

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

表 2-3 出力キューに対する Auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト (帯域幅)	ギガビット対応ポートのキュー (バッファ) サイズ	10/100 イーサネットポートのキュー (バッファ) サイズ
プライオリティ (シェーピング)	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
12.1(14)EA1	このコマンドが導入されました。
12.2(20)SE	cisco-softphone キーワードが追加され、生成された Auto-Qos コンフィギュレーションが変更されました。

使用上のガイドライン

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

Cisco IOS Release 12.2(20)SE より前のリリースでは、Auto-Qos はスイッチ ポート上で Cisco IP Phone を使用した VoIP に対してのみスイッチを設定します。

Cisco IOS Release 12.2(20)SE 以降では、Auto-QoS はスイッチおよびルーテッド ポート上で Cisco IP Phone を使用した VoIP、および Cisco SoftPhone アプリケーションが稼働する装置を使用した VoIP に対してスイッチを設定します。これらのリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートしています。接続された装置は、Cisco Call Manager Version 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場合、他の QoS コマンドを設定する前に、Auto-QoS をイネーブルに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 設定の調整ができます。



(注)

スイッチは Auto-QoS で生成されたコマンドを、CLI (コマンドライン インターフェイス) から入力されたコマンドのように適用します。既存のユーザ設定は、生成されたコマンドの適用を妨げる可能性、または生成されたコマンドによって上書きされる可能性があります (これらは警告なしで発生します)。生成されたコマンドが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が、実行コンフィギュレーションに残っています。上書きされてしまったユーザ入力の設定は、現行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ことによって、復旧できます。生成されたコマンドの適用に失敗した場合、以前の実行コンフィギュレーションが復元されます。

最初に Auto-QoS をイネーブルにしたポートでは、Auto-QoS が生成するグローバル コンフィギュレーション コマンドが実行され、その後インターフェイス コンフィギュレーション コマンドが実行されます。他のポート上で Auto-QoS をイネーブルにした場合、Auto-QoS が生成するインターフェイス コンフィギュレーション コマンドは、そのポート用に実行されます。

最初のポート上で Auto-QoS 機能をイネーブルにした場合、次のアクションが自動的に起こります。

- QoS がグローバルにイネーブルになり (**mls qos** グローバル コンフィギュレーション コマンド)、その後、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のエッジにあるポート上で、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは信頼境界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、Cisco IP Phone の有無を検出します。Cisco IP Phone が検出された場合、ポート上の入力分類は、パケットで受信された QoS 値を信頼するよう設定されます。Cisco IP Phone が検出されない場合、入力分類はパケットで受信された QoS 値を信頼しないよう設定されます。スイッチは、表 2-2 および表 2-3 の設定に対応して、ポート上の入力キューおよび出力キューを構成します。
- Cisco SoftPhone が稼働する装置に接続されたネットワークのエッジにあるポートで、**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適合か不適合かを判断し、パケット上のアクションを指定します。パケットの DSCP 値が 24、26、または 46 であるか、またはパケットが不適合の場合、スイッチは DSCP 値を 0 に変更します。スイッチは、表 2-2 および表 2-3 の設定に対応して、ポート上の入力キューおよび出力キューを設定します。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットで非ルーテッドポートの CoS 値、またはルーテッドポートの DSCP 値を信頼します (トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります)。スイッチは、表 2-2 および表 2-3 の設定に対応して、ポート上の入力キューおよび出力キューを設定します。

スタティック ポート、ダイナミックアクセス ポート、音声 VLAN (仮想 LAN) アクセス ポート、およびトランク ポートで Auto-QoS をイネーブルにできます。Cisco IP Phone が稼働するルーテッドポートで Auto-QoS をイネーブルにする場合、スタティック IP アドレスを IP Phone に割り当てる必要があります。



(注)

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

Auto-QoS をイネーブルにした場合、その名前に *AutoQoS* を含むポリシー マップまたはアグリゲート ポリシーを変更しないでください。ポリシー マップまたはアグリゲート ポリシーを変更する必要がある場合は、まずコピーをとってから、コピーされたポリシー マップまたはポリシーを変更してください。生成されたポリシー マップではなく、新しいポリシー マップを使用するには、インターフェイスから生成されたものを削除し、新しいポリシー マップを適用します。

Auto-QoS がイネーブルの場合、自動生成された QoS 設定を表示させるには、Auto-QoS をイネーブルにする前にデバッグをイネーブルにします。debug auto qos イネーブル EXEC コマンドを使用することで、Auto-QoS のデバッグをイネーブルにできます。詳細は、debug auto qos コマンドを参照してください。

ポート上で 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。このポート用に生成された Auto-QoS インターフェイス コンフィギュレーション コマンドのみ削除されます。Auto-QoS がイネーブルである最後のポートで no auto qos voip コマンドを入力した場合、Auto-QoS 生成のグローバル コンフィギュレーション コマンドが残っていたとしても、Auto-QoS はディセーブルになったと認識されます（グローバル コンフィギュレーションから影響を受ける他のポートのトラフィック障害を回避するため）。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 生成のグローバル コンフィギュレーション コマンドをディセーブルにします。QoS がディセーブルの場合、パケットが修正されなくなるため（パケットの CoS、DSCP、IP precedence の値は変更されない）、ポートの信頼性に関する概念はなくなります。トラフィックは Pass-Through モードに切り替わります（パケットは書き換えなしにスイッチングされ、ポリシングなしのベストエフォートに分類されます）。

例

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

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip trust
```

設定を確認するには、show auto qos interface interface-id 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
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、あるいはポート上のすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos map {cos-dscp dscp1 ... dscp8 dscp-cos dscp-list to cos}	CoS から DSCP へのマッピングまたは DSCP から CoS へのマッピングを定義します。
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR; シェイブド ラウンド ロビン) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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、または 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。

コマンド	説明
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよび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 値を出力キューにマッピング、または 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 trust	ポートの信頼状態を設定します。
queue-set	キューセットに対し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	シェーピングしたウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有のウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

boot auto-copy-sw

自動アップグレードプロセスをイネーブルにするには、スタック マスターから **boot auto-copy-sw** グローバル コンフィギュレーション コマンドを使用します。このコマンドにより、Version-Mismatch (VM) モードのスイッチは、スタック メンバー上で実行中のソフトウェア イメージ、またはスイッチ スタックのフラッシュ メモリの tar ファイル イメージをコピーして、自動的にアップグレードします。自動アップグレードプロセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

boot auto-copy-sw

no boot auto-copy-sw

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト イネーブル

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン VM モードにあるスイッチは、スイッチ スタックとは異なるマイナー バージョン番号が適用されています。VM モードのスイッチは、完全に機能しているメンバーとしてはスイッチ スタックに加入できません。スイッチ スタックが VM モードのスイッチにコピーできるイメージを保有している場合、自動アップグレードプロセスを使用することで、スタック メンバーからのイメージを VM モードのスイッチに自動的にコピーできます。その場合、スイッチは VM モードを終了し、再起動後にスイッチ スタックに完全に機能しているメンバーとして加入します。

自動アップグレード プロセスは、VM モードのスイッチにのみ影響します。既存のスタック メンバーには影響しません。

関連コマンド	コマンド	説明
	show boot	ブート環境変数の設定を表示します。
	show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

boot boothlpr

特別な Cisco IOS イメージをロードするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。特別な Cisco IOS イメージがメモリにロードされると、2 つめの Cisco IOS イメージをメモリにロードして、それを起動できます。この変数を使用するのは、内部開発およびテストの場合だけです。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
```

シンタックスの説明	<i>filesystem:</i>	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。
	<i>/file-url</i>	ブート可能ヘルパー イメージのパス（ディレクトリ） および名前

デフォルト ヘルパー イメージはロードされていません。

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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、BOOTHLP 環境変数の設定を変更します。詳細は、[付録 A「Catalyst 3750 スイッチ ブート ロード 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、スタンドアロン スイッチ上で **boot config-file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot config-file flash:/file-url

no boot config-file

シンタックスの説明

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

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからのみ正常に動作します。

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細は、[付録 A 「Catalyst 3750 スイッチ ブート ローダ 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、スタンドアロン スイッチ上で **boot enable-break** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot enable-break

no boot enable-break

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル。コンソール上で Break キーを押しても自動ブート プロセスを中断できません。

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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン このコマンドは、スタンドアロン スイッチからのみ正常に動作します。

このコマンドを入力すると、フラッシュ ファイル システムが初期化されたあとで Break キーを押すことにより、自動ブート プロセスを中断できます。



(注) このコマンドの設定に関わりなく、スイッチ前面パネルの MODE ボタンを押せば、いつでも自動ブート プロセスを中断できます。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。詳細は、[付録 A 「Catalyst 3750 スイッチ ブート ロード 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 ロード初期化中にダイナミックにファイルをロードして、ブート ロードの機能を拡張するかまたは機能にパッチを当てるには、スイッチ スタックまたはスタンドアロン スイッチ上で **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
```

シンタックスの説明

<i>filesystem:</i>	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。
<i>/file-url</i>	ロード初期化中にダイナミック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。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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

この変数を使用するのは、内部開発およびテストの場合だけです。

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、HELPER 環境変数の設定を変更します。詳細は、[付録 A「Catalyst 3750 スイッチ ブート ロード 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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には、このコマンドの **no** 形式を使用します。

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

no boot helper-config file

シンタックスの説明	<i>filesystem:</i>	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。
	<i>/file-url</i>	ロードするパス (ディレクトリ) およびヘルパー コンフィギュレーション ファイル

デフォルト ヘルパー コンフィギュレーション ファイルは指定されません。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン この変数を使用するのは、内部開発およびテストの場合だけです。

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、HELPER_CONFIG_FILE 環境変数の設定を変更します。詳細は、[付録 A 「Catalyst 3750 スイッチ ブート ロード 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

次回ブート サイクル中にスイッチの手動起動をイネーブルにするには、スタンドアロン スイッチ上で **boot manual** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot manual

no boot manual

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 手動による起動はディセーブルです。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン このコマンドは、スタンドアロン スイッチからのみ正常に動作します。

次にシステムを再起動すると、スイッチはブート ロード モードで起動します。これは *switch:* プロンプトに表示されます。システムを起動する場合は、**boot** ブート ロード コマンドを使用してブート可能イメージの名前を指定します。

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。詳細は、[付録 A「Catalyst 3750 スイッチ ブート ロード 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、スタンドアロン スイッチ上で **boot private-config-file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot private-config-file *filename*

no boot private-config-file

シンタックスの説明	<i>filename</i>	プライベート コンフィギュレーション ファイルの名前
デフォルト	デフォルトのコンフィギュレーション ファイルは、 <i>private-config</i> です。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。
使用上のガイドライン	このコマンドは、スタンドアロン スイッチからのみ正常に動作します。 ファイル名では、大文字と小文字が区別されます。	
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 <i>pconfig</i> 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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* ...| **switch** {*number* | **all**}}

no boot system

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

シンタックスの説明

<i>filesystem</i> :	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。
<i>file-url</i>	ブート可能イメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。
switch	Cisco IOS イメージがロードされるスイッチを指定します。
<i>number</i>	スタック メンバーを指定します。
all	すべてのスタック メンバーを指定します。

デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムを起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SEA	switch { <i>number</i> all } キーワードが追加されました。 boot system コマンドは現在、スイッチ スタックおよびスタンドアロン スイッチ上で正常に動作します。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

スタック マスター上で **boot system filesystem:/file-url** コマンドを入力した場合、次のブート サイクル中に指定のソフトウェア イメージがスタック マスター上でのみロードされます。

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

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

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

archive download-sw 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 3750 スイッチ ブート ロード 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

EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたりするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 モード:

```
channel-group channel-group-number mode {{auto [non-silent]} | {desirable [non-silent]}}
```

LACP モード:

```
channel-group channel-group-number mode {active | passive}
```

On モード:

```
channel-group channel-group-number mode on
```

シンタックスの説明

channel-group-number	チャネル グループ番号を指定します。指定できる範囲は 1 ～ 48 です。
mode	EtherChannel モードを指定します。
active	無条件で 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) 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 グループだけで形成されます。auto がイネーブルの場合、サイレント動作がデフォルトになります。
desirable	PAgP を無条件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、サイレント動作がデフォルトになります。
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、接続された両方のポート グループが on モードである場合のみ、EtherChannel が使用可能になります。
passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。 passive モードは、ポートをネゴシエーション ステートにします。この場合、ポートは受信する 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 グループだけで形成されます。

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

使用上のガイドライン

レイヤ 2 の 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、**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する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。論理ポートが作成されていない状態でチャネル グループが最初の物理ポートを取得すると、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。ポート チャネル インターフェイスを最初に作成した場合、*channel-group-number* と *port-channel-number* を同一にするか、または新しい番号を使用できます。新しい番号を使用した場合、**channel-group** コマンドはダイナミックに新しいポート チャネルを作成します。

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

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用することで、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポートチャネルの論理インターフェイスを手動で設定してください。

EtherChannel を設定したあと、ポートチャネル インターフェイス上で変更された設定は、ポート チャネル インターフェイスが割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートのみに有効です。EtherChannel のすべてのポートのパラメータを変更する場合、ポートチャネル インターフェイスにコンフィギュレーション コマンドを適用します（スパニングツリーのコマンド、またはトランクとしてレイヤ 2 の EtherChannel を設定するコマンドなど）。

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、物理インターフェイス ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネル グループにポートを付与したり、伝送用ポートを使用できます。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、EtherChannel が存在するのは、**on** モードのポート グループが、同じく **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 モードを使用する際は、注意が必要です。これは手動設定で、EtherChannel の両端のポートは同じ設定にする必要があります。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のループが発生することがあります。

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

PAgP および LACP モードの両方で EtherChannel を設定することは避けてください。PAgP および LACP を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック設定ではできません）。個々の EtherChannel グループは PAgP または LACP のどちらかを実行できますが、相互運用はできません。

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する場合、設定が **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

IEEE（米国電気電子学会）802.1x のポートとしてアクティブまたはまだアクティブになっていない EtherChannel のメンバー ポートを設定することは避けてください。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。

**(注)**

Cisco IOS Release 12.2(18)SE より前のソフトウェア リリースの場合、まだアクティブになっていない EtherChannel 上のポートで 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。

EtherChannel のポートとしてセキュア ポートを設定、またはセキュア ポートとして EtherChannel ポートを設定することは避けてください。

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

**注意**

物理 EtherChannel ポート上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジ グループを割り当てることは、ループ発生の原因になるため、行わないようにしてください。

例

次の例では、スタック内の単一のスイッチ上で、EtherChannel を設定する方法を示します。VLAN（仮想 LAN）10 内の 2 つのスタティックアクセス ポートを、PAgP モードが **desirable** のチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

次の例では、スタック内の単一のスイッチ上で、EtherChannel を設定する方法を示します。VLAN 10 内の 2 つのスタティックアクセス ポートを、LACP モードが **active** のチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN10 内のスタティックアクセス ポートとしてスタック メンバー 2 のポートを 2 つ、スタック メンバー 3 のポートを 1 つチャネル 5 に割り当てます。

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

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

関連コマンド

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

channel-protocol

チャネリングを管理するために、ポート上で使用されるプロトコルを制限するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

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

デフォルト

EtherChannel に割り当てられているプロトコルはありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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

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

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

PAgP と LACP には互換性がないため、チャネルの両端は同じプロトコルを使用する必要があります。

例

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

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

設定を確認するには、**show etherchannel [channel-group-number] protocol** 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-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

指定のクラス マップ名のトラフィックを分類する一致条件を（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用して）定義するには、スイッチ スタックまたはスタンドアロン スイッチ上で **class** ポリシーマップ コンフィギュレーション コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

class *class-map-name*

no class *class-map-name*

シンタックスの説明

<i>class-map-name</i>	クラス マップ名

デフォルト

ポリシー マップ クラスマップは定義されていません。

コマンド モード

ポリシーマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用する前に、**policy-map** グローバル コンフィギュレーション コマンドを使用することでポリシー マップを識別してから、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。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 マップをポートに適用します。

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 モードが開始され、次の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** : 分類されたトラフィックにポリサーまたはアグリゲート 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** : 分類され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** または **class-map** コマンドで分類されたトラフィックに、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。他のポートと共有され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適用された場合、*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 に設定してから、平均レート 1 Mbps（メガビット/秒）でトラフィックをポリシングして 20 KB でバーストします。プロファイルを超過したトラフィックは、ポリシングされた DSCP マップから取得した DSCP 値にマーク ダウンされ、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を照合する場合に使用されるクラス マップを作成します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー 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 コマンドで分類されたトラフィックに、信頼状態を定義します。

class-map

パケットと名前を指定したクラスとの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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*

シンタックスの説明

match-all	(任意) このクラス マップ内のすべての一致ステートメントの論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
match-any	(任意) このクラス マップ内の一致ステートメントの論理和をとります。複数の条件が一致する必要があります。
<i>class-map-name</i>	クラス マップ名

デフォルト

クラス マップは定義されていません。

match-all または **match-any** キーワードがどちらとも指定されない場合、デフォルトは **match-all** 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

クラスマップ一致条件の作成または変更を希望するクラスの名前を指定し、クラスマップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。

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、および集約の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できます。

- **description** : クラス マップを記述します (最大 200 文字)。**show class-map** イネーブル EXEC コマンドは、クラスマップの記述およびクラスマップ名を表示します。
- **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** : 現行のクラス マップ名を変更します。すでに使用されている名前にクラス マップ名を変更すると、A class-map with this name already exists メッセージが表示されます。

物理ポート ベースでパケットの分類を定義するために、クラス マップごとに **match** コマンドがサポートされています。この場合、**match-all** および **match-any** キーワードは同等です。

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、103 というアクセスリストである 1 つの一致条件を使い、*class1* と呼ばれるクラス マップ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 マップの *class1* を削除する方法を示します。

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

設定を確認するには、**show class-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で、トラフィックの分類一致条件を定義します (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)。
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 arp inspection log

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査のロギング バッファをクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear ip arp inspection log** イネーブル EXEC コマンドを使用します。

clear ip arp inspection log

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

例

次の例では、ロギング バッファの内容をクリアする方法を示します。

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

ログがクリアされたことを確認するには、**show ip arp inspection log** 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
arp access-list	ARP ACL を定義します。
ip arp inspection log-buffer	ダイナミック ARP 検査のロギング バッファを設定します。
ip arp inspection vlan logging	VLAN (仮想 LAN) 単位で記録されたパケット タイプを制御します。
show inventory log	ダイナミック ARP 検査のロギング バッファの設定および内容を表示します。

clear ip arp inspection statistics

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査の統計情報をクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear ip arp inspection statistics** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明	vlan <i>vlan-range</i> (任意) 指定された VLAN (仮想 LAN) またはすべての VLAN の統計情報をクリアします。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。

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(20)SE	このコマンドが導入されました。

例

次の例では、VLAN 1 の統計情報をクリアする方法を示します。

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

統計情報が削除されたことを確認するには、**show ip arp inspection statistics vlan 1** イネーブル EXEC コマンドを入力します。

関連コマンド	<table><tr><th>コマンド</th><th>説明</th></tr><tr><td>show inventory statistics</td><td>すべての VLAN または指定された VLAN の転送、廃棄、MAC (メディア アクセス制御) 検証の障害、および IP 検証の障害のパケットに関する統計情報を表示します。</td></tr></table>	コマンド	説明	show inventory statistics	すべての VLAN または指定された VLAN の転送、廃棄、MAC (メディア アクセス制御) 検証の障害、および IP 検証の障害のパケットに関する統計情報を表示します。
コマンド	説明				
show inventory statistics	すべての VLAN または指定された VLAN の転送、廃棄、MAC (メディア アクセス制御) 検証の障害、および IP 検証の障害のパケットに関する統計情報を表示します。				

clear ip dhcp snooping database

Dynamic Host Configuration Protocol (DHCP) バインディング データベース エージェントの統計情報をクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear ip 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

このコマンドは、スイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明	statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。

デフォルト	デフォルトは定義されていません。

コマンド モード	イネーブル EXEC

コマンド履歴	リリース	変更内容
	12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン	clear ip dhcp snooping database statistics コマンドを入力すると、スイッチは、統計情報がクリアされてから、バインディング データベースおよびバインディング ファイルのエントリを更新します。

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

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

統計情報がクリアされたことを確認するには、**show ip dhcp snooping database** 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
	ip dhcp snooping	VLAN (仮想 LAN) 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 ipc

Interprocess Communication (IPC; プロセス間通信) プロトコルの統計情報をクリアするには、スイッチスタックまたはスタンドアロンスイッチ上で **clear ipc** イネーブル EXEC コマンドを使用します。

clear ipc {queue-statistics | statistics}

シンタックスの説明

queue-statistics	IPC キュー統計情報をクリアします。
statistics	IPC 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(18)SE	このコマンドが導入されました。

使用上のガイドライン

すべての統計情報をクリアするには、**clear ipc statistics** コマンドを使用します。キュー統計情報のみをクリアするには、**clear ipc queue-statistics** コマンドを使用します。

例

次の例では、すべての統計情報をクリアする方法を示します。

```
Switch# clear ipc statistics
```

次の例では、キュー統計情報のみをクリアする方法を示します。

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

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

clear l2protocol-tunnel counters

プロトコル トンネル ポートのプロトコル カウンタをクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear l2protocol-tunnel counters** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明

<i>interface-id</i>	(任意) プロトコル カウンタがクリアされるインターフェイス (物理インターフェイスまたはポート チャネル) を指定します。

デフォルト

デフォルトは定義されていません。

コマンドモード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが導入されました。

使用上のガイドライン

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

例

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

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

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングに設定されたポートの情報を表示します。

clear lacp

Link Aggregation Control Protocol (LACP) チャネルグループのカウンタをクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear lacp** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	<i>channel-group-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

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

例

次の例では、すべてのチャネルグループ情報をクリアする方法を示します。

```
Switch# clear lacp counters
```

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

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

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

clear mac address-table

指定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバー上のすべてのダイナミック アドレス、または特定の VLAN（仮想 LAN）上のすべてのダイナミック アドレスを MAC（メディア アクセス制御）アドレス テーブルから削除するには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear 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}
```

シンタックスの説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
dynamic address <i>mac-addr</i>	(任意) 指定されたダイナミック MAC アドレスを削除します。
dynamic interface <i>interface-id</i>	(任意) 指定された物理ポートまたはポート チャネル上のすべてのダイナミック MAC アドレスを削除します。
dynamic vlan <i>vlan-id</i>	(任意) 指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4094 です。
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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	clear mac-address-table コマンド(ハイフンあり)は、 clear mac address-table (ハイフンなし) に変更されました。

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
```

情報が削除されたかどうかを確認するには、**show mac address-table** 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
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上の SNMP（簡易ネットワーク管理プロトコル）MAC アドレス通知トラップをイネーブルにします。

clear mac address-table move update

MAC（メディア アクセス制御）アドレス テーブルの移行更新関連カウンタをクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear 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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンド モード イネーブル EXEC

コマンド履歴	リリース	変更内容
	12.2(25)SED	このコマンドが導入されました。

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

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

情報がクリアされたかどうかを確認するには、**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
	mac address-table move update {receive transmit}	スイッチ上で MAC アドレス テーブル移行更新を設定します。
	show mac address-table move update	スイッチの MAC アドレス テーブル移行更新情報を表示します。

clear pagp

Port Aggregation Protocol (PAgP) チャネルグループの情報をクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear pagp** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	<i>channel-group-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

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

例

次の例では、すべてのチャネルグループ情報をクリアする方法を示します。

```
Switch# clear pagp counters
```

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

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

情報が削除されたかどうかを確認するには、**show pagp** 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 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 テーブルからすべてのセキュア アドレスを削除する、またはスイッチ、インターフェイス上の特定タイプ（設定済み、ダイナミック、スティッキー）のすべてのセキュア アドレスを削除するには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear 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}}]]
```

シンタックスの説明

all	すべてのセキュア MAC アドレスを削除します。
configured	設定済みのセキュア MAC アドレスを削除します。
dynamic	ハードウェアで自動学習されたセキュア MAC アドレスを削除します。
sticky	自動学習されたセキュア MAC アドレスまたは設定済みのセキュア MAC アドレスのいずれかを削除します。
address mac-addr	(任意) 指定のダイナミック セキュア MAC アドレスを削除します。
interface interface-id	(任意) 指定の物理ポートまたは 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) 指定した VLAN から指定したセキュア MAC アドレスを削除します。vlan キーワードを入力したあとで、次のいずれかのオプションを入力します。 vlan-id — トランク ポート上で、アドレスを削除する VLAN の VLAN ID を指定します。 access — アクセス ポート上で、アクセス VLAN 上の指定したセキュア MAC アドレスを削除します。 voice — アクセス ポート上で、音声 VLAN 上の指定したセキュア MAC アドレスを削除します。
 (注) voice キーワードは、ポート上で音声 VLAN が設定されており、そのポートがアクセス VLAN ではない場合にだけ指定できます。	

デフォルト

デフォルトは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

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

例 次の例では、MAC アドレス テーブルからすべてのセキュア アドレスをクリア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上で学習されたすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic interface gigabitethernet1/0/1
```

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

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

情報が削除されたかどうかを確認するには、**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
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 <i>mac-address</i>	セキュア MAC アドレスを設定します。
switchport port-security maximum <i>value</i>	セキュア インターフェイス上のセキュア 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、スイッチ スタックまたはスタンドアロン スイッチ上で **clear 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*]

シンタックスの説明	interface interface-id (任意) 指定のインターフェイス上にあるすべてのスパニングツリーのカウンタをクリアします。有効なインターフェイスは、物理ポート、VLAN (仮想 LAN)、およびポート チャネルです。VLAN の使用範囲は 1 ～ 4094 です。ポートチャネルの使用範囲は 1 ～ 48 です。	
デフォルト	デフォルトは定義されていません。	
コマンド モード	イネーブル EXEC	
コマンド履歴	リリース	変更内容
	12.1(14)EA1	このコマンドが導入されました。
使用上のガイドライン	<i>interface-id</i> が指定されていない場合、すべてのインターフェイス上にあるスパニングツリーの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上でスパニングツリーのカウンタをクリアする方法を示します。 Switch# clear spanning-tree counters	
関連コマンド	コマンド	説明
	show spanning-tree	スパニングツリー ステート情報を表示します。

clear spanning-tree detected-protocols

すべてのインターフェイス、または指定されたインターフェイスでプロトコル移行プロセスを再開する（強制的に近接スイッチと再度ネゴシエートさせる）には、スイッチ スタックまたはスタンドアロン スイッチ上で **clear 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*]

シンタックスの説明

interface interface-id (任意) 指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスは、物理ポート、VLAN (仮想 LAN)、およびポート チャネルです。VLAN の使用範囲は 1 ～ 4094 です。ポートチャネルの使用範囲は 1 ～ 48 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus (Rapid-PVST+) プロトコル、または Multiple Spanning-Tree Protocol (MSTP) が動作するスイッチは、組み込みのプロトコル移行機能をサポートしており、IEEE (米国電気電子学会) 802.1D のレガシー スイッチと相互運用させることができます。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、そのポート上で 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) を受信したときに、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 Rapid-PVST または MSTP モードに戻りません。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判断できないためです。この場合、**clear spanning-tree detected-protocols** コマンドを使用します。

例

次の例では、特定のポートでプロトコル移行プロセスを再開する方法を示します。

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

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステート情報を表示します。
spanning-tree link-type	デフォルト リンクタイプの設定を上書きし、RST からフォワーディング ステートに変更する機能をイネーブルにします。

clear vmps statistics

VLAN（仮想 LAN）Query Protocol（VQP）クライアントが保持する統計情報をクリアするには、スイッチ スタックまたはスタンドアロン スイッチ上で **clear vmps statistics** イネーブル EXEC コマンドを使用します。

clear vmps statistics

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンド モード イネーブル EXEC

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

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
```

情報が削除されたかどうかを確認するには、**show vmps statistics** 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 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（仮想 LAN）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、スイッチ スタックまたはスタンドアロン スイッチ上で **clear vtp counters** イネーブル EXEC コマンドを使用します。

clear vtp counters

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンド モード イネーブル EXEC

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

例 次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

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

cluster commander-address

このコマンドは、スイッチ スタックまたはスタンドアロン クラスタ メンバー スイッチから入力する必要はありません。クラスタ コマンド スイッチは、スイッチがクラスタに加入した場合、MAC (メディア アクセス制御) アドレスをクラスタ メンバーのスイッチに自動的に提供します。クラスタ メンバー スイッチは、この情報および他のクラスタ情報をその実行コンフィギュレーション ファイルに追加します。デバッグまたはリカバリ手順の間だけスイッチをクラスタから削除する場合は、クラスタ メンバー スイッチ コンソール ポートから、このグローバル コンフィギュレーション コマンドの **no** 形式を使用します。

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

no cluster commander-address

シンタックスの説明

<i>mac-address</i>	クラスタ コマンド スイッチの MAC アドレス
member number	(任意) 設定されたクラスタ メンバー スイッチの番号指定できる範囲は、0 ～ 15 です。
name name	(任意) 設定されたクラスタの名前 (最大 31 文字)

デフォルト

このスイッチはどのクラスタのメンバーでもありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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。

あるクラスタ メンバー スイッチで **no** 形式を入力すれば、デバッグまたはリカバリ手順の間そのメンバー スイッチをクラスタから削除できます。通常は、メンバーがクラスタ コマンド スイッチと通信ができなくなった場合にのみ、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。通常のスイッチ設定では、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** 行をコンフィギュレーションから削除します。

例

次の例では、実行しているクラスタ メンバーの設定から、その出力の一部を示します。

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

(テキスト出力は省略)

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

(テキスト出力は省略)

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

```
Switch # configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# no cluster commander-address
```

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

cluster discovery hop-count

候補スイッチの拡張検出用にホップカウントの制限を設定するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster discovery hop-count** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cluster discovery hop-count *number*

no cluster discovery hop-count

シンタックスの説明

<i>number</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

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 スイッチから実行されます。

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

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

cluster enable

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

シンタックスの説明

<i>name</i>	クラスタ名（最大 31 文字）。指定できる文字は、英数字、ダッシュ、および下線のみです。
<i>command-switch-member-number</i>	(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ていません。

スイッチがクラスタ コマンド スイッチである場合、メンバー番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、どのクラスタにも属していない任意のコマンド対応スイッチ上で入力します。装置がすでにクラスタのメンバーとして設定されている場合、コマンドはエラーとなります。

クラスタ コマンド スイッチをイネーブルにする場合は、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、このコマンドでクラスタ名が変更されます。

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

cluster holdtime

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

cluster holdtime *holdtime-in-secs*

no cluster holdtime

シンタックスの説明

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

デフォルト

デフォルトのホールド時間は 80 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

クラスタ コマンド スイッチ上でのみ、このコマンドと **cluster timer** グローバル コンフィギュレーション コマンドを入力してください。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、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 メンバーに伝播します。

ホールド時間は、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、ホールド時間をインターバルで除算した値（いずれも単位は秒）の回数分、ハートビート メッセージが連続して脱落します。

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
```

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

cluster member

クラスタに候補を追加するには、クラスタ コマンド スイッチ上で **cluster member** グローバル コンフィギュレーション コマンドを使用します。メンバーをクラスタから削除する場合は、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*

シンタックスの説明

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

デフォルト

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

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

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

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

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

例

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

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

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

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

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

cluster outside-interface

クラスタの Network Address Translation (NAT; ネットワーク アドレス変換) の外部インターフェイスを設定し、IP アドレスのないメンバーがクラスタの外部にある装置と通信できるようにするには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster outside-interface** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cluster outside-interface *interface-id*

no cluster outside-interface

シンタックスの説明

<i>interface-id</i>	外部インターフェイスとして機能するインターフェイス。有効なインターフェイスとしては、物理インターフェイス、ポートチャネル、または VLAN (仮想 LAN) があります。ポートチャネルに指定できる範囲は 1 ～ 48 です。指定できる VLAN 範囲は 1 ～ 4094 です。

デフォルト

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

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ入力できます。クラスタ メンバー スイッチでコマンドを入力すると、エラー メッセージが表示されます。

例

次の例では、VLAN 1 に外部インターフェイスを設定する方法を示します。

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

設定を確認するには、**show running-config** 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。

cluster run

スイッチ上でクラスタリングをイネーブルにするには、**cluster run** グローバル コンフィギュレーション コマンドを使用します。スイッチ上でクラスタリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

cluster run

no cluster run

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのスイッチでクラスタリングがイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

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

例

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

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

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

cluster standby-group

既存の Hot Standby Router Protocol (HSRP) にクラスタをバインドすることにより、クラスタ コマンドスイッチの冗長性をイネーブルにするには、**cluster standby-group** グローバル コンフィギュレーション コマンドを使用します。routing-redundancy キーワードを入力することで、同一の HSRP グループが、クラスタ コマンドスイッチの冗長性およびルーティングの冗長性に対して使用できるようになります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no cluster standby-group

シンタックスの説明

<i>HSRP-group-name</i>	クラスタにバインドされる HSRP グループの名前。グループ名の文字数は最大 32 文字です。
routing-redundancy	(任意) 同一の HSRP スタンバイ グループをイネーブルにし、クラスタ コマンドスイッチの冗長性およびルーティングの冗長性に対して使用します。

デフォルト

クラスタは、どの HSRP グループにもバインドされません。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、クラスタ コマンドスイッチ上でのみ入力できます。クラスタ メンバー スイッチでこれを入力すると、エラー メッセージが表示されます。

クラスタ コマンド スイッチは、クラスタ HSRP バインディング情報をすべてのクラスタ HSRP 対応メンバーに伝播します。各クラスタ メンバー スイッチはバインディング情報を NVRAM（不揮発性 RAM）に保存します。HSRP グループ名は、有効なスタンバイ グループでなければなりません。有効なスタンバイ グループでない場合、エラーが発生してコマンドが終了します。

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

例

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

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

次の例では、ルーティングの冗長性およびクラスタの冗長性に対して *my_hsrp* という名前の HSRP グループを使用する方法を示します。

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

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

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

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

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

設定を確認するには、**show cluster** イネーブル EXEC コマンドを入力します。クラスタ内の冗長性がイネーブルになっているかどうかは出力から確認できます。

関連コマンド

コマンド	説明
standby ip	インターフェイスで HSRP をイネーブルにします。構文情報については、 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands を選択してください。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show standby	スタンバイ グループ情報を表示します。構文情報については、 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands を選択してください。

cluster timer

ハートビート メッセージの間隔を秒単位で設定するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **cluster timer** グローバル コンフィギュレーション コマンドを使用します。間隔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 timer *interval-in-secs*

no cluster timer

シンタックスの説明	<i>interval-in-secs</i> ハートビート メッセージ間隔 (秒)。指定できる範囲は 1 ～ 300 秒です。	
デフォルト	8 秒間隔です。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。
使用上のガイドライン	このコマンドと cluster holdtime グローバル コンフィギュレーション コマンドは、クラスタ コマンド スイッチ上でのみ入力してください。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、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 メンバーに伝播します。 ホールド時間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、ホールド時間をインターバルで除算した値 (いずれも単位は秒) の回数分、ハートビート メッセージが連続して脱落します。	
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。 <pre>Switch(config)# cluster timer 3 Switch(config)# cluster holdtime 30</pre> 設定を確認するには、show cluster 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 cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

define interface-range

インターフェイスレンジ マクロを作成するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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
```

シンタックスの説明

<i>macro-name</i>	インターフェイスレンジ マクロの名前（最大 32 文字）
<i>interface-range</i>	インターフェイス範囲。インターフェイス範囲の有効値については、「使用上の注意事項」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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

マクロ名は、最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。

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

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

- *type {first-interface} - {last-interface}*
- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gigabitethernet 1/0/1 - 2** ならば範囲は指定されますが、**gigabitethernet 1/0/1-2** 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* - *vlan-ID*（VLAN ID の範囲は 1 ～ 4094）
VLAN インターフェイスは、**interface vlan** コマンドで設定してください（**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-range* では使用できません。
- **port-channel** *port-channel-number*（*port-channel-number* の範囲は 1 ～ 48）
- **fastethernet** stack member/module/ {*first port*} - {*last port*}
- **gigabitethernet** stack member/module/ {*first port*} - {*last port*}

define interface-range

物理インターフェイスの場合

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

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

gigabitethernet1/0/1 - 2

複数の範囲を入力することもできます。複数の範囲を定義するときは、カンマ (,) の前の最初のエントリのあとにスペースが必要です。カンマのあとのスペースは任意になります。次に例を示します。

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

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

例

次の例では、複数のインターフェイス マクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet1/0/1 - 2,
gigabitethernet1/0/1 - 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show running-config	定義されたマクロを含む現在の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。

delete

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、スイッチ スタック またはスタンドアロン スイッチ上で **delete** イネーブル EXEC コマンドを使用します。

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

シンタックスの説明

/force	(任意) 削除を確認するプロンプトを抑制します。
/recursive	(任意) 指定されたディレクトリおよびそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除します。
filesystem:	フラッシュ ファイル システムのエイリアスです。 スタック メンバーまたはマスターのスタック上のローカル フラッシュ ファイル システムの構文 flash: スタック マスターから、スタック メンバー上のローカル フラッシュ ファイル システムの構文 flash member number:
/file-url	削除するパス (ディレクトリ) およびファイル名

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

プロンプト動作は、**file prompt** グローバル コンフィギュレーション コマンドの設定によって異なります。デフォルトでは、スイッチは、ファイルを破壊する操作に対して確認のプロンプトを表示します。このコマンドの詳細については、『Cisco IOS Command Reference』Release 12.1 を参照してください。

例

次の例では、新しいイメージのダウンロードが正常に終了したあとに、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
```

ディレクトリが削除されたかどうかを確認するには、**dir filesystem:** 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
archive download-sw	新しいイメージをスイッチにダウンロードし、既存のイメージを上書きまたは保存します。

deny (ARP アクセスリスト コンフィギュレーション)

Dynamic Host Configuration Protocol (DHCP) バインディングとの照合に基づく Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを拒否するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**deny** ARP アクセスリスト コンフィギュレーション コマンドを使用します。アクセス リストから指定された Access Control Entry (ACE; アクセス制御エントリ) を削除する場合は、このコマンドの **no** 形式を使用します。

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

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

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

request	(任意) ARP 要求の一致条件を定義します。 request が指定されない場合、照合はすべての ARP パケットに対して実行されます。
ip	送信側の IP アドレスを指定します。
any	任意の IP または MAC (メディア アクセス制御) アドレスを拒否します。
host sender-ip	指定された送信側の IP アドレスを拒否します。
<i>sender-ip sender-ip-mask</i>	指定された送信側の IP アドレスの範囲を拒否します。
mac	送信側の MAC アドレスを拒否します。
host sender-mac	特定の送信側の MAC アドレスを拒否します。
<i>sender-mac sender-mac-mask</i>	指定された送信側の MAC アドレスの範囲を拒否します。
response ip	ARP 応答の IP アドレス値を定義します。
host target-ip	指定されたターゲット IP アドレスを拒否します。
<i>target-ip target-ip-mask</i>	指定されたターゲット IP アドレスの範囲を拒否します。
mac	ARP 応答の MAC アドレス値を拒否します。
host target-mac	指定されたターゲット MAC アドレスを拒否します。
<i>target-mac target-mac-mask</i>	指定されたターゲット MAC アドレスの範囲を拒否します。
log	(任意) ACE に一致するパケットをロギングします。

デフォルト

デフォルト設定はありません。ただし、ARP アクセス リストの最後に、暗黙的な **deny ip any mac any** コマンドがあります。

コマンド モード

ARP アクセスリスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

一致条件に基づいて ARP パケットを廃棄するのに、拒否コマンドを追加できます。

例 次の例では、ARP アクセス リストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd: を使用して、ホストからの ARP 要求および ARP 応答の両方を拒否する方法を示します。

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

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

deny (IPv6 アクセスリスト コンフィギュレーション)

IPv6 アクセス リストの拒否条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードを開始し、スイッチ スタックまたはスタンドアロン スイッチ上で **deny** コマンドを使用します。拒否条件を削除する場合は、このコマンドの **no** 形式を使用します。

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

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

Internet Control Message Protocol

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

Transmission Control Protocol

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

User Datagram Protocol

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



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

<i>protocol</i>	インターネット プロトコルの名前または番号。ここには、 <i>ahp</i> 、 <i>esp</i> 、 <i>icmp</i> 、 <i>ipv6</i> 、 <i>pcp</i> 、 <i>sctp</i> 、 <i>tcp</i> 、 <i>udp</i> のいずれかのキーワード、または IPv6 のプロトコル番号を示す 0 ～ 255 の数字を指定できます。
<i>source-ipv6-prefix/prefix-length</i>	拒否条件の設定対象となる送信元 IPv6 ネットワークまたはネットワーク クラス この引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。  (注) CLI のヘルプにはプレフィックスの長さの範囲として /0 ～ /128 が表示されますが、スイッチでサポートされる IPv6 アドレス マッチングは、プレフィックスの長さ範囲 /0 ～ /64 と、集約グローバル ユニキャストおよびリンク ローカル ホスト アドレスの場合、Extended Universal Identifier (EUI) ベースの /128 のプレフィックスのみです。
<i>any</i>	IPv6 プレフィックス ::/0 の略称。
<i>host source-ipv6-address</i>	拒否条件の設定対象となる送信元 IPv6 ホスト アドレス この <i>source-ipv6-address</i> 引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
<i>operator [port-number]</i>	(任意) 指定したプロトコルの送信元および宛先ポートを比較する演算子を指定します。演算子は、lt (未満)、gt (より大きい)、eq (等しい)、neq (等しくない)、range (包含範囲) が使用できます。 演算子を <i>source-ipv6-prefix/prefix-length</i> 引数の後に指定した場合、送信元ポートと一致する必要があります。 演算子を <i>destination-ipv6-prefix/prefix-length</i> 引数の後に指定した場合、宛先ポートと一致する必要があります。 range 演算子には、ポート番号を 2 個指定する必要があります。これ以外の演算子には、ポート番号を 1 個指定します。 オプションの <i>port-number</i> 引数には、10 進数の数字、あるいは TCP または UDP ポートの名前を指定します。指定できるポート番号の範囲は、0 ～ 65535 です。TCP のポート名は、TCP をフィルタリングする場合のみ使用できます。UDP のポート名は、UDP をフィルタリングする場合のみ使用できます。
<i>destination-ipv6-prefix/prefix-length</i>	拒否条件の設定対象となる宛先 IPv6 ネットワークまたはネットワーク クラス この引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。  (注) CLI のヘルプにはプレフィックスの長さの範囲として /0 ～ /128 が表示されますが、スイッチでサポートされる IPv6 アドレス マッチングは、プレフィックスの長さ範囲 /0 ～ /64 と、集約グローバル ユニキャストおよびリンク ローカル ホスト アドレスの場合、EUI ベースの /128 のプレフィックスのみです。

<i>host</i>	拒否条件の設定対象となる宛先 IPv6 ホスト アドレス
<i>destination-ipv6-address</i>	この <i>destination-ipv6-address</i> 引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
<i>dscp value</i>	(任意) 区別されるサービス コード ポイント値を、各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と比較します。許容される範囲は 0 ～ 63 です。
<i>fragments</i>	(任意) フラグメント拡張ヘッダーに 0 でないフラグメント オフセットが設定されている非初期フラグメント パケットを一致させます。 fragments キーワードは、プロトコルが ipv6 で、 <i>operator [port-number]</i> 引数が指定されていない場合のみ使用できます。
<i>log</i>	(任意) コンソールに、エントリに一致するパケットに関する情報ロギング メッセージを送信します (コンソールに送信されるメッセージのレベルは、 logging console コマンドで制御できます)。 メッセージには、アクセス リスト名、一連の番号、パケットが拒否されたかどうか、プロトコルが TCP、UDP、ICMP または数値のいずれであるか、該当する場合、送信元アドレスと宛先アドレス、送信元ポート番号と宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、5 分間隔で、前の 5 分間に拒否されたパケットの数が追加されます。
 (注) ポート ACL については、ロギングはサポートされません。	
<i>log-input</i>	(任意) 機能は log キーワードと同じですが、ロギング メッセージに受信インターフェイスも含まれます。
<i>sequence value</i>	(任意) アクセス リスト ステートメントの一連の番号を指定します。許容される範囲は 1 ～ 4294967295 です。
<i>time-range name</i>	(任意) 拒否ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項を指定するには、それぞれ time-range コマンドと、 absolute または periodic コマンドを使用します。
<i>icmp-type</i>	(任意) ICMP パケットをフィルタリングするための ICMP メッセージ タイプを指定します。ICMP パケットは、ICMP メッセージ タイプによってフィルタリングできます。指定できるタイプの範囲は 0 ～ 255 です。
<i>icmp-code</i>	(任意) ICMP パケットをフィルタリングするための ICMP コードを指定します。ICMP メッセージ タイプでフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。指定できるコードの範囲は 0 ～ 255 です。
<i>icmp-message</i>	(任意) ICMP パケットをフィルタリングするための ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージ タイプおよびコードのほか、ICMP メッセージ名によってもフィルタリングできます。使用できる名前については、「Usage Guidelines」セクションを参照してください。
<i>ack</i>	(任意) TCP プロトコルでのみ使用できます。Acknowledgment (ACK) ビットを設定します。

<i>established</i>	(任意) TCP プロトコルでのみ使用できます。接続が確立されていることを示します。TCP データグラムに ACK または RST ビットが設定されている場合に比較が行われます。接続を確立するための初期 TCP データグラムのケースでは、比較は行われません。
<i>fin</i>	(任意) TCP プロトコルでのみ使用できます。Fin ビットを設定します。送信元からそれ以上データは送信されません。
<i>neq</i> {port protocol}	(任意) 所定のポート番号以外のパケットのみを一致させます。
<i>psh</i>	(任意) TCP プロトコルでのみ使用できます。Push function ビットを設定します。
<i>range</i> {port protocol}	(任意) ポート番号の範囲内にあるパケットのみを一致させます。
<i>rst</i>	(任意) TCP プロトコルでのみ使用できます。Reset ビットを設定します。
<i>syn</i>	(任意) TCP プロトコルでのみ使用できます。Synchronize ビットを設定します。
<i>urg</i>	(任意) TCP プロトコルでのみ使用できます。Urgent pointer ビットを設定します。



(注)

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

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセスリスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

deny (IPv6 アクセスリスト コンフィギュレーションモード) コマンドは **deny** (IPv4 アクセスリスト コンフィギュレーションモード) コマンドと同じですが、IPv6 専用です。

IPv6 アクセス リスト コンフィギュレーションモードを開始してパケットのアクセス リスト通過条件を定義するには、**ipv6 access-list** コマンドのあとに **deny** (IPv6) コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーとの比較が行われます。

デフォルトでは、アクセス リストの最初のステートメントは数値 10 で、それ以後のステートメントは 10 ずつ加算されます。

既存のリストに **permit**、**deny**、または **remark** ステートメントを追加することができ、リスト全体を入力しなおす必要はありません。リストの最後以外の任意の場所に新しくステートメントを追加するには、2 つの既存エントリ番号の間のエントリ番号によって属する場所を示し、新しいステートメントを作成します。



(注)

IPv6 ACL には、最後の一致条件として、暗黙的な **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントが設定されています。2 つの **permit** 条件により、ICMPv6 ネイバの検出が可能になります。ICMPv6 のネイバの検出を無効にして、**icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、ACL に明示的な **deny** エントリを設定する必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に少なくとも 1 個のエントリが設定されていなければなりません。

IPv6 ネイバの検出プロセスには、IPv6 ネットワーク レイヤ サービスが使用されます。そのため、デフォルトでは、IPv6 ACL はインターフェイス上での IPv6 ネイバ検出パケットの送受信を暗黙的に有効にします。IPv4 では、IPv6 ネイバ検出プロセスと同等の Address Resolution Protocol (ARP; アドレス解決プロトコル) で専用のデータリンク レイヤ プロトコルが使用されます。そのため、デフォルトでは、IPv4 ACL はインターフェイス上での ARP パケットの送受信を暗黙的に有効にします。

source-ipv6-prefix/prefix-length 引数と *destination-ipv6-prefix/prefix-length* 引数は、トラフィック フィルタリングに使用されます (送信元プレフィックスはトラフィック送信元に基づいてトラフィックのフィルタリングを行い、宛先プレフィックスはトラフィック宛先に基づいてトラフィックのフィルタリングを行います)。

スイッチでサポートされているのは、/0 ~ /64 のプレフィックス、集約グローバルユニキャストおよびリンクローカル ホスト アドレスの場合は EUI ベースの /128 のプレフィックスです。

fragments キーワードは、プロトコルが **ipv6** で、*operator [port-number]* 引数が指定されていない場合のみ使用できます。

次に、ICMP メッセージ名の一覧を示します。

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

例

次の例では、CISCO という名前の IPv6 アクセス リストを設定し、アクセス リストをレイヤ 3 インターフェイスの発信トラフィックに適用します。リストの最初の拒否エントリにより、宛先 TCP ポート番号が 5000 より大きいパケットがインターフェイスから発信されなくなります。リストの 2 番めの拒否エントリにより、送信元 UDP ポート番号が 5000 未満のパケットがインターフェイスから発信されなくなります。また、2 番めの拒否エントリは、一致項目をコンソールに記録します。リストの最初の許可エントリにより、インターフェイスでの ICMP パケットの発信が許可されます。リストの 2 番めの許可エントリにより、インターフェイスでのその他のトラフィックの発信が許可されます。2 番めの許可エントリが必要となるのは、IPv6 アクセス リストの最後に暗黙的な deny-all 条件が存在するためです。

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

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義して、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイスで IPv6 の着信トラフィックおよび発信トラフィックをフィルタリングします。
permit (IPv6 アクセスリスト コンフィギュレーション)	IPv6 アクセス リストの許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストの全内容を表示します。

deny (MAC アクセスリスト コンフィギュレーション)

条件が一致した場合に、非 IP トラフィックの転送を回避するには、スイッチ スタックまたはスタンドアロン スイッチ上で **deny** MAC (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。名前付き MAC アクセス リストから拒否条件を削除する場合は、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]
```

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワード
host src MAC-addr src-MAC-addr mask	ホスト MAC アドレスおよびオプションのサブネット 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 アドレスおよびオプションのサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	(任意) Ethernet II または Subnetwork Access Protocol (SNAP) のカプセル化でパケットの EtherType 番号を使用し、パケットのプロトコルを識別します。 指定できる <i>type</i> の範囲は 0 ～ 65535 です (16 進数)。 <i>mask</i> は、一致テストの前に EtherType に適用される <i>don't care</i> (無視) 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 Digital Equipment Corporation (DEC) -Amber を選択します。
cos cos	(任意) 0 ～ 7 の Class of Service (CoS; サービス クラス) 番号を選択し、プライオリティを設定します。CoS のフィルタリングはハードウェア内でのみ実行可能です。 cos オプションが設定されると、警告メッセージが表示されます。
dec-spanning	(任意) EtherType 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 <i>lsap-number mask</i>	(任意) 802.2 のカプセル化でパケットの LSAP 番号 (0 ~ 65535) を使用し、パケットのプロトコルを識別します。 <i>mask</i> は、一致テストの前に LSAP 番号に適用される <i>don't care</i> 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tring には表示されますが、一致条件としてサポートされていません。

Internetwork Packet Exchange (IPX) トラフィックをフィルタリングする場合、使用される IPX のカプセル化タイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 専門用語および Cisco IOS 専門用語で指定の IPX のカプセル化タイプのフィルタ条件は、表 2-4 にリストされています。

表 2-4 IPX のフィルタリング条件

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

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 (アクセス制御リスト) のデフォルトアクションは拒否します。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

deny (MAC アクセスリスト コンフィギュレーション)

host キーワードを使用した場合、アドレス マスクを入力できません。**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 リストに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa へ送信される、NETBIOS トラフィックを拒否するための名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

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

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

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

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

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

設定を確認するには、**show access-lists** 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
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	スイッチで設定される ACL を表示します。

dot1x

IEEE（米国電気電子学会）802.1x をグローバルにイネーブルにするには、スイッチ スタックまたはスタンドアロンスイッチ上で **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}

シンタックスの説明

system-auth-control	スイッチ上で IEEE 802.1x をグローバルにイネーブルにします。
guest-vlan supplicant	スイッチ上で、任意のゲスト 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 はディセーブルです。任意のゲスト VLAN の動作はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	guest-vlan supplicant キーワードが追加されました。

使用上のガイドライン

IEEE 802.1x をグローバルにイネーブルにする前に、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）をイネーブルにし、認証方式のリストを指定する必要があります。方式リストには、ユーザを認証するために使用する順番と認証方式が記載されています。

スイッチ上で 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 を設定するインターフェイスから EtherChannel の設定を削除しておく必要があります。

使用している装置で、IEEE 802.1x 認証のための Cisco Access Control Server（ACS）アプリケーションと、EAP-Transparent LAN Services（TLS; 透過型 LAN サービス）および EAP-MD5 が動作していて、使用しているスイッチで Cisco IOS Release 12.1(14)EA1 が稼働している場合、その装置では ACS Version 3.2.1 以降が稼働していることを確認してください。

スイッチ上で任意の IEEE 802.1x のゲスト VLAN 動作をグローバルにイネーブルにするには、**guest-vlan supplicant** キーワードを使用します。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、スイッチ上で 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、スイッチ上で任意のゲスト VLAN 動作をグローバルにイネーブルにする方法を示します。

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

設定を確認するには、**show dot1x [interface interface-id]** 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
dot1x guest-vlan	アクティブな VLAN をイネーブルにし、IEEE 802.1x のゲスト 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 <i>interface-id</i>]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x auth-fail max-attempts

ポートが制限 VLAN に移行するまでに許容可能な最大認証試行回数を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no dot1x auth-fail max-attempts

シンタックスの説明

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

デフォルト

デフォルト値は 3 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	このコマンドが導入されました。

使用上のガイドライン

VLAN で許容される最大認証試行回数を設定した場合、変更内容が反映されるのは、再認証タイマーが時間切れになったあとです。

例

次の例では、ポート 3 が制限 VLAN に移行するまでに許容可能な最大認証試行回数として 2 を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 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
dot1x auth-fail vlan [<i>vlan-id</i>]	オプションの制限 VLAN 機能をイネーブルにします。
dot1x max-reauth-req [<i>count</i>]	ポートが無許可ステートに変わるまでに、スイッチが認証プロセスを再始動する最大回数を設定します。
show dot1x [<i>interface interface-id</i>]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x auth-fail vlan

ポートで制限 VLAN をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x 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*

シンタックスの説明

<i>vlan-id</i>	1 ～ 4094 の範囲で VLAN を指定します。

デフォルト

制限 VLAN は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

次のように設定されたポート上で制限 VLAN を設定できます。

- シングルホスト（デフォルト）モード
- 自動認証モード

再認証をイネーブルにする必要があります。再認証がディセーブルになっていると、制限 VLAN のポートは再認証要求を受信しません。再認証プロセスを開始するには、制限 VLAN が、ポートからリンクダウン イベントまたは Extensible Authentication Protocol (EAP) ログオフ イベントを受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、ホストが切断されてもポートでリンクダウン イベントが受信されないことがあり、その結果、次の再認証試行が行われるまで新しいホストが検出できないことがあります。

サブリカントが認証に失敗すると、ポートは制限 VLAN に移行し、EAP *success* メッセージがサブリカントに送信されます。サブリカントは実際の認証失敗を通知されないため、この制限されたネットワーク アクセスに混乱が生じることがあります。EAP *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と、サブリカントは EAP-start メッセージを送信し、60 秒（デフォルト）ごとに認証を試みます。
- EAP *success* メッセージを受信するまで DHCP を実装できないホスト（Windows XP が動作する装置など）もあります。

サブリカントは、認証サーバから EAP *success* メッセージを受信したあと、正しくないユーザ名とパスワードの組み合わせをキャッシュし、再認証時にその情報を再使用することがあります。サブリカントが正しいユーザ名とパスワードの組み合わせを送信するまで、ポートは制限 VLAN の状態のままになります。

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

1 つの VLAN を、制限 VLAN と音声 VLAN の両方として設定することはできません。このような設定をした場合、シスログ メッセージが生成されます。

制限 VLAN ポートが無許可ステートに移行すると、認証プロセスが再開されます。サブリカントが認証プロセスに再度失敗すると、認証サーバは保持ステートで待ちます。サブリカントが正しく再認証されると、IEEE 802.1x ポートは再初期化され、正常な IEEE 802.1x ポートとして扱われます。

制限 VLAN を別の VLAN として設定しなおすと、制限 VLAN 内のポートも変更され、ポートは現在の許可ステートを保持します。

シャットダウンすると、または VLAN データベースから制限 VLAN を削除すると、制限 VLAN 内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 VLAN 設定がまだ存在しているため、認証サーバは保持ステートになりません。制限 VLAN がアクティブでない間も、制限 VLAN がアクティブになったときにポートがただちに制限 VLAN になるように、認証試行はカウントされます。

制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でのみサポートされます。このため、ポートが制限 VLAN になると、サブリカントの MAC アドレスが MAC アドレス テーブルに追加され、ポートに到達するそれ以外の MAC アドレスは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 VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [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
dot1x auth-fail max-attempts [max-attempts]	サブリカントを制限 VLAN に割り当てるまでに許容可能な認証試行回数を設定します。
show dot1x [interface interface-id]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x control-direction

ポート制御を単一方向制御または双方向制御に変更するには、**dot1x control-direction** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x control-direction {in | both}

no dot1x control-direction {in | both}

シンタックスの説明

in	ポート上の単一方向制御をイネーブルにします。
both	ポート上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)SEC	このコマンドが導入されました。

使用上のガイドライン

キーワード **both** を使用した場合と、このコマンドの **no** 形式を使用した場合とでは、同じコマンドになります。

キーワード **both** およびこのコマンドの **no** 形式を使用すると、ポートのデフォルト設定は双方向に変更されます。

例

次の例では、単一方向制御をイネーブルにする方法を示します。

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

次の例では、双方向制御をイネーブルにする方法を示します。

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

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

show dot1x all イネーブル EXEC コマンドの出力結果は、ポート名とポートのステータスのぞき、すべてのスイッチで同じです。ポートに未認証のホストが設定されている場合、次の内容に似た画面が表示されます。

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

単一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** コマンドの出力は次のようになります。

```
ControlDirection = In
```

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを入力してもコンフィギュレーションが競合するためにポートがこのモードに対応できない場合は、**show dot1x all** コマンドの出力は次のようになります。

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

関連コマンド

コマンド	説明
show dot1x all [interface <i>interface-id</i>]	指定したインターフェイスの制御方向ポート設定のステータスを表示します。

dot1x critical

アクセス不能認証バイパス機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x critical** インターフェイス コンフィギュレーション コマンドを使用します。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。

dot1x critical

no dot1x critical

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト アクセス不能認証バイパス機能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)SED	このコマンドが導入されました。

使用上のガイドライン この機能は、単一ホスト モードの IEEE 802.1x ポート上でのみサポートされます。ポートをクリティカル ポートとして設定しようとする、またはホスト モードを複数ホスト モードに変更すると、次のメッセージが表示されます。

```
%Command rejected:Critical ports are only allowed in single-host mode
```

クライアントで Windows XP が動作していて、クライアントが接続されるクリティカル ポートがクリティカル認証ステートである場合、Windows XP により、インターフェイスが認証されない旨のレポートが作成されることがあります。

Windows XP クライアントが DHCP 用に設定されていて、DHCP サーバで生成される IP アドレスを使用している場合、クリティカル ポートで EAP-Success メッセージを受信しても DHCP 設定プロセスが再開されないことがあります。

IEEE 802.1x ポートで、アクセス不能認証バイパス機能と制限付き VLAN を設定できます。スイッチが制限付き VLAN でクリティカル ポートの再認証を試行し、RADIUS サーバがすべて使用できない場合、ポートの状態はクリティカル認証ステートに移行し、ポートは制限付き VLAN のままとなります。

同一のスイッチ ポート上で、アクセス不能バイパス機能とポート セキュリティの両方を設定できます。

例 次の例では、ポート 1 上でアクセス不能認証バイパス機能をイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 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
<code>show dot1x [interface interface-id]</code>	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x default

IEEE（米国電気電子学会）802.1x パラメータをデフォルト値にリセットするには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x default** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト値は次のとおりです。

- ポートごとの 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（強制認証）。
- 再認証の試行間隔の秒数は 3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最大再伝送回数は 2 回です。
- ホスト モードはシングルホストです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

例

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

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

設定を確認するには、**show dot1x [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
<code>show dot1x [interface interface-id]</code>	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x guest-vlan

アクティブな VLAN（仮想 LAN）を IEEE 802.1x のゲスト VLAN として指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**dot1x guest-vlan** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x guest-vlan vlan-id
```

```
no dot1x guest-vlan
```

シンタックスの説明

<i>vlan-id</i>	アクティブな VLAN を IEEE 802.1x のゲスト 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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	このコマンドは修正され、デフォルトのゲスト VLAN 動作を変更しました。
12.2(25)SEC	使用上の注意事項が変更されました。

使用上のガイドライン

次のいずれかのスイッチ ポートでゲスト VLAN を設定できます。

- 非プライベート VLAN に属するスタティックアクセス ポート。
- セカンダリ プライベート VLAN に属するプライベート VLAN ポート。スイッチ ポートに接続する全ホストは、端末状態が正しく妥当性評価され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および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。

IEEE 802.1x が動作していないクライアント（スイッチに接続されたデバイスまたはワークステーション）に制限されたサービスを提供するよう、スイッチ上の IEEE 802.1x ポートごとにゲスト VLAN を設定できます。ユーザは、IEEE 802.1x 認証用に自分のシステムをアップグレードできます。Windows 98 システムなどの一部のホストでは、IEEE 802.1x 対応でない場合があります。

IEEE 802.1x ポート上でゲスト VLAN をイネーブルにする場合で、Extensible Authentication Protocol over LAN (EAPOL) -Request/Identity フレームへの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によって送信されない場合、スイッチはクライアントをゲスト VLAN に割り当てます。

Cisco IOS Release 12.2(25)SE より前では、スイッチは EAPOL パケット履歴を保持せず、インターフェイス上で EAPOL パケットが削除されたかどうかに関係なく、ゲスト VLAN への認証アクセスに失敗したクライアントを許可していました。この任意の動作をイネーブルにするには、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを使用します。

Cisco IOS Release 12.2(25)SE 以降では、スイッチは EAPOL パケット履歴を保持します。リンクの存続時間の間にインターフェイス上で別の EAPOL パケットが検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートになっている場合、ポートは無許可ステートになり、認証プロセスが再開されます。EAPOL 履歴はリンクが切断されるとリセットされます。

この動作をイネーブルにするには、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを入力します。

スイッチ ポートがゲスト VLAN に移行されると、IEEE 802.1x 非対応のクライアントのアクセスがいくつでも許可されます。IEEE 802.1x 対応のクライアントが、ゲスト VLAN が設定された同じポートに加入する場合、ポートはユーザ設定されたアクセス VLAN の無許可ステートになり、認証が再開されます。

ゲスト VLAN は、単一ホスト モードまたは複数ホスト モードの IEEE 802.1x ポート上でサポートされます。

Remote Switched Port Analyzer (RSPAN) VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外、アクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッド ポート) またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートのみです。

Dynamic Host Configuration Protocol (DHCP) クライアントが接続された IEEE 802.1x ポートにゲスト 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る場合があります。クライアントの DHCP プロセスがタイムアウトして 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、スイッチの IEEE 802.1x 認証プロセスを再始動するために設定を変更することもできます。IEEE 802.1x 認証プロセスの設定値を小さくします (**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)。設定値を小さくする度合は、接続されている IEEE 802.1x クライアントのタイプによって異なります。

例

次の例では、VLAN 5 を IEEE 802.1x のゲスト 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として 3、EAP-Request/Identity フレームに対するクライアントからの応答をスイッチが待機する (要求の再送を待機する) 秒数として 15 を設定し、IEEE 802.1x ポートが DHCP クライアントに接続されたときに VLAN 2 をゲスト 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、任意のゲスト VLAN 動作をイネーブルにし、VLAN 5 を IEEE 802.1x のゲスト VLAN として指定する方法を示します。

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

設定を確認するには、**show dot1x [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
dot1x	任意のゲスト VLAN のサブ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 の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 コマンドを **auto** に設定された IEEE 802.1x 許可ポート上で、単一のホスト（クライアント）または複数のホストに設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**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]

シンタックスの説明

multi-host	スイッチ上で複数のホストをイネーブルにします。
single-host	スイッチ上で単一のホストをイネーブルにします。

デフォルト

デフォルト設定は、シングルホスト モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。 dot1x multiple-hosts インターフェイス コンフィギュレーション コマンドはこのコマンドに変更されました。

使用上のガイドライン

IEEE 802.1x 対応のポートを単一のクライアントに制限する場合、または IEEE 802.1x 対応ポートに複数のクライアントを適用する場合にこのコマンドを使用します。マルチホストのモードでは、接続されたホストのうち 1 つが許可されれば、すべてのホストのネットワーク アクセスも許可されます。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、指定したポート上で **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する方法、1 つのポート上で IEEE 802.1x をイネーブルにする方法、およびマルチホスト モードをイネーブルにする方法を示します。

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

設定を確認するには、**show dot1x [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 dot1x [interface interface-id]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x initialize

ポート上で新しく認証セッションを初期化する前に、指定の IEEE 802.1x 対応ポートを、手動で無許可ステートに戻すには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x initialize** イネーブル EXEC コマンドを使用します。

dot1x initialize interface interface-id

シンタックスの説明

interface interface-id	ポートが初期化されます。

デフォルト

デフォルト設定はありません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用し、IEEE 802.1x の状態にあるマシンを初期化することで、認証環境を新規に設定します。このコマンドを入力したあと、ポートのステータスは無許可になります。

このコマンドに **no** 形式はありません。

例

次の例では、ポートを手動で初期化する方法を示します。

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

無許可のポートの状態を確認するには、**show dot1x [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 dot1x [interface interface-id]	指定したポートの IEEE 802.1x の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変わるまでに、スイッチが認証プロセスを再始動する上限回数を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *count*

no dot1x max-reauth-req

シンタックスの説明

<i>count</i>	ポートが無許可ステートに変わるまでに、スイッチが認証プロセスを再始動する回数。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(18)SE	このコマンドが導入されました。
12.2(25)SEC	<i>count</i> の範囲が変更されました。

使用上のガイドライン

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

例

次の例では、ポートが無許可ステートに変わるまでにスイッチが認証プロセスを再始動する回数として 4 を設定する方法を示します。

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

設定を確認するには、**show dot1x [interface interface-id]** 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
dot1x max-req	スイッチが、認証プロセスを再始動する前に、Extensible Authentication Protocol (EAP) フレームをクライアントに送信する最大回数を設定します (応答を受信しないことが前提)。
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 の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始動する前に、Extensible Authentication Protocol (EAP) フレームを認証サーバからクライアントに送信する最大回数を設定するには (応答を受信しないことが前提)、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req *count*

no dot1x max-req

シンタックスの説明

<i>count</i>	スイッチが、認証プロセスを再始動する前に、EAP フレームを認証サーバから再送信する回数。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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	コマンドはインターフェイス コンフィギュレーション モードに変更されました。

使用上のガイドライン

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

例

次の例では、スイッチが、認証プロセスを再始動する前に EAP フレームを認証サーバからクライアントに送信する回数として 5 を設定する方法を示します。

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

設定を確認するには、**show dot1x [interface interface-id]** 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
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 (米国電気電子学会) 802.1x のステータスを表示します。

dot1x multiple-hosts

このコマンドは現在使用されていません。

過去のリリースで、**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドは、スイッチ スタックまたはスタンドアロン スイッチ上で、IEEE (米国電気電子学会) 802.1x の許可ポートで複数のホスト (クライアント) を設定するために使用されました。

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	dot1x multiple-hosts インターフェイス コンフィギュレーション コマンドは dot1x host-mode インターフェイス コンフィギュレーション コマンドに変更されました。

関連コマンド

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

dot1x port-control

ポートの許可ステートを手動で制御するには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x port-control** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

```
no dot1x port-control
```

シンタックスの説明

auto	ポート上で IEEE（米国電気電子学会）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タスに移行させます。
force-authorized	ポート上で IEEE 802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステータスに移行させます。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試行をすべて無視し、ポートを強制的に無許可ステータスに移行させることによって、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通してクライアントに認証サービスを提供できません。

デフォルト

デフォルトの設定は **force-authorized** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

特定のポート上で 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、スイッチ上の 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 のスタティックアクセス ポート、音声 VLAN（仮想 LAN）のポート、およびレイヤ 3 のルーテッド ポート上でサポートされます。

ポートが、次のポートの 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、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、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 ポートへの変更に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、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 [仮想 LAN] Query Protocol [VQP]) ポートで IEEE 802.1x をイネーブルにしようとする、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 — IEEE 802.1x のポートとしてアクティブまたはまだアクティブになっていない EtherChannel のメンバーであるポートを設定することは避けてください。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。



(注) Cisco IOS Release 12.2(18)SE より前のソフトウェア リリースの場合、まだアクティブになっていない EtherChannel 上のポートで 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。

- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN) の宛先ポート — SPAN または RSPAN の宛先ポート上の IEEE 802.1x をイネーブルにできます。ただし、SPAN または RSPAN の宛先としてポートが削除されないかぎり、IEEE 802.1x はディセーブルです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x をイネーブルにできます。

スイッチ上で、IEEE 802.1x をグローバルにディセーブルにする場合、**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。特定のポート上で、IEEE 802.1x をディセーブルにする場合、**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、ポートで IEEE 802.1x をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
```

設定を確認するには、**show dot1x [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 dot1x [interface interface-id]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x re-authenticate

指定の IEEE（米国電気電子学会）802.1x 対応ポートの再認証を手動で開始するには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x re-authenticate** イネーブル EXEC コマンドを使用します。

dot1x re-authenticate interface *interface-id*

シンタックスの説明

interface <i>interface-id</i>	再認証するインターフェイスのスタック スイッチ番号、モジュール、およびポート番号

デフォルト

デフォルト設定はありません。

コマンドモード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すれば、再認証試行（re-authperiod）および自動再認証の間に設定した秒数を待たずにクライアントを再認証できます。

例

次の例では、ポートに接続された装置を手動で再認証する方法を示します。

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

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	再認証の試行間隔（秒）を指定します。

dot1x re-authentication

このコマンドは現在使用されていません。

過去のリリースで、**dot1x re-authentication** グローバル コンフィギュレーション コマンドは、スイッチ スタックまたはスタンドアロン スイッチ上で、定期的な再認証の試行間隔を設定するために使用されました。

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	dot1x re-authentication グローバル 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 コマンドに変更されました。

関連コマンド

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

dot1x reauthentication

定期的なクライアントの再認証をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x reauthentication

no dot1x reauthentication

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

定期的な再認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。 dot1x re-authentication グローバル コンフィギュレーション コマンド（ハイフン付き）がこのコマンドに変更されました。

使用上のガイドライン

dot1x timeout reauth-period インターフェイス コンフィギュレーション コマンドを使用して、定期的に再認証を行う間隔を設定します。

例

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

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

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

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

設定を確認するには、**show dot1x [interface interface-id]** 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
dot1x re-authenticate	IEEE 802.1x 対応ポートの再認証を手動で開始します。
dot1x timeout reauth-period	再認証の試行間隔（秒）を指定します。
show dot1x [interface interface-id]	指定したポートの IEEE 802.1x のステータスを表示します。

dot1x timeout

IEEE（米国電気電子学会）802.1x のタイマーを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}
```

シンタックスの説明

quiet-period <i>seconds</i>	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 { <i>seconds</i> <i>server</i> }	再認証の試行間隔（秒）を指定します。 キーワードの意味は次のとおりです。 seconds — 1 ～ 65535 の間で秒数を指定します。デフォルトは 3600 秒です。 server — Session-Timeout RADIUS 属性の値を秒数で指定します (Attribute[27])。
server-timeout <i>seconds</i>	認証サーバに対して、スイッチの packets 再送信を待機する秒数。指定できる範囲は、30 ～ 65535 です。
supp-timeout <i>seconds</i>	IEEE 802.1x クライアントに対して、スイッチの packets 再送信を待機する秒数。指定できる範囲は、30 ～ 65535 です。
tx-period <i>seconds</i>	スイッチが Extensible Authentication Protocol (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。指定できる範囲は、5 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

reauth-period は 3600 秒です。

quiet-period は 60 秒です。

tx-period は 5 秒です。

supp-timeout は 30 秒です。

server-timeout は 30 秒です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	supp-timeout および server-timeout キーワードが追加され、コマンドがインターフェイス コンフィギュレーション モードに変更されました。
12.2(18)SE	server-timeout キーワード、 supp-timeout キーワード、および tx-period キーワードの範囲が変更されました。
12.2(25)SEC	tx-period キーワードの指定範囲が変更され、 reauth-period server キーワードが追加されました。

使用上のガイドライン

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

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにした場合にのみ、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドが、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい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、再認証の試行間隔を 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 属性の値を再認証の試行間隔の秒数で設定する方法を示します。

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

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

次の例では、スイッチから認証サーバへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config)# dot1x timeout server-timeout 45
```

次の例では、EAP Request フレームに対してスイッチからクライアントへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

次の例では、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
```

設定を確認するには、**show dot1x** 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
dot1x max-req	スイッチが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最大回数を設定します。
dot1x reauthentication	クライアントの定期的な再認証をイネーブルにします。
show dot1x	すべてのポートの IEEE 802.1x のステータスを表示します。

duplex

ポートの動作のデュプレックス モードを指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **duplex** インターフェイス コンフィギュレーション コマンドを使用します。ポートを デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

duplex {auto | full | half}

no duplex

シンタックスの説明

auto	自動によるデュプレックス設定をイネーブルにします(接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードかを判断します)。
full	全二重モードをイネーブルにします。
half	半二重モードをイネーブルにします (10 Mbps [メガビット/秒] または 100 Mbps で動作しているインターフェイスのみ)。1000 Mbps または 10000 Mbps で動作しているインターフェイスについては、半二重モードを設定することはできません。

デフォルト

ファスト イーサネットおよびギガビット イーサネット ポートの場合、デフォルトは **auto** です。

100 BASE-x SFP モジュールの場合、デフォルトは **full** です (-x は、-BX、-FX、-FX-FE、および -LX)。

1000 BASE-x 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ていません (-x は、-BX、-CWDM、-LX、-SX、および -ZX)。

スイッチでサポートされる SFP モジュールの詳細については、製品のリリース ノートを参照してください。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

ファスト イーサネット ポートでは、接続された装置がデュプレックス パラメータをオート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、接続された装置がデュプレックス パラメータをオート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、接続された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 インターフェイス上でサポートされます。ただし、これらのインターフェイスが半二重モードで動作するようには設定できません。

一部のポートは、全二重または半二重に設定できます。このコマンドの適用可能性は、スイッチが接続されている装置によって異なります。

回線の両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはリンクの反対にある終端の装置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。

Cisco IOS Release 12.2(20)SE1 から、速度が **auto** に設定されている場合にデュプレックス設定を設定できます。

**注意**

インターフェイスの速度およびデュプレックス モードの設定を変更することで、再設定の間、インターフェイスのシャットダウンとインターフェイスの再イネーブル化が発生する場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、全二重で動作するようインターフェイスを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
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の設定を表示します。
speed	10/100 または 10/100/1000 Mbps インターフェイス上で速度を設定します。

errdisable detect cause

特定の原因、またはすべての原因に対して、errdisable 検出をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。

errdisable detect cause {all | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap}

no errdisable detect cause {all | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap}

シンタックスの説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査のエラー検出をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol (DHCP) スヌーピングのエラー検出をイネーブルにします。
dtp-flap	Dynamic Trunking Protocol (DTP) フラップのエラー検出をイネーブルにします。
gbic-invalid	無効な GBIC (ギガビット インターフェイス コンバータ) モジュールのエラー検出をイネーブルにします。
 (注) Catalyst 3750 スイッチ上では、このエラーは無効な Small Form-Factor Pluggable (SFP) モジュールを指します。	
l2ptguard	レイヤ 2 プロトコルトンネル errdisable の原因に対して、エラー検出をイネーブルにします。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。
pagp-flap	Port Aggregation Protocol (PAgP) フラップ errdisable の原因に対してエラー検出をイネーブルにします。

コマンドのデフォルト設定

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	loopback キーワードが追加されました。
12.1(19)EA1	dhcp-rate-limit キーワードが追加されました。
12.2(20)SE	arp-inspection キーワードが追加されました。
12.2(25)SE	l2ptguard キーワードが追加されました。

使用上のガイドライン

原因 (**all** や **dhcp-rate-limit** など) とは、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上で検出された場合、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。

この原因に対して、**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を設定した場合、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。回復メカニズムを設定していない場合、**shutdown** および **no shutdown** コマンドを入力し、**errdisable** ステートから手動でインターフェイスを回復する必要があります。

例

次の例では、リンクフラップ **errdisable** の原因に対する **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
```

設定を確認するには、**show errdisable detect** 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 errdisable detect	errdisable の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

回復メカニズムの変数を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap | psecure-violation |
security-violation | udld | vmmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit
| dtp-flap | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap | psecure-violation |
security-violation | udld | vmmps} | {interval interval}}
```

シンタックスの説明

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。
arp-inspection	Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査 errdisable ステートから回復するタイマーをイネーブルにします。
channel-misconfig	EtherChannel 設定不良 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	Dynamic Host Configuration Protocol (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 トランッキング 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 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 3750 スイッチ上では、このエラーは無効な Small Form-Factor Pluggable (SFP) errdisable ステートを指します。	
l2ptguard	レイヤ 2 プロトコル トンネル 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。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	Port Aggregation Protocol (PAgP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE (米国電気電子学会) 802.1x の違反ディセーブル 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 (仮想 LAN) Membership Policy Server (VMPS; VLAN メンバーシップ ポリシー サーバ) errdisable ステートから回復するタイマーをイネーブルにします。
interval interval	指定された errdisable ステートから回復する時間を指定します。指定できる範囲は 30 ～ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルト間隔は 300 秒です。
 (注) errdisable 回復のタイマーは、設定された間隔の値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。	

デフォルト

すべての原因に対して回復はディセーブルです。

デフォルトの回復間隔は 300 秒です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	security-violation キーワードが追加されました。 gbic-invalid キーワードが SFP モジュール ポートに対してサポートされます。
12.1(19)EA1	dhcp-rate-limit キーワードが追加されました。
12.2(18)SE	channel-misconfig キーワードが追加されました。
12.2(20)SE	arp-inspection キーワードが追加されました。
12.2(25)SE	l2ptguard キーワードが追加されました。

使用上のガイドライン

原因 (**all** や **bpduguard** など) は、errdisable ステートが発生した理由として定義されています。原因がインターフェイス上で検出された場合、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。

原因の回復をイネーブルにしない場合、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** コマンドを入力する必要があります。

例

次の例では、BPDU ガード errdisable の原因に対して回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
```

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

設定を確認するには、**show errdisable recovery** 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 errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

exception crashinfo

Cisco IOS イメージのエラー時にスイッチで拡張クラッシュ情報ファイルが作成されるよう設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチで拡張クラッシュ情報ファイルが作成されます。

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)SEC	このコマンドが導入されました。

使用上のガイドライン

基本クラッシュ情報ファイルには、エラーとなった Cisco IOS イメージの名前とバージョン、プロセス レジスタのリスト、スタック トレースが記述されます。拡張クラッシュ情報ファイルには、スイッチのエラー原因の特定に役立つ追加情報が記述されます。

スタック マスターで **exception crashinfo** グローバル コンフィギュレーション コマンドを入力すると、スタック メンバーの Cisco IOS イメージでエラーが発生したときに、すべてのスタック メンバーで拡張クラッシュ情報ファイルが作成されるよう設定されます。

スイッチで拡張クラッシュ情報ファイルが作成されないよう設定するには、**no exception crashinfo** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スイッチで拡張クラッシュ情報ファイルが作成されないよう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。

flowcontrol

インターフェイスに対する受信フロー制御ステートを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。特定の装置に対してフロー制御 **send** が実行可能、かつオンの状態で、終端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。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、輻輳している間のデータ パケットの損失を防ぎます。

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

flowcontrol receive {desired | off | on}



(注)

Catalyst 3750 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。

シンタックスの説明

receive	インターフェイスがリモート装置からフロー制御パケットを受信できるかどうかを設定します。
desired	インターフェイスは、フロー制御パケットを送信する必要がある接続された装置、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された装置と連携して稼働できます。
off	接続された装置がフロー制御パケットをインターフェイスに送信する機能はオフになります。
on	インターフェイスは、フロー制御パケットを送信する必要がある接続された装置、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された装置と連携して稼働できます。

デフォルト

デフォルトは、**flowcontrol receive off** に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このスイッチでは、送信フロー制御の休止フレームはサポートされません。

on および **desired** キーワードは同一の結果になることに注意してください。

flowcontrol コマンドを使用してポートが輻輳中にトラフィック レートを制御するよう設定する場合、フロー制御はポート上で次の条件のうちの 1 つに設定されます。

- **receive on** または **desired** : ポートは休止フレームを送信できませんが、休止フレームの送信に必要、または送信ができる装置を接続して一緒に使用できます。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、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

表 2-5 は、各設定の組み合わせによるローカル ポートおよびリモート ポート上のフロー制御の結果を示したものです。テーブルは **receive desired** キーワードの使用時と **receive on** キーワードの使用時の結果が同一になることを前提としています。

表 2-5 フロー制御設定およびローカル/リモート ポート フロー制御解決

フロー制御設定		フロー制御解決	
ローカル装置	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 gigabitethernet1/0/1
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 チャネルの論理インターフェイスへのアクセス、または作成を行うには、スイッチ スタックまたはスタンドアロン スイッチ上で **interface port-channel** グローバル コンフィギュレーション コマンドを使用します。ポートチャネルを削除する場合は、このコマンドの **no** 形式を使用します。

```
interface port-channel port-channel-number
```

```
no interface port-channel port-channel-number
```

シンタックスの説明

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

デフォルト

ポートチャネル論理インターフェイスは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	<i>port-channel-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

レイヤ 2 の EtherChannel に関しては、物理ポートをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを取得すると、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。ポートチャネル インターフェイスを最初に作成した場合、*channel-group-number* と *port-channel-number* を同一にするか、または新しい番号を使用できます。新しい番号を使用した場合、**channel-group** コマンドはダイナミックに新しいポート チャネルを作成します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用することで、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポートチャネルの論理インターフェイスを手動で設定してください。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。



注意

ポートチャネル インターフェイスをルーテッド ポートとして使用する場合、チャネル グループに割り当てられた物理ポート上にレイヤ 3 アドレスを割り当てないようにしてください。



注意

レイヤ 3 のポートチャネル インターフェイスとして使用されているチャネル グループの物理ポート上で、ブリッジ グループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol (CDP) を使用する場合には、これを物理ポート上でのみ設定してください。ポートチャネル インターフェイスでは設定できません。
- IEEE (米国電気電子学会) 802.1x のポートとしてアクティブな EtherChannel のメンバーであるポートを設定することは避けてください。まだアクティブになっていない EtherChannel 上のポートで IEEE 802.1x をイネーブルにしても、そのポートは EtherChannel に加入しません。

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

例

次の例では、ポート チャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
Switch(config)# interface port-channel 5
```

設定を確認するには、**show running-config** または **show etherchannel channel-group-number detail** 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-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。

interface range

インターフェイス レンジ コンフィギュレーション モードの開始、および複数のポートにおけるコマンドを同時に実行するには、スイッチ スタックまたはスタンドアロン スイッチ上で **interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス範囲を削除する場合は、このコマンドの **no** 形式を使用します。

```
interface range {port-range | macro name}
```

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

シンタックスの説明

<i>port-range</i>	ポート範囲。 <i>port-range</i> 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。
<i>macro name</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

インターフェイス レンジ コンフィギュレーション モードを開始すると、入力したすべてのインターフェイスのパラメータは、その範囲内のすべてのインターフェイスに適用されます。

VLAN (仮想 LAN) では、既存の VLAN の Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) でのみ **interface range** コマンドを使用できます。VLAN の 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設定変更は、すべて NVRAM (不揮発性 RAM) に保存されますが、インターフェイス範囲自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力できます。

- 最大 5 つまでのインターフェイス範囲を指定
- 定義済みのインターフェイスレンジマクロ設定を指定

範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、各範囲をカンマ (,) で区切ることにより、1 つのコマンドで最大 5 つのインターフェイス範囲を定義できます。

port-range タイプおよびインターフェイスの有効値は次のとおりです。

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

- **gigabitethernet** stack member/module/{*first port*} - {*last port*} (module は常に 0)
物理インターフェイスの場合
 - stack member は、スタック内のスイッチ識別に使用する番号です。番号に指定できる範囲は 1 ～ 9 で、スタック メンバーの最初の初期化の際に、スイッチに割り当てられます。
 - module は常に 0 です。
 - 使用可能範囲は、*type stack member/0/number - number* です (例: **gigabitethernet 1/0/1 - 2**)。
- **port-channel** port-channel-number - port-channel-number (*port-channel-number* の範囲は 1 ～ 48)



(注) ポート チャンネルを指定して **interface range** コマンドを使用する場合、範囲内の最初と最後のポート チャンネル番号はアクティブなポート チャンネルとする必要があります。

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 gigabitethernet1/0/1 -2
```

複数の範囲を定義するときは、カンマ (,) の前に入力される最初のエントリのあとにもスペースが必要です。

```
interface range fastethernet1/0/1 - 2, gigabitethernet1/0/1 - 2
```

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。

port-range に 1 つのインターフェイスを指定することもできます。その場合、コマンドの内容は **interface interface-id** グローバル コンフィギュレーション コマンドと同様になります。

インターフェイスの範囲の設定に関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、**interface range** コマンドを使用して、インターフェイス レンジ 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適用する方法を示します。

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

次の例では、同じ機能に対して 1 つのポート範囲マクロ *macro1* を使用方法を示します。この利点は、*macro1* を削除するまで再利用できることです。

```
Switch(config)# define interface-range macro1 gigabitethernet1/0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイス レンジのマクロを作成します。
show running-config	スイッチの現在の実行コンフィギュレーション情報を表示します。構文情報については、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択してください。

interface vlan

動的な Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) へのアクセス、または作成を行い、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、スイッチ スタックまたはスタンドアロン スイッチ上で **interface vlan** グローバル コンフィギュレーション コマンドを使用します。SVI を削除する場合は、このコマンドの **no** 形式を使用します。

```
interface vlan vlan-id
```

```
no interface vlan vlan-id
```

シンタックスの説明

<i>vlan-id</i>	VLAN (仮想 LAN) 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

SVI は、特定の VLAN に対して、初めて **interface vlan *vlan-id*** コマンドを入力すると作成されます。*vlan-id* は、ISL (スイッチ間リンク) 上のデータ フレーム、IEEE 802.1Q カプセル化トランク、またはアクセス ポートで設定された VLAN ID と関連した VLAN タグに対応します。



(注) SVI を作成しても物理ポートと関連付けられるまでアクティブにはなりません。

no interface vlan *vlan-id* コマンドを入力して SVI を削除した場合、削除されたインターフェイスは **show interfaces** イネーブル EXEC コマンドからの出力には表示されなくなります。



(注) VLAN 1 のインターフェイスは削除できません。

削除した SVI は、削除したインターフェイスに対して **interface vlan *vlan-id*** コマンドを入力することで、元に戻すことができます。インターフェイスは元に戻りますが、前の設定内容は消えてしまいます。

スイッチスタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響がでる可能性もあります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用し、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てできます。詳細は、**sdm prefer** コマンドを参照してください。

■ interface vlan

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

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

設定を確認するには、**show interfaces** および **show interfaces 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 interfaces vlan vlan-id	すべてのインターフェイスまたは指定の VLAN の管理ステータスおよび動作ステータスを表示します。

ip access-group

レイヤ 2 またはレイヤ 3 インターフェイスへのアクセスを制御するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip 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のアクセス グループ、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 | out}
```

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

シンタックスの説明

<i>access-list-number</i>	IP Access Control List (ACL; アクセス制御リスト) の番号。指定できる範囲は 1 ～ 199、または 1300 ～ 2699 です。
<i>name</i>	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
in	着信パケットに対するフィルタリングを指定します。
out	発信パケットに対するフィルタリングを指定します。このキーワードは、レイヤ 3 のインターフェイス上でのみ有効です。

デフォルト

インターフェイスにアクセス リスト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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	コマンドのサポートがレイヤ 2 インターフェイスまで拡張されました。

使用上のガイドライン

インターフェイスに、名前付き、番号付き標準 IP アクセス リストまたは拡張 IP アクセス リストを適用できます。名前によるアクセス リストを定義する場合、**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 リストを定義する場合、**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。標準アクセス リストの範囲は 1 ～ 99 および 1300 ～ 1999、または拡張アクセス リストの範囲は 100 ～ 199 および 2000 ～ 2699 の番号を使用できます。

このコマンドを使用し、アクセス リストをレイヤ 2 またはレイヤ 3 のインターフェイスに適用できます。ただし、レイヤ 2 のインターフェイス（ポート ACL）には、次のような制限があることに注意してください。

- ACL は着信方向に対してのみ適用できます。**out** キーワードはレイヤ 2 のインターフェイスでサポートされていません。
- インターフェイスごとの IP ACL および MAC（メディア アクセス制御）ACL は 1 つずつのみ適用できます。
- レイヤ 2 のインターフェイスはロギングをサポートしていません。**log** キーワードが IP ACL で指定された場合、無視されます。
- レイヤ 2 のインターフェイスに適用された IP ACL は、IP パケットのみをフィルタにかけます。非 IP パケットにフィルタをかける場合、**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 MAC 拡張 ACL で使用します。

ユーザは同一のスイッチ上で、ルータ ACL、入力ポート ACL、VLAN（仮想 LAN）マップを使用できます。ただし、ポートの ACL はルータの ACL または VLAN マップより優先されます。

- 入力ポートの ACL がインターフェイスに適用され、さらにインターフェイスがメンバーとなっている VLAN に VLAN マップが適用された場合、ACL のポート上で受信した着信パケットは、そのポート ACL でフィルタリングにかけられます。他のパケットは VLAN マップのフィルタが適用されます。
- 入力ルータの ACL および入力ポートの ACL が Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。他のポートで受信した着信ルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信ルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタのみが適用されます。他のポートで受信した着信ルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタのみ適用されます。
- VLAN マップ、出力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタのみが適用されます。発信ルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタのみ適用されます。

IP の ACL は、発信または着信のレイヤ 3 インターフェイス両方に適用できます。

レイヤ 3 のインターフェイスでは、IP の ACL を各方向に 1 つ適用できます。

VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつのみ設定できます。

通常の着信アクセス リストでは、スイッチがパケットを受信したあと、アクセス リストと照合することでパケットの送信元アドレスを確認します。IP の拡張アクセス リストはオプションで、宛先 IP アドレスやプロトコル タイプ、ポート番号など、パケットの他のフィールドの部分を確認できます。アクセス リストがパケットを許可した場合、スイッチはパケットの処理を継続します。アクセス リストがパケットを拒否した場合、スイッチはパケットを廃棄します。アクセス リストがレイヤ 3 インターフェイスに適用された場合、パケットの廃棄にともない（デフォルト設定）、Internet Control Message Protocol (ICMP) Host Unreachable メッセージが生成されます。ICMP Host Unreachable メッセージは、レイヤ 2 インターフェイスで廃棄されたパケットに対しては生成されません。

通常の発信アクセス リストでは、パケットを受信して、それを制御されたインターフェイスへ送信したあと、スイッチがアクセス リストと照合することでパケットを確認します。アクセス リストがパケットを許可した場合、スイッチはパケットを送信します。アクセス リストがパケットを拒否した場合、スイッチはパケットを廃棄し、デフォルトの設定では、ICMP Host Unreachable メッセージが生成されます。

指定のアクセス リストが存在しない場合、すべてのパケットが通過します。

例

次の例では、IP アクセス リスト 101 をポートの着信パケットに適用する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
```

設定を確認するには、**show ip interface**、**show access-lists**、または **show ip access-lists** イネーブル EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>access list</code>	番号付けされた 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。
<code>ip access-list</code>	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。
<code>show access-lists</code>	スイッチで設定される ACL を表示します。
<code>show ip access-lists</code>	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。
<code>show ip interface</code>	インターフェイスのステータスおよび設定情報を表示します。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、各 Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) の IP アドレス、レイヤ 3 スイッチのルーテッド ポートの IP アドレスを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ip 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**]

シンタックスの説明

<i>ip-address</i>	IP アドレス
<i>subnet-mask</i>	関連する IP サブネットのマスク
secondary	(任意) 設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

デフォルト

IP アドレスは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

Telnet セッションで、スイッチの IP アドレスを削除した場合、スイッチとの接続が切断されます。

ホストは Internet Control Message Protocol (ICMP) Mask Request メッセージを使用してサブネット マスクを判断できます。ルータは、この ICMP Mask Reply メッセージの要求に対して応答します。

no ip address コマンドを使って IP アドレスを削除することで、特定のインターフェイス上の IP 処理をディセーブルにできます。スイッチが、その IP アドレスのうちの 1 つを使用している他のホストを検出した場合、コンソールにエラー メッセージを送信します。

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないことを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求は適切に処理され、インターフェイスも IP のルーティング テーブルでルーティングされます。



(注)

ネットワーク セグメント上のすべてのルータがセカンダリ アドレスを使用した場合、同一のセグメント上にある他の装置も、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスに整合性がないと、すぐにルーティングでループが発生します。

Open Shortest Path First (OSPF) のルーティングの場合、インターフェイスのすべてのセカンダリ アドレスが、プライマリ アドレスと同一の OSPF 領域にあることを確認してください。

スイッチが、Bootstrap Protocol (BOOTP) または Dynamic Host Configured Protocol (DHCP) サーバから IP アドレスを受信し、そのスイッチ IP アドレスを **no ip address** コマンドで削除した場合、IP 処理はディセーブルとなり、BOOTP 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。

レイヤ 3 スイッチは、各ルーテッドポートおよび SVI に割り当てられた IP アドレスを持つことができます。設定するルーテッドポートおよび SVI の数はソフトウェアでは制限されていません。ただし、この数と設定された他の機能の数との相互関係によっては、ハードウェア制限により、CPU 使用率に影響がでる可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用し、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てできます。詳細は、**sdm prefer** コマンドを参照してください。

例

次の例では、サブネット ネットワークでレイヤ 2 スイッチの IP アドレスを設定する方法を示します。

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

次の例では、レイヤ 3 スイッチ上のポートに IP アドレスを設定する方法を示します。

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

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 arp inspection filter vlan

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査がイネーブルの場合、スタティック IP アドレスが設定されたホストからの ARP 要求および応答を許可または拒否するには、スイッチ スタックまたはスタンドアロン スイッチで **ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection filter arp-acl-name vlan vlan-range [static]

no ip arp inspection filter arp-acl-name vlan vlan-range [static]

シンタックスの説明

<i>arp-acl-name</i>	ARP Access Control List (ACL; アクセス制御リスト) 名。
<i>vlan-range</i>	VLAN (仮想 LAN) 番号または VLAN 範囲 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ~ 4094 です。
static	(任意) ARP ACL の暗黙的拒否を明示的拒否として扱い、ACL 内の以前のコマンドと一致しないパケットを廃棄するには、 static を指定します。Dynamic Host Configuration Protocol (DHCP) バインディングは、使用されません。 このキーワードを指定しない場合は、パケットを拒否する ACL に明示的拒否が存在しないということになり、パケットが ACL 内のコマンドと一致しない場合には、DHCP バインディングがパケットを許可するか拒否するかを決定します。

デフォルト

定義された ARP ACL は、いずれの VLAN にも適用されません。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン

ARP ACL が、ダイナミック ARP 検査用に VLAN に適用される場合、IP から MAC (メディアアクセス制御) へのアドレスを含む ARP パケット バインディングだけが ACL に照合されます。ACL がパケットを許可すると、スイッチがこれを転送します。その他のすべてのタイプのパケットは、確認されずに入力 VLAN にブリッジされます。

明示的な拒否ステートメントによりスイッチがパケットを拒否した場合、このパケットは廃棄されます。暗黙的な拒否ステートメントによりスイッチがパケットを拒否した場合、パケットは DHCP バインディングのリストに照合されます (ACL がスタティックでない場合のみ。スタティックの場合は、パケットはバインディングに照合されません)。

ARP ACL を定義する、または以前定義されたリストの最後にコマンドを追加するには、**arp access-list acl-name** グローバル コンフィギュレーション コマンドを使用します。

例 次の例では、ダイナミック ARP 検査用に ARP ACL *static-hosts* を VLAN 1 に適用する方法を示します。

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

設定を確認するには、**show ip arp inspection vlan 1** 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
arp access-list	ARP ACL を定義します。
deny (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングとの照合に基づいた ARP パケットを拒否します。
permit (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングとの照合に基づいた ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細情報を表示します。
show inventory vlan vlan-range	指定された VLAN 用のダイナミック ARP 検査の設定および動作ステータスを表示します。

ip arp inspection limit

インターフェイス上の着信 Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求および応答のレートを制限するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。これにより、DoS 攻撃の場合にダイナミック ARP 検査でスイッチ リソースをすべて消費してしまう状況が避けられます。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。

ip arp inspection limit {rate pps [burst interval seconds] | none}

no ip arp inspection limit

シンタックスの説明

rate pps	1 秒あたりに処理される着信パケット数の上限を指定します。指定できる範囲は 0 ～ 2048 pps (パケット / 秒) です
burst interval seconds	(任意) インターフェイスを高いレートの ARP パケットに関してモニタする連続した間隔 (秒) を指定します。指定できる範囲は 1 ～ 15 秒です。
none	処理が可能な着信 ARP パケットのレートの上限は、指定されません。

デフォルト

レートは、信頼性のないインターフェイス上で 15 pps です。この場合ネットワークは、毎秒 15 くらいの新しいホストと接続しているホストを持つスイッチドネットワークであることが前提です。

レートは、すべての信頼性のあるインターフェイス上で無制限です。

バースト間隔は 1 秒です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

レートは、信頼性があるインターフェイスおよび信頼性がないインターフェイスの両方で適用されます。トランクに適切なレートを設定して、ダイナミック ARP 検査がイネーブルな複数の VLAN のパケットを処理します。または、**none** キーワードを使用して、レートを無制限にします。

スイッチが、バースト期間 (秒) に毎秒連続して設定されたレート以上のパケットを受信すると、インターフェイスは **errdisable** ステートになります。

インターフェイスで明示的にレート制限を設定していない場合は、インターフェイスで信頼状態が変更されると、レート制限もまたその信頼状態のデフォルト値に変更されます。レート制限が設定されると、信頼状態が変更された場合でも、インターフェイスはそのレート制限を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

より高いレートのトランク ポートには、その集約を反映させるよう設定する必要があります。着信パケットのレートが、ユーザ設定のレートを超えた場合、スイッチはインターフェイスを **errdisable** ステートにします。**errdisable** 回復機能により、ポートは **errdisable** ステートから回復設定に従って自動的に削除されます。

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

EtherChannel ポートの着信 ARP パケット レートは、すべてのチャネル メンバーからの着信 ARP パケット レートの合計と同等になります。すべてのチャネル メンバー上の着信 ARP パケット レートを調べた場合に限り、EtherChannel ポートのレート制限を設定してください。

例

次の例では、ポート上の着信 ARP 要求のレートを 25 pps に制限し、インターフェイス モニタリングの間隔を連続 5 秒に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

設定を確認するには、**show ip arp inspection interfaces interface-id** 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 inventory interfaces	指定されたインターフェイス、またはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。

ip arp inspection log-buffer

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査のロギング バッファを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip arp inspection log-buffer** イネーブル EXEC コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection log-buffer {entries number | logs number interval seconds}

no ip arp inspection log-buffer {entries | logs}

シンタックスの説明

entries number	バッファにロギングされるエントリ数。指定できる範囲は、0 ～ 1024 です。
logs number interval seconds	システム メッセージを生成するのに必要な指定された間隔のエントリ数 logs number に指定できる範囲は 0 ～ 1024 です。値が 0 の場合、エントリはロギング バッファにあります。システム メッセージは生成されないことを意味します。 interval seconds に指定できる範囲は 0 ～ 86400 秒 (1 日) です。値が 0 の場合、システム メッセージがただちに生成される (およびロギング バッファは常に空である) ことを意味します。

デフォルト

ダイナミック ARP 検査がイネーブルの場合、拒否された、または廃棄された ARP パケットがロギングされます。

ログ エントリの数は 32 です。

システム メッセージ数は、毎秒 5 つに制限されています。

ロギングレート間隔は、1 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

logs および **interval** キーワードには、0 の値は許可されません。

logs および **interval** の設定は、相互作用します。**logs number X** が **interval seconds Y** よりも大きい場合、X を Y で除算した数 (X/Y) のシステム メッセージが、毎秒送信されます。X が Y 以下の場合、Y を X で除算した数 (Y/X) 秒ごとに、1 つのシステム メッセージが送信されます。たとえば、**logs number** が 20 で、**interval seconds** が 4 の場合、ロギング バッファにエントリがある場合でも、スイッチは毎秒 5 つのエントリのシステム メッセージを生成します。

1 つのロギング バッファ エントリで、複数のパケットを表せます。たとえば、インターフェイスが同じ ARP パラメータを持つ同じ VLAN (仮想 LAN) 上で多量のパケットを受信した場合、スイッチはパケットをロギング バッファ内の 1 つのエントリとして組み合わせて、システム メッセージを単一のエントリとして生成します。

ロギング バッファがオーバーフローの場合は、ログ イベントがロギング バッファのサイズに適合していないことを意味し、**show ip arp inspection log** イネーブル EXEC コマンドの表示が影響されます。表示中の A -- は、パケット カウントおよび時間以外のすべてのデータの代わりに表示されます。エントリには、その他の統計情報は提供されません。表示中にこのエントリがある場合は、ロギング バッファのエントリ数を増やすか、ロギング レートを上げてください。

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

例 次の例では、ロギング バッファが最大 45 エントリを維持するよう設定する方法を示します。

```
Switch(config)# ip arp inspection log-buffer entries 45
```

次の例では、ロギング レートを 4 秒当たり 20 ログ エントリに設定する方法を示します。この設定では、ロギング バッファにエントリがある場合でも、スイッチは毎秒 5 つのエントリのシステム メッセージを生成します。

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

設定を確認するには、**show ip arp inspection log** 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
arp access-list	ARP Access Control List (ACL; アクセス制御リスト) を定義します。
clear ip arp inspection log	ダイナミック ARP 検査のロギング バッファをクリアします。
ip arp inspection vlan logging	VLAN 単位で記録されたパケット タイプを制御します。
show inventory log	ダイナミック ARP 検査のロギング バッファの設定および内容を表示します。

ip arp inspection trust

検査される着信 Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを決定する信頼状態を、インターフェイスに設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト インターフェイスには、信頼性がありません。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン スイッチでは、ARP パケットが信頼性のあるインターフェイス上で受信したことを確認せず、単にパケットを転送します。

信頼性のないインターフェイスでは、スイッチはすべての ARP 要求および応答を代行受信します。スイッチは、代行受信したパケットが有効な IP から MAC (メディア アクセス制御) アドレス バインディングを持っていることを確認してから、ローカル キャッシュを更新し、パケットを適切な宛先に転送します。スイッチは、無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング コンフィギュレーションに従って、ロギング バッファ内にロギングします。

例 次の例では、ポートを信頼性のある状態に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

設定を確認するには、**show ip arp inspection interfaces interface-id** 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
	ip arp inspection log-buffer	ダイナミック ARP 検査のロギング バッファを設定します。
	show inventory interfaces	指定されたインターフェイス、またはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
	show inventory log	ダイナミック ARP 検査のロギング バッファの設定および内容を表示します。

ip arp inspection validate

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査の特定の確認を実行するには、スイッチスタックまたはスタンドアロン スイッチ上で **ip arp inspection validate** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate [src-mac] [dst-mac] [ip]

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

src-mac	イーサネット ヘッダーの送信元 MAC (メディア アクセス制御) アドレスを、ARP 本体の送信側 MAC アドレスと照合して確認します。確認は、ARP 要求および ARP 応答の両方で実行されます。 イネーブルの場合、異なる MAC アドレスを持つパケットは無効と分類され、廃棄されます。
dst-mac	イーサネット ヘッダーの宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと照合して確認します。この確認は、ARP 応答に実行されます。 イネーブルの場合、異なる MAC アドレスを持つパケットは無効と分類され、廃棄されます。
ip	無効および予想外の IP アドレスと ARP 本体を照合して確認します。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信側 IP アドレスは、すべての ARP 要求および応答で照合されます。ターゲット IP アドレスは、ARP 応答でのみ確認されます。

デフォルト

確認は実行されません。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン

キーワードは、少なくとも 1 つ指定する必要があります。各コマンドは、前のコマンドを上書きします。すなわち、あるコマンドで **src-mac** および **dst-mac** 確認がイネーブルで、その次のコマンドで IP 確認のみがイネーブルの場合、**src-mac** および **dst-mac** 確認は、次のコマンドのためにディセーブルになります。

最初に **src-mac** キーワードを指定した場合は、**dst-mac** および **ip** キーワードも指定できます。最初に **ip** キーワードを指定した場合は、ほかのキーワードを指定できません。

このコマンドの **no** 形式は、指定された確認をディセーブルにするだけです。イネーブルのオプションがない場合は、すべての確認がディセーブルになります。

例

次の例では、送信元 MAC 確認をイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection validate src-mac
```

設定を確認するには、**show ip arp inspection vlan *vlan-range*** 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 inventory vlan <i>vlan-range</i>	指定された VLAN（仮想 LAN）用のダイナミック ARP 検査の設定および動作ステータスを表示します。

ip arp inspection vlan

VLAN（仮想 LAN）単位で、ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip arp inspection vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image（EMI）と呼ばれていました。

シンタックスの説明

<i>vlan-range</i>	VLAN 番号または VLAN 範囲 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。

デフォルト

すべての VLAN で ARP 検査はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

ダイナミック ARP 検査をイネーブルとする VLAN を指定する必要があります。

ダイナミック ARP 検査は、アクセス ポート、トランク ポート、EtherChannel ポート、またはプライベート VLAN ポートでサポートされています。

例

次の例では、ダイナミック ARP 検査を VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection vlan 1
```

設定を確認するには、**show ip arp inspection vlan *vlan-range*** 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
arp access-list	ARP Access Control List（ACL; アクセス制御リスト）を定義します。
show inventory vlan <i>vlan-range</i>	指定された VLAN 用のダイナミック ARP 検査の設定および動作ステータスを表示します。

ip arp inspection vlan logging

VLAN（仮想 LAN）単位でロギングされるパケット タイプを制御するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。このロギング制御をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}
```

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image（EMI）と呼ばれていました。

シンタックスの説明

<i>vlan-range</i>	ロギングを設定する VLAN を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
acl-match {matchlog none}	パケットのロギングが Access Control List (ACL; アクセス制御リスト) に基づいて行われるよう指定します。 キーワードの意味は次のとおりです。 matchlog — Access Control Entry (ACE; アクセス制御エントリ) で指定されたロギング コンフィギュレーションに基づいたログ パケット。このコマンドで matchlog キーワードを指定、および permit または deny Address Resolution Protocol (ARP; アドレス解決プロトコル) アクセスリスト コンフィギュレーション コマンドで log キーワードを指定すると、ACL で許可または拒否された ARP パケットが、ロギングされます。 none — ACL と一致するパケットをロギングしません。
dhcp-bindings {permit all none}	パケットのロギングは、Dynamic Host Configuration Protocol (DHCP) バインディング照合に基づいて行われるよう指定します。 キーワードの意味は次のとおりです。 all — DHCP バインディングに一致するすべてのパケットをロギングします。 none — DHCP バインディングと一致するパケットをロギングしません。 permit — DHCP バインディングで許可されたパケットをロギングします。

デフォルト

すべての拒否された、またはすべての廃棄されたパケットがロギングされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

logged という用語は、エントリがログ バッファに置かれ、システム メッセージが生成されることを意味します。

acl-match および **dhcp-bindings** キーワードは、互いに組み合わせて使用できます。すなわち、ACL 一致を設定する場合は、DHCP バインディング コンフィギュレーションはディセーブルにはなりません。ロギング基準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。いずれのオプションも指定されていない場合、ARP パケットが拒否されると、すべてのタイプのロギングがログにリセットされます。オプションは、次のとおりです。

- **acl-match** — ACL 一致でのロギングは、拒否でのロギングにリセットされます。
- **dhcp-bindings** — DHCP バインディングでのロギングは、拒否でのロギングにリセットされます。

acl-match または **dhcp-bindings** キーワードがどちらとも指定されない場合は、拒否されたパケットすべてが、ロギングされます。

ACL の最後付近の暗黙的な拒否には、**log** キーワードが含まれます。これは、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドで **static** キーワードを使用すると、ACL が DHCP バインディングを上書きするという意味です。ARP ACL の最後で **deny ip any mac any log** ACE を明示的に指定しないかぎり、拒否されたパケットがロギングされる場合があります。

例

次の例では、VLAN 1 に ARP 検査を設定して、ACL の **permit** コマンドと一致するパケットをロギングする方法を示します。

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

設定を確認するには、**show ip arp inspection vlan vlan-range** 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
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査のロギング バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査のロギング バッファを設定します。
show inventory log	ダイナミック ARP 検査のロギング バッファの設定および内容を表示します。
show inventory vlan vlan-range	指定された VLAN 用のダイナミック ARP 検査の設定および動作ステータスを表示します。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping

no ip dhcp snooping

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピングはディセーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、DHCP スヌーピングをグローバルにイネーブル化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）でスヌーピングをイネーブルにしないと、DHCP スヌーピングはアクティブになりません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping
```

設定を確認するには、**show ip dhcp snooping** 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
ip dhcp snooping vlan	VLAN（仮想 LAN）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

Dynamic Host Configuration Protocol (DHCP) スヌーピング バインディング データベースを設定して、バインディング エントリをデータベースに追加するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping 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場合は、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

このコマンドは、スイッチで IP サービスが動作している場合に限り使用できます。IP サービスは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

<i>mac-address</i>	MAC (メディア アクセス制御) アドレスを指定します。
<i>vlan vlan-id</i>	VLAN (仮想 LAN) 番号を指定します。指定できる範囲は、1 ～ 4094 です。
<i>ip-address</i>	IP アドレスを指定します。
<i>interface interface-id</i>	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。
<i>expiry seconds</i>	バインディング エントリが有効でなくなる間隔 (秒) を指定します。指定できる範囲は、1 ～ 4294967295 です。

デフォルト

デフォルトのデータベースは定義されていません。

コマンド モード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

スイッチのテストまたはデバッグを行う際は、このコマンドを使用します。

DHCP スヌーピング バインディング データベースで、各データベース エントリ (バインディング) には、IP アドレス、対応する MAC アドレス、リース時間 (16 進数)、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、最大 8192 のバインディングを含めます。

設定されたバインディングのみを表示するには、**show ip dhcp snooping binding** イネーブル EXEC コマンドを使用します。ダイナミックおよびスタティックに設定されたバインディングのみを表示するには、**show ip source binding** イネーブル EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポート上で期限切れの時間が 1000 秒の DHCP バインディング コンフィギュレーションを生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/0/1 expiry 1000
```

設定を確認するには、**show ip dhcp snooping binding** または **show ip dhcp source binding** 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
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 データベースのダイナミックに設定されたバインディング、および設定情報を表示します。
show ip source binding	DHCP スヌーピング バインディング データベースのダイナミックおよびスタティックに設定されたバインディングを表示します。

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 エージェントまたはバインディング ファイルを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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にする、タイムアウト値をリセットする、または書き込み遅延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[number]:/filename | ftp://user:password@host/filename |
http://[[username:password]@]{hostname | host-ip}/{/directory}/image-name.tar |
rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}
```

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

このコマンドは、スイッチで IP サービスが動作している場合に限り使用できます。IP サービスは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

flash[number]:/filename	データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。 (任意) スタック マスターのスタック メンバー番号を指定するには、 <i>number</i> パラメータを使用します。 <i>number</i> に指定できる範囲は 1 ～ 9 です。
ftp://user:password@host/filename	データベース エージェントまたはバインディング ファイルが FTP (ファイル転送プロトコル) サーバにあることを指定します。
http://[[username:password]@]{hostname host-ip}/{/directory}/image-name.tar	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
rcp://user@host/filename	データベース エージェントまたはバインディング ファイルが Remote Control Protocol (RCP) 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 Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバにあることを指定します。
timeout seconds	データベース転送プロセスが完了するのを待ち、一定時間が経過したら停止させるための時間 (秒単位) を指定します。 デフォルト値は 300 秒です。指定できる範囲は 0 ～ 86400 です。無制限の時間を定義するには 0 を使用します。この場合、無限に転送の試行を継続します。

write-delay seconds	バインディング データベースの変更後、転送が遅延される必要のある期間 (秒) 指定します。デフォルト値は 300 秒です。指定できる範囲は、15 ～ 86400 です。

デフォルト

データベース エージェントまたはバインディング ファイルの URL は、定義されていません。

タイムアウト値は 300 秒 (5 分) です。

書き込み遅延値は 300 秒 (5 分) です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング バインディング データベースには、最大 8192 のバインディングを含めます。

データベースのリース時間を正確なものにするために、Network Time Protocol (NTP) をイネーブルに設定し、次の機能がイネーブルでかつ設定されてい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 パケットの送信元 IP アドレス

NTP が設定されている場合、スイッチは、スイッチ システム クロックが NTP と同期化されているときにのみ、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 (不揮発性メモリ) およびフラッシュ メモリのストレージ容量には制限があるため、バインディング ファイルを TFTP サーバに保存することを推奨します。ネットワークベースの URL (TFTP および FTP など) 上の設定された URL に空のファイルを作成する必要があります。その後初めて、スイッチはこの URL でバインディング ファイルにバインディングを書き込みます。

DHCP スヌーピング バインディング データベースをスタック マスター NVRAM に保存するには、**ip dhcp snooping database flash[number]:filename** コマンドを使用します。データベースは、スタック メンバー NVRAM に保存されません。

ip dhcp snooping database timeout コマンドを 0 秒に設定した状態でデータベースが TFTP ファイルに書き込まれる場合、TFTP サーバがダウンすると、データベース エージェントが無制限に転送の試行を継続します。この処理の続行中は、他の転送は開始できません。サーバがダウンするとファイルの書き込みは行えないため、このことは大して重要ではありません。

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

タイムアウト値をリセットするには、**no ip dhcp snooping database timeout** コマンドを使用します。

書き込み遅延値をリセットするには、**no ip dhcp snooping database write-delay** コマンドを使用します。

例

次の例では、*directory* というディレクトリにある IP アドレス 10.1.1.1 で、バインディング ファイルを保存する方法を示します。*file* という名前のファイルは、TFTP サーバ上にあるものとします。

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

次の例では、スタック マスター NVRAM に *file01.txt* というバインディング ファイルを保存する方法を示します。

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

設定を確認するには、**show ip dhcp snooping database** 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
ip dhcp snooping	VLAN（仮想 LAN）上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping information option

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、スイッチ スタックまたはスタンドアロン スイッチで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。DHCP オプション 82 データ挿入をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option

no ip dhcp snooping information option

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP オプション 82 データが挿入されます。

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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用して DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルで、スイッチが DHCP 要求をホストから受信した場合、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）およびパケットを受信したポート ID、**vlan-mod-port**（回線 ID サブオプション）が含まれています。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、IP アドレスの割り当てや、単一のリモート ID や回線 ID に割り当て可能な IP アドレス数の制限といったポリシーの適用に、リモート ID、回線 ID、またはこの両方を使用できます。DHCP サーバは DHCP 応答のオプション 82 フィールドをエコーします。

DHCP サーバは、スイッチによって要求がサーバにリレーされた場合に、スイッチへの応答をユニキャストします。クライアントおよびサーバが同じサブネット上にある場合、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 と、可能であれば回線 ID を検査して、初めからオプション 82 データが挿入されていたかを確認します。スイッチはオプション 82 フィールドを削除し、DHCP 要求を送信した DHCP ホストに接続しているスイッチ ポートにそのパケットを転送します。

例

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

```
Switch(config)# ip dhcp snooping information option
```

設定を確認するには、**show ip dhcp snooping** 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 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

アグリゲーション スイッチが、エッジ スイッチに接続される可能性のある信頼性のないポートで受信される、オプション 82 情報を持つ Dynamic Host Configuration Protocol (DHCP) パケットを受け取るように設定するには、アグリゲーション スイッチ上で **ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、エッジ スイッチに接続される可能性のある信頼性のないポートで受信する、オプション 82 情報を持つ DHCP パケットを廃棄します。

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)SEA	このコマンドが導入されました。

使用上のガイドライン

ネットワーク エッジでは、ホストが接続されているエッジ スイッチにより DHCP オプション 82 情報を挿入する場合があります。また、アグリゲーション スイッチ上で DHCP スヌーピング、IP ソース ガード、またはダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査などの DHCP セキュリティ機能をイネーブルにする場合もあります。ただし、アグリゲーション スイッチ上で DHCP スヌーピングがイネーブルの場合、スイッチは信頼性の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、信頼性のあるインターフェイス上で接続された装置の DHCP スヌーピング バインディングを学習しません。

ホストが接続されているエッジ スイッチでオプション 82 情報を挿入し、アグリゲーション スイッチ上で 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 スイッチが信頼性のないポート上で DHCP スヌーピング パケットを受信した場合でも、アグリゲーション スイッチはホストのバインディングを学習できます。また、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、信頼性のあるポートとして設定される必要があります。



(注)

信頼性のない装置が接続されているアグリゲーション スイッチでは、**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した場合、信頼性のない装置がオプション 82 情報をスプーフィングする可能性があります。

例 次の例では、アクセス スイッチでエッジ スイッチからの信頼性のないパケットのオプション 82 情報を確認せずに、そのパケットを受け取るよう設定する方法を示します。

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

設定を確認するには、**show ip dhcp snooping** 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 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秒あたりに受信可能な Dynamic Host Configuration Protocol (DHCP) メッセージの数を設定するには、スイッチ スタックまたはスタンドアロン スイッチで **ip dhcp snooping limit rate** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping limit rate rate

no ip dhcp snooping limit rate

シンタックスの説明

<i>rate</i>	インターフェイスが1秒あたりに受信可能な DHCP メッセージ数。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
12.1(19)EA1	このコマンドが導入されました。
12.2(18)SE	指定できる範囲が 1 ～ 2048 に変更されました。

使用上のガイドライン

通常、レート制限は信頼性のないインターフェイスに適用されます。信頼性のあるインターフェイスにレート制限を設定したい場合、信頼性のあるインターフェイスはスイッチ内にある（スヌーピングされていないものも含む）複数の VLAN（仮想 LAN）上の DHCP トラフィックを集計する場合があります。インターフェイスのレート制限を高めめの値に調整する必要がある点に留意してください。

レート制限を超過した場合、インターフェイスは **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、すべての原因がタイムアウトになると、インターフェイスは動作を再試行します。エラー回復メカニズムをイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで **errdisable** ステータスに置かれます。

例

次の例では、メッセージのレート制限をインターフェイスで1秒あたり150メッセージに設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

設定を確認するには、**show ip dhcp snooping** 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	回復メカニズムを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping trust

Dynamic Host Configuration Protocol (DHCP) スヌーピングのためにポートを信頼性があるものとして設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping trust

no ip dhcp snooping trust

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピング信頼性はディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

DHCP サーバまたは他のスイッチやルータに接続されたポートは信頼性のあるポートとして設定します。DHCP クライアントに接続されたポートは信頼性のないポートとして設定します。

例

次の例では、特定のポート上で DHCP スヌーピング信頼性をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

設定を確認するには、**show ip dhcp snooping** 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 ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping verify

スイッチが、信頼性のないポート上で Dynamic Host Configuration Protocol (DHCP) パケットの送信元 MAC (メディア アクセス制御) アドレスがクライアントのハードウェアアドレスと一致することを確認するよう設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping verify** グローバル コンフィギュレーション コマンドを使用します。スイッチで MAC アドレスを確認しないように設定する場合は、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト スイッチは、信頼性のないポートで受信した DHCP パケット内の送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスに一致することを確認します。

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(18)SE	このコマンドが導入されました。

使用上のガイドライン サービスプロバイダーのネットワークでは、スイッチが信頼性のないポートで DHCP クライアントからのパケットを受信すると、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どうか自動的に確認されます。アドレスが一致した場合、パケットは転送されます。アドレスが一致しない場合、パケットは廃棄されます。

例 次の例では、MAC アドレスの確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

設定を確認するには、**show ip dhcp snooping** 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 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）で Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

シンタックスの説明

vlan <i>vlan-range</i>	DHCP スヌーピングをイネーブルにする VLAN ID または VLAN の範囲を指定します。指定できる範囲は、1 ～ 4094 です。 単一の VLAN ID を入力する場合は、VLAN ID 番号で識別される VLAN ID を入力します。複数の VLAN ID を入力する場合はカンマで区切ります。VLAN ID を範囲指定する場合は、ハイフンで区切るか、開始の VLAN ID と終了の VLAN ID をスペースで区切って入力します。

デフォルト

すべての VLAN で 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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

VLAN で DHCP スヌーピングをイネーブルにするには、まず DHCP スヌーピングをグローバルにイネーブルにする必要があります。

例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

設定を確認するには、**show ip dhcp snooping** 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 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

インターフェイスに Internet Group Management Protocol (IGMP) を適用することで、レイヤ 2 インターフェイス上のすべてのホストが 1 つまたは複数の IP マルチキャスト グループに加入できるかどうかを制御するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*

no ip igmp filter

シンタックスの説明	<i>profile number</i> 適用する IGMP プロファイル番号。指定できる範囲は、1 ～ 4294967295 です。

デフォルト	IGMP のフィルタは適用されていません。

コマンド モード	インターフェイス コンフィギュレーション

コマンド履歴	<table border="1"> <tr> <th>リリース</th> <th>変更内容</th> </tr> <tr> <td>12.1(11)AX</td> <td>このコマンドが導入されました。</td> </tr> </table>	リリース	変更内容	12.1(11)AX	このコマンドが導入されました。
リリース	変更内容				
12.1(11)AX	このコマンドが導入されました。				

使用上のガイドライン	IGMP フィルタはレイヤ 2 の物理インターフェイスのみに適用できます。ルーテッド ポート、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、または EtherChannel グループに属するポートに対しては IGMP フィルタを適用できません。

IGMP のプロファイルは 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 つのポートに対して 1 つのプロファイルのみ適用できます。

例	次の例では、ポートに IGMP プロファイルの 22 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 22
```

設定を確認するには、**show running-config** イネーブル EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド	<table border="1"> <tr> <th>コマンド</th> <th>説明</th> </tr> <tr> <td>ip igmp profile</td> <td>指定の IGMP プロファイル番号を設定します。</td> </tr> <tr> <td>show ip igmp profile</td> <td>指定の IGMP プロファイルの特性を表示します。</td> </tr> <tr> <td>show running-config interface <i>interface-id</i></td> <td>スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択してください。</td> </tr> </table>	コマンド	説明	ip igmp profile	指定の 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 <i>interface-id</i>	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択してください。
コマンド	説明								
ip igmp profile	指定の 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 <i>interface-id</i>	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択してください。								

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能な Internet Group Management Protocol (IGMP) グループの最大数を設定したり、転送テーブル内でエントリが最大数に達する場合の IGMP スロットリング動作を設定したりするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数を制限なしのデフォルト設定に戻したり、レポートを廃棄するデフォルトのスロットリング動作に戻したりするには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

number	インターフェイスが加入できる IGMP グループの最大数。指定できる範囲は 0 ～ 4294967294 です。デフォルトの設定は無制限です。
action deny	IGMP スヌーピング転送テーブル内のエントリが最大数に達すると、次の IGMP 加入レポートを廃棄します。これがデフォルトの動作になります。
action replace	IGMP スヌーピング転送テーブル内のエントリが最大数に達すると、既存のグループが、IGMP レポートを受信した新しいグループに変わります。

デフォルト

グループの最大数のデフォルト設定は、無制限です。

スイッチがインターフェイス上の IGMP グループ エントリの最大数を学習したあとに行われるデフォルトのスロットリング動作は、インターフェイスが受信した次の IGMP レポートを廃棄することで、インターフェイスへの 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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	action {deny replace} キーワードが追加されました。

使用上のガイドライン

このコマンドは、レイヤ 2 物理インターフェイスと論理 EtherChannel インターフェイスでのみ使用可能です。ルーテッド ポート、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、または EtherChannel グループに属するポートに対しては IGMP 最大グループを設定できません。

IGMP スロットリング動作を設定するときには、次の注意事項に従ってください。

- スロットリング動作を **deny** と設定して最大グループ制限を設定する場合、すでに転送テーブル内にあるエントリは、削除されませんが期限切れになります。これらのエントリが期限切れになると、転送テーブル内のエントリが最大数に達したときに、スイッチはインターフェイスで受信される次の IGMP レポートを廃棄します。
- スロットリング動作を **replace** と設定して最大グループ制限を設定する場合、すでに転送テーブル内にあるエントリは削除されます。IGMP スヌーピング転送テーブル内のエントリが最大数に達すると、ランダムに選択したマルチキャスト エントリが、受信した IGMP レポートに変わります。
- 最大グループ制限がデフォルト（無制限）に設定されている場合、**ip igmp max-groups {deny | replace}** コマンドを入力しても無効になります。

例

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、IGMP スヌーピング転送テーブル内のエントリが最大数に達したときに、既存のグループを、IGMP レポートを受信した新しいグループに置き換えるよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** イネーブル EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
show running-config interface <i>interface-id</i>	インターフェイスが加入できる IGMP グループの最大数やスロットリング動作など、スイッチのインターフェイス上の実行コンフィギュレーションを表示します。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、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp 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。このモードから、スイッチ ポートの IGMP メンバーシップ レポートをフィルタリングするために使用する、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*

シンタックスの説明

<i>profile number</i>	設定する IGMP プロファイル番号。指定できる範囲は、1 ～ 4294967295 です。

デフォルト

IGMP プロファイルは定義されていません。設定された場合、IGMP プロファイルとの照合におけるデフォルト アクションは、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny** : 一致するアドレスを拒否します (デフォルトの条件)。
- **exit** : IGMP プロファイル コンフィギュレーション モードを終了します。
- **no** : コマンドを無効にする、またはデフォルトにリセットします。
- **permit** : 一致するアドレスを許可します。
- **range** : プロファイルに対する IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

範囲を入力する場合、小さい方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に大きい方の IP マルチキャスト アドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つのみです。

例

次の例では、IP マルチキャスト アドレスの指定の範囲を許可する IGMP プロファイル 40 の設定方法を示します。

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

コマンド設定を確認するには、**show ip igmp profile** イネーブル EXEC コマンドを使用します。

関連コマンド

コマンド	説明
ip igmp filter	指定のインターフェイスに対し、IGMP プロファイルを適用します。
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) スヌーピングをスイッチ上でグローバルにイネーブル、または VLAN (仮想 LAN) ごとにイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [vlan vlan-id]

no ip igmp snooping [vlan vlan-id]

シンタックスの説明

vlan vlan-id	(任意) 指定の VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

デフォルト

スイッチ上で、IGMP スヌーピングはグローバルにイネーブルです。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1
```

コマンド設定を確認するには、**show ip igmp snooping** 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
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	スイッチ上で設定される IGMP クエリアの設定情報および動作情報を表示します。

ip igmp snooping last-member-query-interval

Internet Group Management Protocol (IGMP) の設定可能脱退タイマーをグローバルにまたは VLAN (仮想 LAN) ベースごとにイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [vlan *vlan-id*] last-member-query-interval *time*

no ip igmp snooping [vlan *vlan-id*] last-member-query-interval

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN で IGMP スヌーピングと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 または 1006 ～ 4094 です。
<i>time</i>	タイムアウトする間隔 (秒)。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)SEB	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、IGMP スヌーピングでは使用できません。

VLAN 上で脱退タイマーを設定すると、グローバル設定が上書きされます。

IGMP で設定可能な脱退時間は、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ています。

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 ミリ秒に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
```

コマンド設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan immediate-leave	IGMP 即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをグループのメンバーとして設定します。
show ip igmp snooping	IGMP スヌーピング設定を表示します。

ip igmp snooping querier

レイヤ 2 ネットワークの Internet Group Management Protocol (IGMP) クエリア機能をグローバルにイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp 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。キーワードと合わせてコマンドを使用し、VLAN (仮想 LAN) インターフェイス上で IGMP クエリア機能をイネーブルにして設定します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping querier [vlan vlan-id] [address ip-address | max-response-time response-time |
    query-interval interval-count | tcn query [count count | interval interval] | timer expiry | version
    version]
```

```
no ip igmp snooping querier [vlan vlan-id] [address | max-response-time | query-interval | tcn query
    { count count | interval interval} | timer expiry | version]
```

シンタックスの説明

vlan vlan-id	(任意) 指定の VLAN で IGMP スヌーピングと IGMP クエリア機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
address ip-address	(任意) 送信元 IP アドレスを指定します。IP アドレスを指定しない場合は、クエリアが IGMP クエリアに設定されたグローバルな IP アドレスを使用しようと試みます。
max-response-time response-time	(任意) IGMP クエリアレポートを待つ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 クエリア間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 の間隔で実行される TCN クエリー数を設定します。指定できる範囲は、1 ～ 10 です。 interval interval — TCN クエリー間隔を設定します。指定できる範囲は、1 ～ 255 です。
timer expiry	(任意) IGMP クエリアが期限切れになるまでの時間を設定します。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 を選択してください。

デフォルト

IGMP スヌーピング クエリア機能は、スイッチ上でグローバルにディセーブルに設定されています。

IGMP スヌーピング クエリアがイネーブルの場合に、マルチキャスト対応装置からの 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)SEA	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングをイネーブルにして、IGMP クエリー メッセージを送信する装置（クエリア）の IGMP バージョンおよび IP アドレスを検出する場合は、このコマンドを使用します。

デフォルトでは、IGMP スヌーピング クエリアは IGMP バージョン 2（IGMPv2）を使用する装置を検出するように設定されています。IGMP バージョン 1（IGMPv1）を使用しているクライアントを検出するには設定されていません。装置が IGMPv2 を使用する場合は、手動で **max-response-time** 値を設定できます。装置が IGMPv1 を使用する場合は、**max-response-time** を設定できません（値を設定することはできず、0 に設定されています）。

IGMPv1 が稼働する RFC に準拠しない装置は、**max-response-time** 値が 0 でない値を持つ一般的な IGMP クエリー メッセージを拒否する可能性があります。装置が一般的な IGMP クエリー メッセージを受け取るようにするには、IGMP スヌーピング クエリアで IGMPv1 を稼働するように設定します。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface（FDDI）VLAN 専用で、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピング クエリア機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピング クエリアの間隔を 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
```

コマンド設定を確認するには、**show ip igmp snooping** 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
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、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp 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 ルータに転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

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

スイッチは IGMP レポート抑制を使用してマルチキャスト ルータ クエリーごとに 1 つの IGMP レポートをマルチキャスト装置に転送します。IGMP ルータ抑制がイネーブル (デフォルト) の場合、スイッチはグループのすべてのホストの中から最初に来る IGMP レポートを、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 ルータに送信しません。この機能により、マルチキャスト装置に重複レポートを送信することが避けられます。

マルチキャスト ルータ クエリーに、IGMPv1 および IGMPv2 レポートのみに対する要求が含まれている場合、スイッチはグループのすべてのホストの中から最初に来る IGMPv1 または IGMPv2 レポートのみを、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 ルータのクエリーに IGMPv3 レポートに対する要求も含まれている場合、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装置に転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにする場合、すべての IGMP レポートがすべてのマルチキャスト ルータに転送されます。

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
```

コマンド設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにします。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn

Internet Group Management Protocol (IGMP) Topology Change Notification (TCN; トポロジー変更通知)の動作を設定するには、スイッチスタックまたはスタンドアロンスイッチ上で **ip igmp snooping tcn** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping tcn {flood query count count | query solicit}
```

```
no ip igmp snooping tcn {flood query count | query solicit}
```

シンタックスの説明

flood query count count	マルチキャスト トラフィックのフラッディングが発生する一般的な IGMP 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 イベント中に発生する、フラッディング モードからの回復処理を高速化するために、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 フラッディング クエリー カウントは2です。

TCN クエリー要求はディセーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEB	このコマンドが導入されました。

使用上のガイドライン

TCN イベント後のマルチキャスト トラフィックのフラッディング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** コマンドで TCN フラッディング クエリー カウントを1に設定した場合、一般的なクエリーを1回受信したあとにフラッディングが停止します。カウントを7に設定した場合、TCN イベントによるマルチキャスト トラフィックのフラッディングは、一般的なクエリーを7回受信するまで続きます。グループは、TCN イベント中に受信した一般的なクエリーに基づいて再学習されます。

スパニングツリーのルートであるかどうかに関係なく、スイッチでのグローバル脱退メッセージの送信をイネーブルにするには、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。このコマンドにより、TCN イベント中に発生するフラッディング モードからの回復処理の高速化も行われます。

例

次の例では、マルチキャスト トラフィックのフラッディングが発生する一般的な IGMP クエリーの数として7を指定する方法を示します。

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

コマンド設定を確認するには、**show ip igmp snooping** 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
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn flood	インターフェイス上のフラッディングを、IGMP スヌーピング スパニングツリー TCN 動作として指定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn flood

マルチキャスト フラッディングを Internet Group Management Protocol (IGMP) スヌーピング スパニングツリー Topology Change Notification (TCN; トポロジー変更通知) の動作として設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip 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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト スパニングツリー TCN イベント中、インターフェイス上でマルチキャスト フラッディングはイネーブルです。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(25)SEB	このコマンドが導入されました。

使用上のガイドライン スイッチが TCN を受信すると、一般的なクエリーを 2 回受信するまで、すべてのポートでマルチキャスト トラフィックのフラッディングが発生します。スイッチに、異なるマルチキャスト グループに加入しているホストが接続された多数のポートがある場合、フラッディングがリンクの容量を超え、パケット損失が発生することがあります。

ip igmp snooping tcn flood query count count グローバル コンフィギュレーション コマンドを使用することにより、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、インターフェイスでマルチキャスト フラッディングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

コマンド設定を確認するには、**show ip igmp snooping** 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
	ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにします。
	ip igmp snooping tcn	スイッチで IGMP TCN の動作を設定します。
	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（仮想 LAN）ごとに Internet Group Management Protocol（IGMP）スヌーピング即時脱退処理をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp snooping immediate-leave** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* immediate-leave

no ip igmp snooping vlan *vlan-id* immediate-leave

シンタックスの説明

<i>vlan-id</i>	指定の VLAN で IGMP スヌーピングと即時脱退機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

デフォルト

IGMP の即時脱退処理はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface（FDDI）VLAN 専用で、IGMP スヌーピングでは使用できません。

即時脱退機能を設定するには、VLAN の各ポート上で最大 1 つのレシーバーが設定されていなければなりません。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
```

コマンド設定を確認するには、**show ip igmp snooping** 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
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	スイッチ上で設定される IGMP クエリアの設定情報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、あるいはマルチキャスト学習方式を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}
```

```
no ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}
```

シンタックスの説明

<i>vlan-id</i>	IGMP スヌーピングをイネーブルにし、指定の VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
<i>interface interface-id</i>	次のホップ インターフェイスをマルチキャスト ルータに指定します。キーワードの意味は次のとおりです。 fastethernet <i>interface number</i> — ファスト イーサネット IEEE（米国電気電子学会） 802.3 インターフェイス gigabitethernet <i>interface number</i> — ギガビット イーサネット IEEE 802.3z インターフェイス port-channel <i>interface number</i> — チャネル インターフェイス。指定できる範囲は 0 ～ 48 です。
learn { <i>cgmp</i> <i>pim-dvmrp</i> }	マルチキャスト ルータの学習方式を指定します。キーワードの意味は次のとおりです。 cgmp — Cisco Group Management Protocol (CGMP) パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するよう設定します。 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。

デフォルト

デフォルトでは、マルチキャスト ルータ ポートはありません。

デフォルトの学習方式は **pim-dvmrp** です。IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、IGMP スヌーピングでは使用できません。

CGMP の学習方式は制御トラフィックの減少に役立ちます。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

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
```

コマンド設定を確認するには、**show ip igmp snooping** 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
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	スイッチ上で設定される IGMP クエリアの設定情報および動作情報を表示します。

ip igmp snooping vlan static

Internet Group Management Protocol (IGMP) スヌーピングをイネーブルにし、レイヤ 2 ポートをマルチキャストグループのメンバーとしてスタティックに追加するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp 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場合は、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* static *ip-address* interface *interface-id*

no ip igmp snooping vlan *vlan-id* static *ip-address* interface *interface-id*

シンタックスの説明

<i>vlan-id</i>	指定の VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
<i>ip-address</i>	指定のグループ IP アドレスを持ったマルチキャスト グループのメンバーとして、レイヤ 2 ポートを追加します。
<i>interface interface-id</i>	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 <i>interface number</i> — ファスト イーサネット IEEE（米国電気電子学会）802.3 インターフェイス • gigabitethernet <i>interface number</i> — ギガビット イーサネット IEEE 802.3z インターフェイス • port-channel <i>interface number</i> — チャネル インターフェイス。指定できる範囲は 0 ～ 48 です。

デフォルト

デフォルトでは、マルチキャスト グループのメンバーとしてスタティックに設定されたポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、IGMP スヌーピングでは使用できません。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、インターフェイス上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
gigabitethernet1/0/1
Configuring port gigabitethernet1/0/1 on group 0100.5e02.0203
```

コマンド設定を確認するには、**show ip igmp snooping** 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
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	スイッチ上で設定される IGMP クエリアの設定情報および動作情報を表示します。

ip snap forwarding

Subnetwork Access Protocol (SNAP) カプセル化を使用した IP Version 4 (IPv4) および IP Version 6 (IPv6) フレームの転送をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip snap forwarding** グローバル コンフィギュレーション コマンドを使用します。このフレームの転送をディセーブルにするにはこのコマンドの **no** 形式を使用します。

ip snap forwarding

no ip snap forwarding

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

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

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(25)SEC	このコマンドが導入されました。

使用上のガイドライン SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をイネーブルにするには、**ip snap forwarding** グローバル コンフィギュレーション コマンドを使用します。

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

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

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

設定を確認するには、**show running-config** 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 source binding

スイッチ上のスタティクな IP 送信元バインディングを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip source binding** グローバル コンフィギュレーション コマンドを使用します。スタティクなバインディングを削除する場合は、このコマンドの **no** 形式を使用します。

ip source binding mac-address vlan vlan-id ip-address interface interface-id

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

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

mac-address	MAC (メディア アクセス制御) アドレスを指定します。
vlan vlan-id	VLAN (仮想 LAN) 番号を指定します。指定できる範囲は 1 ～ 4094 です。
ip-address	IP アドレスを指定します。
interface interface-id	IP 送信元バインディングを追加または削除するインターフェイスを指定します。

デフォルト

IP 送信元バインディングは設定されていません。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

スタティクな IP 送信元バインディング エントリには、IP アドレス、それに対応する MAC アドレス、および対応する VLAN 番号が含まれます。エントリは、MAC アドレスおよび VLAN 番号に基づいています。エントリの変更で、IP アドレスだけを変更した場合、スイッチは新しいエントリを作成せずに更新します。

例

次の例では、スタティクな IP 送信元バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/0/1
```

次の例では、スタティクなバインディングを追加して、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet1/0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet1/0/1
```

設定を確認するには、**show ip source binding** 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
ip verify source	インターフェイスの IP ソース ガードをイネーブルにします。
show ip source binding	スイッチの IP 送信元バインディングを表示します。
show ip verify source	スイッチまたは特定のインターフェイスの IP ソース ガード コンフィギュレーションを表示します。

ip ssh

Secure Shell (SSH; セキュア シェル) version 1 (SSHv1) または SSH version 2 (SSHv2) を実行するようにスイッチを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip 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。このコマンドを使用するには、スイッチで暗号化ソフトウェア イメージが実行されている必要があります。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。

ip ssh version [1 | 2]

no ip ssh version [1 | 2]

シンタックスの説明

1	(任意) SSHv1 を実行するようにスイッチを設定します。
2	(任意) SSHv2 を実行するようにスイッチを設定します。

デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは SSH クライアントでサポートされる最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

スイッチは SSHv1 または SSHv2 サーバをサポートします。また、SSHv1 クライアントについてもサポートします。SSH サーバおよび SSH クライアントに関する詳細情報は、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 サーバで生成される Rivest, Shamir, and Adelman (RSA) 鍵ペアは SSHv2 サーバで使用可能で、その逆も可能です。

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
```

コマンド設定を確認するには、**show ip ssh** または **show ssh** 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 ip ssh	SSH サーバがイネーブルであるかどうかを表示し、SSH サーバのバージョンと設定情報を表示します。構文情報については、 Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands を選択してください。
show ssh	SSH サーバのステータスを表示します。構文情報については、 Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands を選択してください。

ip verify source

インターフェイスで IP ソース ガードをイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip verify source** グローバル コンフィギュレーション コマンドを使用します。IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source [port-security]

no ip verify source

シンタックスの説明

port-security (任意) IP アドレスおよび MAC (メディア アクセス制御) アドレスのフィルタリングにより、IP ソース ガードをイネーブルにします。

port-security キーワードを入力しない場合、IP 送信元アドレスのフィルタリングによる IP ソース ガードはイネーブルになります。

デフォルト

IP ソース 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(20)SE	このコマンドが導入されました。

使用上のガイドライン

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

送信元 IP アドレスと MAC アドレスのフィルタリングにより IP ソース ガードをイネーブルにするには、**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用します。

送信元 IP アドレスと MAC アドレスのフィルタリングにより IP ソース ガードをイネーブルにする場合は、インターフェイス上のポート セキュリティをイネーブルにする必要があります。

例

次の例では、送信元 IP アドレスのフィルタリングにより IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source
```

次の例では、送信元 IP アドレスおよび MAC アドレスのフィルタリングにより IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source port-security
```

設定を確認するには、**show ip source binding** 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
ip source binding	スイッチ上のスタティックなバインディングを設定します。
show ip verify source	スイッチまたは特定のインターフェイスの IP ソース ガード コンフィギュレーションを表示します。

ipv6 access-list

IPv6 アクセス リストを定義し、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ipv6 access-list** グローバル コンフィギュレーション コマンドを使用します。アクセス リストを削除する場合は、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

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



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

<i>access-list-name</i>	IPv6 アクセス リストの名前。名前には、スペースと引用符を使用することはできず、最初の文字を数字にすることもできません。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

ipv6 access-list コマンドは **ip access-list** コマンドと同じですが、IPv6 専用です。



(注)

IPv6 ACL は一意の名前によって定義されています (IPv6 では番号付けされた ACL はサポートされていません)。IPv4 ACL と IPv6 ACL に同じ名前を付けることはできません。

IPv6 トラフィックを、IPv6 オプション ヘッダーおよびオプションの上位レイヤ プロトコル タイプ情報に基づいてフィルタリングする方法の詳細については、**ipv6 access-list** および **permit (IPv6 アクセスリスト コンフィギュレーション)** コマンドの項を参照してください。変換された IPv6 ACL 設定の例については、「例」のセクションを参照してください。



(注)

IPv6 ACL には、最後の一致条件として、暗黙的な **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントが設定されています。2 つの **permit** 条件により、ICMPv6 ネイバの検出が可能になります。ICMPv6 のネイバの検出を無効にして、**icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、ACL に明示的な **deny** エントリを設定する必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に少なくとも 1 個のエントリが設定されていなければなりません。

IPv6 ネイバ検出プロセスでは、IPv6 ネットワーク レイヤ サービスを使用するため、デフォルトでは、IPv6 ACL はインターフェイス上で暗黙的に IPv6 ネイバ検出パケットの送受信を可能にします。IPv4 では、IPv6 ネイバ検出プロセスと同等の Address Resolution Protocol (ARP; アドレス解決プロトコル) で個別のデータリンク レイヤ プロトコルが使用されます。そのため、デフォルトでは、IPv4 ACL はインターフェイス上で暗黙的に ARP パケットの送受信を可能にします。

IPv6 ACL を IPv6 インターフェイスに適用するには、**ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドと *access-list-name* 引数を使用します。レイヤ 3 の物理インターフェイスとルーテッド ACL 用スイッチ仮想インターフェイスには着信と発信両方の IPv6 ACL を適用できますが、ポート ACL 用のレイヤ 2 インターフェイスには着信 IPv6 ACL しか適用できません。



(注)

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

例

次の例では、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにし、list2 という名前の IPv6 ACL を設定し、インターフェイスの発信トラフィックに ACL を適用します。最初の ACL エントリによって、ネットワーク FE80:0:0:2::/64 (送信元 IPv6 アドレスの最初の 64 ビットとしてリンク ローカル プレフィクス FE80:0:0:2 を持つパケット) のパケットがインターフェイスから発信されないようにします。ACL の 2 番目のエントリにより、インターフェイスでのその他のトラフィックの発信が許可されます。2 番目のエントリが必要となるのは、IPv6 ACL の最後には、それぞれ暗黙的な **deny-all** 条件が存在するためです。

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



(注)

暗黙的な拒否条件に依存する、またはトラフィックのフィルタリングのために **deny any any** ステートメントを指定する IPv6 ACL には、プロトコル パケットのフィルタリングを回避するため、リンク ローカル アドレス用の **permit** ステートメントが記述されていなければなりません。また、トラフィックのフィルタリングのために **deny** ステートメントを使用する IPv6 ACL では、リストの最後のステートメントとして **permit any any** ステートメントを使用する必要もあります。

関連コマンド

コマンド	説明
deny (IPv6 アクセスリスト コンフィギュレーション)	IPv6 アクセス リストの拒否条件を設定します。
ipv6 traffic-filter	インターフェイスで IPv6 の着信トラフィックおよび発信トラフィックをフィルタリングします。
permit (IPv6 アクセスリスト コンフィギュレーション)	IPv6 アクセス リストの許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストの全内容を表示します。

ipv6 mld snooping

IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピングをグローバルに、または指定の VLAN (仮想 LAN) 上でイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で、キーワードなしで **ipv6 mld 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。MLD スヌーピングを、スイッチ、スイッチスタック、または VLAN 上でディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
ipv6 mld snooping [vlan vlan-id]
```

```
no ipv6 mld snooping [vlan vlan-id]
```



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN で MLD スヌーピングをイネーブルまたはディセーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 または 1006 ～ 4094 です。

デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングがイネーブルです。ただし、VLAN スヌーピングを有効にするには、MLD スヌーピングをグローバルにイネーブルにしておく必要があります。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

MLD スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスでディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、デフォルト ステート (イネーブル) のすべての VLAN インターフェイスでイネーブルになります。VLAN 設定は、MLD スヌーピングがディセーブルになっているインターフェイスのグローバル設定を上書きします。

MLD スヌーピングがグローバルにディセーブルになっている場合、VLAN 上でイネーブルにすることはできません。MLD スヌーピングがグローバルにイネーブルになっている場合、個々の VLAN 上でディセーブルにすることができます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) を使用している場合、Catalyst 3750 または Catalyst 3560 スイッチが VLAN でクエリーを受信できるように、Catalyst 6500 スイッチの拡張 VLAN で IPv6 MLD スヌーピングをイネーブルにする必要があります。通常範囲の VLAN (1 ~ 1005) の場合、Catalyst 6500 スイッチの VLAN で IPv6 MLD スヌーピングをイネーブルにする必要はありません。

VLAN ID 1002 ~ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

例

次の例では、MLD スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping
```

次の例では、MLD スヌーピングを VLAN でディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 11
```

設定を確認するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントがエージングアウトになる前に送信される IP version 6 (IPv6) Multicast Listener Discovery (MLD) Multicast Address Specific Queries (MASQ) を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping last-listener-query-count** グローバル コンフィギュレーション コマンドを使用します。クエリー カウントをデフォルト設定にリセットする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN (仮想 LAN) で last-listener クエリー カウントを設定します。指定できる VLAN ID の範囲は 1 ～ 1001 または 1006 ～ 4094 です。
<i>integer_value</i>	指定できる範囲は、1 ～ 7 です。

コマンドのデフォルト設定

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です (グローバル カウントを使用)。

コマンド 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	このコマンドが導入されました。

使用上のガイドライン

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

MLD スヌーピングでは、IPv6 マルチキャスト ルータは、マルチキャスト グループに属するホストにクエリーを定期的に出します。ホストをマルチキャスト グループから脱退させる場合、メッセージを残さずに脱退することも、クエリーに対して Multicast Listener Done メッセージ (IGMP 脱退メッセージと同等) を返して脱退することもできます。即時脱退が設定されていない場合 (グループのマルチキャスト クライアントが同じポートに存在する場合は設定しない)、設定された last-listener クエリー カウントにより、MLD クライアントがエージングアウトになるまでの MASQ 数が決まります。

VLAN に対して last-listener クエリー カウントが設定されている場合、グローバルに設定されている値に対してこのカウントが上書きされます。VLAN カウントが設定されていない (デフォルトの 0 に設定されている) 場合、グローバル カウントが使用されます。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

例

次の例では、last-listener クエリー カウントをグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

次の例では、VLAN 10 の last-listener クエリー カウントを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-interval	IPv6 MLD スヌーピングの last-listener クエリー 間隔を設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping querier	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN で IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピングの last-listener クエリー間隔を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用します。この間隔は、マルチキャスト ルータが、Multicast Address Specific Query (MASQ) を発行したあと、ポートをマルチキャスト グループから削除するまでに待ち合わせる最大時間です。クエリー時間をデフォルト設定にリセットする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN (仮想 LAN) で last-listener クエリー間隔を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 または 1006 ～ 4094 です。
<i>integer_value</i>	マルチキャスト ルータが、MASQ を発行したあと、ポートをマルチキャスト グループから削除するまでに待ち合わせる間隔 (1000 分の 1 秒単位) を設定します。指定できる範囲は 100 ～ 32768 です。デフォルト値は 1000 (1 秒) です。

コマンドのデフォルト設定

デフォルトのグローバル クエリー間隔 (最大応答時間) は 1000 (1 秒) です。

デフォルトの VLAN クエリー間隔 (最大応答時間) は 0 (グローバル カウントを使用) 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	このコマンドが導入されました。

使用上のガイドライン

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

MLD スヌーピングでは、IPv6 マルチキャスト ルータは、MLD 脱退メッセージを受信すると、マルチキャスト グループに属するホストにクエリーを送出します。一定時間、ポートから MASQ への応答がない場合、ルータはマルチキャスト アドレスのメンバーシップ データベースからそのポートを削除します。last-listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除するまでにルータが待ち合わせる最大時間です。

VLAN クエリー間隔を設定すると、この値がグローバル クエリー間隔を上書きします。VLAN 間隔を 0 に設定した場合、グローバル値が使用されます。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

例

次の例では、last-listener クエリー間隔をグローバルに 2 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

次の例では、VLAN 1 の last-listener クエリー間隔を 5.5 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピングの last-listener クエリーカウントを設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping querier	IPv6 MLD スヌーピングの last-listener クエリー間隔を設定します。

ipv6 mld snooping listener-message-suppression

IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピング リスナー メッセージ抑制をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。MLD スヌーピング リスナー メッセージ抑制をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

コマンドのデフォルト設定

デフォルトは、MLS スヌーピング リスナー メッセージ抑制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)SED	このコマンドが導入されました。

使用上のガイドライン

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

MLD スヌーピング リスナー メッセージ抑制は、IGMP スヌーピング レポート抑制と同等です。この機能をイネーブルにすると、グループに対して受信した MLDv1 レポートが、各レポート転送時間に対して 1 回のみ IPv6 マルチキャスト ルータに転送されます。これにより、重複レポートの転送が回避できます。

例

次の例では、MLD スヌーピング リスナー メッセージ抑制をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

次の例では、MLD スヌーピング リスナー メッセージ抑制をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除するまでにスイッチが送信する IP version 6 (IPv6) Multicast Listener Discovery (MLD) クエリーの数を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping robustness-variable** グローバル コンフィギュレーション コマンドを使用します。VLAN ごとに設定するには、VLAN ID を入力します。変数をデフォルト設定にリセットする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [vlan *vlan-id*] robustness-variable *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] robustness-variable



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN (仮想 LAN) で信頼性変数を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 または 1006 ～ 4094 です。
<i>integer_value</i>	指定できる範囲は、1 ～ 3 です。

コマンドのデフォルト設定

デフォルトのグローバル信頼性変数 (リスナーを削除するまでに送信するクエリーの数) は 2 です。

デフォルトの VLAN 信頼性変数 (マルチキャスト アドレスのエージングアウトまでに送信するクエリーの数) は 0 で、システムはリスナーのエージングアウトにグローバル信頼性変数を使用します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

信頼性は、ポートがマルチキャスト グループから削除されるまでに送信される、ポートからの応答がない MLDv1 クエリーの数によって測定されます。MLDv1 クエリーに設定した回数について MLDv1 レポートを受信しない場合、ポートは削除されます。グローバル値によって、応答のないリスナーを削除するまでにスイッチが待ち合わせるクエリーの回数が決まり、この値は VLAN 値が設定されていないすべての VLAN に適用されます。

VLAN に対して信頼性の値を設定すると、グローバル値が上書きされます。VLAN 信頼性値が 0 の場合 (デフォルト)、グローバル値が使用されます。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

例 次の例では、応答のないリスナー ポートを削除するまでにスイッチがクエリーを 3 回送出するようグローバル信頼性変数を設定する方法を示します。

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

次の例では、VLAN 1 の信頼性変数を設定する方法を示します。この値によって、VLAN のグローバル設定が上書きされます。

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピングの last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping tcn

IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notification (TCN; トポロジー変更通知) を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping tcn** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定にリセットする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping tcn {flood query count integer_value | query solicit}

no ipv6 mld snooping tcn {flood query count integer_value | query solicit}



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

flood query count integer_value	フラッディング クエリー カウント (受信を要求するポートにのみマルチキャスト データを転送する前に送信するクエリーの数) を設定します。指定できる範囲は、1 ～ 10 です。
query solicit	TCN クエリーの要求をイネーブルにします。

コマンドのデフォルト設定

TCN クエリー要求はディセーブルです。

イネーブルの場合、デフォルト フラッディング クエリー カウントは2です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

例

次の例では、TCN クエリー要求をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

次の例では、フラッディング クエリー カウントを5に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping vlan

VLAN（仮想 LAN）インターフェイスで IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング パラメータを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**ipv6 mld snooping vlan** グローバル コンフィギュレーション コマンドを使用します。パラメータをデフォルト設定にリセットする場合は、このコマンドの **no** 形式を使用します。

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]



(注) このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management（SDM）テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	VLAN 番号を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
immediate-leave	(任意) VLAN インターフェイス上で、MLD の即時脱退処理をイネーブルにします。この機能をインターフェイス上でディセーブルにする場合は、このコマンドの no 形式を使用します。
mrouter interface	(任意) マルチキャスト ルータ ポートを設定します。設定を削除する場合は、このコマンドの no 形式を使用します。
static <i>ipv6-multicast-address</i>	(任意) 指定の IPv6 マルチキャスト アドレスでマルチキャスト グループを設定します。
interface <i>interface-id</i>	レイヤ 2 ポートをグループに追加します。mrouter またはスタティック インターフェイスは、物理ポート、または 1 ～ 48 の範囲内の port-channel インターフェイスとすることができます。

コマンドのデフォルト設定

MLD スヌーピングの即時脱退処理はディセーブルです。

デフォルトでは、スタティック IPv6 マルチキャスト グループはありません。

デフォルトでは、マルチキャスト ルータ ポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

即時脱退機能を設定するには、VLAN の各ポート上で 1 つのレシーバーのみが設定されていなければなりません。設定は、NVRAM（不揮発性 RAM）に保存されます。

static キーワードは MLD メンバー ポートをスタティックに設定するために使用されます。

設定内容、スタティック ポートおよびグループは、NVRAM に保存されます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN（1006 ～ 4094 の範囲）を使用している場合、Catalyst 3750 または Catalyst 3560 スイッチが VLAN でクエリーを受信できるように、Catalyst 6500 スイッチの拡張 VLAN で IPv6 MLD スヌーピングをイネーブルにする必要があります。通常範囲の VLAN（1 ～ 1005）の場合、Catalyst 6500 スイッチの VLAN で IPv6 MLD スヌーピングをイネーブルにする必要はありません。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface（FDDI）VLAN 専用で、MLD スヌーピングでは使用できません。

例

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

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface
gigabitethernet1/0/2
```

設定を確認するには、**show ipv6 mld snooping vlan vlan-id** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。
show ipv6 mld snooping	IPv6 MLD スヌーピング設定を表示します。

ipv6 traffic-filter

インターフェイス上で IPv6 トラフィックをフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。レイヤ 3 インターフェイス（ルータ ACL）では着信と発信の両方の IPv6 トラフィックをフィルタリングできますが、レイヤ 2 インターフェイス（ポート ACL）では着信トラフィックのみがフィルタリングできます。インターフェイスで IPv6 トラフィックのフィルタリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

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

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



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

<i>access-list-name</i>	IPv6 のアクセス名を指定します。
<i>in</i>	着信 IPv6 トラフィックを指定します。
<i>out</i>	発信 IPv6 トラフィックを指定します。



(注)

このキーワードは、レイヤ 2 の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

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

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

ipv6 traffic-filter コマンドは、物理インターフェイス（レイヤ 2 または レイヤ 3 のポート）、レイヤ 3 ポート チャネル、または Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) で使用できます。

レイヤ 3 インターフェイス（ルータ ACL）については着信と発信の両方のフィルタリングがサポートされていますが、レイヤ 2 ポート（ポート ACL）については着信のフィルタリングしかサポートされていません。

任意のポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用されている場合、そのポート ACL はパケットのフィルタリングに使用され、ポート VLAN の SVI のルータ ACL は無視されます。

例 次の例では、*cisco* という名前のアクセス リストの定義に従って、IPv6 設定インターフェイスで着信 IPv6 トラフィックをフィルタリングします。

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

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、定義したアクセス リストの拒否 / 許可条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストの全内容を表示します。
show ipv6 interface	IPv6 用に設定したインターフェイスの利用状況ステータスを表示します。

l2protocol-tunnel

アクセスポート、IEEE（米国電気電子学会）802.1Q トンネルポート、またはポートチャネルでレイヤ 2 プロトコルのトンネリングをイネーブルにするには、スイッチスタックまたはスタンドアロンスイッチ上で **l2protocol-tunnel** インターフェイスコンフィギュレーションコマンドを使用します。Cisco Discovery Protocol（CDP）、Spanning-Tree Protocol（STP; スパニングツリープロトコル）、または VLAN Trunking Protocol（VTP; VLAN [仮想 LAN] トランクキングプロトコル）パケットのトンネリングをイネーブルにできます。Port Aggregation Protocol（PAgP）、Link Aggregation Control Protocol（LACP）、または UniDirectional Link Detection（UDLD; 単一方向リンク検出）パケットのポイントツーポイントトンネリングもイネーブルにできます。インターフェイスでトンネリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

l2protocol-tunnel	CDP、STP、および VTP パケットのポイントツーマルチポイントトンネリングをイネーブルにします。
cdp	(任意) CDP のトンネリングをイネーブルにし、CDP のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
stp	(任意) STP のトンネリングをイネーブルにし、STP のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
vtp	(任意) VTP のトンネリングをイネーブルにし、VTP のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
point-to-point	(任意) PAgP、LACP、および UDLD パケットのポイントツーポイントトンネリングをイネーブルにします。
pagp	(任意) PAgP のポイントツーポイントトンネリングをイネーブルにし、PAgP のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
lacp	(任意) LACP のポイントツーポイントトンネリングをイネーブルにし、LACP のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
udld	(任意) UDLD のポイントツーポイントトンネリングをイネーブルにし、UDLD のシャットダウンスレッショールドまたは廃棄スレッショールドを指定します。
shutdown-threshold	(任意) インターフェイスがシャットダウンされる前に受信するシャットダウンスレッショールドを、レイヤ 2 プロトコルパケットの最大レート/秒に設定します。
drop-threshold	(任意) インターフェイスがパケットを廃棄する前に受信する廃棄スレッショールドを、レイヤ 2 プロトコルパケットの最大レート/秒に設定します。
value	インターフェイスがシャットダウンされる、またはインターフェイスがパケットを廃棄する前に、カプセル化用に受信されるスレッショールドを、パケット/秒単位で指定します。指定できる範囲は 1 ～ 4096 です。デフォルトの設定にスレッショールドはありません。

デフォルト

デフォルト設定では、レイヤ 2 プロトコル パケットはトンネリングされません。

デフォルト設定では、レイヤ 2 プロトコル パケット数のシャットダウン スレッシュホールドはありません。

デフォルト設定では、レイヤ 2 プロトコル パケット数の廃棄スレッシュホールドはありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 パケットをトンネリングするには、プロトコル タイプに関係なく、このコマンドを入力する必要があります。

ポート チャネルにこのコマンドを入力する場合、チャネル内のポートすべては同じ設定になっている必要があります。

サービスプロバイダーのネットワークにまたがるレイヤ 2 プロトコル トンネリングでは、確実にレイヤ 2 情報はネットワークを介してすべてのカスタマー ロケーションに伝播されます。プロトコル トンネリングがイネーブルの場合、プロトコル パケットは、ネットワーク上の送信のために一般的なシスコ マルチキャスト アドレスでカプセル化されます。パケットが宛先に到達すると、一般的な MAC (メディア アクセス制御) アドレスはレイヤ 2 プロトコル MAC アドレスに変更されます。

CDP、STP、VTP それぞれに対して、または 3 種類すべてのプロトコルに対してレイヤ 2 プロトコル トンネリングをイネーブルにできます。

サービスプロバイダー ネットワークでは、ポイントツーポイント ネットワーク トポロジをエミュレートして EtherChannel の作成を増強するために、レイヤ 2 プロトコル トンネリングを使用できます。PAgP または LACP 用のサービスプロバイダー スイッチ上でプロトコル トンネリングがイネーブルの場合、リモート カスタマー スイッチは Protocol Data Unit (PDU; プロトコル データ ユニット) を受信し、EtherChannel の自動作成をネゴシエートできます。

PAgP、LACP、および UDLD パケットのトンネリングをイネーブルにするには、ポイントツーポイント ネットワーク トポロジを備えている必要があります。リンクダウン検出時間を短縮するには、PAgP または LACP パケットのトンネリングをイネーブルにするときにインターフェイス上の UDLD もイネーブルにする必要があります。

PAgP、LACP、UDLD のそれぞれに対して、または 3 種類すべてのプロトコルに対してポイントツーポイント プロトコル トンネリングをイネーブルにできます。

**注意**

PAgP、LACP、UDLD トンネリングは、ポイントツーポイント トポロジのエミュレートのためだけに使用します。多くのポートにトンネリングされたパケットを送信するという誤った設定により、ネットワーク障害が発生します。

インターフェイスがシャットダウンする前にインターフェイス上で受信されるプロトコル パケット数 / 秒を制御するには、**shutdown-threshold** キーワードを入力します。プロトコル オプションがキーワードで指定されていない場合、トンネリングされたレイヤ 2 プロトコル タイプごとにスレッシュホールドが適用されます。インターフェイスに廃棄スレッシュホールドを設定する場合、シャットダウンスレッシュホールド値は廃棄スレッシュホールド値以上である必要があります。

シャットダウン スレッシュホールド値に達すると、インターフェイスは **errdisable** の状態になります。**errdisable recovery cause l2ptguard** グローバル コンフィギュレーション コマンドを入力して、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 **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。**l2ptguard** のエラー回復メカニズムがイネーブルでない場合、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。

インターフェイスがパケットを廃棄する前にインターフェイス上で受信されるプロトコル パケット数/秒を制御するには、**drop-threshold** キーワードを入力します。プロトコル オプションがキーワードで指定されていない場合、トンネリングされたレイヤ 2 プロトコル タイプごとにスレッシュホールドが適用されます。インターフェイスにシャットダウン スレッシュホールドを設定する場合、廃棄スレッシュホールド値はシャットダウンスレッシュホールド値以下である必要があります。

廃棄スレッシュホールド値に達すると、インターフェイスはパケットを受信するレートが廃棄スレッシュホールド値を下回るまでレイヤ 2 プロトコル パケットを廃棄します。

設定は、NVRAM（不揮発性 RAM）に保存されます。

レイヤ 2 プロトコル トンネリングに関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、CDP パケットのプロトコル トンネリングをイネーブルにし、シャットダウン スレッシュホールドを 50 パケット/秒に設定する方法を示します。

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

次の例では、STP パケットのプロトコル トンネリングをイネーブルにし、廃棄スレッシュホールドを 400 パケット/秒に設定する方法を示します。

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

次の例では、PAgP および UDLD パケットのポイントツーポイント プロトコル トンネリングをイネーブルにし、PAgP 廃棄スレッシュホールドを 1000 パケット/秒に設定する方法を示します。

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

関連コマンド

コマンド	説明
l2protocol-tunnel cos	トンネリングされたレイヤ 2 プロトコル パケットすべてに、Class of Service (CoS; サービス クラス) 値を設定します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングに設定されたポートに関する情報（ポート、プロトコル、CoS、スレッシュホールドを含む）を表示します。

l2protocol-tunnel cos

トンネリングされたレイヤ 2 プロトコル パケットすべてに、Class of Service (CoS; サービス クラス) 値を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **l2protocol-tunnel cos** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel cos value

no l2protocol-tunnel cos

シンタックスの説明

<i>value</i>	トンネリングされたレイヤ 2 プロトコル パケットに CoS プライオリティ値を指定します。CoS 値がインターフェイスのデータ パケットに設定されている場合、デフォルトではこの CoS 値を使用します。CoS 値がインターフェイスに設定されていない場合、デフォルト値は 5 です。指定できる範囲は 0 ～ 7 です。7 が最高のプライオリティです。

デフォルト

デフォルトでは、インターフェイス上のデータに設定された CoS 値を使用します。CoS 値が設定されていない場合、すべてのトンネリングされたレイヤ 2 プロトコル パケットのデフォルト値は 5 です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが導入されました。

使用上のガイドライン

イネーブルの場合、トンネリングされたレイヤ 2 プロトコル パケットはこの CoS 値を使用します。値は NVRAM（不揮発性 RAM）に保存されます。

例

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

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

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングに設定されたポートの情報 (CoS を含む) を表示します。

lacp port-priority

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

lacp port-priority priority

no lacp port-priority

シンタックスの説明	<i>priority</i>	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
	12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン	lacp port-priority インターフェイス コンフィギュレーション コマンドにより、LACP チャネル グループ内に 8 個を超えるポートが存在する場合に、バンドルされるポート、ホットスタンバイ モードになるポートを指定します。 LACP チャネル グループには、同じタイプのイーサネット ポートを最大 16 個指定できます。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。 ポートのプライオリティの比較においては、数値的に低い値ほどプライオリティが高くなります。LACP チャネル グループ内に 8 個を超えるポートがある場合、LACP ポート プライオリティの数値が小さい（プライオリティが高い）順に 8 個のポートがチャネル グループにバンドルされ、プライオリティが低いポートがホットスタンバイ モードになります。LACP ポート プライオリティが同じポートが 2 個以上ある場合（デフォルト設定の 65535 で設定されている場合など）、ポート番号の内部値によりプライオリティが決まります。	



(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にポートがある場合のみ有効になります。リンクを制御するスイッチの決定方法については、 lacp system-priority グローバル コンフィギュレーション コマンドの項を参照してください。

LACP ポート プライオリティと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。

物理ポート上の LACP の設定に関する情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」を参照してください。

例

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

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

設定を確認するには、**show lacp [channel-group-number] internal** 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-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	すべてのチャンネル グループまたは指定のチャンネル 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、スイッチ スタックまたはスタンドアロン スイッチ上で **lacp system-priority** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp system-priority *priority*

no lacp system-priority

シンタックスの説明	<i>priority</i>	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
	12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン **lacp system-priority** コマンドにより、ポート プライオリティ を制御する LACP リンク内のスイッチが決まります。

LACP チャネル グループには、同じタイプのイーサネット ポートを最大 16 個指定できます。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 8 個を超えるポートがある場合、リンクの制御側のスイッチは、ポート プライオリティに従って、チャネルにバンドルするポートとホットスタンバイ モードにするポートを決定します。他のスイッチのポート プライオリティ（リンクの非制御側）は無視されます。

プライオリティの比較においては、数値的に低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 プライオリティについて数値が低い（プライオリティが高い）システムが制御システムになります。両方のスイッチの LACP システム プライオリティが同じである場合（どちらもデフォルト設定の 32768 で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）によって制御システムが決まります。

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

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

物理ポート上の LACP の設定に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」を参照してください。

例 次の例では、LACP のシステム プライオリティを設定する方法を示します。

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

設定を確認するには、**show lacp sys-id** 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-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 で使用されるシステム ID を表示します。

logging event power-inline-status

Power over Ethernet (PoE) イベントのロギングをイネーブルにするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。PoE ステータス イベントのロギングをディセーブルにする場合は、このコマンドの **no** 形式を使用しますが、このコマンドの **no** 形式を使用しても、PoE エラー イベントはディセーブルになりません。

logging event power-inline-status

no logging event power-inline-status

シンタックスの説明

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

デフォルト

PoE イベントのロギングはイネーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

power-inline-status キーワードは PoE インターフェイスでのみ使用できます。

例

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

```
Switch(config-if)# interface fastethernet1/0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

関連コマンド

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

logging file

ロギング ファイルのパラメータを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **logging file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

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

デフォルト

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

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

logging file flash:filename グローバル コンフィギュレーション コマンドを使用して、ログをフラッシュ メモリに保存したあとに、**more flash:filename** イネーブル EXEC コマンドで内容を表示させることができます。

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

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

例

次の例では、通知レベルのログ メッセージをフラッシュ メモリのファイルに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、スイッチ スタックまたはスタンドアロン スイッチ上で **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の MAC ACL、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 access-list extended** グローバル コンフィギュレーション コマンドを使用することで、MAC ACL を作成できます。

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

```
no mac access-group {name}
```

シンタックスの説明

name	名前付き MAC アクセス リストを指定します。
in	ACL が入力方向に適用されるよう指定します。発信 ACL は、レイヤ 2 インターフェイス上ではサポートされません。

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 インターフェイス限定）

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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

レイヤ 2 インターフェイス上で、IP アクセス リストを使用して IP トラフィックをフィルタリング、および 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。IP ACL および MAC ACL の両方をインターフェイスに適用することで、同一のレイヤ 2 インターフェイス上で IP、非 IP トラフィックをフィルタリングできます。複数の IP および MAC アクセス リストを同一のレイヤ 2 インターフェイスに適用することもできます。

MAC ACL がすでにレイヤ 2 インターフェイス上に設定されていて、新しい MAC ACL をインターフェイスに適用する場合、新しい ACL は既に設定されているものと置き換えられます。

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

着信パケットが MAC ACL が適用されたインターフェイス上で受信されると、スイッチは ACL の一致条件を確認します。条件が一致した場合、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 を設定する場合の詳細については、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」を参照してください。

例 次の例では、*macacl2* という名前が付いた MAC 拡張 ACL をインターフェイスに適用する方法を示します。

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

設定を確認するには、**show mac access-group** イネーブル EXEC コマンドを入力します。スイッチ上で設定された ACL を表示させるには、**show access-lists** 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 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）アドレスに基づいたアクセス リストを作成するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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ことで、拡張 MAC アクセスリスト コンフィギュレーション モードになります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac access-list extended *name*

no mac access-list extended *name*

シンタックスの説明

<i>name</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

名前付き MAC 拡張リストは VLAN(仮想 LAN) マップおよびクラス マップとともに使用されます。名前付き MAC 拡張 ACL は、VLAN マップまたはレイヤ 2 インターフェイスに適用できます。レイヤ 3 インターフェイスには適用できません。

mac access-list extended コマンドを入力することで、MAC アクセスリスト コンフィギュレーション モードをイネーブルにできます。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** : 拒否するパケットを指定します。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、またはデフォルトに設定します。
- **permit** : 転送するパケットを指定します。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 リストに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、*mac1* という名前が付いた MAC 拡張アクセスリストを作成し、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-mac1)#
```

次の例では、*mac1* という名前が付いた MAC 拡張アクセス リストを削除する方法を示します。

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

設定を確認するには、**show access-lists** 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
deny (MAC アクセスリスト コンフィギュレーション)	(拡張 MAC アクセスリスト コンフィギュレーション モードで) MAC ACL を設定します。
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。
vlan access-map	VLAN マップを定義し、アクセスマップ コンフィギュレーション モードを開始して、照合に使用する MAC ACL およびそれに対応する動作を指定できるようにします。

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 テーブル内に維持される時間を設定するには、スイッチ スタックまたはスタンドアロン スイッチ 上で **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 に対して適用されます。

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

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

シンタックスの説明

0	この値はエージング 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す。
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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	mac-address-table aging-time コマンド（ハイフンあり）は、 mac address-table aging-time コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

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

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

例

次の例では、すべての VLAN でエージング 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
```

設定を確認するには、**show mac address-table aging-time** 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 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 テーブル移行更新機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **mac address-table move update** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table move update {receive | transmit}

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

シンタックスの説明

receive	スイッチで MAC アドレス テーブル移行更新メッセージが処理されるよう指定します。
transmit	プライマリ リンクがダウンしてスタンバイ リンクがアップした場合に、スイッチがネットワーク内の他のスイッチに MAC アドレス テーブル移行更新メッセージを送信するよう指定します。

コマンド モード

グローバル コンフィギュレーション

デフォルト

デフォルトでは、MAC アドレス テーブル移行更新機能はディセーブルです。

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

プライマリ（転送）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、MAC アドレス テーブル移行更新機能により、スイッチは高速双方向コンバージェンスを行います。

プライマリ リンクがダウンしてスタンバイ リンクがアップした場合に、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するよう設定することができます。アップリンク スイッチで MAC アドレス テーブル移行更新メッセージを受信して処理するよう設定できます。

例

次の例では、アクセス スイッチで MAC アドレス テーブル移行更新メッセージを送信するよう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 スイッチで MAC アドレス テーブル移行更新メッセージを取得して処理するよう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 テーブル移行更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレス テーブル移行更新メッセージ処理をデバッグします。
show mac address-table move update	スイッチの MAC アドレス テーブル移行更新情報を表示します。

mac address-table notification

スイッチ スタック上で MAC (メディア アクセス制御) アドレス通知機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **mac address-table notification** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table notification [*history-size value*] [*interval value*]

no mac address-table notification [*history-size* | *interval*]

シンタックスの説明

history-size value	(任意) MAC 通知履歴テーブルのエントリの最大数を設定します。指定できる範囲は 0 ～ 500 エントリです。
interval value	(任意) 通知トラップ間隔を設定します。この時間量が過ぎると、スイッチ スタックは通知トラップを送信します。指定できる範囲は 0 ～ 2147483647 秒です。

デフォルト

MAC アドレス通知機能はディセーブルです。

トラップ間隔は 1 秒です。

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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	mac-address-table notification コマンド (ハイフンあり) は、 mac address-table notification コマンド (ハイフンなし) に変更されました。

使用上のガイドライン

MAC アドレス通知機能は、新しく MAC アドレスが転送テーブルに追加されたり、そこから古いアドレスが削除されたりするたびに、SNMP (簡易ネットワーク管理プロトコル) トラップを Network Management System (NMS; ネットワーク管理システム) に送信します。MAC 通知は、ダイナミックまたはセキュア MAC アドレスについてのみ生成されます。自アドレス、マルチキャストアドレス、または他のスタティック アドレスについては、イベントは生成されません。

history-size オプションを設定すると、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

mac address-table notification コマンドを使用すれば、MAC アドレス通知機能がイネーブルになります。また、**snmp trap mac-notification** インターフェイス コンフィギュレーション コマンドでインターフェイス上の MAC アドレス通知トラップをイネーブルにし、**snmp-server enable traps mac-notification** グローバル コンフィギュレーション コマンドでスイッチが MAC アドレストラップを NMS に送信するよう設定する必要があります。

例 次の例では、MAC アドレステーブル通知機能をイネーブルにし、時間の間隔を 60 秒、履歴サイズを 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上の SNMP MAC 通知トラップをイネーブルにします。

mac address-table static

MAC（メディア アクセス制御）アドレス テーブルにスタティック アドレスを追加するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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*]

シンタックスの説明

mac-addr	アドレス テーブルに追加する宛先 MAC アドレス（ユニキャストまたはマルチキャスト）。この宛先アドレスを持つパケットが指定した VLAN（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 <i>vlan-id</i>	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 <i>interface-id</i>	受信されたパケットを転送するインターフェイス。有効なインターフェイスとしては、物理ポートおよびポート チャンネルがあります。

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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	mac-address-table static コマンド（ハイフンあり）は、 mac address-table static コマンド（ハイフンなし）に変更されました。

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たパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet6/0/1
```

設定を確認するには、**show mac address-table** 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。

mac address-table static drop

ユニキャスト MAC（メディア アクセス制御）アドレス フィルタリングをイネーブルにして、特定の送信元または宛先 MAC アドレスのトラフィックを廃棄するようにスイッチを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **mac address-table static drop** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table static mac-addr vlan vlan-id drop

no mac address-table static mac-addr vlan vlan-id

シンタックスの説明

mac-addr	ユニキャスト送信元または宛先 MAC アドレス。この MAC アドレスを持つパケットは廃棄されます。
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（仮想 LAN）を指定します。有効な VLAN 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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

この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ていません。CPU に転送されるパケットもサポートされていません。
- ユニキャスト MAC アドレスをスタティック MAC アドレスとして追加して、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、どのコマンドが最後に入力されたかにより、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、その MAC アドレスを持つパケットを廃棄します。2 番めに入力したコマンドは、最初のコマンドを上書きします。

たとえば、**mac address-table static mac-addr vlan vlan-id interface interface-id** グローバル コンフィギュレーション コマンドを入力したあとに **mac address-table static mac-addr vlan vlan-id drop** コマンドを入力した場合、スイッチは指定した MAC アドレスを送信元または宛先としている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 コマンドを入力したあとに **mac address-table static mac-addr vlan vlan-id interface interface-id** コマンドを入力した場合、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て、送信元または宛先アドレスが c2f3.220a.12f4 の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。VLAN 4 でこの MAC アドレスを送信元または宛先としたパケットを受信すると、パケットは廃棄されます。

```
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するか、またはインターフェイスにマクロ設定を適用してこれを追跡するには、スイッチ スタックまたはスタンドアロン スイッチ上で **macro apply** インターフェイス コンフィギュレーション コマンドを使用します。

```
macro {apply | trace} macro-name [parameter {value}] [parameter {value}][parameter {value}]
```

シンタックスの説明

apply	指定のインターフェイスに対してマクロを適用します。
trace	マクロをインターフェイスに適用してマクロをデバッグするには、 trace キーワードを使用します。
<i>macro-name</i>	マクロ名を指定します。
parameter value	(任意) インターフェイス特有の固有パラメータ値を指定します。最大 3 組のキーワード値のペアを入力できます。パラメータのキーワード照合では、大文字と小文字が区別されます。キーワードが一致した場合は、すべて該当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
12.1(19)EA1	このコマンドが導入されました。
12.2(18)SE	parameter value キーワードが追加されました。

使用上のガイドライン

macro trace macro-name インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスで動作しているマクロの適用や表示を行ったり、構文また設定エラーを判断するためにマクロをデバッグしたりできます。

マクロを適用する場合に、構文エラーまたは設定エラーのいずれかによりコマンドがエラーになっても、マクロは引き続き残りのコマンドをインターフェイスに適用します。

固有の値を割り当てる必要があるマクロを作成する場合、**parameter value** キーワードによってインターフェイスに特有の値を指定します。

キーワード照合では、大文字と小文字が区別されます。キーワードが一致した場合は、すべて該当する値に置き換えられます。完全に一致したキーワードは、長い文字列の一部の場合であっても、一致したとみなされ、該当する値に置き換えられます。

マクロによっては、パラメータ値を必要とするキーワードを含むものもあります。マクロで必要とされる任意の値のリストを表示するには、**macro apply macro-name ?** コマンドを使用します。キーワードの値を入力せずにマクロを適用した場合、コマンドは無効になり、適用されません。

これは、スイッチ ソフトウェアに組み込まれたシスコのデフォルトの SmartPort マクロです。これらのマクロやマクロ内のコマンドを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

インターフェイス上でシスコのデフォルトの SmartPort マクロを適用する場合は、次の注意事項に留意してください。

- スイッチ上のマクロをすべて表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC コマンドを使用します。
- **\$** で始まるキーワードには、一意のパラメータ値が必要です。シスコのデフォルトのマクロに必要な値を付加するには、**parameter value** キーワードを使用します。

シスコのデフォルトのマクロでは、**\$** 文字を使用して、必要とされるキーワードを識別するのに役立っています。マクロ作成時にキーワードを定義するのに、**\$** 文字を使用する場合の制限事項はありません。

インターフェイスにマクロを適用すると、インターフェイスにマクロ名が自動的に追加されます。適用したコマンドとマクロ名を表示するには、**show running-configuration interface interface-id** ユーザ EXEC コマンドを使用します。

インターフェイス範囲に適用したマクロは、単一インターフェイスに適用されるマクロと同じように動作します。インターフェイス範囲を使用する場合、マクロは範囲内の個々のインターフェイスに対して順次適用されます。インターフェイスでマクロ コマンドがエラーになっても、残りのインターフェイスに対して引き続き適用されます。

マクロがインターフェイスに適用した設定を削除するには、**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ください。

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作成したマクロは、インターフェイスに適用できます。次の例では、**duplex** というユーザ作成の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 コマンドを使用します。インターフェイスに適用する場合に、マクロに構文エラーや設定エラーがないか確認できます。次の例では、インターフェイス上の **duplex** というユーザ作成のマクロのトラブルシューティング方法を示します。

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

次の例では、シスコのデフォルトの **cisco-desktop** マクロを表示する方法と、インターフェイス上でマクロを適用してアクセス VLAN（仮想 LAN）ID を 25 に設定する方法を示します。

```
Switch# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

関連コマンド

コマンド	説明
macro description	インターフェイスに適用されるマクロに関する記述を追加します。
macro global	スイッチにマクロを適用するか、スイッチにマクロを適用して追跡します。
macro global description	スイッチに適用されるマクロに関する記述を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロに対するマクロ定義を表示します。

macro description

どのマクロがインターフェイスに適用されているかという記述を入力するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。この記述を削除する場合は、このコマンドの **no** 形式を使用します。

macro description *text*

no macro description *text*

シンタックスの説明	description <i>text</i>	指定したインターフェイスに適用されるマクロに関する記述を入力します。

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
	12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン コメント テキストやマクロ名をインターフェイスと関連付けるには、**description** キーワードを使用します。複数のマクロが単一インターフェイスに適用されている場合、記述テキストは最後に適用されたマクロからのものになります。

次の例では、インターフェイスに記述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	インターフェイスにマクロを適用するか、インターフェイスにマクロを適用して追跡します。
	macro global	スイッチにマクロを適用するか、スイッチにマクロを適用して追跡します。
	macro global description	スイッチに適用されるマクロに関する記述を追加します。
	macro name	マクロを作成します。
	show parser macro	すべてのマクロまたは指定したマクロに対するマクロ定義を表示します。

macro global

スイッチにマクロを適用するか、またはスイッチにマクロ設定を適用してこれを追跡するには、スイッチ スタックまたはスタンドアロン スイッチ上で **macro global** グローバル コンフィギュレーション コマンドを使用します。

```
macro global {apply | trace} macro-name [parameter {value}] [parameter {value}][parameter {value}]
```

シンタックスの説明

apply	スイッチに対してマクロを適用します。
trace	スイッチにマクロを適用し、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) スイッチ特有の固有パラメータ値を指定します。最大 3 組のキーワード値のペアを入力できます。パラメータのキーワード照合では、大文字と小文字が区別されます。キーワードが一致した場合は、すべて該当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(20)SE	このコマンドが導入されました。

使用上のガイドライン

macro trace macro-name グローバル コンフィギュレーション コマンドを使用して、スイッチ上で動作しているマクロの適用や表示を行ったり、構文また設定エラーを判断するためにマクロをデバッグしたりできます。

マクロを適用する場合に、構文エラーまたは設定エラーのいずれかによりコマンドがエラーになっても、マクロは引き続き残りのコマンドをスイッチに適用します。

固有の値を割り当てる必要があるマクロを作成する場合、**parameter value** キーワードによってスイッチに特有の値を指定します。

キーワード照合では、大文字と小文字が区別されます。キーワードが一致した場合は、すべて該当する値に置き換えられます。完全に一致したキーワードは、長い文字列の一部の場合であっても、一致したとみなされ、該当する値に置き換えられます。

マクロによっては、パラメータ値を必要とするキーワードを含むものもあります。マクロで必要とされる任意の値のリストを表示するには、**macro global apply macro-name ?** コマンドを使用します。キーワードの値を入力せずにマクロを適用した場合、コマンドは無効になり、適用されません。

これは、スイッチ ソフトウェアに組み込まれたシスコのデフォルトの SmartPort マクロです。これらのマクロやマクロ内のコマンドを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

インターフェイス上でシスコのデフォルトの SmartPort マクロを適用する場合は、次の注意事項に留意してください。

- スイッチ上のマクロをすべて表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC コマンドを使用します。
- **\$** で始まるキーワードには、一意のパラメータ値が必要です。シスコのデフォルトのマクロに必要な値を付加するには、**parameter value** キーワードを使用します。
シスコのデフォルトのマクロでは、**\$** 文字を使用して、必要とされるキーワードを識別するのに役立っています。マクロ作成時にキーワードを定義するのに、**\$** 文字を使用する場合の制限事項はありません。

インターフェイスにマクロを適用すると、インターフェイスにマクロ名が自動的に追加されます。適用したコマンドとマクロ名を表示するには、**show running-configuration** ユーザ EXEC コマンドを使用します。

マクロに含まれる各コマンドの **no** 形式を入力することによってのみ、グローバルにマクロが適用し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作成したマクロを、スイッチに適用できます。次の例では、**snmp** マクロを表示する方法、およびマクロを適用し、ホスト名を **test-server** に設定して、IP precedence 値を 7 に設定する方法を示します。

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

-----
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

マクロをデバッグするには、**macro global trace** グローバル コンフィギュレーション コマンドを使用します。スイッチに適用する場合に、マクロに構文エラーや設定エラーがないか確認できます。次の例では、**ADDRESS** パラメータ値が入力されなかったために、残りのマクロがスイッチに適用されても、**snmp-server host** コマンドがエラーとなることを示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

関連コマンド

コマンド	説明
macro apply	インターフェイスにマクロを適用するか、インターフェイスにマクロを適用して追跡します。
macro description	インターフェイスに適用されるマクロに関する記述を追加します。
macro global description	スイッチに適用されるマクロに関する記述を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロに対するマクロ定義を表示します。

macro global description

スイッチに適用されているマクロに関する記述を入力するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。この記述を削除する場合は、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*

シンタックスの説明

description <i>text</i>	スイッチに適用されるマクロに関する記述を入力します。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン

コメント テキストやマクロ名をスイッチと関連付けるには、**description** キーワードを使用します。複数のマクロがスイッチに適用されている場合、記述テキストは最後に適用されたマクロからのものになります。

次の例では、スイッチに記述を追加する方法を示します。

```
Switch(config)# macro global description udlld 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	インターフェイスにマクロを適用するか、インターフェイスにマクロを適用して追跡します。
macro description	インターフェイスに適用されるマクロに関する記述を追加します。
macro global	スイッチにマクロを適用するか、スイッチにマクロを適用して追跡します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロに対する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、スイッチ スタックまたはスタンドアロン スイッチ上で **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*

シンタックスの説明

<i>macro-name</i>	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
12.1(19)EA1	このコマンドが導入されました。
12.2(20)SE	ヘルプ スtring # macro keywords が追加されました。

使用上のガイドライン

マクロには、最大 3000 文字を含めることができます。1 行ごとにマクロ コマンドを 1 つ入力します。マクロの終わりには **@** 文字を使用します。マクロ内にコメント テキストを入力するには、行頭に **#** 文字を使用します。

キーワードを指定するのに、ヘルプ スtringを使用してマクロ内の必須キーワードを定義します。マクロとともに使用できるキーワードを定義するには、**# macro keywords word** を入力します。スペースで区切られたヘルプ スtringを最大 3 つまで入力できます。3 つ以上のマクロ キーワードを入力した場合は、最初の 3 つのみが表示されます。

マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** および **macro name sample-macro** は、2 つの別々のマクロになります。

マクロ作成時には、**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を変更したりしないでください。**exit**、**end**、または **interface interface-id** に続くコマンドが、別のコマンド モードで実行されてしまいます。

このコマンドの **no** 形式は、マクロ定義を削除するだけです。マクロがすでに適用されているインターフェイスの設定には影響しません。マクロがインターフェイスに適用した設定を削除するには、**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ください。別の方法として、元のマクロ内にあるすべての対応するコマンドの **no** 形式を含む既存のマクロに対しての方法 **anti-macro** を作成できます。その後、インターフェイスに **anti-macro** を適用します。

マクロを変更するには、既存のマクロと同じ名前の新しいマクロを作成してください。新しく作成されたマクロは既存のマクロを上書きしますが、元のマクロが適用されていたインターフェイスの設定には影響しません。

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
@
```

次の例では、**# macro keywords** を使用してマクロを作成する方法を示します。

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

次の例では、マクロをインターフェイスに適用する前に、必須キーワード値を表示する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# macro apply test ?
WORD keyword to replace with a value e.g. $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
```

```
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g. $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID 2 $MAX ?
WORD Value of second keyword to replace
```

関連コマンド

コマンド	説明
macro apply	インターフェイスにマクロを適用するか、インターフェイスにマクロを適用して追跡します。
macro description	インターフェイスに適用されるマクロに関する記述を追加します。
macro global	スイッチにマクロを適用するか、スイッチにマクロを適用して追跡します。
macro global description	スイッチに適用されるマクロに関する記述を追加します。
show parser macro	すべてのマクロまたは指定したマクロに対するマクロ定義を表示します。

match (アクセスマップ コンフィギュレーション)

VLAN (仮想 LAN) マップを設定して、パケットを1つまたは複数のアクセス リストと照合するには、スイッチ スタックまたはスタンドアロン スイッチ上で **match** アクセスマップ コンフィギュレーション コマンドを使用します。一致パラメータを削除する場合は、このコマンドの **no** 形式を使用します。

```
match {ip address {name | number} [name | number] [name | number]...} | {mac address {name} [name] [name]...}
```

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

シンタックスの説明	ip address パケットを IP アドレス アクセス リストと照合するためのアクセス マップを設定します。
mac address	パケットを MAC (メディア アクセス制御) アドレス アクセス リストと照合するためのアクセス マップを設定します。
<i>name</i>	パケットの照合先となるアクセス リストの名前
<i>number</i>	パケットの照合先となるアクセス リストの番号。このオプションは、MAC アクセス リストに使用できません。

デフォルト VLAN マップに適用された一致パラメータはありません。

コマンド モード アクセスマップ コンフィギュレーション

コマンド履歴	リリース 変更内容
	12.1(11)AX このコマンドが導入されました。

使用上のガイドライン **vlan access-map** グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

アクセス リスト名または番号を1つ入力する必要があります。その他はオプションです。1つまたは複数のリストに対してパケットの照合を行うことができます。リスト内で一致したものは、エントリの一致とみなされます。

アクセスマップ コンフィギュレーション モードで、**match** コマンドを使用し、VLAN に適用する VLAN マップの一致条件を定義します。パケットが条件に一致した場合に発生するアクションを設定するには、**action** コマンドを使用します。

パケットは、同一のプロトコル タイプのアクセス リストに対してのみ照合されます。IP パケットは IP アクセス リストに対して、他のパケットは MAC アクセス リストに対して照合されます。

IP および MAC アドレスは同一のマップ エントリで指定できます。

■ match (アクセスマップコンフィギュレーション)

例

次の例では、アクセス リスト *al2* に定義された一致条件とパケットが一致した場合、インターフェイスが IP パケットを廃棄するようにする VLAN アクセス マップ *vmap4* を定義して、VLAN 5 および VLAN 6 に適用する方法を示します。

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

設定を確認するには、**show vlan access-map** 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
access-list	標準番号付き Access Control List (ACL; アクセス制御リスト) 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。
action	パケットが ACL のエントリと一致した場合にとられるアクションを指定します。
ip access list	名前付きアクセス リストを作成します。構文情報については、 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands を選択してください。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
show vlan access-map	スイッチ上に作成されている VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

match (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 **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。一致条件を削除する場合は、このコマンドの **no** 形式を使用します。

```
match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip
precedence ip-precedence-list}
```

```
no match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip
precedence ip-precedence-list}
```

シンタックスの説明

access-group <i>acl-index-or-name</i>	IP 標準または拡張 Access Control List (ACL; アクセス制御リスト) や MAC (メディア アクセス制御) ACL の番号または名前。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
input-interface <i>interface-id-list</i>	階層型ポリシー マップのインターフェイスレベル クラス マップが適用される物理ポートを指定します。1 つのポート (1 つのエントリとみなす)、スペースで区切られたポートのリスト (各ポートを 1 つのエントリとみなす)、またはハイフンで区切られたポート範囲 (2 つのエントリとみなす) を指定することにより、リスト内で最大 6 つのエントリを指定できます。
ip dscp <i>dscp-list</i>	着信パケットと照合するために指定する、最大 8 個までの IP Differentiated Services Code Point (DSCP) 値のリスト。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。汎用的に使用する値に対してはニーモニック名を入力することもできます。
ip precedence <i>ip-precedence-list</i>	着信パケットと照合する最大 8 個までの IP precedence 値のリスト。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。汎用的に使用する値に対して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

一致条件は定義されません。

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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	input-interface <i>interface-id-list</i> キーワードが追加されました。

使用上のガイドライン

パケットを分類するために、着信パケットのどのフィールドを調べる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 に対するマッチングのみサポートされます。

物理ポート ベースでパケットの分類を定義するために、クラス マップごとに **match** コマンドがサポートされています。この場合、**match-all** および **match-any** キーワードは同等です。

match (クラスマップコンフィギュレーション)

match ip dscp dscp-list または **match ip precedence ip-precedence-list** コマンドについては、汎用的に使用する値用に、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、**match ip dscp 10** コマンドとして入力しても同じ結果になります。**match ip precedence critical** コマンドを、**match ip precedence 5** コマンドとして入力しても同じ結果になります。サポートされているニーモニックの一覧に関しては、**match ip dscp ?** または **match ip precedence ?** コマンドを入力し、コマンドラインのヘルプ スtring を参照してください。

階層型ポリシー マップでインターフェイスレベル クラス マップを設定している場合は、**input-interface interface-id-list** キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定できます。

例

次の例では、*class2* というクラス マップを作成する方法を示します。このクラス マップは、10、11、12 の DSCP 値を持つ着信トラフィックと一致します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次の例では、*class3* と呼ばれるクラス マップを作成する方法を示します。クラス マップは、5、6、7 の IP precedence 値を持つ着信トラフィックと一致します。

```
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 の一致条件を削除し、*acl1* を使用してトラフィックを分類する方法を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

次の例では、階層型ポリシー マップのインターフェイスレベル クラス マップが適用される物理ポートのリストを指定する方法を示します。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 gigabitethernet2/0/2
Switch(config-cmap)# exit
```

次の例では、階層型ポリシー マップのインターフェイスレベル クラス マップが適用される物理ポート範囲を指定する方法を示します。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 - gigabitethernet2/0/5
Switch(config-cmap)# exit
```

設定を確認するには、**show class-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を照合する場合に使用されるクラス マップを作成します。
show class-map	Quality of Service (QoS; サービス品質) クラス マップを表示します。

mdix auto

インターフェイス上で Automatic Media-Dependent-Interface Crossover (Auto-MDIX) 機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。Auto-MDIX がイネーブルになると、インターフェイスは自動的に必要なケーブル接続のタイプ（ストレートまたはクロス）を検出し、適切な接続を設定します。Auto-MDIX をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdix auto

no mdix auto

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Auto-MDIX はイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.2(18)SE	デフォルト設定が、ディセーブルからイネーブルに変更されました。

使用上のガイドライン

インターフェイス上で Auto-MDIX をイネーブルにする場合、この機能が正常に動作するように、インターフェイスの速度およびデュプレックスも **auto** に設定する必要があります。

接続されたインターフェイス上の片方または両方で、Auto-MDIX をイネーブルにした（速度およびデュプレックスの自動ネゴシエーションに対応させた）場合、ケーブル タイプ（ストレートまたはクロス）が適切でない場合でもリンクがオンになります。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps（メガビット/秒）インターフェイス上および 10/100/1000BASE-TX Small Form-Factor Pluggable (SFP) モジュール インターフェイス上でサポートされます。1000BASE-SX、1000BASE-LX SFP モジュール インターフェイス上ではサポートされません。

例

次の例では、ポートで Auto-MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスでの Auto-MDIX の動作状態を確認するには、**show controllers ethernet-controller interface-id phy** 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 controllers ethernet-controller interface-id phy	インターフェイスの内部レジスタの一般情報（Auto-MDIX の動作状態を含む）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、スイッチ スタックまたはスタンドアロン スイッチ上で **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** コマンドが入力されると、システム内のすべてのポート上のデフォルトのパラメータで QoS がイネーブルになります。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos

no mls qos

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS はディセーブルです。この場合、パケットは修正されないため (パケットの CoS [サービス クラス]、Differentiated Services Code Point [DSCP]、IP precedence の値は変更されません)、ポートの信頼性に関する概念がなくなります。トラフィックは Pass-Through モードに切り替わります (パケットは書き換えなしにスイッチングされ、ポリシングなしのベスト エフォートに分類されます)。

mls qos グローバル コンフィギュレーション コマンドで QoS がイネーブルになり、他のすべての QoS の設定がデフォルトの状態であれば、トラフィックは、ポリシングなしのベスト エフォートとして分類されます (DSCP 値および CoS 値は 0 に設定)。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼状態は、信頼性なし (untrusted) の状態です。デフォルトの入力および出力キューの設定が有効です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

QoS 分類、ポリシング、マーク ダウンまたは廃棄、キューイング、およびトラフィックのシェーピング機能を使用するため、QoS は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、ポートに適用できます。ただし、**mls qos** コマンドを入力していない場合、QoS 処理はディセーブルになります。

QoS 設定に使用されるポリシーマップおよびクラスマップは、**no mls qos** コマンドでコンフィギュレーションから削除されません。ただし、ポリシーマップに対応するエントリは、システム リソースを確保するためにスイッチ ハードウェアから削除されます。以前の設定で QoS を再度イネーブルにする場合、**mls qos** コマンドを使用します。

このコマンドでスイッチの QoS ステータスを切り替えることで、キューのサイズが変更 (再割り当て) されます。キューのサイズ変更の間、ハードウェアの再設定時に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用に新規に着信したパケットを廃棄します。

例

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

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

設定を確認するには、**show mls qos** 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
<code>show mls qos</code>	QoS 情報を表示します。

mls qos aggregate-policer

ポリサー パラメータを定義するには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。これは、同一のポリシー マップ内の複数のクラスで共有できます。ポリサーは最大許容送信レート、送信の最大バースト サイズ、および最大値を超えた場合にとられるアクションを定義します。アグリゲート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
```

シンタックスの説明

<i>aggregate-policer-name</i>	police aggregate ポリシーマップ クラス コンフィギュレーション コマンドで参照されるアグリゲート ポリサー名。
<i>rate-bps</i>	平均トラフィック レートをビット / 秒 (bps) で指定します。指定できる範囲は、8000 ~ 1000000000 です。
<i>burst-byte</i>	通常のパーストサイズ (バイト) を指定します。指定できる範囲は、8000 ~ 1000000 です。
exceed-action drop	指定されたレートを超えると、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	指定されたレートを超えると、スイッチがパケットの Differentiated Services Code Point (DSCP) を、ポリシングされた DSCP マップで指定された DSCP に変更し、パケットを送信するよう指定します。

デフォルト

アグリゲート ポリサー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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

ポリサーが複数のクラスで共有されている場合、アグリゲート ポリサーを定義します。

1 つのポートに対するポリサーは、別のポートの他のポリサーと共有できません。2 つの異なるポートからのトラフィックは、ポリシー目的で集約できません。

物理ポートを複数制御するポートの Application Specific Integrated Circuit (ASIC; 特定用途向け IC) 装置は、256 のポリサー (255 のポリサーと 1 つの **no** ポリサー) をサポートします。ポート単位でサポートされるポリサーの最大数は 64 です。ポリサーはソフトウェアの要求に応じて割り当てられ、ハードウェアおよび ASIC の限度で制限されます。ポートごとにポリサーを保存できません (ポートに割り当てられるポリサーに対する保証はありません)。

同一のポリシー マップで、アグリゲート ポリサーを複数のクラスに適用できます。異なるポリシー マップでアグリゲート ポリサーを使用することはできません。

ポリシー マップで使用中のアグリゲート ポリサーは削除できません。**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 コマンドを最初に使用し、すべてのポリシー マップからアグリゲート 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。**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、バケットの深さ（バケットが溢れるまで耐えられる最大バースト値）を設定します。**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、または **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドの *rate-bps* オプションを使用し、バケットから削除されるトークンの速度（平均レート）を設定します。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、アグリゲート ポリサーのパラメータを定義する方法およびポリシー マップ内の複数のクラスにポリサーを適用する方法を示しています。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 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
police aggregate	異なるクラスで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) アグリゲート ポリサーの設定を表示します。

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、ポート上のすべての着信パケットにデフォルトの CoS 値を割り当てたりするには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos cos** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos cos {default-cos | override}
```

```
no mls qos cos {default-cos | override}
```

シンタックスの説明

<i>default-cos</i>	デフォルト CoS 値をポートに割り当てます。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。
override	着信パケットの CoS を無効にし、すべての着信パケットにデフォルトのポート CoS 値を適用します。

デフォルト

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

デフォルト値を使用して、CoS および Differentiated Services Code Point (DSCP) 値を、タグ付けされていない (着信パケットが CoS 値を持っていない場合) すべての着信パケットに割り当てることができます。また、**override** キーワードを使用して、デフォルトの CoS および 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または低いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドはその設定された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 値を割り当てます。着信パケットがタグ付きの場合、パケットの CoS 値は、入力ポートで、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、ポートでデフォルト ポート CoS を 4 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

次の例では、ポートで、ポートに着信するパケットすべてにデフォルト ポート CoS 値の 4 を割り当てる方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

設定を確認するには、**show mls qos interface** 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 mls qos interface	QoS 情報を表示します。

mls qos dscp-mutation

Differentiated Services Code Point (DSCP) の信頼性のあるポートに対して、DSCP/DSCP 合成マップを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 の合成なし) 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*

シンタックスの説明

<i>dscp-mutation-name</i>	DSCP/DSCP 合成マップ名。このマップは以前 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たものです。

デフォルト

デフォルトの DSCP/DSCP 合成マップはヌルのマップです。これによって、着信 DSCP が同一の DSCP 値に対してマッピングされます。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

2 つの Quality of Service (QoS; サービス品質) ドメインが保有する DSCP の定義が異なる場合、DSCP/DSCP 合成マップを使用し、他のドメインの定義に一致するように DSCP 値のセットを変換します。DSCP/DSCP 合成マップを、QoS 管理ドメインの境界にある受信ポート (入力合成) に適用します。

入力合成を使用して新しい DSCP 値でパケット内の DSCP 値が上書きされ、QoS はこの新しい値でパケットを処理します。スイッチは新しい DSCP 値でポートにパケットを送信します。

入力ポート上では複数の DSCP/DSCP 合成マップを設定できます。

マップは DSCP の信頼性があるポートに対してのみ適用されます。DSCP/DSCP 合成マップを信頼性のないポート、CoS または IP precedence の信頼性のあるポートに適用した場合、コマンドはポートが DSCP の信頼性を得るまで有効になりません。

例

次の例では、*dscpmutation1* という名前の DSCP/DSCP 合成マップを定義し、ポートにマップを適用する方法を示します。

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

次の例では、*dscpmutation1* という名前の DSCP/DSCP 合成マップをポートから削除し、マップをデフォルトにリセットする方法を示します。

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

設定を確認するには、**show mls qos maps** 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 map dscp-mutation	DSCP/DSCP 合成マップを定義します。
mls qos trust	ポートの信頼状態を設定します。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos map

Class of Service (CoS; サービス クラス) /Differentiated Services Code Point (DSCP) マップ、DSCP/CoS マップ、DSCP/DSCP 合成マップ、IP precedence/DSCP マップ、およびポリシングされた DSCP のマップを定義するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}
```

シンタックスの説明

cos-dscp <i>dscp1...dscp8</i>	CoS/DSCP マップを定義します。 <i>dscp1...dscp8</i> には、CoS 値 0 ～ 7 に対応した 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 <i>dscp-list to cos</i>	DSCP/CoS マップを定義します。 <i>dscp-list</i> には、最大 8 個の DSCP 値をスペースで区切って入力します。指定できる範囲は 0 ～ 63 です。その後ろに、 to キーワードを入力します。 <i>cos</i> 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 <i>dscp-mutation-name</i> <i>in-dscp to out-dscp</i>	DSCP/DSCP 合成マップを定義します。 <i>dscp-mutation-name</i> には、合成マップ名を入力します。 <i>in-dscp</i> には、最大 8 個の DSCP 値をスペースで区切って入力します。その後ろに、 to キーワードを入力します。 <i>out-dscp</i> には、単一の DSCP 値を入力します。 指定できる範囲は、0 ～ 63 です。
ip-prec-dscp <i>dscp1...dscp8</i>	IP precedence/DSCP マップを定義します。 <i>dscp1...dscp8</i> には、IP precedence 値 0 ～ 7 に対応した 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 <i>dscp-list to mark-down-dscp</i>	ポリシングされた DSCP マップを定義します。 <i>dscp-list</i> には、最大 8 個の DSCP 値をスペースで区切って入力します。その後ろに、 to キーワードを入力します。 <i>mark-down-dscp</i> には、対応するポリシングされた（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 合成マップはヌルのマップです。これによって、着信 DSCP が同一の DSCP 値に対してマッピングされます。

デフォルトのポリシングされた DSCP マップはヌルのマップです。これによって、着信 DSCP が同一の DSCP 値に対してマッピングされます。

コマンドモード グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

マップはすべてグローバルに定義されています。DSCP/DSCP 合成マップ以外のすべてのマップはすべてのポートに適用されます。DSCP/DSCP 合成マップは指定のポートに対して適用されます。

例

次の例では、IP precedence/DSCP マップを定義し、DSCP 値 (0、10、20、30、40、50、55、60) に IP precedence 値 (0 ～ 7) を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、ポリシングされた 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。マーキングされた DSCP 値で、明示的に設定されていないものは修正されません。

```
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 合成マップを定義する方法を示します。すべてのエントリで、明示的に設定されていないものは修正されません (ヌルのマップで指定されているままになります)。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

設定を確認するには、**show mls qos maps** 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 dscp-mutation	DSCP/DSCP 合成マップを DSCP の信頼性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

キューセット（各ポートの4つの出力キュー）にバッファを割り当てるには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos queue-set output buffers** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos queue-set output *qset-id* buffers *allocation1* ... *allocation4*

no mls qos queue-set output *qset-id* buffers

シンタックスの説明

<i>qset-id</i>	キューセットの ID。キューセットに属する各ポートの4つの出力キューのすべての特性を定義します。指定できる範囲は、1～2です。
<i>allocation1</i> ... <i>allocation4</i>	各キュー（キュー1～4の4つの値）に割り当てられたバッファ領域（%）。 <i>allocation1</i> 、 <i>allocation3</i> 、および <i>allocation4</i> で指定できる範囲は 0～99 です。 <i>allocation2</i> の場合は 1～100 です（CPU バッファを含む）。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つのキュー間で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領域の1/4を使用します。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.2(18)SE	指定できる <i>allocation2</i> の範囲が、0～100 から 20～100 に変更されました。
12.2(20)SE	<i>allocation1</i> 、 <i>allocation3</i> 、および <i>allocation4</i> の範囲が、0～100 から 0～99 に変更されました。 <i>allocation2</i> は、20～100 から 1～100 に変更されました。

使用上のガイドライン

4つの割り当て値を指定し、各値はスペースで区切ります。

トラフィックの重要性に合わせてバッファを割り当てます。たとえば、プライオリティが最高のトラフィックのキューにはバッファ領域を多く与えます。

異なるトラフィックのクラスを、異なる特性で設定するには、このコマンドを **mls qos queue-set output *qset-id* threshold** グローバル コンフィギュレーション コマンドとともに使用します。



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更してください。

例

次の例では、ポートをキューセット2にマッピングする方法を示します。バッファ領域の40%を出力キュー1に、20%ずつを出力キュー2、3、4に割り当てます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** 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 threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、キューセットに最大のメモリ割り当てを設定します。
queue-set	キューセットに対し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	キューセットに対する出力キューの設定を表示します。

mls qos queue-set output threshold

Weighted Tail-drop (WTD) スレッシュホールドを設定することで、バッファの可用性を保証し、キューセット（各ポートの 4 つの出力キュー）に対して最大のメモリ割り当てを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos queue-set output threshold** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2
reserved-threshold maximum-threshold
```

```
no mls qos queue-set output qset-id threshold [queue-id]
```

シンタックスの説明

<i>qset-id</i>	キューセットの ID。キューセットに属する各ポートの 4 つの出力キューのすべての特性を定義します。指定できる範囲は、1 ～ 2 です。
<i>queue-id</i>	コマンドが実行されるキューセットで指定するキュー。指定できる範囲は、1 ～ 4 です。
<i>drop-threshold1</i> <i>drop-threshold2</i>	メモリに割り当てられたキューのパーセンテージで表される 2 つの WTD スレッシュホールド。指定できる範囲は 1 ～ 400% です。
<i>reserved-threshold</i>	キューに保証される（予約される）メモリの容量。これは割り当てられるメモリのパーセンテージで表されます。指定できる範囲は 1 ～ 100% です。
<i>maximum-threshold</i>	最大の状態でキューをイネーブルにし、予約された以上のバッファを取得します。これはパケットが廃棄される前にキューが使用できる最大のメモリ容量です。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) がイネーブルであれば、WTD もイネーブルになります。

表 2-9 に、デフォルトの WTD スレッシュホールドの設定を示します。

表 2-9 デフォルトの出力キューの WTD スレッシュホールドの設定

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

12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

固定されたバッファ数をキューセットの 4 つのキューに割り当てるには、**mls qos queue-set output qset-id buffers** グローバル コンフィギュレーション コマンドを使用します。

廃棄スレッシホールドのパーセンテージは 100% より多くすることが可能で、最大まで設定できます（最大スレッシホールドが 100% を超えている場合）。



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更してください。

スイッチは各出力キューに最低量のバッファを予約するバッファの割り当て方式を使用し、キューやポートがバッファをすべて消費してしまったり、他のキューのバッファを使用したりすることのないよう、要求キューに対しバッファ領域を許可するかどうかを判断します。スイッチは目的のキューが予約された量（制限内）以上のバッファを消費したかどうかを判断します。また、最大バッファ（制限以上）のすべてを消費したかどうか、一般プールが空いているかどうか（バッファの空きがあるか）を判断します。キューが制限を超えていない場合、スイッチは、予約プールまたは一般プール（空いていれば）からバッファ領域を割り当てます。一般プールにバッファの空きがない場合、またはキューが制限を超えている場合、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 の廃棄スレッシホールドに 40% および 60% の割り当てメモリを設定し、割り当てメモリの 100% を保証（予約）します。また、パケットが廃棄される前にキューが確保できる最大メモリとして 200% を設定します。

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** インタープリ 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	キューセットに対しバッファを割り当てます。
queue-set	キューセットに対し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	キューセットに対する出力キューの設定を表示します。

mls qos rewrite ip dscp

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）ようスイッチを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。パケットの DSCP フィールドの修正（書き換え）を行わず、DSCP トランスペアレンシーをイネーブルにするようスイッチを設定する場合は、このコマンドの **no** 形式を使用します。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DSCP トランスペアレンシー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)SE	このコマンドが導入されました。

使用上のガイドライン

DSCP トランスペアレンシーは、出力するときのパケットの DSCP フィールドにのみ影響を与えます。**no mls qos rewrite ip dscp** コマンドを使用して DSCP トランスペアレンシーをイネーブルにする場合、スイッチは着信パケットの DSCP フィールドを修正せず、発信パケットの DSCP フィールドは着信パケットの DSCP フィールドと同じです。



(注)

DSCP トランスペアレンシーをイネーブルにすると、IEEE（米国電気電子学会）802.1Q トンネリング ポート上のポートの信頼性の設定には影響しません。

デフォルトでは、DSCP トランスペアレンシーはディセーブルです。スイッチは着信パケットの DSCP フィールドを修正します。発信パケットの DSCP フィールドは、ポートの信頼性の設定、ポリシングおよびマーキング、DSCP/DSCP 合成マップなど Quality of Service (QoS; サービス品質) の設定に基づいています。

DSCP トランスペアレンシーの設定に関係なく、スイッチはトラフィックのプライオリティを示す Class of Service (CoS; サービス クラス) 値を生成するのに使用するパケットの内部 DSCP 値を修正します。また、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のに内部 DSCP 値を使用します。

たとえば、QoS がイネーブルで、着信パケットの DSCP 値が 32 である場合、スイッチはポリシー マップ設定に基づき内部 DSCP 値を修正し、この値を 16 に変更します。DSCP トランスペアレンシーがイネーブルの場合、発信 DSCP 値は 32 です（着信 DSCP 値と同じ）。DSCP トランスペアレンシーがディセーブルの場合、発信 DSCP 値は内部 DSCP 値に基づくので 16 となります。

例 次の例では、DSCP トランスペアレンシーをイネーブルにし、着信 IP パケットの DSCP 値を変更しないようスイッチを設定する方法を示します。

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

次の例では、DSCP トランスペアレンシーをディセーブルにし、着信 IP パケットの DSCP 値を変更するようスイッチを設定する方法を示します。

```
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 トランスペアレンシー設定を表示します。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

入力キューに Shaped Round Robin (SRR; シェイプドラウンドロビン) ウェイトを割り当てるには、スイッチスタックまたはスタンドアロン スイッチ上で **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。ウェイトの比率は、SRR スケジューラが各キューからパケットをデキューイングする頻度の比率です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos srr-queue input bandwidth *weight1 weight2*

no mls qos srr-queue input bandwidth

シンタックスの説明

weight1 weight2 *weight1* および *weight2* の比率は、SRR スケジューラが入力キュー 1 および 2 からパケットをデキューイングする頻度の比率を決定します。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

ウェイト 1 およびウェイト 2 が 4 に設定されています (2 つのキューが帯域幅を 1/2 ずつ共有します)。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

SRR は、**mls qos srr-queue input priority-queue *queue-id* bandwidth *weight*** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定した設定のウェイトに対するプライオリティ キューを処理します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth *weight1 weight2*** グローバル コンフィギュレーション コマンドで設定されたウェイトで指定されている通りに処理します。

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、どの入力キューがプライオリティ キューになるかを指定します。

例

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。プライオリティ キューイングはディセーブルで、キュー 1 に割り当てられる共有帯域幅の比率は 25/(25+75)、キュー 2 には 75/(25+75) とします。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

この例では、キュー 2 はキュー 1 の 3 倍の帯域幅を持ち、キュー 1 よりも 3 倍の頻度で処理されます。

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 およびキュー 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、設定された 10% の帯域幅でキュー 1 (プライオリティ キュー) を処理します。その後、SRR はキュー 1 およびキュー 2 の間に残っている 90% の帯域幅を均等に割り当てます (各キューに 45% の割り当て)。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** または **show mls qos input-queue** 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 srr-queue input buffers	入力キュー間に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、または CoS 値をキューおよびスレッシホールド 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、または DSCP 値をキューおよびスレッシホールド 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	入力キューに対し Weighted Tail-Drop (WTD) スレッシホールドのパーセンテージを割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service (QoS; サービス品質) 情報を表示します。

mls qos srr-queue input buffers

入力キュー間にバッファを割り当てるには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos srr-queue input buffers** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos srr-queue input buffers *percentage1 percentage2*

no mls qos srr-queue input buffers

シンタックスの説明

percentage1 percentage2 入力キュー 1 および 2 に割り当てるバッファのパーセンテージ。指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。

デフォルト

バッファの 90% がキュー 1 に、10% がキュー 2 に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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

バースト性がある着信トラフィックでも、キューが処理できるようにバッファを割り当ててください。

例

次の例では、バッファ領域の 60% を入力キュー 1 に、40% を入力キュー 2 に割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos input-queue** インタープリタ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR; シェイブドラウンドロビン) ウェイトを割り当てます。
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、または 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、または 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	入力キューに対し Weighted Tail-Drop (WTD) スレッシュホールドのパーセンテージを割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	Quality of Service (QoS; サービス品質) 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、または 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 **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻す場合は、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
```

シンタックスの説明

queue queue-id	キュー番号を指定します。 <i>queue-id</i> 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。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 7 です。
threshold threshold-id cos1...cos8	CoS 値をキューのスレッシュホールド ID にマッピングします。 <i>threshold-id</i> に指定できる範囲は 1 ～ 3 です。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 7 です。

デフォルト

表 2-10 に、デフォルトの CoS 入力キューのスレッシュホールドのマッピングを示します。

表 2-10 デフォルトの CoS 入力キューのスレッシュホールドのマッピング

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

入力ポートで割り当てられた CoS は、入力キューまたは出力キュー、およびスレッシュホールドを選択します。

スレッシュホールド 3 の廃棄スレッシュホールドのパーセンテージはあらかじめ定義されます。パーセンテージはキューがいっぱいの状態に設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用して、2 つの Weighted Tail-drop (WTD) スレッシュホールドのパーセンテージを入力キューに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対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、CoS 値 0 ～ 3 を入力キュー 1 およびスレッシュホールド ID の 1（廃棄スレッシュホールドは 50%）にマッピングする方法を示します。CoS 値 4、5 を入力キュー 1 およびスレッシュホールド ID の 2（廃棄スレッシュホールドは 70%）にマッピングします。

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 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 srr-queue input bandwidth	入力キューに対し Shaped Round Robin（SRR; シェイブドラウンドロビン）ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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	入力キューに対し WTD スレッシュホールドのパーセンテージを割り当てます。
show mls qos maps	Quality of Service（QoS; サービス品質）の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、または 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 **mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻す場合は、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
```

シンタックスの説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> に指定できる範囲は 1 ～ 2 です。
<i>dscp1...dscp8</i>	DSCP 値を入力キューにマッピングします。 <i>dscp1...dscp8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 63 です。
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	DSCP 値をキューのスレッシュホールド ID にマッピングします。 <i>threshold-id</i> に指定できる範囲は 1 ～ 3 です。 <i>dscp1...dscp8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 63 です。

デフォルト

表 2-11 に、デフォルトの DSCP 入力キューのスレッシュホールドのマッピングを示します。

表 2-11 デフォルトの DSCP 入力キューのスレッシュホールドのマッピング

DSCP 値	キュー ID — スレッシュホールド 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

入力ポートで割り当てられた DSCP は入力キューまたは出力キュー、およびスレッシュホールドを選択します。

スレッシュホールド 3 の廃棄スレッシュホールドのパーセンテージはあらかじめ定義されます。パーセンテージはキューがいっぱいの状態に設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用して、2 つの Weighted Tail-drop (WTD) スレッシュホールドのパーセンテージを入力キューに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対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

コマンドごとに最大 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 およびスレッシュホールド 1（廃棄スレッシュホールドは 50%）にマッピングする方法を示しています。DSCP 値 20 ～ 26 を入力キュー 1 およびスレッシュホールド 2（廃棄スレッシュホールドは 70%）にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25
26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 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 srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR; シェイブドラウンドロビン) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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 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	入力キューに対し WTD スレッシュホールドのパーセンテージを割り当てます。
show mls qos maps	Quality of Service (QoS; サービス品質) のマッピング情報を表示します。

mls qos srr-queue input priority-queue

リングが輻輳している場合、入力プライオリティ キューを設定して、スタック リング上で帯域幅を保証するには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos srr-queue input priority-queue queue-id bandwidth weight

no mls qos srr-queue input priority-queue queue-id

シンタックスの説明

<i>queue-id</i>	入力のキュー ID。指定できる範囲は 1 ～ 2 です。
<i>bandwidth weight</i>	スタック リングの帯域幅のパーセンテージ。指定できる範囲は、0 ～ 40 です。

デフォルト

プライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

プライオリティ キューは、優先する必要があるトラフィックにのみ使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューはスタック リング上で帯域幅の一部として保証され、オーバー サブスクライブ型のスタック上（バックプレーンが送受信する以上のトラフィック、またはキューが満杯でフレームを廃棄している状態）の大量のネットワーク トラフィックによる遅延とジッタを軽減します。

大きい値はスタック全体に影響を与え、スタック パフォーマンスを低下させるため、保証される帯域幅の合計は制限されます。

Shaped Round Robin (SRR; シェイブドラウンドロビン) 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** キーワードで指定した設定のウェイトに対するプライオリティ キューを処理します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドで設定されたウェイトで指定されている通りに処理します。

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、帯域幅のウェイトを 0 に設定します（たとえば、**mls qos srr-queue input priority-queue queue-id bandwidth 0**）。

例

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 およびキュー 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、設定された 10% の帯域幅でキュー 1（プライオリティ キュー）を処理します。その後、SRR はキュー 1 およびキュー 2 の間に残っている 90% の帯域幅を均等に割り当てます（各キューに 45% の割り当て）。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** または **show mls qos input-queue** 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 srr-queue input bandwidth	入力キューに対し SRR ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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、または 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 threshold	入力キューに対し Weighted Tail-Drop (WTD) スレッシュホールドのパーセンテージを割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service (QoS; サービス品質) 情報を表示します。

mls qos srr-queue input threshold

入力キューに Weighted Tail-drop (WTD) スレッシュホールドのパーセンテージを割り当てるには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2
```

```
no mls qos srr-queue input threshold queue-id
```

シンタックスの説明

<i>queue-id</i>	入力キューの ID。指定できる範囲は、1 ～ 2 です。
<i>threshold-percentage1</i>	2 つの WTD スレッシュホールド パーセンテージの値。各スレッシュホールド値は、キューに割り当てられたキュー記述子の総数のパーセンテージです。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。
<i>threshold-percentage2</i>	

デフォルト

Quality of Service (QoS; サービス品質) がイネーブルであれば、WTD もイネーブルになります。
2 つの WTD スレッシュホールドは 100% に設定されています。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

QoS は Class of Service (CoS; サービス クラス) / スレッシュホールド マップまたは Differentiated Services Code Point (DSCP) / スレッシュホールド マップを使用し、スレッシュホールド 1 および 2 に対してマッピングされている、CoS または DSCP 値を判断します。スレッシュホールド 1 を超えている場合、このスレッシュホールドに割り当てられている CoS または DSCP を持つパケットは、スレッシュホールドを超えない状態になるまで廃棄されます。ただし、スレッシュホールド 2 に割り当てられたパケットのキューイングは継続され、スレッシュホールド 2 を超えないかぎり送信が続行されます。

各キューは、設定可能な（明示的）廃棄スレッシュホールドを 2 つ、および事前設定された（暗黙的）廃棄スレッシュホールド（full）を 1 つ持っています。

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、CoS/ スレッシュホールド マップを設定します。また、**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、DSCP/ スレッシュホールド マップを設定します。

例

次の例では、2 つのキューのテールドロップ廃棄スレッシュホールドを設定する方法を示します。キュー 1 のスレッシュホールドは 50% および 100% で、キュー 2 のスレッシュホールドは 70% および 100% です。

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos input-queue** 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 srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR; シェイプド ラウンド ロビン) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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、または 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。
show mls qos input-queue	入力キューの設定を表示します。
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、または 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 **mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻す場合は、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
```

シンタックスの説明

queue queue-id	キュー番号を指定します。 <i>queue-id</i> 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。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 7 です。
threshold threshold-id cos1...cos8	CoS 値をキューのスレッシュホールド ID にマッピングします。 <i>threshold-id</i> に指定できる範囲は 1 ～ 3 です。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 7 です。

デフォルト

表 2-12 に、デフォルトの CoS 出力キューのスレッシュホールドのマッピングを示します。

表 2-12 デフォルトの CoS 出力キューのスレッシュホールドのマッピング

CoS 値	キュー ID — スレッシュホールド 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スレッシュホールド 3 の廃棄スレッシュホールドのパーセンテージはあらかじめ定義されます。パーセンテージはキューがいっぱいの状態に設定されます。



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更できます。

mls qos queue-set output *qset-id* threshold グローバル コンフィギュレーション コマンドを使用して、2 つの Weighted Tail-drop (WTD) スレッシュホールドのパーセンテージを出力キューに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対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ～ 3 を出力キュー 1 および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に 50% および 70% の割り当てメモリを設定し、割り当てメモリの 100% を保証 (予約) します。また、パケットが廃棄される前にキューが確保できる最大メモリとして 200% を設定します。

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface *[interface-id]* buffers** または **show mls qos queue-set** 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 srr-queue output dscp-map	Differentiated Services Code Point (DSCP) 値を出力キューにマッピング、または 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 queue-set output threshold	WTD スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
queue-set	キューセットに対し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 のマッピング情報を表示します。
show mls qos queue-set	キューセットに対する出力キューの設定を表示します。

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、または 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 **mls qos srr-queue output dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻す場合は、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
```

シンタックスの説明

queue queue-id	キュー番号を指定します。 <i>queue-id</i> 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。 <i>dscp1...dscp8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 63 です。
threshold threshold-id dscp1...dscp8	DSCP 値をキューのスレッシュホールド ID にマッピングします。 <i>threshold-id</i> に指定できる範囲は 1 ～ 3 です。 <i>dscp1...dscp8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は、0 ～ 63 です。

デフォルト

表 2-13 に、デフォルトの DSCP 出力キューのスレッシュホールドのマッピングを示します。

表 2-13 デフォルトの DSCP 出力キューのスレッシュホールドのマッピング

DSCP 値	キュー ID — スレッシュホールド 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スレッシュホールド 3 の廃棄スレッシュホールドのパーセンテージはあらかじめ定義されます。パーセンテージはキューがいっぱいの状態に設定されます。



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更してください。

mls qos queue-set output *qset-id* threshold グローバル コンフィギュレーション コマンドを使用して、2 つの Weighted Tail-drop (WTD) スレッシュホールドのパーセンテージを出力キューに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対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

コマンドごとに最大 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 および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に 50% および 70% の割り当てメモリを設定し、割り当てメモリの 100% を保証 (予約) します。また、パケットが廃棄される前にキューが確保できる最大メモリとして 200% を設定します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** 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 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、または 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 queue-set output threshold	WTD スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
queue-set	キューセットに対し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 のマッピング情報を表示します。
show mls qos queue-set	キューセットに対する出力キューの設定を表示します。

mls qos trust

ポートの信頼状態を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP) 値、または IP precedence フィールドを調べることにより分類が実行されます。ポートを信頼性が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]

シンタックスの説明

cos	(任意) パケットの CoS 値を使用して、入力パケットを分類します。タグのないパケットについては、ポートのデフォルト CoS 値を使用します。
device cisco-phone	(任意) Cisco IP Phone (信頼性のある境界) から送信された CoS 値または DSCP 値を信頼することにより、信頼性の設定に応じて着信パケットを分類します。
dscp	(任意) パケットの 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。パケットにタグがある場合、非 IP パケットにはパケットの CoS が使用されます。タグのないパケットの場合、デフォルト ポートの CoS 値が使用されます。
ip-precedence	(任意) パケットの IP precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS が使用されます。タグのないパケットの場合、デフォルト ポートの CoS 値が使用されます。

デフォルト

ポートは信頼されていません。コマンド入力時、キーワードが指定されていない場合、デフォルトは **dscp** 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	device cisco-phone キーワードが追加されました。
12.2(20)SE	「使用上の注意事項」は、Cisco IP Phone がスイッチまたはルーテッド ポートに接続された場合に、スイッチが信頼状態を設定する方法について説明するよう改定されました。

使用上のガイドライン

Quality of Service (QoS; サービス品質) ドメインに着信するパケットは、QoS 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。

信頼性のある DSCP または信頼性のある IP precedence を使用してポートが設定され、着信パケットが非 IP パケットである場合、CoS/DSCP マップが使用され、CoS 値から対応する DSCP 値を抽出します。CoS は、トランク ポートのパケット CoS または非トランク ポートのポート デフォルト CoS になることができます。

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) 変更することが可能です。

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 を変更できます。

信頼性のある境界機能は、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にセキュリティ問題を防ぎます。スイッチおよび IP Phone に接続されたポートの両方で 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、信頼性のある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、ハイ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 で信頼性の設定を行う場合、着信パケットの DSCP または IP precedence 値が信頼されます。IP Phone に接続されたスイッチポート上で、**mls qos cos override** インターフェイス コンフィギュレーション コマンドを設定した場合、スイッチは着信する音声またはデータの packets を上書きし、デフォルトの CoS 値をそれらに割り当てます。

内部 QoS ドメインの境界には、ポートを DSCP に信頼されている状態に設定可能で、DSCP 値が QoS ドメイン間で異なる場合、DSCP/DSCP 合成マップを適用できます。

ポートの信頼状態 (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**) を使用した分類は、相互に排他的な関係です。設定された最後の 1 つが以前の設定を上書きします。

例

次の例では、ポートが着信パケットの IP precedence フィールドを信頼するよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust ip-precedence
```

次の例では、ポートに接続された Cisco IP Phone が、信頼性のある装置であることを指定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust device cisco-phone
```

設定を確認するには、**show mls qos interface** 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 cos	デフォルトのポート CoS 値を定義するか、あるいはポート上のすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos dscp-mutation	DSCP/DSCP 合成マップを DSCP の信頼性あ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 合成マップ、IP precedence/DSCP マップ、およびポリシングされた DSCP マップを定義します。
show mls qos interface	QoS 情報を表示します。

mls qos vlan-based

物理ポート上で VLAN（仮想 LAN）ベースの Quality of Service（QoS; サービス品質）をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用します。この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

mls qos vlan-based

no mls qos vlan-based

シンタックスの説明 引数またはキーワードはありません。

デフォルト VLAN ベースの QoS はディセーブルです。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	12.2(25)SE	このコマンドが導入されました。

使用上のガイドライン 階層型ポリシー マップを Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に適用する前に、物理ポートを階層型ポリシー マップのセカンダリ インターフェイス レベルで指定する場合、物理ポート上で **mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用します。

階層型ポリシングを設定する場合、階層型ポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに影響します。インターフェイスレベルのトラフィック分類内の各ポリサーは、その分類用に指定された物理ポートにのみ影響を与えます。

階層型ポリシー マップを設定する詳細な手順については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Classifying, Policing, and Marking Traffic by Using Hierarchical Policy Maps」を参照してください。

例 次の例では、物理ポート上で VLAN ベースのポリシングをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos vlan-based
```

設定を確認するには、**show mls qos 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 mls qos interface	QoS 情報を表示します。

monitor session

新規に 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) の送信元または宛先セッションを開始するには、スイッチ スタックまたはスタンドアロン スイッチ上で **monitor session** グローバル コンフィギュレーション コマンドを使用します。これにより、ネットワーク セキュリティ デバイス (Cisco Intrusion Detection System [IDS; 侵入検知システム] センサ アプライアンスなど) の宛先ポート上にある入力トラフィックをイネーブルにして、既存の SPAN または RSPAN セッションでのインターフェイスまたは VLAN (仮想 LAN) の追加または削除を実行し、SPAN 送信元トラフィックを特定 VLAN に制限 (フィルタリング) します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元、宛先インターフェイス、またはフィルタを削除したりする場合は、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では、このコマンドの **no** 形式による encapsulation オプションは無視されます。

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate]
[ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}] | {remote vlan vlan-id}

monitor session session_number filter vlan vlan-id [, | -]

monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, |
-] [both | rx | tx]} | {remote vlan vlan-id}

no monitor session {session_number | all | local | remote}

no monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate]
[ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}] | {remote vlan vlan-id}

no monitor session session_number filter vlan vlan-id [, | -]

no monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id
[, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

シンタックスの説明

<i>session_number</i>	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は、1 ～ 66 です。
destination	SPAN または RSPAN の宛先を指定します。宛先は物理ポートである必要があります。
interface interface-id	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート (タイプ、スタック メンバー、モジュール、ポート番号を含む) です。 送信元インターフェイス では、 ポート チャネル も有効なインターフェイス タイプです。使用可能な範囲は 1 ～ 48 です。
encapsulation replicate	(任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するよう指定します。選択されていない場合のデフォルトは、ネイティブ形式 (タグなし) でパケットを送信する設定になっています。 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 の場合、RSPAN VLAN ID によって元の VLAN ID が上書きされるため、パケットは常にタグなしで送信されます。
ingress	(任意) 入力トラフィック転送をイネーブルにします。
dot1q vlan vlan-id	デフォルト VLAN として、指定の VLAN を持つ IEEE 802.1Q カプセル化の着信パケットを受け入れます。
isl	ISL (スイッチ間リンク) カプセル化を使用した入力転送を指定します。
untagged vlan vlan-id	デフォルト VLAN として、指定の VLAN を持つタグなしカプセル化の着信パケットを受け入れます。

vlan <i>vlan-id</i>	ingress キーワードのみが使用された場合、入力トラフィックにはデフォルトの VLAN が設定されます。
remote vlan <i>vlan-id</i>	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークン リングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用）に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、直前の範囲とインターフェイスまたは VLAN の範囲を区切ります。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 <i>vlan-id</i>	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。 <i>vlan-id</i> で指定できる範囲は 1 ～ 4094 です。
source	SPAN または RSPAN の送信元を指定します。物理ポート、ポート チャネル、VLAN が送信元になることができます。
both、rx、tx	（任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
source vlan <i>vlan-id</i>	VLAN ID として SPAN の送信元インターフェイスを指定します。使用可能な範囲は 1 ～ 4094 です。
all、local、remote	すべての SPAN および RSPAN、すべてのローカル SPAN、すべての RSPAN セッションをクリアするには、 no monitor session コマンドに all、local、remote を指定します。

デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタされます。

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

入力転送は宛先ポートではディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	ingress {dot1q vlan vlan-id isl untagged vlan vlan-id vlan vlan-id} キーワードが追加されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を通過するトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定できます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

スイッチ スタック上で、最大 64 の宛先ポートを保有できます。

SPAN または RSPAN の宛先ポートとして 10 ギガビット イーサネット ポートを設定すると、リンクの回線速度は低下します。

各セッションは複数の入出力送信元ポートまたは VLAN を持つことができますが、1 つのセッションで送信元ポートおよび送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN (VSPAN) を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタされた VLAN ID のパケットのみが宛先ポートに送信されます。

1 つポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用することにより、一連のインターフェイスまたはインターフェイス範囲、一連の VLAN または VLAN 範囲を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ (,) の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン (-) の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定できません。EtherChannel グループのメンバーである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートとして設定できません。

EtherChannel に参加している間、個々のポートをモニタできます。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 のバンドル全体をモニタできます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにはできません。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 をイネーブルにできますが、ポートが SPAN 宛先として削除されるまでは、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 メッセージを返します)。SPAN または RSPAN 送信元ポートでは IEEE 802.1x をイネーブルにできません。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタされます。**monitor session session_number filter vlan vlan-id** コマンドを使用し、トランクの送信元ポート上の SPAN トラフィックを特定の VLAN のみに制限できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元にはなりません。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- 他のキーワードなしで、**monitor session session_number destination interface interface-id** を入力した場合、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session session_number destination interface interface-id ingress** を入力した場合、出力のカプセル化はタグなしとなり、入力のカプセル化は、次に続くキーワード (**dot1q**、**isl**、または **untagged**) により異なります。
- 他のキーワードなしで、**monitor session session_number destination interface interface-id encapsulation replicate** を入力した場合、出力のカプセル化は送信元インターフェイスのカプセル化方式を複製し、入力転送はイネーブルになりません。(これはローカル SPAN のみに適用します。RSPAN はカプセル化の複製をサポートしていません)。
- **monitor session session_number destination interface interface-id encapsulation replicate ingress** を入力した場合、出力のカプセル化は送信元インターフェイスのカプセル化方式を複製します。入力のカプセル化は、次に続くキーワード (**dot1q**、**isl**、または **untagged**) により異なります (これはローカル SPAN のみに適用します。RSPAN はカプセル化の複製をサポートしていません)。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバー 1 の送信元ポート 1 からスタック メンバー 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Switch(config)# no monitor session 2 destination gigabitethernet1/0/2
```

次の例では、既存のセッションの SPAN トラフィックを特定の VLAN のみに制限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 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、モニタされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q のカプセル化をサポートするセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックは送信元を複製します (入力トラフィックは IEEE 802.1Q カプセル化を使用します)。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
encapsulation replicate ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィック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タグなしになります）。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
encapsulation replicate ingress untagged vlan 5
```

設定を確認するには、**show monitor** イネーブル EXEC コマンドを入力します。**show running-config** イネーブル EXEC コマンドを入力すれば、スイッチ上で設定された SPAN および RSPAN を表示させることができます。SPAN 情報は出力の最後付近に表示されます。

関連コマンド

コマンド	説明
remote-span	VLAN コンフィギュレーションモードで RSPAN VLAN を設定します。
show monitor	SPAN および RSPAN セッション情報を表示します。
show running-config	現在の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。

mvr (グローバル コンフィギュレーション)

スイッチ上の Multicast VLAN Registration (MVR) 機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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*]

シンタックスの説明

group <i>ip-address</i>	スイッチ上の MVR グループ IP マルチキャスト アドレスをスタティックに設定します。 スタティックに設定した IP マルチキャスト アドレスまたは連続アドレスを削除したり、IP アドレスが入力されない場合にすべてのスタティックに設定された MVR IP マルチキャスト アドレスを削除したりする場合は、このコマンドの no 形式を使用します。
count	(任意) 複数の連続 MVR グループ アドレスを設定します。指定できる範囲は 1 ～ 256 です。デフォルト値は 1 です。
mode	(任意) MVR の動作モードを指定します。 デフォルトは compatible モードです。
compatible	MVR モードを設定して、Catalyst 2900 XL および 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 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 <i>value</i>	(任意) レシーバー ポートで Internet Group Management Protocol (IGMP) レポート メンバーシップを待つ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 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。デフォルト値は 5/10 すなわち 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 <i>vlan-id</i>	(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 はディセーブルです。

MVR モードは、**compatible** モードです。

スイッチに IP マルチキャスト アドレスは設定されていません。

グループ IP アドレス カウントは 0 です。

クエリー応答時間は 5/10 すなわち 1/2 秒です。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

最大 256 個の MVR マルチキャスト グループを 1 つのスイッチに設定できます。

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、スイッチ上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、スイッチ上のエイリアス 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 スイッチと相互運用している場合、スイッチ間でまたは予約された IP マルチキャスト アドレス（範囲が 224.0.0.xxx）とでエイリアスを割り当てる IP アドレスを設定しないでください。

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 スイッチと相互運用している場合は、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。

スイッチ上で MVR は IGMP スヌーピングと共存可能です。

マルチキャスト ルーティングと MVR はスイッチ上で共存できません。MVR がイネーブルの状態、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにした場合、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作はキャンセルされ、エラー メッセージが表示されます。

例

次の例では、MVR をイネーブルにする方法を示します。

```
Switch(config)# mvr
```

現行の最大マルチキャスト グループの設定を表示するには、**show mvr** イネーブル EXEC コマンドを使用します。

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
```

スイッチ上で設定された IP マルチキャスト グループ アドレスを表示するには、**show mvr members** イネーブル EXEC コマンドを使用します。

次の例では、最大クエリ応答時間を 1 秒 (10/10) に設定する方法を示します。

```
Switch(config)# mvr querytime 10
```

次の例では、VLAN 2 をマルチキャスト VLAN として設定する方法を示します。

```
Switch(config)# mvr vlan 2
```

設定を確認するには、**show mvr** 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
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。また、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 のポートを Multicast VLAN Registration (MVR) のレシーバーまたは送信元ポートとして設定することで、即時脱退機能を設定し、IP マルチキャスト VLAN (仮想 LAN) と IP アドレスにポートをスタティックに割り当てるには、スイッチ スタックまたはスタンドアロン スイッチ上で **mvr** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mvr [immediate | type {receiver | source} | vlan vlan-id group [ip-address]]
```

```
no mvr [immediate | type {source | receiver} | vlan vlan-id group [ip-address]]
```

シンタックスの説明

immediate	(任意) ポート上の 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、このコマンドの no mvr immediate 形式を使用します。
type	(任意) MVR レシーバー ポートまたは送信元ポートとして、ポートを設定します。 デフォルトのポート タイプは MVR 送信元ポートでもレシーバー ポートでもありません。 no mvr type コマンドは、ポートを送信元でもレシーバーでもないポートとして、リセットします。
receiver	マルチキャスト データのみを受信できるサブスクリバ ポートとしてポートを設定します。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	設定されたマルチキャスト グループのマルチキャスト データを送受信できるアップリンク ポートとしてポートを設定します。スイッチ上のすべての送信元ポートは 1 つのマルチキャスト VLAN に属しています。
vlan vlan-id group	(任意) 指定の VLAN ID を持ったマルチキャスト グループのスタティックなメンバーとして、ポートを追加します。 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) 指定のマルチキャスト VLAN ID に指定された MVR IP マルチキャスト グループ アドレスをスタティックに設定します。これは、ポートが加入しているマルチキャスト グループの IP アドレスです。

デフォルト

ポートはレシーバーとしても送信元としても設定されません。

即時脱退機能はすべてのポート上でディセーブルになっています。

レシーバー ポートは設定されたマルチキャスト グループのいずれのメンバーでもありません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

ポートが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 ポートになれません。スイッチ上のレシーバー ポートは異なる VLAN に存在できますが、マルチキャスト VLAN には属せません。

MVR に参加しているポートは、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。即時脱退機能なしで、スイッチが、レシーバー ポートのグループから Internet Group Management Protocol (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 の 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 の MAC ベースのクエリーが送信されません。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 コマンドはポートをスタティックに設定し、IP マルチキャスト アドレスに送信されるマルチキャスト トラフィックを受信します。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ないかぎり、グループのメンバーとして残ります。**compatible** モードでは、コマンドはレシーバー ポートに対してのみ適用しますが、**dynamic** モードでは、送信元ポートにも適用できます。レシーバー ポートは IGMP join メッセージを使用することで、マルチキャスト グループにダイナミックに参加することもできます。

compatible モードでは、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR ポートは、プライベート VLAN ポートにはできません。

例

次の例では、ポートを MVR レシーバー ポートとして設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

設定されたレシーバー ポートと送信元ポートを表示するには、**show mvr interface** イネーブル EXEC コマンドを使用します。

次の例では、ポートで即時脱退をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 上のポートを、IP マルチキャスト グループ 228.1.23.4 のスタティックなメンバーとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

設定を確認するには、**show mvr members** 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
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	設定された MVR インターフェイス、またはレシーバー ポートが属するマルチキャスト グループを表示します。また、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 ポートから受信する着信パケットの送信元アドレスを学習するには、スイッチ スタックまたはスタンドアロン スイッチ上で **pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
pagp learn-method {aggregation-port | physical-port}
```

```
no pagp learn-method
```

シンタックスの説明

aggregation-port	論理ポートチャネルで学習するアドレスを指定します。スイッチは、EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。この設定は、デフォルトです。アグリゲートポート学習の場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートで学習するアドレスを指定します。スイッチは、送信元アドレスの学習に使用した EtherChannel 内の同じポートを使用して、送信元にパケットを送信します。チャネルの一方の終端は、特定の宛先 MAC (メディア アクセス制御) または IP アドレスのチャネルのポートと同一のポートを使用します。

デフォルト

デフォルトは、aggregation-port (論理ポート チャネル) です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。



(注)

CLI (コマンドラインインターフェイス) を経由して **physical-port** キーワードが指定された場合でも、Catalyst 3750 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学習のみです。**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 ハードウェアに影響を与えません。ただし、PAgP と Catalyst 1900 スイッチのような物理ポートからのアドレス学習のみをサポートする装置との相互運用が必要になります。

Catalyst 3750 スイッチに対するリンクのパートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用し、スイッチを物理ポート ラーナーとして設定するよう強く推奨します。また、**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、送信元 MAC アドレスに基づいた負荷分散方式を設定するよう推奨します。この状況でのみ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

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

次の例では、学習方式を設定し、EtherChannel 内のポートチャネル上のアドレスを学習する方法を示します。

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

設定を確認するには、**show running-config** または **show pagp channel-group-number internal** イネーブ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp port-priority	EtherChannel 経由ですべてのトラフィックを送信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。

pagp port-priority

EtherChannel を経由するすべての Port Aggregation Protocol (PAgP) トラフィックが送信されるポートを選択するには、スイッチ スタックまたはスタンドアロン スイッチ上で **pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼働状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*

no pagp port-priority

シンタックスの説明

priority プライオリティ番号は 0 ～ 255 です。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

動作可能で同一の EtherChannel 内のメンバーシップを持つ、プライオリティが最高の物理ポートは、PAgP 送信に選ばれます。



(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 3750 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学習のみです。**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 ハードウェアに影響を与えません。ただし、PAgP と Catalyst 1900 スイッチのような物理ポートからのアドレス学習のみをサポートする装置との相互運用が必要になります。

Catalyst 3750 スイッチに対するリンクのパートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用し、スイッチを物理ポート ラーナーとして設定するよう強く推奨します。また、**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、送信元 MAC (メディア アクセス制御) アドレスに基づいた負荷分散方式を設定するよう推奨します。この状況でのみ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** または **show pagp channel-group-number internal** 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
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。

permit (ARP アクセスリスト コンフィギュレーション)

Dynamic Host Configuration Protocol (DHCP) バインディングとの照合に基づいた Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを許可するには、**permit** ARP アクセスリスト コンフィギュレーション コマンドを使用します。Access Control List (ACL; アクセス制御リスト) から指定された Access Control Entry (ACE; アクセス制御エントリ) を削除する場合は、このコマンドの **no** 形式を使用します。

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

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

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

request	(任意) ARP 要求の一致を要求します。 request が指定されない場合、照合はすべての ARP パケットに対して実行されます。
ip	送信側の IP アドレスを指定します。
any	任意の IP または MAC (メディア アクセス制御) アドレスを受け付けます。
host sender-ip	指定された送信側の IP アドレスを受け付けます。
sender-ip sender-ip-mask	指定された送信側の IP アドレスの範囲を受け付けます。
mac	送信側の MAC アドレスを指定します。
host sender-mac	指定された送信側の MAC アドレスを受け付けます。
sender-mac sender-mac-mask	指定された送信側の MAC アドレスの範囲を受け付けます。
response ip	ARP 応答の IP アドレス値を定義します。
host target-ip	(任意) 指定されたターゲット IP アドレスを受け付けます。
target-ip target-ip-mask	(任意) 指定されたターゲット IP アドレスの範囲を受け付けます。
mac	ARP 応答の MAC アドレス値を指定します。
host target-mac	(任意) 指定されたターゲット MAC アドレスを受け付けます。

■ permit (ARP アクセスリスト コンフィギュレーション)

<i>target-mac</i>	(任意) 指定されたターゲット MAC アドレスの範囲を受け付けます。
<i>target-mac-mask</i>	
log	(任意) ACE に一致するパケットをロギングします。 ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで matchlog キーワードも設定している場合は、一致するパケットはロギングされます。

デフォルト

デフォルト設定はありません。

コマンド モード

ARP アクセスリスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

一致条件に基づいた ARP パケットを転送するのに、許可コマンドを追加できます。

例

次の例では、ARP アクセス リストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd: を使用して、ホストからの ARP 要求および ARP 応答の両方を許可する方法を示します。

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

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

permit (IPv6 アクセスリスト コンフィギュレーション)

IPv6 アクセス リストの許可条件を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **permit** IPv6 アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を削除する場合は、このコマンドの **no** 形式を使用します。

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

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



(注)

flow-label、**reflect**、および **routing** キーワードは、コマンドラインのヘルプ ストリングには表示されませんが、サポートされていません。

Internet Control Message Protocol (ICMP)

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

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

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



(注)

flow-label、**reflect**、および **routing** キーワードは、コマンドラインのヘルプ ストリングには表示されませんが、サポートされていません。

このコマンドは、スイッチで拡張 IP サービス イメージが動作していて、Switch Database Management (SDM) デュアル IPv4 および IPv6 テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

<i>protocol</i>	インターネット プロトコルの名前または番号。ここには、 ahp 、 esp 、 icmp 、 ipv6 、 pcp 、 sctp 、 tcp 、 udp のいずれかのキーワード、または IPv6 のプロトコル番号を示す 0 ～ 255 の数字を指定できます。
<i>source-ipv6-prefix/ prefix-length</i>	許可条件の設定対象となる送信元 IPv6 ネットワークまたはネットワーク クラス。 この引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
 (注)	CLI のヘルプにはプレフィックスの長さの範囲として /0 ～ /128 が表示されますが、スイッチでサポートされる IPv6 アドレス マッチングは、プレフィックスの長さ範囲 /0 ～ /64 と、集約グローバルユニキャストおよびリンク ローカル ホスト アドレスの場合、Extended Universal Identifier (EUI) ベースの /128 のプレフィックスのみです。
<i>any</i>	IPv6 プレフィックス ::/0 の略称。
<i>host source-ipv6-address</i>	許可条件の設定対象となる送信元 IPv6 ホスト アドレス。 この <i>source-ipv6-address</i> 引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
<i>operator [port-number]</i>	(任意) 指定したプロトコルの送信元および宛先ポートを比較する演算子を指定します。演算子は、 lt (未満)、 gt (より大きい)、 eq (等しい)、 neq (等しくない)、 range (包含範囲) が使用できます。 演算子を <i>source-ipv6-prefix/prefix-length</i> 引数の後に指定した場合、送信元ポートと一致する必要があります。 演算子を <i>destination-ipv6-prefix/prefix-length</i> 引数の後に指定した場合、宛先ポートと一致する必要があります。 range 演算子には、ポート番号を 2 個指定する必要があります。これ以外の演算子には、ポート番号を 1 個指定します。 オプションの <i>port-number</i> 引数には、10 進数の数字、あるいは TCP または UDP ポートの名前を指定します。指定できるポート番号の範囲は、0 ～ 65535 です。TCP のポート名は、TCP をフィルタリングする場合のみ使用できます。UDP のポート名は、UDP をフィルタリングする場合のみ使用できます。
<i>destination-ipv6-prefix/ prefix-length</i>	許可条件の設定対象となる宛先 IPv6 ネットワークまたはネットワーク クラス。 この引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
 (注)	CLI のヘルプにはプレフィックスの長さの範囲として /0 ～ /128 が表示されますが、スイッチでサポートされる IPv6 アドレス マッチングは、プレフィックスの長さ範囲 /0 ～ /64 と、集約グローバルユニキャストおよびリンク ローカル ホスト アドレスの場合、EUI ベースの /128 のプレフィックスのみです。

host	許可条件の設定対象となる宛先 IPv6 ホストアドレス。
destination-ipv6-address	この destination-ipv6-address 引数はコロン間に 16 ビット値を使用して、アドレスが 16 進数で指定されている、RFC 2373 に記載されている形式である必要があります。
dscp value	(任意) 区別されるサービス コード ポイント値を、各 IPv6 パケットヘッダーのトラフィック クラス フィールドのトラフィック クラス値と比較します。許容される範囲は 0 ～ 63 です。
fragments	(任意) フラグメント拡張ヘッダーに 0 でないフラグメント オフセットが設定されている非初期フラグメント パケットを一致させます。 fragments キーワードは、プロトコルが ipv6 で、 operator [port-number] 引数が指定されていない場合のみ使用できます。
log	(任意) コンソールに、エントリに一致するパケットに関する情報ロギング メッセージを送信します (コンソールに記録されるメッセージのレベルは、 logging console コマンドで制御できます)。 メッセージには、アクセス リスト名、一連の番号、パケットが許可されたかどうか、プロトコルが TCP、UDP、ICMP または数値のいずれであるか、該当する場合、送信元アドレスと宛先アドレス、送信元ポート番号と宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、5 分間隔で、前の 5 分間に許可されたパケットの数が追加されます。
log-input	(任意) 機能は log キーワードと同じですが、ロギング メッセージに受信インターフェイスも含まれます。
parameter value	(任意) 再帰 IPv6 アクセス リストをタイムアウトとみなすアイドル時間の間隔 (秒単位)。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 180 秒です。
sequence value	(任意) アクセス リスト ステートメントの一連の番号を指定します。許容される範囲は 1 ～ 4294967295 です。
time-range name	(任意) 許可ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項を指定するには、それぞれ time-range コマンドと、 absolute または periodic コマンドを使用します。
icmp-type	(任意) ICMP パケットをフィルタリングするための ICMP メッセージタイプを指定します。ICMP パケットは、ICMP メッセージタイプによってフィルタリングできます。指定できるタイプの範囲は 0 ～ 255 です。
icmp-code	(任意) ICMP パケットをフィルタリングするための ICMP コードを指定します。ICMP メッセージタイプでフィルタリングされる ICMP パケットは、ICMP メッセージコードによってもフィルタリングできます。指定できるコードの範囲は 0 ～ 255 です。
icmp-message	(任意) ICMP パケットをフィルタリングするための ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージタイプおよびコードのほか、ICMP メッセージ名によってもフィルタリングできます。使用できる名前については、「Usage Guidelines」セクションを参照してください。
ack	(任意) TCP プロトコルでのみ使用できます。Acknowledgment (ACK) ビットを設定します。
established	(任意) TCP プロトコルでのみ使用できます。接続が確立されていることを示します。TCP データグラムに ACK または RST ビットが設定されている場合に比較が行われます。接続を確立するための初期 TCP データグラムのケースでは、比較は行われません。

<i>fin</i>	(任意) TCP プロトコルでのみ使用できます。Fin ビットを設定します。送信元からそれ以上データは送信されません。
<i>neq</i> { <i>port</i> <i>protocol</i> }	(任意) 所定のポート番号以外のパケットのみを一致させます。
<i>psh</i>	(任意) TCP プロトコルでのみ使用できます。Push function ビットを設定します。
<i>range</i> { <i>port</i> <i>protocol</i> }	(任意) ポート番号の範囲内にあるパケットのみを一致させます。
<i>rst</i>	(任意) TCP プロトコルでのみ使用できます。Reset ビットを設定します。
<i>syn</i>	(任意) TCP プロトコルでのみ使用できます。Synchronize ビットを設定します。
<i>urg</i>	(任意) TCP プロトコルでのみ使用できます。Urgent pointer ビットを設定します。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセスリスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが導入されました。

使用上のガイドライン

permit (IPv6 アクセスリスト コンフィギュレーションモード) コマンドは **permit** (IPv4 アクセスリスト コンフィギュレーション モード) コマンドに相似していますが、IPv6 専用です。

IPv6 アクセス リスト コンフィギュレーションモードを開始してパケットのアクセス リスト通過条件を定義するには、**ipv6 access-list** コマンドのあとに **permit** (IPv6) コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーとの比較が行われます。

デフォルトでは、アクセス リストの最初のステートメントは数値 10 で、それ以後のステートメントは 10 ずつ加算されます。

既存のリストに **permit**、**deny**、または **remark** ステートメントを追加することができ、リスト全体を入力しなす必要はありません。リストの最後以外の任意の場所に新しくステートメントを追加するには、新しいステートメントに 2 つの既存エントリ番号の間に入るエントリ番号を付けて作成し、属する場所を示します。

IPv6 ACL の詳細は、**ipv6 access-list** コマンドの項を参照してください。



(注)

IPv6 ACL には、最後の一致条件として、暗黙的な **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがそれぞれ設定されています。2 つの **permit** 条件により、ICMPv6 ネイバの検出が可能になります。ICMPv6 のネイバの検出を無効にして、**icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、ACL に明示的な **deny** エントリを設定する必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に少なくとも 1 個のエントリが設定されていなければなりません。

IPv6 ネイバの検出プロセスには、IPv6 ネットワーク レイヤ サービスが使用されます。そのため、デフォルトでは、IPv6 ACL はインターフェイス上での IPv6 ネイバ検出パケットの送受信を暗黙的に有効にします。IPv4 では、IPv6 ネイバ検出プロセスと同等の Address Resolution Protocol (ARP; アドレス解決プロトコル) で専用のデータリンク レイヤ プロトコルが使用されます。そのため、デフォルトでは、IPv4 ACL はインターフェイス上での ARP パケットの送受信を暗黙的に有効にします。

source-ipv6-prefix/prefix-length 引数と *destination-ipv6-prefix/prefix-length* 引数は、トラフィックフィルタリングに使用されます (送信元プレフィックスはトラフィック送信元に基づいてトラフィックのフィルタリングを行い、宛先プレフィックスはトラフィック宛先に基づいてトラフィックのフィルタリングを行います)。

スイッチでサポートされているのは、/0 ~ /64 のプレフィックス、集約グローバルユニキャストおよびリンクローカル ホスト アドレスの場合は EUI ベースの /128 のプレフィックスです。

fragments キーワードは、*operator [port-number]* 引数が指定されていない場合のみ使用できます。

次に、ICMP メッセージ名の一覧を示します。

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

例

次の例では、OUTBOUND および INBOUND という名前の 2 つの IPv6 アクセス リストを設定し、両方のアクセス リストをレイヤ 3 インターフェイスの発信トラフィックおよび着信トラフィックに適用します。OUTBOUND リストの第 1 および第 2 の許可エントリにより、ネットワーク 2001:0DB8:0300:0201::/64 のすべての TCP および UDP パケットがインターフェイスから発信されることが許可されます。OUTBOUND リストの拒否エントリによって、ネットワーク FE80:0:0:0201::/64 (送信元 IPv6 アドレスの最初の 64 ビットとしてリンク ローカル プレフィックス FE80:0:0:0201 を持つパケット) のパケットがインターフェイスから発信されないようにします。OUTBOUND リストの第 3 の許可エントリにより、インターフェイスでの ICMP パケットの発信がすべて許可されます。

INBOUND リストの許可エントリにより、インターフェイスでの ICMP パケットの着信がすべて許可されます。

```
Switch(config)#ipv6 access-list OUTBOUND
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# permit udp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# deny FE80:0:0:0201::/64 any
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)#ipv6 access-list INBOUND
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter OUTBOUND out
Switch(config-if)# ipv6 traffic-filter INBOUND in
```



(注)

OUTBOUND または INBOUND アクセス リストの最後のエントリとして **permit any any** ステートメントが記述されていない場合、TCP、UDP、および ICMP パケットのみがインターフェイスでの発着信を許可されます（アクセス リストの最後に暗黙的な **deny-all** 条件があると、インターフェイス上でその他すべてのパケット タイプが拒否されます）。

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義して、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイスで IPv6 の着信トラフィックおよび発信トラフィックをフィルタリングします。
deny (IPv6 アクセスリスト コンフィギュレーション)	IPv6 アクセス リストの拒否条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストの全内容を表示します。

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転送される非 IP トラフィックを許可するには、スイッチ スタックまたはスタンドアロン スイッチ上で **permit** MAC (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。拡張 MAC アクセス リストから許可条件を削除する場合は、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 | lvc-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 | lvc-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tringには表示されますが、一致条件としてサポートされていません。

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワード
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	ホスト MAC アドレスおよびオプションのサブネット 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 <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	宛先 MAC アドレスおよびオプションのサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
<i>type mask</i>	(任意) Ethernet II または Subnetwork Access Protocol (SNAP) のカプセル化でパケットの EtherType 番号を使用し、パケットのプロトコルを識別します。 - 指定できる <i>type</i> の範囲は 0 ～ 65535 です (16 進数)。 <i>mask</i> は、一致テストの前に EtherType に適用される <i>don't care</i> (無視) 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 Digital Equipment Corporation (DEC) -Amber を選択します。
cos <i>cos</i>	(任意) 0 ～ 7 の任意の Class of Service (CoS; サービス クラス) 番号を選択し、プライオリティを設定します。CoS のフィルタリングはハードウェア内でのみ実行可能です。 cos オプションが設定されると、警告メッセージが表示されます。
dec-spanning	(任意) EtherType 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。
lavr-sca	(任意) EtherType DEC-LAVC-SCA を選択します。
lsap <i>lsap-number mask</i>	(任意) 802.2 のカプセル化でパケットの LSAP 番号 (0 ～ 65535) を使用し、パケットのプロトコルを識別します。 <i>mask</i> は、一致テストの前に LSAP 番号に適用される <i>don't care</i> 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。

Internetwork Packet Exchange (IPX) トラフィックをフィルタリングする場合、使用される IPX のカプセル化タイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 専門用語および Cisco IOS 専門用語で指定の IPX のカプセル化タイプのフィルタ条件は、表 2-14 にリストされています。

表 2-14 IPX のフィルタリング条件

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

デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC Access Control List (ACL; アクセス制御リスト) のデフォルト アクションは拒否します。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

host キーワードを使用した場合、アドレス マスクを入力できません。**any** 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 リストに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

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

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

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

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

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

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

設定を確認するには、**show access-lists** 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
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	スイッチで設定される ACL を表示します。

police

分類されたトラフィックのポリサーを定義するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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送信レート、送信の最大バースト サイズ、および最大値を超えた場合にとられるアクションを定義します。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}]

シンタックスの説明

<i>rate-bps</i>	平均トラフィック レートをビット / 秒 (bps) で指定します。指定できる範囲は、1000000 ～ 10000000000 です。
<i>burst-byte</i>	通常のパーストサイズ (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) 指定されたレートを超えると、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	(任意) 指定されたレートを超えると、スイッチはパケットの Differentiated Services Code Point (DSCP) を、ポリシングされた DSCP マップで指定された DSCP に変更し、パケットを送信するよう指定します。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

階層型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 ポリシー マップでは **police** ポリシーマップ コマンドのみが使用できます。

物理ポートを複数制御するポートの Application Specific Integrated Circuit (ASIC; 特定用途向け IC) 装置は、256 のポリサー (255 のポリサーと 1 つの **no** ポリサー) をサポートします。ポート単位でサポートされるポリサーの最大数は 64 です。ポリサーはソフトウェアの要求に応じて割り当てられ、ハードウェアおよび ASIC の限度で制限されます。ポートごとにポリサーを予約することはできません。ポートに割り当てられるポリサーに対する保証はありません。

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。**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、パケットの深さ (パケットが溢れるまで耐えられる最大バースト値) を設定します。**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 *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、パケットから削除されるトークンの速度 (平均レート) を設定します。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

ポリシー マップの **police aggregate** コマンドを 10 ギガビット イーサネット インターフェイスで使用すると、エラーになります。

例

次の例では、トラフィックがバーストサイズ 20 KB で、1 Mbps（メガビット/秒）の平均レートを超えた場合、パケットを廃棄するポリサーを設定する方法を示します。着信パケットの DSCP は信頼され、修正されません。

```
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、ポリシングされた DSCP マップで定義された値で DSCP 値をマーク ダウンし、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	指定のクラスマップ名で、トラフィックの分類一致条件を定義します（ 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）。
mls qos map policed-dscp	ポリシングされた DSCP マップを DSCP の信頼性あ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 コマンドで分類されたトラフィックに、信頼状態を定義します。

police aggregate

同一のポリシー マップにある複数のクラスにアグリゲート ポリサーを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で **police aggregate** 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。ポリサーは最大許容送信レート、送信の最大バースト サイズ、および最大値を超えた場合にとられるアクションを定義します。指定のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police aggregate aggregate-policer-name

no police aggregate aggregate-policer-name

シンタックスの説明

aggregate-policer-name 集約ポリサー名

デフォルト

アグリゲート ポリサー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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

物理ポートを複数制御するポートの Application Specific Integrated Circuit (ASIC; 特定用途向け IC) 装置は、256 のポリサー (255 のポリサーと 1 つの **no** ポリサー) をサポートします。ポート単位でサポートされるポリサーの最大数は 64 です。ポリサーはソフトウェアの要求に応じて割り当てられ、ハードウェアおよび ASIC の限度で制限されます。ポートごとにポリサーを予約することはできません。ポートに割り当てられるポリサーに対する保証はありません。

mls qos aggregate-policer グローバル コンフィギュレーション コマンドを使用して、アグリゲート ポリサーのパラメータを設定します。同一のポリシー マップで、アグリゲート ポリサーを複数のクラスに適用できます。異なるポリシー マップでアグリゲート 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。

police aggregate コマンドを使用してポリシー マップを 10 ギガビット イーサネット インターフェイスに適用すると、エラーになります。

階層型ポリシー マップでは、アグリゲート ポリサーは設定できません。

例

次の例では、アグリゲート ポリサーのパラメータを定義する方法、およびポリシー マップ内の複数のクラスにポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 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 aggregate-policer	ポリサーのパラメータを定義します（ポリシー マップ内で複数のクラスが共有できます）。
show mls qos aggregate-policer	Quality of Service（QoS; サービス品質）アグリゲート ポリサーの設定を表示します。

policy-map

複数の物理ポートまたは Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に適用可能なポリシー マップを作成または変更し、ポリシーマップ コンフィギュレーション モードを開始するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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*

シンタックスの説明

policy-map-name ポリシー マップ名

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 パケットである場合に、Differentiated Services Code Point (DSCP) に 0 を設定し、パケットがタグ付きの場合 Class of Service (CoS; サービス クラス) に 0 を設定します。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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	SVI 上のポリシー マップのサポートが追加されました。

使用上のガイドライン

policy-map コマンドを入力すると、ポリシーマップ コンフィギュレーション モードが開始され、次のコマンドが使用可能になります。

- **class** : 指定したクラス マップの分類一致条件を定義します。詳細は、「[class](#)」(p.2-40) を参照してください。
- **description** : ポリシー マップを記述します (最大 200 文字)。
- **exit** : ポリシーマップ 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** : 現行のポリシー 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。

一致条件がクラス 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、クラスに一致条件が定義されている場合だけです。クラスの一致条件を設定する場合、**class-map** グローバル コンフィギュレーションおよび **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 ベースのパケット分類を定義します。

1つの入力ポートまたはSVIに対してサポートされるポリシー マップは1つのみです。複数の物理ポートまたはSVIに対して、同一のポリシー マップを適用できます。

Cisco IOS Release 12.2(25)SE より前のソフトウェア リリースでは、ポリシー マップを適用し、物理ポート上でのみポリシングを設定できます。信頼状態を設定し、新しい DSCP または IP precedence 値をパケットに設定し、あるいは各ポリサーまたはアグリゲート ポリサーを定義できます。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 ガイドの「Configuring QoS」の章の「Policing on Physical Ports」を参照してください。

Cisco IOS Release 12.2(25)SE 以降のソフトウェア リリースでは、階層型以外のポリシー マップを物理ポートまたはSVIに適用できます。階層型以外のポリシー マップは、Cisco IOS Release 12.2(25)SE より前のソフトウェア リリースのポートベースのポリシー マップと同じです。ただし、階層型ポリシー マップに適用できるのはSVIだけです。

階層型ポリシー マップには次の2つのレベルがあります。第一レベルのVLAN（仮想LAN）レベルは、SVI上のトラフィック フローに対して実行すべきアクションを指定します。第二レベルのインターフェイスレベルは、SVIに属する物理ポート上のトラフィックに対して実行すべきアクションを指定し、インターフェイスレベル ポリシー マップで指定されます。

プライマリ VLAN レベルのポリシー マップでは、信頼状態のみを設定する、あるいは新しい DSCP または IP precedence 値のみをパケットに設定できます。セカンダリ インターフェイスレベルのポリシー マップでは、SVIに属する物理ポート上の各ポリサーのみを設定できます。

階層型ポリシー マップがSVIに適用されたあと、インターフェイスレベルのポリシー マップは変更、または階層型ポリシー マップから削除できません。新しいインターフェイスレベルのポリシー マップも階層型ポリシー マップに追加できません。これらの変更を行う場合、まず階層型ポリシー マップをSVIから削除する必要があります。

階層型ポリシー マップの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring QoS」の章の「Policing on SVIs」を参照してください。

例

次の例では、*policy1* という名前のポリシー マップを作成する方法を示します。このコマンドが入力ポートに適用された場合、*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 DSCP を10に設定してから、平均レート1Mbps（メガビット/秒）でトラフィックをポリシングし、20KBでバーストします。プロファイルを超えたトラフィックは、ポリシングされたDSCP マップから取得したDSCP値にマーク ダウンされ、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、*polymap2* という名前のポリシー マップで複数のクラスを設定する方法を示します。

```
Switch(config)# policy-map polymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

次の例では、階層型ポリシー マップを作成し、SVI に適用する方法を示します。

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet2/0/2 - gigabitethernet2/0/3
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

次の例では、*policy-map2* 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で、トラフィックの分類一致条件を定義します (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を照合する場合に使用されるクラスマップを作成します。
service-policy	ポートにポリシー マップを適用します。
show mls qos vlan	SVI に適用された Quality of Service (QoS; サービス品質) ポリシー マップを表示します。
show policy-map	QoS ポリシー マップを表示します。

port-channel load-balance

EtherChannel のポート間で負荷分散方式を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

シンタックスの説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散
dst-mac	宛先ホストの MAC (メディア アクセス制御) アドレスに基づいた負荷分散。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいた負荷分散
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散
src-ip	送信元ホストの IP アドレスに基づいた負荷分散
src-mac	送信元 MAC アドレスに基づいた負荷分散。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。

デフォルト

デフォルトの方式は、**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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

これらの転送方式の使用に関する情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」を参照してください。

例

次の例では、負荷分散方式を **dst-mac** に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

設定を確認するには、**show running-config** または **show etherchannel load-balance** 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
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。

power inline

Power over Ethernet (PoE) ポート上で電源管理モードを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **power inline** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power inline {auto [max max-wattage] | never | static [max max-wattage]}
```

```
no power inline {auto | never | static}
```

シンタックスの説明

auto	受電装置検出をイネーブルにします。十分な電力を使用できる場合、装置を検出したあと自動的に電力を PoE ポートに割り当てます。
max max-wattage	(任意) ポートに割り当てられた電力を制限します。指定できる範囲は 4000 ~ 15400 ミリワットです。値を指定しない場合、最大値が割り当てられます。
never	装置検出をディセーブルにします。ポートへの電力をディセーブルにします。
static	受電装置検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートに事前に電力を割り当てます (確保します)。

デフォルト

デフォルトの設定は **auto** (イネーブル) です。

最大ワットは 15400 ミリワットです。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。
12.2(25)SE	static および max max-wattage オプションが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートでのみサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline auto
^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全ポートでサポートされます。

高出力の受電装置を許可しないようにするには、**max max-wattage** オプションを使用します。この設定では、受電装置が最大ワット数を超える電力を要求する Cisco Discovery Protocol (CDP) メッセージを送信すると、スイッチはポートの電力を落とします。受電装置の IEEE (米国電気電子学会) クラスの最大値が最大ワット数を超える場合、スイッチは装置に電力を供給しません。電力はグローバル パワー バジェットに再利用されます。



(注)

power inline max max-wattage コマンドが 15.4 W 未満に設定されている場合、スイッチはクラス 0 装置またはクラス 3 装置に電力を供給しません。

スイッチが受電装置への電力を拒否した場合（受電装置が CDP メッセージを介してより多くの電力を要求する、または IEEE クラスの最大値が最大ワット数を超えた場合）、PoE ポートは **power-deny** ステートになります。スイッチはシステム メッセージを生成し、**show power inline** ユーザ EXEC コマンド出力の **Oper** カラムでは **power-deny** が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max max-wattage** コマンドを使用します。スイッチは、PoE をスタティック モードで設定されたポートに割り当ててから、電力を auto モードで設定されたポートに割り当てます。スイッチが装置検出以外に設定されている場合、スイッチはスタティック ポート用に電力を確保します。接続する装置がない場合でも、またポートがシャットダウン ステートであるかないかに関係なく、スイッチはスタティック ポートで電力を確保します。スイッチは設定された最大ワットをポートに割り当て、その割り当て量は IEEE クラス、または受電装置からの CDP メッセージによって調整されません。電力は事前に割り当てられているので、受電装置がスタティック ポートに接続されている場合、最大ワット以下の電力を使用するあらゆる受電装置には電力が保証されています。ただし、受電装置の IEEE クラスが最大ワット数よりも大きい場合、スイッチは装置に電力を供給しません。スイッチが CDP メッセージを通じて受電装置が最大ワット数を超える電力を必要としていることを学習した場合、受電装置はシャットダウンされます。

ポートがスタティック モードであり、スイッチが事前に電力を割り当てできない場合（たとえば、パワー バジェット全体がすでに他の auto またはスタティック ポートに割り当てられているので）、次のメッセージが表示されます。Command rejected:power inline static:pwr not available. ポート設定は変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定する場合、ポートは設定された速度およびデュプレックス設定を使用してオートネゴシエートします。これは接続装置の電力要件を決定するのに必要です（接続装置が受電装置であるかどうかに関係なく）。電力要件を決定したあと、スイッチはインターフェイスをリセットせずに設定された速度およびデュプレックス設定を使用して、インターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定する場合、ポートは設定された速度およびデュプレックス設定に戻ります。

ポートと接続したシスコ製受電装置がポートにある場合、ポートを設定するのに **power inline never** コマンドを使用しないでください。誤ったリンクアップがポート上で発生し、ポートを **errdisable** ステートにします。

**注意**

Cisco IOS Release 12.2(20)SE1 より前のリリースでは、受電装置を取り外したあとでも電力がまだ PoE ポートに供給されることがありました。これにより、あとで非受電装置をポートに接続した場合、非受電装置の損傷が発生します。ご使用のスイッチが Cisco IOS Release 12.2(20)SE1 以降で稼働しているか確認してください。

例

次の例では、受電装置の検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# power inline auto
```

次の例では、クラス 1 またはクラス 2 の受電装置を許可するよう PoE を設定する方法を示します。

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# power inline never
```

設定を確認するには、**show power inline** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのログギングをイネーブルにします。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline consumption

IEEE 分類で装置用に指定されている電力量を、各受電装置で使用するワット数を指定することにより上書きするには、スイッチ スタックまたはスタンドアロン スイッチで、**power inline consumption** グローバルまたはインターフェイス コンフィギュレーション コマンドを使用します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

power inline consumption default wattage

no power inline consumption default

シンタックスの説明

<i>wattage</i>	スイッチがポートのために確保する電力を指定します。指定できる範囲は 4000 ～ 15400 ミリワットです。

デフォルト

Power over Ethernet (PoE) のデフォルト電力は 15400 ミリワットです。

コマンド モード

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

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが導入されました。

使用上のガイドライン

シスコ製の受電装置を PoE ポートに接続すると、スイッチは Cisco Discovery Protocol (CDP) に基づいて装置の実際の電力消費を判定し、それに応じてパワー バジレットを調節します。これは、サードパーティの IEEE 受電装置には適用されません。これらの装置では、スイッチが電力要求を許可すると、受電装置の IEEE 分類に従ってパワー バジレットを調節します。受電装置がクラス 0 (クラス ステータスが不明) またはクラス 3 の場合、実際に必要な電力量とは関係なく、スイッチは装置用に 15400 ミリワットを確保します。受電装置が実際の消費よりも高いクラスをレポートした場合、または電力分類をサポートしていない場合 (デフォルトがクラス 0)、グローバル パワー バジレットの追跡に IEEE クラス情報を使用するため、スイッチは電力を供給する装置を少なくすることができます。

power inline consumption wattage コンフィギュレーション コマンドを使用することにより、IEEE 分類によって指定されたデフォルトの電力要件を上書きすることができます。IEEE 分類によって要求された量と装置で実際に必要となった量の差は、別の装置で使用できるように、グローバル パワー バジレットに戻されます。そのため、スイッチのパワー バジレットを拡大して、有効に利用することができます。

たとえば、各 PoE ポートにおいてスイッチのバジレットが 15400 ミリワットである場合、クラス 0 の受電装置 24 台のみに接続できます。クラス 0 装置の電力要件が実際には 5000 ミリワットであるとする、消費ワット数を 5000 ミリワットに設定して、最大 48 台の装置を接続できます。24 ポートまたは 48 ポート スイッチで利用できる PoE 総出力電力は、370000 ミリワットです。



注意

スイッチのパワー バジレットの計画は慎重に行い、供給電力を超過しないようにしてください。

power inline consumption default wattage コマンドまたは **no power inline consumption default** コマンドを入力すると、次の警告メッセージが表示されます。

%CAUTION: Interface *interface-id*: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply. Refer to documentation.



(注)

パワー バジレットを手動で設定する場合、スイッチと受電装置をつなぐケーブルでの電力損失も考慮してください。

IEEE 電力分類の詳細情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」を参照してください。

このコマンドは、PoE 対応ポートでのみサポートされています。PoE がサポートされていないスイッチまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全スイッチまたはポートでサポートされます。

例

次の例では、グローバル コンフィギュレーション コマンドを使用して、スイッチで各 PoE ポートに 5000 ミリワットの電力を確保する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply. Refer to documentation.
```

次の例では、インターフェイス コンフィギュレーション コマンドを使用して、スイッチで指定の PoE ポートに接続された受電装置に 12000 ミリワットの電力を確保する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline consumption default 12000
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply. Refer to documentation.
```

設定を確認するには、**show power inline consumption default** 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
power inline	PoE ポートで電源管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

priority-queue

ポートで出力緊急キューをイネーブルにするには、**priority-queue** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

priority-queue out

no priority-queue out

シンタックスの説明

out	出力緊急キューをイネーブルにします。

デフォルト

出力緊急キューはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

priority-queue out コマンドを設定する場合、Shaped Round Robin (SRR; シェイプド ラウンド ロビン) に参加しているキューが 1 つ少ないため、SRR ウェイト比率に影響します。つまり、**srr-queue bandwidth shape** 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 コマンドの *weight1* が無視されます (比率計算に使用されません)。緊急キューは優先キューで、このキューが処理されて空になったあとに他のキューが処理されます。

緊急キューがイネーブルか、または出力キューで SRR ウェイトに基づいて処理されている場合は、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の場合、キュー 1 用の SRR シェーピングおよび共有ウェイトを上書きします。
- 出力緊急キューがディセーブルで SRR シェーピングおよび共有ウェイトが設定されている場合、シェーピング モードがキュー 1 の共有モードを上書きし、SRR はシェーピング モードでこのキューを処理します。
- 出力緊急キューがディセーブルで SRR シェーピング ウェイトが設定されていない場合、SRR は共有モードでこのキューを処理します。

例

次の例では、SRR ウェイトが設定された場合の出力緊急キューをイネーブルにする方法を示します。出力緊急キューは設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

次の例では、SRR シェーピングおよび共有ウェイトが設定されたあとに、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは共有モードを上書きします。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

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

関連コマンド

コマンド	説明
show mls qos interface queueing	(任意) キューイングの指針 (SRR、プライオリティ キューイング)、キューに対応したウェイト、および Class of Service (CoS; サービス クラス) / 出力キュー マップを表示します。
srr-queue bandwidth shape	シェーピングしたウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有のウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

private-vlan

プライベート VLAN (仮想 LAN) を設定して、プライベート VLAN のプライマリおよびセカンダリ VLAN 間のアソシエーションを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**private-vlan** VLAN コンフィギュレーション コマンドを使用します。VLAN を標準の VLAN コンフィギュレーションに戻す場合は、このコマンドの **no** 形式を使用します。

private-vlan {association [add | remove] secondary-vlan-list | community | isolated | primary}

no private-vlan {association | community | isolated | primary}

シンタックスの説明

association	プライマリ VLAN とセカンダリ VLAN 間のアソシエーションを作成します。
<i>secondary-vlan-list</i>	1 つまたは複数のセカンダリ VLAN を指定して、プライベート VLAN で、プライマリ VLAN と関連付けられるようにします。
add	セカンダリ VLAN をプライマリ VLAN と関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN のアソシエーションをクリアします。
community	VLAN をコミュニティ VLAN として指定します。
isolated	VLAN をコミュニティ VLAN として指定します。
primary	VLAN をコミュニティ VLAN として指定します。

デフォルト

デフォルトでは、プライベート VLAN は設定されていません。

コマンド モード

VLAN コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

プライベート VLAN を設定する前に、VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) (VTP トランスペアレント モード) をディセーブルにする必要があります。プライベート VLAN の設定後は、VTP モードをクライアントまたはサーバ モードに変更しないでください。

VTP は、プライベート VLAN コンフィギュレーションを伝播しません。プライベート VLAN のレイヤ 2 データベースを統合し、プライベート VLAN トラフィックのフラッドイングを防ぐには、レイヤ 2 ネットワークのすべてのスイッチ上でプライベート VLAN を手動で設定する必要があります。

プライベート VLAN コンフィギュレーションには、VLAN 1 または VLAN 1002 ～ 1005 を含めません。拡張 VLAN (VLAN ID 1006 ～ 4094) は、プライベート VLAN で設定可能です。

セカンダリ (独立またはコミュニティ) VLAN は、プライマリ VLAN 1 つとだけ関連付けられます。プライマリ VLAN には、1 つの独立 VLAN とそれに関連付けられた複数のコミュニティ VLAN を保有できます。

- セカンダリ VLAN を、プライマリ VLAN として設定できません。
- secondary_vlan_list* パラメータには、スペースを含めません。カンマで区切られた複数の項目を含めます。各項目は、単一の VLAN ID またはハイフンで連結したプライベート VLAN ID の範囲です。リストには、1 つの独立型 VLAN および複数のコミュニティ VLAN を含めます。

- プライマリ VLAN またはセカンダリ VLAN のいずれかを削除した場合、VLAN に関連付けられたポートは非アクティブになります。

コミュニティ VLAN は、コミュニティ ポート間で、およびコミュニティ ポートから該当するプライマリ VLAN 上のプロミスキャス ポートにトラフィックを送信します。

独立 VLAN は、独立ポートがプロミスキャス ポートと通信するのに使用されます。この VLAN は、ほかのコミュニティ ポートまたは独立ポートへのトラフィックの伝送に、同じプライマリ VLAN ドメインを使用しません。

プライマリ VLAN は、ゲートウェイからプライベート ポート上のカスタマーのエンド ステーションにトラフィックを送信します、

レイヤ 3 VLAN インターフェイス (Switch Virtual Interface [SVI; スイッチ仮想インターフェイス]) を、プライマリ VLAN に対してのみ設定します。セカンダリ VLAN のレイヤ 3 VLAN インターフェイスは設定できません。セカンダリ VLAN の SVI は、VLAN がセカンダリ VLAN として設定されている間は、非アクティブになります。

private-vlan コマンドは、VLAN コンフィギュレーション モードを終了してから有効になります。

プライベート VLAN ポートを EtherChannel として設定しないでください。ポートが、プライベート VLAN コンフィギュレーションに含まれている間は、その EtherChannel のコンフィギュレーションは非アクティブです。

プライベート VLAN を Remote Switched Port Analyzer (RSPAN) VLAN として設定しないでください。

プライベート VLAN を音声 VLAN として設定しないでください。

プライベート VLAN を備えたスイッチ上にフォールバック ブリッジングを設定しないでください。

プライベート VLAN には、複数の VLAN が含まれますが、プライベート VLAN 全体で実行しているのは、1 つの Spanning-Tree Protocol (STP; スパニングツリー プロトコル) インスタンスのみになります。セカンダリ VLAN が、プライマリ VLAN と関連付けられている場合、プライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。

ホスト ポートおよびプロミスキャス ポートの設定の詳細については、**switchport mode private-vlan** コマンドを参照してください。

プライベート VLAN と他の機能との相互作用の詳細については、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、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、および VLAN 502 と 503 をコミュニティ VLAN として設定し、それらをプライベート VLAN と関連付ける方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

設定を確認するには、**show vlan private-vlan** または **show interfaces status** 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 status	インターフェイスのステータス（所属する VLAN を含む）を表示します。
show vlan private-vlan	スイッチ スタックで設定されたプライベート VLAN および VLAN アソシエーションを表示します。
switchport mode private-vlan	プライベート VLAN ポートを、ホスト ポートまたはプロミスキャス ポートとして設定します。

private-vlan mapping

プライベート VLAN（仮想 LAN）のプライマリ VLAN とセカンダリ VLAN 間でマッピングを作成して、両方の VLAN で同じプライマリ VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を共有できるようにするには、スイッチ スタックまたはスタンドアロン スイッチ上の SVI で **private-vlan mapping** インターフェイス コンフィギュレーション コマンドを使用します。プライベート VLAN マッピングを SVI 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。

private-vlan mapping {[add | remove] *secondary-vlan-list*}

no private-vlan mapping

シンタックスの説明

<i>secondary-vlan-list</i>	プライマリ VLAN SVI にマッピングされる 1 つまたは複数のセカンダリ VLAN を指定します。
add	(任意) セカンダリ VLAN をプライマリ VLAN SVI にマッピングします。
remove	(任意) セカンダリ VLAN とプライマリ VLAN SVI 間のマッピングを削除します。

デフォルト

デフォルトでは、プライベート VLAN SVI マッピングは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

プライベート VLAN を設定する場合は、スイッチが VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) トランスペアレント モードである必要があります。

プライマリ VLAN の SVI は、レイヤ 3 で作成されます。

レイヤ 3 VLAN インターフェイス (SVI) を、プライマリ VLAN に対してのみ設定します。セカンダリ VLAN のレイヤ 3 VLAN インターフェイスは設定できません。セカンダリ VLAN の SVI は、VLAN がセカンダリ VLAN として設定されている間は、非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めません。カンマで区切られた複数の項目を含めます。各項目は、単一の VLAN ID またはハイフンで連結したプライベート VLAN ID の範囲です。リストには、1 つの独立型 VLAN および複数のコミュニティ VLAN を含めます。

セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN の SVI によりルーティングされます。

セカンダリ VLAN は、1 つのプライマリ SVI にのみマッピングされます。プライマリ VLAN をセカンダリ VLAN として設定する場合、このコマンドで指定されるすべての SVI は、ダウンします。

有効なレイヤ 2 プライベート VLAN アソシエーションを持たない 2 つの VLAN 間で、マッピングを設定する場合、マッピング コンフィギュレーションは有効ではありません。

例

次の例では、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする方法を示します。

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

次の例では、セカンダリ VLAN 303 から VLAN 20 SVI を介して、305 および 307 へのセカンダリ VLAN トラフィックのルーティングを許可する方法を示します。

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

設定を確認するには、**show interfaces private-vlan mapping** 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 private-vlan mapping	VLAN SVI のプライベート VLAN マッピング情報を表示します。

queue-set

キューセットに対してポートをマッピングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **queue-set** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

queue-set *qset-id*

no queue-set *qset-id*

シンタックスの説明

<i>qset-id</i>	キューセットの ID。キューセットに属する各ポートの 4 つの出力キューのすべての特性を定義します。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 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
12.1(11)AX	このコマンドが導入されました。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** 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	キューセットに対しバッファを割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
show mls qos interface buffers	Quality of Service (QoS; サービス品質) 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 スイッチまたはスイッチ スタックからのクラスタ メンバー スイッチ上でコマンドを実行するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **rcommand** ユーザ EXEC コマンドを使用します。セッションを終了する場合は、**exit** コマンドを入力します。

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

シンタックスの説明

<i>n</i>	クラスタ メンバーを識別する番号。指定できる範囲は、0 ～ 15 です。
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 <i>hw-addr</i>	クラスタ メンバー スイッチの MAC(メディア アクセス制御)アドレス

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

スイッチがクラスタ コマンド スイッチで、クラスタ メンバー スイッチ *n* が存在していない場合、エラー メッセージが表示されます。スイッチ番号を取得するには、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。

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するには、このコマンドを使用します。

Catalyst 2900 XL、3500 XL、2950、2960、2970、3550、3560、および 3570 スイッチの場合、Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチ CLI (コマンド ライン インターフェイス) にアクセスします。たとえば、このコマンドをクラスタ コマンド スイッチからユーザ レベルで入力した場合、メンバー スイッチはユーザ レベルでアクセスされます。このコマンドをクラスタ コマンド スイッチからイネーブル レベルで使用した場合、コマンドはイネーブル レベルでリモート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継承するため、メンバー スイッチがクラスタに加入してもパスワードを要求するプロンプトは表示されません。

例

次の例では、メンバー 3 でセッションを開始する方法を示します。**exit** コマンドを入力するか、あるいはセッションを閉じるまで、このコマンドに続くすべてのコマンドは、メンバー 3 へ向けられます。

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

関連コマンド

コマンド	説明
show cluster members	クラスタ メンバーに関する情報を表示します。

reload

スタック メンバーをリロードし、設定の変更を有効にするには、**reload** イネーブル EXEC コマンドを使用します。

reload [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]

シンタックスの説明

<i>LINE</i>	リロードする理由を指定します。
at	リロードを実行する時間 (hh:mm) を指定します。
cancel	中断しているリロードをキャンセルします。
in	リロードを実行する時間間隔 (mmm または hhh:mm) を指定します。
slot <i>stack-member-number</i>	指定のスタック メンバー上で変更を保存し、再起動します。
standby-cpu	スタンバイ Route Processor (RP; ルートプロセッサ) をリロードします。

デフォルト

スタック メンバーをただちにリロードし、設定の変更を有効にします。

コマンドモード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
Switch(config)# reload
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

次の例では、特定のスタック メンバーをリロードする方法を示します。

```
Switch(config)# reload slot 6
Proceed with reload? [confirm] y
```

次の例では、単一スイッチのスイッチ スタック (メンバー スイッチが 1 つだけ) をリロードする方法を示します。

```
Switch(config)# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

関連コマンド

コマンド	説明
rcommand	特定のスタック メンバーにアクセスします。
switch priority	スタック メンバーのプライオリティ値を変更します。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

remote command

すべてのまたは指定のスタック メンバーをモニタするには、**remote command** イネーブル EXEC コマンドを使用します。

remote command {**all** | *stack-member-number*} *LINE*

シンタックスの説明

all	すべてのスタック メンバーに適用します。
<i>stack-member-number</i>	スタック メンバーを指定します。指定できる範囲は、1 ～ 9 です。
<i>LINE</i>	実行するコマンドを指定します。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

ストリングを実行する LINE コマンドで使用するコマンド (**debug**、**show**、または **clear** など) は、指定のスタック メンバーまたはスイッチ スタックに適用されます。

例

次の例では、スイッチ スタックで **undebug** コマンドを実行する方法を示します。

```
Switch(config)# remote command all undebug all
Switch :1 :
-----
All possible debugging has been turned off
Switch :5 :
-----
All possible debugging has been turned off
Switch :9 :
-----
All possible debugging has been turned off
```

次の例では、スタック メンバー 5 で **debug udld event** コマンドを実行する方法を示します。

```
Switch(config)# remote command 5 undebug all
Switch :5 :
-----
UDLD events debugging is on
```

関連コマンド

コマンド	説明
reload	特定のスタック メンバーにアクセスします。
switch priority	スタック メンバーのプライオリティ値を変更します。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

remote-span

VLAN (仮想 LAN) を Remote Switched Port Analyzer (RSPAN) VLAN として設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 の指定を 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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト RSPAN VLAN は定義されません。

コマンド モード VLAN コンフィギュレーション (config-VLAN)

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

config-VLAN モード (**vlan** グローバル コンフィギュレーション コマンドを使用) でのみ RSPAN VLAN を設定できます。**vlan database** イネーブル EXEC コマンドでは VLAN コンフィギュレーション モードにはなりません。

VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) がイネーブルの場合、RSPAN 機能は 1005 より低い VLAN ID に VTP によって伝播されます。RSPAN VLAN ID が拡張された範囲にある場合、手動で中間スイッチを設定しなければなりません (送信元スイッチおよび宛先スイッチ間の RSPAN VLAN にあります)。

RSPAN の **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、次のような特性があります。

- MAC (メディア アクセス制御) アドレスの学習は発生しません。
- RSPAN VLAN のトラフィックはトランク ポート上にもみ流れます。
- Spanning-Tree Protocol (STP; スパニングツリー プロトコル) は、RSPAN VLAN で実行できますが、RSPAN の宛先ポート上では実行されません。

既存の VLAN が、RSPAN VLAN として設定された場合、その VLAN は最初に削除され、次に RSPAN VLAN として再度作成されます。RSPAN 機能がディセーブルにならないかぎり、どのアクセス ポートもアクティブにはなりません。

例 次の例では、VLAN を RSPAN VLAN として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
```

設定を確認するには、**show vlan remote-span** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
monitor session	ポート上で SPAN および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。
vlan (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

Dynamic Host Configuration Protocol (DHCP) スヌーピング バインディング データベースを更新するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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[number]:/filename | ftp://user:password@host/filename |
nvrRam:/filename | rcp://user@host/filename | tftp://host/filename}] [validation none]
```

このコマンドは、スイッチで IP サービスが動作している場合に限り使用できます。IP サービスは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

flash[number]:/filename	(任意) データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。スタック マスターのスタック メンバー番号を指定するには、 <i>number</i> パラメータを使用します。 <i>number</i> に指定できる範囲は 1 ～ 9 です。
ftp://user:password@host/filename	(任意) データベース エージェントまたはバインディング ファイルが FTP (ファイル転送プロトコル) サーバにあることを指定します。
nvrAm:/filename	(任意) データベース エージェントまたはバインディング ファイルが NVRAM (不揮発性 RAM) にあることを指定します。
rcp://user@host/filename	(任意) データベース エージェントまたはバインディング ファイルが Remote Control Protocol (RCP) サーバにあることを指定します。
tftp://host/filename	(任意) データベース エージェントまたはバインディング ファイルが Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバにあることを指定します。
validation none	(任意) スイッチが、URL で指定されたバインディング ファイルのエントリに対して Cyclic Redundancy Check (CRC; 巡回冗長検査) を確認しないよう指定します。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン URL を指定しない場合、スイッチは設定された URL からファイルの読み込みを試行します。

例 次の例では、ファイルの CRC 値を確認せずに、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

設定を確認するには、**show ip dhcp snooping database** 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
	ip dhcp snooping	VLAN (仮想 LAN) 上で DHCP スヌーピングをイネーブルにします。
	ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
	show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

rmon collection stats

イーサネット グループの統計（ブロードキャストおよびマルチキャスト パケットに関する使用率の統計、Cyclic Redundancy Check [CRC; 巡回冗長検査] 整合性エラーおよび衝突に関するエラー統計も含む）を収集するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。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]
```

シンタックスの説明

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

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 gigabitethernet2/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

設定を確認するには、**show rmon statistics** 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 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) リソース割り当てに使用するテンプレートを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。システム リソースを割り当てるテンプレートを使用することで、アプリケーションで使用する機能を最大限にサポートできます。テンプレートを使用することにより、ユニキャスト ルーティングまたは VLAN（仮想 LAN）コンフィギュレーションにおいてシステム利用率を最大限にしたり、アグリゲータ テンプレート（Catalyst 3750-12S のみ）をデスクトップ テンプレートに変更したり、またはデュアル IPv4/IPv6 テンプレートを選択して IPv6 フォワーディングをサポートしたりできます（スイッチ スタックで拡張 IP サービス イメージが稼働している場合に限りサポート）。デフォルトの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 {access | default | dual-ipv4-and-ipv6 {default | vlan} | routing | vlan} [desktop]

no sdm prefer

シンタックスの説明

access	Access Control List (ACL; アクセス制御リスト) におけるシステム使用率を最大限にします。ACL が多数ある場合、このテンプレートを使用します。
default	スイッチでデフォルトのテンプレートを使用するように設定します。Catalyst 3750-12S スイッチでは、デフォルトのデスクトップ テンプレートに設定するには、 desktop キーワードを使用します（デスクトップ スイッチでデフォルトのデスクトップ テンプレートに設定する、またはアグリゲータ スイッチでデフォルトのアグリゲータ 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）。
dual-ipv4-and-ipv6 {default vlan}	IPv4 および IPv6 ルーティングの両方をサポートするテンプレートを選択します。 default — IPv4 および IPv6 のレイヤ 2、レイヤ 3 機能を均等に動作させます。 vlan — IPv4 および IPv6 の VLAN においてシステム使用率を最大限にします。  (注) このオプションはすべてのスイッチで表示されますが、スイッチ スタックまたはスイッチで拡張 IP サービス イメージが稼働している場合にのみサポートされます。
routing	ユニキャスト ルーティングにおいてシステム使用率を最大限にします。通常、ネットワークの中心にあるルータまたはアグリゲータでこのテンプレートを使用します。
vlan	VLAN のシステム使用率を最大限にします。このテンプレートは、ルーティングを行わないレイヤ 2 スイッチの使用に対して、システム リソースを最大にします。
desktop	Catalyst 3750-12S スイッチ上でのみ使用し（アグリゲータ テンプレートがデフォルト）、 default 、 routing 、 vlan のテンプレートを選択します。

デフォルト

デフォルトのテンプレートはすべての機能を均等に動作させます。

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	アグリゲータ テンプレートが追加されました。
12.2(25)SEA	dual-ipv4-and-ipv6 テンプレートが追加されました。
12.2(25)SED	アクセス テンプレートが追加されました。

使用上のガイドライン

この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** コマンドを入力した場合、**show sdm prefer** により、現在使用している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が表示されます。

デスクトップ スイッチは、デスクトップ テンプレートのみサポートします。アグリゲータ スイッチ (Catalyst 3750-12S) はデスクトップおよびアグリゲータ テンプレートの両方をサポートします。アグリゲータ スイッチ上で、デスクトップ キーワードを入力しない場合、アグリゲータ テンプレートが選択されます。

すべてのスタック メンバーは同一の SDM デスクトップまたはアグリゲータ テンプレート (スタック マスター上に保存) を使用します。新しいスイッチ メンバーがスタックに追加された場合、スタック マスター上に保存されている SDM の設定は、スイッチ コンフィギュレーション ファイルおよび VLAN データベース ファイルを使用して、個々のスイッチで設定されたテンプレートを上書きします。

スタック全体で IPv6 を使用するには、スタック内のすべてのスイッチで拡張 IP サービス イメージを稼働している必要があります。IPv6 パケットのフォワーディングをイネーブルにすると、ハードウェア内のすべてのスタック メンバー スイッチが IPv6 パケットを転送します。

スタック メンバーがマスター スイッチ上で稼働しているテンプレートをサポートできない場合、スイッチは SDM ミスマッチ モードに入り、マスター スイッチが SDM テンプレートを変更しないようにします。その場合、スイッチはスタックのメンバーとして機能することはできません。

- マスター スイッチが Catalyst 3750-12S で、アグリゲータ テンプレートからデスクトップ テンプレートに変更し、スイッチをリロードした場合、スタック全体がデスクトップ テンプレートを選択した状態で動作します。このため、Ternary CAM (TCAM) エントリの数がデスクトップ テンプレートのサイズを超えた場合、設定が失われる可能性があります。
- Catalyst 3750-12S マスター上のテンプレートをデスクトップテンプレートからアグリゲータ テンプレートに変更し、スイッチをリロードした場合、スタックのメンバーであったすべてのデスクトップ スイッチは SDM ミスマッチ モードに入ります。
- アグリゲータ テンプレートを実行している Catalyst 3750-12S スイッチを、スタック マスターがデスクトップ スイッチのスタックに追加する場合、スタックは、スタック マスター上で選択されているデスクトップテンプレートで操作を実行します。そのため、TCAM エントリの数がデスクトップテンプレートのサイズを超えた場合、Catalyst 3750-12S スタック メンバー上にある設定は失われる可能性があります。

スタックに関する詳細情報は、ソフトウェア コンフィギュレーション ガイドの「Managing Switch Stacks」を参照してください。

アクセス テンプレートを使用すると、大量の ACL が必要な場合に、ACL のためのシステム リソースを最大にできます。

デフォルトのテンプレートは、システム リソースを均等に使用します。

sdm prefer vlan [desktop] グローバル コンフィギュレーション コマンドは、ルーティングしないレイヤ 2 スイッチングのスイッチ上でのみ使用します。VLAN テンプレートを使用する場合、システム リソースはルーティング エントリに予約されません。ルーティングはソフトウェアで実行されます。この場合、CPU に負荷がかかり、ルーティングのパフォーマンスが大幅に低下します。

スイッチ上でルーティングがイネーブルになっていない場合、ルーティング テンプレートは使用しないでください。**sdm prefer routing [desktop]** 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で、他の機能にルーティング テンプレートのユニキャスト ルーティングに割り当てたメモリを使用させないようにします。

スイッチ上で IPv6 ルーティングをイネーブルにしない場合、IPv4/IPv6 テンプレートは使用しないでください。**sdm prefer ipv4-and-ipv6 {default | vlan} [desktop]** 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、リソースを IPv4 と IPv6 に振り分けて、IPv4 フォワーディングに割り当てられたリソースを制限します。

表 2-15 では、デスクトップまたはアグリゲータ スイッチの IPv4 限定テンプレートでサポートされる各リソースの概算を示します。テンプレートの値は 8 つのルーティングされたインターフェイスおよび約 1000 の VLAN に基づいていて、テンプレートが選択されたときに設定されたおおよそのハードウェアの境界になります。ハードウェア リソースのセクションが埋まっている場合、処理できないものはすべて CPU に送信されるため、スイッチのパフォーマンスに著しく影響します。

表 2-15 IPv4 テンプレートに割り当てられた機能のリソースの概算

リソース	デスクトップ テンプレート				アグリゲータ テンプレート			
	アクセ ス	デフォ ルト	ルーティ ング	VLAN	アクセ ス	デフォ ルト	ルーティ ング	VLAN
ユニキャスト MAC アドレス	4 K	6 K	3 K	12 K	6 K	6 K	6 K	12 K
Internet Group Management Protocol (IGMP) グループおよびマルチキャスト ルート	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K
ユニキャスト ルート	6 K	8 K	11 K	0	12 K	12 K	20 K	0
• ホストに直接接続	4 K	6 K	3 K	0	6 K	6 K	6 K	0
• 間接ルート	2 K	2 K	8 K	0	6 K	6 K	14 K	0
ポリシーベースのルーティング Access Control Entry (ACE; アクセス制御エントリ)	512	0	512	0	512	0	512	0
Quality of Service (QoS; サービス品質) 分類 ACE	512	512	512	512	896	896	512	896
セキュリティの ACE	2 K	1 K	1 K	1 K	4 K	1 K	1 K	1 K
レイヤ 2 VLAN	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K

表 2-16 では、デスクトップまたはアグリゲータ スイッチの IPv4/IPv6 テンプレートでサポートされる各リソースの概算を示します。

表 2-16 デュアル IPv4/IPv6 テンプレートに割り当てられた機能のリソースの概算

リソース	デスクトップ IPv4/IPv6 テンプレート		アグリゲータ IPv4/IPv6 テンプレート	
	デフォルト	VLAN	デフォルト	VLAN
ユニキャスト MAC アドレス	2 K	8 K	2 K	8 K
IPv4 IGMP グループおよびマルチキャスト ルータ	1 K	1 K	2 K	0
IPv4 ユニキャスト ルートの総数	3 K	0	3 K	0
• IPv4 ホストに直接接続	2 K	0	2 K	0
• 間接 IPv4 ルート	1 K	0	1 K	1 K
IPv6 マルチキャスト グループ	1 K	1 K	1 K	1 K
IPv6 ユニキャスト ルートの総数	3 K	0	3 K	0
• IPv6 アドレスに直接接続	2 K	0	2 K	0

表 2-16 デュアル IPv4/IPv6 テンプレートに割り当てられた機能のリソースの概算（続き）

リソース	デスクトップ IPv4/IPv6 テンプレート		アグリゲータ IPv4/IPv6 テンプレート	
	デフォルト	VLAN	デフォルト	VLAN
• 間接 IPv6 ユニキャスト ルート	1 K	0	1 K	0
IPv4 ポリシーベースのルーティング ACE	0	0	0	0
IPv4 または MAC の QoS ACE（総数）	512	512	876	876
IPv4 または MAC のセキュリティ ACE（総数）	1 K	1 K	512	1 K
IPv6 ポリシーベースのルーティング ACE	0	0	0	0
IPv6 QoS ACE	510	510	876	876
IPv6 セキュリティ ACE	510	510	876	876

例 次の例では、デスクトップ スイッチ上でアクセス テンプレートを設定する方法を示します。

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

次の例では、デスクトップ スイッチ上でルーティング テンプレートを設定する方法を示します。

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

次の例では、アグリゲータ スイッチ上でデスクトップ ルーティング テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer routing desktop
Switch(config)# exit
Switch# reload
```

次の例では、デスクトップ スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

次の例では、スイッチのテンプレートをデフォルトのテンプレートに変更する方法を示します。アグリゲータ スイッチ上では、デフォルトの集約のテンプレートが、デスクトップ スイッチ上では、デスクトップ テンプレートが選択されます。

```
Switch(config)# no sdm prefer
Switch(config)# exit
Switch# reload
```

次の例では、アグリゲータ スイッチ上でデスクトップ デフォルト テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer default desktop
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
<code>show sdm prefer</code>	現在使用されている SDM テンプレート、または使用可能なテンプレート、および機能ごとのリソース割り当てを概算で表示します。

service password-recovery

パスワードの回復メカニズムをイネーブル（デフォルト）にするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。このメカニズムを使用すると、スイッチに物理的にアクセス可能なエンドユーザは、スイッチの起動処理中に **Mode** ボタンを押してブート プロセスを中断して、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の一部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の状態、ブート プロセスを中断するには、システムをデフォルト設定に戻すことに同意しなければなりません。

service password-recovery

no service password-recovery

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

システム管理者は、**no service password-recovery** コマンドを使用し、一部のパスワード回復機能をディセーブルにできます。これを行うと、エンドユーザはシステムをデフォルト設定に戻すことに同意しないかぎり、パスワードのリセットが許可されません。

パスワードの回復手順は、スイッチに物理的にアクセス可能なユーザが、装置の起動中 **Mode** ボタンをポートの 1X 上の LED が消えるまで 1 ～ 2 秒間押します。ボタンが解放されれば、システムは初期化を続行します。パスワード回復のメカニズムがディセーブルの場合、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)?
```

システムをリセットしてデフォルト設定に戻さないよう選択した場合、**Mode** ボタンが押されなかったものとして通常のブートプロセスが継続します。システムをリセットしてデフォルト設定に戻す場合、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*（存在する場合）も削除されます。

**(注)**

no service password-recovery コマンドを使用して、エンドユーザのパスワードアクセスを制御する場合、エンドユーザがパスワード回復プロセスを使用してシステムをデフォルト値に戻す状況を考慮し、スイッチとは別の場所に **config** ファイルのコピーを保存しておくよう推奨します。スイッチ上に **config** ファイルのバックアップを保存することは避けてください。

スイッチが VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) のトランスペアレントモードで動作している場合、*vlan.dat* ファイルもスイッチとは別の場所にコピーをとり、保存しておくよう推奨します。

service password-recovery または **no service password-recovery** コマンドをスタックマスター上で入力した場合、コマンドはスタック中に伝播され、スタック内のすべてのスイッチに適用されます。

パスワードの回復がイネーブルかどうか確認するには、**show version** イネーブル EXEC コマンドを入力します。

例

次の例では、スイッチ上またはスイッチ スタック上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。ユーザはデフォルト設定に戻すことに同意が得られた場合のみパスワードをリセットできます。

```
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、物理ポートまたは Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) 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

シンタックスの説明

input policy-map-name 物理ポートまたは SVI 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tring には表示されますが、サポートされていません。収集された統計は無視してください。**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 マップは適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	ポリシー マップは現在、物理ポートまたは SVI に適用されています。
12.2(25)SED	階層型ポリシー マップは現在、SVI に適用されています。

使用上のガイドライン

1 つの入力ポートに対してサポートされるポリシー マップは 1 つのみです。Cisco IOS Release 12.2(25)SE より前のソフトウェア リリースでは、ポリシー マップは物理ポート上でのみ設定できます。

Cisco IOS Release 12.2(25)SE 以降のリリースでは、ポリシー マップは物理ポートまたは SVI 上で設定できます。物理ポート上で **no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して VLAN (仮想 LAN) ベースの Quality of Service (QoS; サービス品質) をディセーブルにすると、そのポート上にポートベースのポリシー マップを設定できます。物理ポート上で **mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して VLAN ベースの QoS をイネーブルにした場合、スイッチは前に設定されたポートベースのポリシー マップを削除します。階層型ポリシー マップが設定され、SVI に適用されたあと、インターフェイスレベルのポリシー マップはこのインターフェイスで有効になります。

Cisco IOS Release 12.2(25)SE より前のソフトウェア リリースでは、ポリシー マップを物理ポートの着信トラフィックに対してのみ適用できます。Cisco IOS Release 12.2(25)SE 以降のソフトウェア リリースでは、ポリシー マップを物理ポートまたは SVI の着信トラフィックに適用できます。Cisco IOS Release 12.2(25)SED 以降のソフトウェア リリースでは、VLAN レベルのポリシー マップで定義された各クラスに対して、異なるインターフェイス レベルのポリシー マップを設定できます。階層型ポリシー マップの詳細情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring QoS」の章を参照してください。

ポートの信頼状態（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**）を使用した分類は、相互に排他的な関係です。設定された最後の 1 つが以前の設定を上書きします。

police aggregate コマンドを使用してポリシー マップを 10 ギガビット イーサネット インターフェイスに適用すると、エラーになります。

例

次の例では、物理入力ポートに *plcmap1* を適用する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから *plcmap2* を削除する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# no service-policy input plcmap2
```

次の例では、VLAN ベースの QoS がイネーブルの場合に *plcmap1* を入力 SVI に適用する方法を示します。

```
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input plcmap1
```

次の例では、階層型ポリシー マップを作成し、SVI に適用する方法を示します。

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list 101 permit ip any any
Switch(config)#class-map cm-1
Switch(config-cmap)#match access 101
Switch(config-cmap)#exit
Switch(config)#exit
Switch#
Switch#
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#class-map cm-interface-1
Switch(config-cmap)#match input g3/0/1 - g3/0/2
Switch(config-cmap)#exit
Switch(config)#policy-map port-plcmap
Switch(config-pmap)#class-map cm-interface-1
Switch(config-pmap-c)#police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#policy-map vlan-plcmap
Switch(config-pmap)#class-map cm-1
Switch(config-pmap-c)#set dscp 7
Switch(config-pmap-c)#service-policy port-plcmap-1
Switch(config-pmap-c)#exit
Switch(config-pmap)#class-map cm-2
Switch(config-pmap-c)#match ip dscp 2
Switch(config-pmap-c)#service-policy port-plcmap-1
Switch(config-pmap-c)#exit
Switch(config-pmap)#class-map cm-3
Switch(config-pmap-c)#match ip dscp 3
Switch(config-pmap-c)#service-policy port-plcmap-2
Switch(config-pmap-c)#exit
Switch(config-pmap)#class-map cm-4
Switch(config-pmap-c)#trust dscp
Switch(config-pmap-c)#exit
Switch(config)#int vlan 10
Switch(config-if)#
Switch(config-if)#ser input vlan-plcmap
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

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。

session

指定のスタック メンバーにアクセスするには、スタック マスター上で **session** イネーブル EXEC コマンドを使用します。

session *stack-member-number*

シンタックスの説明

<i>stack-member-number</i>	スタック メンバー番号を指定します。指定できる範囲は、1 ～ 9 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スタック メンバーにアクセスすると、スタック メンバーの番号がシステム プロンプトに追加されます。

例

次の例では、スタック メンバー 6 にアクセスする方法を示します。

```
Switch(config)# session 6
Switch-6#
```

関連コマンド

コマンド	説明
reload	スタック メンバーをリロードし、設定の変更を有効にします。
switch priority	スタック メンバーのプライオリティ値を変更します。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

set

パケットの Differentiated Services Code Point (DSCP) 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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}
```

シンタックスの説明

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。汎用的に使用する値に対してはニーモニック名を入力することもできます。
[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。汎用的に使用する値に対して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

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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	ip dscp new-dscp キーワードは dscp new-dscp に変更されました。 set ip dscp new-dscp コマンドは set dscp new-dscp コマンドに変更されました。
12.2(25)SEC	ip キーワードは任意です。

使用上のガイドライン

Cisco IOS Release 12.2(25)SE 以降では、**set ip dscp** コマンドを使用すると、スイッチによってこのコマンドはスイッチ コンフィギュレーションの **set dscp** に変更されます。**set ip dscp** コマンドを入力すると、この設定はスイッチ コンフィギュレーションの **set dscp** として表示されます。

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

set コマンドは、同一ポリシー マップ内の **trust** ポリシーマップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

set dscp new-dscp または **set ip precedence new-precedence** コマンドについては、汎用的に使用する値用に、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、**set dscp 10** コマンドとして入力しても同じ結果になります。**set ip precedence critical** コマンドを、**set ip precedence 5** コマンドとして入力しても同じ結果になります。サポートされているニーモニックの一覧に関しては、**set dscp ?** または **set ip precedence ?** コマンドを入力し、コマンドラインのヘルプ スtring 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。

例

次の例では、ポリサーが設定されていないすべての FTP（ファイル転送プロトコル）トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
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	指定のクラスマップ名で、トラフィックの分類一致条件を定義します（ 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）。
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 コマンドで分類されたトラフィックに、信頼状態を定義します。

setup

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

setup

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン **setup** コマンドを使用する場合、次の情報を確認してください。

- IP アドレスおよびネットワーク マスク
- 使用環境に対するパスワードの指針
- スイッチがクラスタ コマンドスイッチおよびクラスタ名として使用されるかどうか

setup コマンドを入力すると、System Configuration Dialog という対話形式のダイアログが表示されます。このダイアログでは、設定プロセスの手順を示し情報の提供が行われます。各プロンプトの隣の括弧に表示される値は、**setup** コマンド機能または **configure** イネーブル EXEC コマンドを使用して設定された最後のデフォルト値です。

各プロンプトでヘルプ テキストが提供されています。ヘルプ テキストにアクセスするには、プロンプトで疑問符 (?) のキーを入力します。

何も変更せず、また System Configuration Dialog を最後まで実行せずにイネーブル EXEC のプロンプトに戻るには、**Ctrl-C** を押します。

変更が完了した場合、セットアップ プログラムにより、セットアップ セッション中に作成されたコンフィギュレーション コマンドスクリプトが表示されます。コンフィギュレーションを NVRAM (不揮発性 RAM) に保存できます。保存しないでセットアップ プログラムやコマンドライン プロンプトに戻ることもできます。

例

次の例では、**setup** コマンドの出力を示します。

```
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
GigabitEthernet6/0/1      unassigned      YES unset   up          up
GigabitEthernet6/0/2      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$0XclwyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
```

```

password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet6/0/1
no ip address
!
interface GigabitEthernet6/0/2
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、スイッチ スタックまたはスタンドアロン スイッチ上で **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場合は、このコマンドの **no** 形式を使用します。

setup express

no setup express

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 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
	12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン 新しい（未設定の）スイッチ上で Express Setup をイネーブルにする場合、Mode ボタンを 2 秒間押すことで Express Setup を開始できます。IP アドレス 10.0.0.1 を使用し、イーサネット ポートからスイッチにアクセスできます。その後、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 プログラムでスイッチを設定できます。

設定されたスイッチ上で Mode ボタンを 2 秒間押すと、Mode ボタンの上の LED が点滅し始めます。Mode ボタンを 10 秒間押すと、スイッチの設定は削除され、スイッチが再起動します。その後、スイッチを新規のスイッチとして、Web ベースの Express Setup または CLI ベースのセットアップ プログラムで設定できます。



(注) スイッチの設定（CLI ベースのセットアップ プログラムの最初に **no** を入力することも含む）に変更が加えられると、直後から Express Setup による設定を使用できなくなります。Mode ボタンを 10 秒間押さないかぎり、Express Setup を再び実行できません。これにより、スイッチの設定は削除され、スイッチが再起動されます。

スイッチ上で Express Setup がアクティブな場合に、**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 は稼働しなくなります。スイッチの IP アドレス 10.0.0.1 は有効ではなくなり、この IP アドレスを使用している接続も終了します。

no setup express コマンドの主な目的は、Mode ボタンを 10 秒間押したためにスイッチの設定が誤って削除されてしまうことを回避するためのものです。

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
```

Express Setup モードがイネーブルかどうかを確認するには、Mode ボタンを押します。

- 未設定のスイッチ上では、Mode ボタンの上の LED が 3 秒後にグリーンになります。
- 設定されたスイッチ上では、Mode の LED が 2 秒後に点滅し、10 秒後にグリーンになります。

**注意**

Mode ボタンを 10 秒間押し続けた場合、スイッチの設定は削除され、スイッチが再起動します。

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 ボタンを押すことで、Express Setup モードがディセーブルかどうかを確認できます。Express Setup モードがスイッチ上でイネーブルでない場合、Mode の LED がグリーンで点滅（点灯ではない）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かどうか表示します。

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]
```

シンタックスの説明

<i>name</i>	(任意) ACL の名前です。
<i>number</i>	(任意) ACL の番号です。指定できる範囲は、1 ～ 2699 です。
hardware counters	(任意) スイッチおよびルーテッドパケットのグローバルハードウェア ACL 統計を表示します。
ipc	(任意) Interprocess Communication (IPC) プロトコルのアクセスリスト設定ダウンロード情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring には表示されますが、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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	ipc キーワードが追加されました。

使用上のガイドライン

スイッチは IP 標準および拡張アクセス リストのみサポートします。そのため、割り当てられる番号は 1 ～ 199 および 1300 ～ 2699 のみです。

このコマンドでは、設定されている 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
<code>access-list</code>	スイッチ上で、標準または拡張番号付きアクセス 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。
<code>ip access list</code>	スイッチに名前付き 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。
<code>mac access-list extended</code>	スイッチに名前付きまたは番号付きの 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 Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) を使用して、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]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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(20)SE	このコマンドが導入されました。

使用上のガイドライン

archive download-sw イネーブル EXEC コマンドを使用して、TFTP サーバにイメージをダウンロードした場合、**archive download-sw** コマンドの出力によりダウンロードのステータスが示されます。

TFTP サーバを保有していない場合は、Network Assistant または組み込み型デバイス マネージャを使用して HTTP によりイメージをダウンロードできます。**show archive status** コマンドは、ダウンロードの進行状況を示します。

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 archive status** コマンドの出力を示します。

```
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 arp access-list

Address Resolution Protocol (ARP; アドレス解決プロトコル) アクセス制御 (リスト) の詳細情報を表示するには、**show arp access-list** ユーザ EXEC コマンドを使用します。

show arp access-list [*acl-name*] [| {**begin** | **exclude** | **include**} *expression*]

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明	<i>acl-name</i>	(任意) Access Control List (ACL; アクセス制御リスト) の名前です。
	begin	(任意) <i>expression</i> と一致する行から表示を開始します。
	exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
	include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
	<i>expression</i>	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(20)SE	このコマンドが導入されました。

使用上のガイドライン 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 arp access-list** コマンドの出力を示します。

```
Switch> show arp access-list
ARP access list rose
    permit ip 10.101.1.1 0.0.0.255 mac any
    permit ip 20.3.1.0 0.0.0.255 mac any
```

関連コマンド	コマンド	説明
	arp access-list	ARP ACL を定義します。
	deny (ARP アクセスリスト コンフィギュレーション)	Dynamic Host Configuration Protocol (DHCP) バインディングとの照合に基づいた ARP パケットを拒否します。
	ip arp inspection filter vlan	スタティックな IP アドレスで設定されたホストからの ARP 要求および ARP 応答を許可します。
	permit (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングとの照合に基づいた ARP パケットを許可します。

show auto qos

Automatic QoS (Auto-QoS) がイネーブルのインターフェイス上で入力された 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]]

シンタックスの説明

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
12.1(14)EA1	このコマンドが導入されました。
12.2(20)SE	コマンド出力の情報が変更され、ユーザの注意事項が更新されました。

使用上のガイドライン

Cisco IOS Release 12.2(20)SE より前のリリースでは、**show auto qos [interface [interface-id]]** コマンド出力は生成された Auto-QoS の初期設定を示します。

Cisco IOS Release 12.2(20)SE 以降では、**show auto qos** コマンド出力は各インターフェイスで入力された Auto-QoS コマンドのみを示します。**show auto qos interface interface-id** コマンド出力は、特定のインターフェイスで入力された Auto-QoS コマンドを示します。

Auto-QoS 設定およびユーザの変更部分を表示するには、**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 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あとの **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone
```

```
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

```
GigabitEthernet2/0/6
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 2/0/5
GigabitEthernet2/0/5
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 GigabitEthernet2/0/4
  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 GigabitEthernet2/0/5
  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 GigabitEthernet2/0/6
  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 fastethernet1/0/2
FastEthernet1/0/2
auto qos voip cisco-phone
```

■ show auto qos

次の例では、スイッチ上で Auto-QoS が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、インターフェイス上で Auto-QoS が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 gigabitethernet3/0/1
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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、すべてのスタック メンバーの **show boot** コマンドの出力を示します。表 2-17 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:/c3750-ipservices-mz
Config file         :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break        :no
Manual Boot         :yes
HELPER path-list    :
Auto upgrade        :yes
-----
Switch 1
-----
BOOT path-list      :flash:/c3750-ipservices-mz
Config file         :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break        :no
Manual Boot         :yes
HELPER path-list    :
Auto upgrade        :no

(テキスト出力は省略)
```

表 2-17 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される実行可能ファイルのリストをセミコロンで区切って表示します。 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。 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 システムで見つかった最初のブート 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	起動中のブレイクがイネーブルか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できます。
Manual Boot	スイッチを自動で起動するか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 ロード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 ロード 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 ロードの初期化中にダイナミックにロードされるロード可能ファイルのリストをセミコロンで区切って表示します。ヘルパー ファイルは、ブート ロードの機能を拡張したり、パッチを当てます。
Auto upgrade	スイッチ スタックが、互換性のないスイッチがスタックに加入できるよう、ソフトウェア バージョンの自動コピーが設定されているかどうかを表示します。 Version-Mismatch (VM) モードにあるスイッチは、スイッチ スタックとは異なるスタック プロトコルのバージョンが適用されています。そのため、VM モードのスイッチはスイッチのスタックに加入できません。スイッチ スタックが VM モードのスイッチにコピーできるイメージを保有し、boot auto-copy-sw 機能がイネーブルの場合、他のスタック メンバーからのイメージを VM モードのスイッチに自動的にコピーします。その場合、スイッチは VM モードを終了し、再起動後にスイッチ スタックに加入します。

関連コマンド	コマンド	説明
	boot auto-copy-sw	VM モードのスイッチを自動的にアップグレードするには、自動アップグレード (auto-upgrade) プロセスをイネーブルにします。
	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	自動ブート プロセスの中断をイネーブルにします。
	boot manual	次のブート サイクル中、スイッチの手動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	次のブート サイクル中にロードする Cisco IOS イメージを指定します。

show cable-diagnostics tdr

Time Domain Reflector (TDR; タイム ドメイン反射率計) の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*]

シンタックスの説明

<i>interface-id</i>	TDR が実行されたインターフェイスを指定します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

TDR は、10/100/100 銅線イーサネット ポート上でのみサポートされます。10/100 ポート、10 ギガビット モジュール ポート、または Small Form-Factor Pluggable (SFP) モジュール ポートではサポートされていません。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、Catalyst 3750G-24PS または 3750G-48PS スイッチ以外のスイッチでの **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 gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length Remote pair Pair status
-----
Gil/0/2    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
```

次の例では、Catalyst 3750G-24PS または 3750G-48PS スイッチでの **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 gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length Remote pair Pair status
-----
Gil/0/2    auto  Pair A      0    +/- 4 meters N/A      Open
          Pair B      0    +/- 4 meters N/A      Open
          Pair C      0    +/- 4 meters N/A      Open
          Pair D      0    +/- 4 meters N/A      Open
```

表 2-18 に、**show cable-diagnostics tdr** コマンド出力内のフィールドの説明を示します。

表 2-18 show cable-diagnostics tdr コマンド出力のフィールドの説明

フィールド	説明
Interface	TDR が実行されたインターフェイス
Speed	接続の速度
Local pair	TDR がローカル インターフェイスでテストしている配線ペア名
Pair length	使用しているスイッチに関する問題があるケーブルの位置。TDR は以下の場合のみ位置を判別できます。 - ケーブルが適切に接続されていて、リンクがアップであり、インターフェイス速度が 1000 Mbps（メガビット/秒）である。 - ケーブルがオープンである。 - ケーブルに短絡がある。
Remote pair	ローカル ペアが接続されている配線ペア名。ケーブルが適切に接続されていてリンクがアップの場合のみ、TDR がリモート ペアを判別できます。
Pair status	TDR が動作している配線ペアの状態 - Normal — 配線ペアが適切に接続されています。 - Not completed — テストが動作中で完了していません。 - Not supported — インターフェイスが TDR をサポートしていません。 - Open — 配線ペアがオープンです。 - Shorted — 配線ペアが短絡しています。

次の例では、TDR が動作している場合の **show interface interface-id** コマンドの出力を示します。

```
Switch# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が動作していない場合の **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 gigabitethernet1/0/2
% TDR test was never issued on Gi1/0/2
```

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 をイネーブルにして実行します。

show class-map

トラフィックを分類するための一致条件を定義する Quality of Service (QoS; サービス品質) クラスマップを表示するには、**show class-map** ユーザ EXEC コマンドを使用します。

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>class-map-name</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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を照合する場合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 スイッチおよびクラスタ メンバー スイッチ上で入力できます。

show cluster [**| {begin | exclude | include}** *expression*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

クラスタのメンバーでないスイッチ上で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 スイッチ上で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 スイッチのスタックまたはクラスタ コマンド スイッチ上で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 スイッチ上で **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 スイッチ上で **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 スイッチ上で **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たクラスタ コマンド スイッチ上で **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たクラスタ メンバー スイッチ上で **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、および任意で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、スイッチ スタックまたはクラスタ コマンド スイッチ上で **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*]

シンタックスの説明

detail	(任意) すべての候補に関する詳細を表示します。
mac-address <i>H.H.H.</i>	(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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

スイッチがクラスタ コマンド スイッチでない場合は、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 カラムの値に E が表示された場合、スイッチは拡張検出によって検出されています。SN カラムの値が 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 カウントは、クラスタ コマンド スイッチから候補スイッチまでの装置数です。

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
```

MAC Address	Name	Device Type	PortIf	FEC	Hops	SN	PortIf	FEC
00d0.7961.c4c0	StLouis-2	WS-C3750-12T	Gi6/0/1		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た、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-C3750-12T
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
  Local port:           Gi6/0/1   FEC number:
  Upstream port:        GI6/0/11  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 メンバーの情報を表示するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **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*]

シンタックスの説明

<i>n</i>	(任意) クラスタ メンバーを識別する番号。指定できる範囲は、0 ～ 15 です。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

```

SN	MAC Address	Name	PortIf	FEC	Hops	---Upstream---			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-C3750
  MAC address:      0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:       Gi6/0/1      FEC number:
  Upstream port:    GI6/0/11     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-C3750
  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-C3750
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:          Gi6/0/1  FEC number:
  Upstream port:       Fa6/0/11 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) の状態、および CPU に届くパケットに対する送受信の統計を表示するには、**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*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用することで、Cisco のテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ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、**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の内部レジスタから読み込まれる、各インターフェイスの送受信の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まれる各インターフェイスの送受信の統計情報を表示するには、キーワードを指定せずに **show controllers ethernet-controller** イネーブル EXEC コマンドを使用します。**phy** キーワードを使用することでインターフェイスの内部レジスタを表示、または **port-asic** キーワードを指定することでポートの Application Specific Integrated Circuit (ASIC; 特定用途向け IC) の情報を表示させます。

```
show controllers ethernet-controller [interface-id] [phy [detail]] [port-asic {configuration |
statistics}] [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	物理インターフェイス (タイプ、スタック メンバー、モジュール、ポート番号を含む)
phy	(任意) 装置またはインターフェイスに対するスイッチの Physical Layer Device (PHY) 上にある内部レジスタのステータスを表示します。表示には、インターフェイスの Automatic Media-Dependent-Interface Crossover (Auto-MDIX) 機能の動作状態が含まれます。
detail	(任意) PHY 内部レジスタの詳細情報を表示します。
port-asic	(任意) ポートの ASIC 内部レジスタの情報を表示します。
configuration	ポートの ASIC 内部レジスタの設定を表示します。
statistics	ポートの ASIC 統計情報 (Rx/Sup キューおよびその他の統計情報を含む) を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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 モードでは *interface-id* キーワードのみがサポートされます)

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	XENPAK モジュール シリアル Electrically Erasable Programmable Read-Only Memory (EEPROM; 電氣的消去再書き込み可能 ROM) の内容が表示されるようになりました。

使用上のガイドライン

キーワードを指定しない場合、トラフィックの統計が表示されます。基本的にはすべての、または指定されたインターフェイスに対する Remote Monitoring (RMON) 統計情報が表示されます。

phy または **port-asic** キーワードを入力した場合は、主にシスコのテクニカル サポート担当のスイッチのトラブルシューティングに役立つ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、1つの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2-19に *Transmit* フィールドの説明を、表2-20に *Receive* フィールドの説明を示します。

```
Switch# show controllers ethernet-controller gigabitethernet6/0/1
Transmit GigabitEthernet6/0/1          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
0 511 byte frames
0 1023 byte frames
0 1518 byte frames
0 Too large frames
0 Good (1 coll) frames
```

表 2-19 Transmit フィールドの説明

フィールド	説明
Bytes	インターフェイスで送信される総バイト数
Unicast Frames	ユニキャストアドレスに送信される総フレーム数
Multicast frames	マルチキャストアドレスに送信される総フレーム数
Broadcast frames	ブロードキャストアドレスに送信される総フレーム数
Too old frames	パケットが期限切れのために出力ポートで廃棄されたフレーム数
Deferred frames	2 × 最大パケット時間の経過後に送信されないフレーム数
MTU exceeded frames	最大許容フレーム サイズより大きいフレームの数
1 collision frames	1 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
2 collision frames	2 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
3 collision frames	3 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
4 collision frames	4 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
5 collision frames	5 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
6 collision frames	6 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
7 collision frames	7 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
8 collision frames	8 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数

表 2-19 Transmit フィールドの説明（続き）

フィールド	説明
9 collision frames	9 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
10 collision frames	10 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
11 collision frames	11 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
12 collision frames	12 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
13 collision frames	13 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
14 collision frames	14 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
15 collision frames	15 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数
Excessive collisions	16 コリジョンが発生したあとで、インターフェイスで正常に送信できなかったフレームの数
Late collisions	フレームの送信後、フレームの送信中にレイト コリジョンが検出されたために廃棄されたフレーム数
VLAN discard frames	CFI ¹ ビットが設定されているためにインターフェイスで廃棄されたフレーム数
Excess defer frames	最大パケット時間の経過後に送信されないフレーム数
64 byte frames	インターフェイスで送信される 64 バイトの総フレーム数
127 byte frames	インターフェイスで送信される 65 ～ 127 バイトの総フレーム数
255 byte frames	インターフェイスで送信される 128 ～ 255 バイトの総フレーム数
511 byte frames	インターフェイスで送信される 256 ～ 511 バイトの総フレーム数
1023 byte frames	インターフェイスで送信される 512 ～ 1023 バイトの総フレーム数
1518 byte frames	インターフェイスで送信される 1024 ～ 1518 バイトの総フレーム数
Too large frames	インターフェイスで送信される、最大許容フレーム サイズより大きいフレームの数
Good (1 coll) frames	1 コリジョンが発生したあとで、インターフェイスで正常に送信されるフレームの数。この値には、1 コリジョンが発生したあとで、正常に送信されないフレーム数は含まれません。

1. CFI = Canonical Format Indicator

表 2-20 Receive フィールドの説明

フィールド	説明
Bytes	インターフェイスで受信されるフレームで使用するメモリ総数（バイト）で、FCS ¹ 値や正しく形成されていないフレームを含みます。この値には、フレーム ヘッダー ビットは含まれません。
Unicast frames	ユニキャスト アドレスに向けられたインターフェイスで正常に受信される総フレーム数
Multicast frames	マルチキャスト アドレスに向けられたインターフェイスで正常に受信される総フレーム数
Broadcast frames	ブロードキャスト アドレスに向けられたインターフェイスで正常に受信される総フレーム数
Unicast bytes	インターフェイスで受信されるユニキャスト フレームで使用するメモリ総数（バイト）で、FCS 値や正しく形成されていないフレームを含みます。この値には、フレーム ヘッダー ビットは含まれません。
Multicast bytes	インターフェイスで受信されるマルチキャスト フレームで使用するメモリ総数（バイト）で、FCS 値や正しく形成されていないフレームを含みます。この値には、フレーム ヘッダー ビットは含まれません。
Broadcast bytes	インターフェイスで受信されるブロードキャスト フレームで使用するメモリ総数（バイト）で、FCS 値や正しく形成されていないフレームを含みます。この値には、フレーム ヘッダー ビットは含まれません。
Alignment errors	アライメント エラーがあるインターフェイスで受信される総バイト数

表 2-20 Receive フィールドの説明（続き）

フィールド	説明
FCS errors	有効な長さ（バイト）であっても、正しい FCS 値を持たないインターフェイスで受信されるフレームの総数
Oversize frames	インターフェイスで受信される、最大許容フレーム サイズより大きいフレームの数
Undersize frames	64 バイトより小さなインターフェイスで受信されるフレーム数
Collision fragments	インターフェイスで受信されるコリジョン フラグメントの数
Minimum size frames	最小フレーム サイズの総フレーム数
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	インターフェイスで受信されるオーバーラン フレームの総数
Pause frames	インターフェイスで受信されるポーズ フレームの数
Symbol error frames	シンボル エラーのインターフェイスで受信されるフレーム数
Invalid frames, too large	最大許容 MTU ² サイズ（FCS ビットを含み、フレーム ヘッダーは含まない）よりも大きく、FCS エラーまたはアライメント エラーがある、受信フレームの数
Valid frames, too large	インターフェイスで受信される、最大許容フレーム サイズより大きいフレームの数
Invalid frames, too small	64 バイト（FCS ビットを含み、フレーム ヘッダーは含まない）よりも小さく、FCS エラーまたはアライメント エラーがある、受信フレームの数
Valid frames, too small	64 バイト（または VLAN [仮想 LAN] タグ付きフレームは 68 バイト）よりも小さく、有効な FCS 値を持つインターフェイスで受信されるフレーム数。フレーム サイズには FCS ビットが含まれますが、フレーム ヘッダー ビットは含まれません。
Too old frames	パケットが期限切れのために入力ポートで廃棄されたフレーム数
Valid oversize frames	インターフェイスで受信された、最大許容フレーム サイズより大きく、有効な FCS 値を持つフレーム数。フレーム サイズには FCS ビットが含まれますが、VLAN タグは含まれません。
System FCS error frames	有効な長さ（バイト）であっても、正しい FCS 値を持たないインターフェイスで受信されるフレームの総数
RxPortFifoFull drop frames	インターフェイスで受信されたにもかかわらず、入力キューが満杯のために廃棄されたフレームの総数

1. FCS = Frame Check Sequence

2. MTU = Maximum Transmission Unit（最大伝送ユニット）

次の例では、指定のインターフェイスの **show controllers ethernet-controller phy** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/0/2 phy
Control Register                : 0001 0001 0100 0000
Control STATUS                  : 0111 1001 0100 1001
Phy ID 1                        : 0000 0001 0100 0001
Phy ID 2                        : 0000 1100 0010 0100
Auto-Negotiation Advertisement : 0000 0011 1110 0001
Auto-Negotiation Link Partner  : 0000 0000 0000 0000
Auto-Negotiation Expansion Reg  : 0000 0000 0000 0100
Next Page Transmit Register     : 0010 0000 0000 0001
Link Partner Next page Register : 0000 0000 0000 0000
1000BASE-T Control Register     : 0000 1111 0000 0000
1000BASE-T Status Register      : 0100 0000 0000 0000
Extended Status Register        : 0011 0000 0000 0000
PHY Specific Control Register    : 0000 0000 0111 1000
PHY Specific Status Register     : 1000 0001 0100 0000
Interrupt Enable                 : 0000 0000 0000 0000
Interrupt Status                 : 0000 0000 0100 0000
Extended PHY Specific Control    : 0000 1100 0110 1000
Receive Error Counter           : 0000 0000 0000 0000
Reserved Register 1             : 0000 0000 0000 0000
Global Status                   : 0000 0000 0000 0000
LED Control                     : 0100 0001 0000 0000
Manual LED Override             : 0000 1000 0010 1010
Extended PHY Specific Control    : 0000 0000 0001 1010
Disable Receiver 1              : 0000 0000 0000 1011
Disable Receiver 2              : 1000 0000 0000 0100
Extended PHY Specific Status     : 1000 0100 1000 0000
Auto-MDIX                       : On   [AdminState=1   Flags=0x00052248]
```

次の例では、10 ギガビット イーサネット インターフェイスの **show controllers ethernet-controller tengigabitethernet1/0/1 phy** コマンドの出力を示します。XENPAK モジュール シリアル EEPROM の内容が表示されます。

EEPROM マップおよび出力のフィールド説明の詳細については、次のサイトの XENPAK Multisource Agreement (MSA) を参照してください。

http://www.xenpak.org/MSA/XENPAK_MSA_R2.1.pdf

http://www.xenpak.org/MSA/XENPAK_MSA_R3.0.pdf

どのバージョンの XENPAK マニュアルを読むべきか判断するには、出力の *XENPAK MSA Version supported* フィールドを確認してください。バージョン 2.1 は 15 (16 進数) で、バージョン 3.0 は 1E (16 進数) です。

```
Switch# show controllers ethernet-controller tengigabitethernet1/0/1 phy
```

```
TenGigabitEthernet1/0/1 (gpn:472, port-number:1)
```

```
-----

XENPAK Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
  XENPAK MSA Version supported      :0x15
  NVR Size in bytes                 :0x100
  Number of bytes used              :0xD0
  Basic Field Address               :0xB
  Customer Field Address            :0x77
  Vendor Field Address              :0xA7
  Extended Vendor Field Address     :0x100
  Reserved                          :0x0
  Transceiver type                  :0x1 =XENPAK
  Optical connector type            :0x1 =SC
  Bit encoding                      :0x1 =NRZ
  Normal BitRate in multiple of 1M b/s :0x2848
  Protocol Type                    :0x1 =10GgE

Standards Compliance Codes :
  10GbE Code Byte 0                 :0x2 =10GBASE-LR
  10GbE Code Byte 1                 :0x0
  SONET/SDH Code Byte 0             :0x0
  SONET/SDH Code Byte 1             :0x0
  SONET/SDH Code Byte 2             :0x0
  SONET/SDH Code Byte 3             :0x0
  10GFC Code Byte 0                 :0x0
  10GFC Code Byte 1                 :0x0
  10GFC Code Byte 2                 :0x0
  10GFC Code Byte 3                 :0x0
  Transmission range in 10m         :0x3E8
Fibre Type :
  Fibre Type Byte 0                 :0x40 =NDSF only
  Fibre Type Byte 1                 :0x0 =Unspecified

Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
Package Identifier OUI   :0x41F420
Transceiver Vendor OUI   :0x3400871
Transceiver vendor name  :CISCO-OPNEXT,INC
Part number provided by transceiver vendor      :800-24558-01
Revision level of part number provided by vendor :01
Vendor serial number      :ONJ0735003U
Vendor manufacturing date code :2003082700

Reserved1 :00 00 00 00 00 00 00
Basic Field Checksum :0x6C

Customer Writable Area :
  0x00:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Vendor Specific :
  0x00:41 00 20 F4 88 84 28 94 C0 00 30 14 06 39 00 D9
  0x10:03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30:00 00 00 00 11 5E 19 E9 BF 1B AD 98 03 9B DF 87
  0x40:CC F6 45 FF 99 00 00 00 00 00 00 00 00 00 C0 48
  0x50:46 D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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 の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers tcam	システム内のすべての 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 ASIC のレジスタ状態を示します。
show idprom	指定したインターフェイスの IDPROM 情報を表示します。

show controllers power inline

指定した Power over Ethernet (PoE) コントローラのレジスタの値を表示するには、**show controllers power inline** ユーザ EXEC コマンドを使用します。

```
show controllers power inline [instance] [module switch-number] [| {begin | exclude | include}
expression]
```

シンタックスの説明

<i>instance</i>	(任意) 電源コントローラのインスタンス。各インスタンスは 4 つのポートに対応します。詳細については、「使用上の注意事項」を参照してください。インスタンスを指定しない場合、すべてのインスタンスの情報が表示されます。
module switch-number	(任意) 指定のスタック メンバーのポートのみを表示します。スイッチ番号は 1 ～ 9 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

Catalyst 3750-48PS スイッチでは、指定できる *instance* 範囲は 0 ～ 11 です。

Catalyst 3750-24PS スイッチでは、指定できる *instance* 範囲は 0 ～ 5 です。

Catalyst 3750G-48PS スイッチでは、指定できる *instance* 範囲は 0 ～ 2 です。0 ～ 2 以外のインスタンスの場合、スイッチは出力しません。

Catalyst 3750G-24PS スイッチでは、指定できる *instance* 範囲は 0 ～ 1 です。0 ～ 1 以外のインスタンスの場合、スイッチは出力しません。

このコマンドは、すべてのスイッチで表示されますが、PoE スイッチに対してのみ有効です。PoE をサポートしていないスイッチの情報は使用できません。

このコマンドを使用することで、Cisco のテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ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、Catalyst 3750G-48PS または 3750G-24PS スイッチ以外のスイッチでの **show controllers power inline** コマンドの出力を示します。

```
Switch> show controllers power inline
Module 1, Controller Instance 0, Address 0x40
  Interrupt      Reg 0x0  = 0x0
  Intr Mask      Reg 0x1  = 0xF6
  Power Event    Reg 0x2  = 0x0
  Detect Event   Reg 0x4  = 0x0
  Fault Event    Reg 0x6  = 0x0
  T-Start Event  Reg 0x8  = 0x0
  Supply Event   Reg 0xA  = 0x0
  Port 1 Status  Reg 0xC  = 0x24
  Port 2 Status  Reg 0xD  = 0x24
  Port 3 Status  Reg 0xE  = 0x3
  Port 4 Status  Reg 0xF  = 0x3
  Power Status   Reg 0x10 = 0xFF
  Pin Status     Reg 0x11 = 0x0
  Operating Mode Reg 0x12 = 0xAA
  Disconnect Enable Reg 0x13 = 0xA0
  Detect/Class Enable Reg 0x14 = 0xFF
  Reserved       Reg 0x15 = 0x0
  Timing Config  Reg 0x16 = 0x2
  Misc Config    Reg 0x17 = 0xA0
  ID Revision    Reg 0x1A = 0x64
```

```
Module 1, Controller Instance 1, Address 0x42
(テキスト出力は省略)
```

次の例では、Catalyst 3750G-24PS スイッチでの **show controllers power inline** コマンドの出力を示します。

```
Switch> show controllers power inline
Alchemy instance 0, address 0
  Pending event flag :N N N N N N N N N N N
  Current State      :00 05 10 51 61 11
  Current Event      :00 01 00 10 40 00
  Timers             :00 C5 57 03 12 20 04 B2 05 06 07 07
  Error State        :00 00 00 00 10 00
  Error Code         :00 00 00 00 00 00 00 00 00 00 00 00
  Power Status       :N Y N N Y N N N N N N
  Auto Config        :N Y Y N Y Y Y Y Y Y Y
  Disconnect         :N N N N N N N N N N N
  Detection Status   :00 00 00 30 00 00
  Current Class      :00 00 00 30 00 00
  Tweetie debug      :00 00 00 00
  POE Commands pending at sub:
    Command 0 on each port :00 00 00 00 00 00
    Command 1 on each port :00 00 00 00 00 00
    Command 2 on each port :00 00 00 00 00 00
    Command 3 on each port :00 00 00 00 00 00
```

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのログギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電源管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

show controllers tcam

システム内のすべての Ternary CAM (TCAM)、および CAM コントローラのすべての TCAM インターフェイスの Application Specific Integrated Circuit (ASIC; 特定用途向け IC) のレジスタ状態を表示するには、**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*]

シンタックスの説明

asic	(任意) ポートの ASIC TCAM 情報を表示します。
number	(任意) 指定のポート 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 レジスタの詳細情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	asic [number] キーワードが追加されました。

使用上のガイドライン

このコマンドを使用することで、Cisco のテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ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、**show controllers tcam** コマンドの出力を示します。

```
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 の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers ethernet-controller	ハードウェアまたはインターフェイスの内部レジスタから読み込まれる、各インターフェイスの送受信の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幅使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*]

シンタックスの説明

<i>interface-id</i>	(任意) スイッチ インターフェイスの ID
begin	(任意) 指定された <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) 指定された <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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)SE	このコマンドが導入されました。

使用上のガイドライン

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 utilization** コマンドの出力を示します。

```
Switch> show controllers utilization
Port          Receive Utilization  Transmit Utilization
Fa1/0/1        0                    0
Fa1/0/2        0                    0
Fa1/0/3        0                    0
Fa1/0/4        0                    0
Fa1/0/5        0                    0
Fa1/0/6        0                    0
Fa1/0/7        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
```

次の例では、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 gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

表 2-21 show controllers utilization のフィールドの説明

フィールド	説明
Receive Bandwidth Percentage Utilization	スイッチの受信された帯域幅の使用率を表示します。すべてのポート上で受信したトラフィック量をスイッチの受信容量で除算した合計値です。
Transmit Bandwidth Percentage Utilization	スイッチの送信された帯域幅の使用率を表示します。すべてのポート上で送信したトラフィック量をスイッチの送信容量で除算した合計値です。
Fabric Percentage Utilization	スイッチの送受信した帯域幅使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 dot1q-tunnel

IEEE（米国電気電子学会）802.1Q トンネル ポートに関する情報を表示するには、**show dot1q-tunnel** ユーザ EXEC コマンドを使用します。

show dot1q-tunnel [*interface interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

interface interface-id	(任意) IEEE 802.1Q トンネリング情報を表示するインターフェイスを指定します。指定できるインターフェイスは、物理ポートおよびポート チャネルです。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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)EA1	このコマンドが導入されました。

使用上のガイドライン

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 dot1q-tunnel** コマンドの出力を示します。

```
Switch> show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet1/0/1
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
```

関連コマンド

コマンド	説明
show vlan dot1q tag native	IEEE 802.1Q ネイティブ VLAN（仮想 LAN）のタギング ステータスを表示します。
switchport mode dot1q-tunnel	インターフェイスを IEEE 802.1Q トンネル ポートとして設定します。

show dot1x

スイッチまたは指定されたポートの IEEE（米国電気電子学会）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]
```

シンタックスの説明

all	(任意) すべてのポートの IEEE 802.1x のステータスを表示します。
interface <i>interface-id</i>	(任意) 指定のポート（タイプ、スタック メンバー、モジュール、ポート番号を含む）の IEEE 802.1x のステータスを表示します。
statistics interface <i>interface-id</i>	(任意) 指定のポート（タイプ、スタック メンバー、モジュール、ポート番号を含む）の IEEE 802.1x の統計情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	all キーワードが追加されました。
12.2(25)SED	表示の、許可ステート マシン ステートおよびポート ステータス フィールドに auth-fail-vlan の項目が追加されました。

使用上のガイドライン

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。ポートを指定した場合は、該当する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           = Disabled
Supplicant Allowed In Guest Vlan = Disabled
Dot1x Protocol Version   = 1
802.1X AAA Server Status = Alive
```

```
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet1/0/1
```

```
-----
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 VLAN を設定している場合の、**show dot1x all** イネーブル EXEC コマンドの出力を示します。

```
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 VLAN を設定している場合の、**show dot1x interface interface-id** イネーブル EXEC コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet1/0/1
  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、制限 VLAN を設定していて、アクセス不能認証機能をイネーブルにしている、ポートがクリティカル認証ステートでない場合の、**show dot1x interface interface-id** イネーブル EXEC コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet1/0/1
  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 = 2946
  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      = Enabled
```

次の例では、制限 VLAN を設定していて、アクセス不能認証機能をイネーブルにしている、ポートがクリティカル認証ステートである場合の、**show dot1x interface interface-id** イネーブル EXEC コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet1/0/1
  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 = N/A
  PortStatus        = AUTHORIZED (AUTH-FAIL-VLAN/CRITICAL)
  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     = Enabled
```

次の例では、**show dot1x statistics interface interface-id** コマンドの出力を示します。表 2-22 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 gigabitethernet1/0/1
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 2-22 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 フレームの数
TxReq	送信された EAP-Request フレーム (Request/Identity フレーム以外) の数
TxTotal	送信されたすべてのタイプの Extensible Authentication Protocol over LAN (EAPOL) フレームの数
RxStart	受信された有効な EAPOL-Start フレームの数
RxLogoff	受信された EAPOL-Logoff フレームの数
RxRespId	受信された EAP-Response/Identity フレームの数
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数
RxTotal	受信されたすべてのタイプの有効な EAPOL フレームの数

表 2-22 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 の形式で受信したパケットの数
LastRxSrcMac	最後に受信した EAPOL フレームで伝送された送信元 MAC（メディア アクセス制御）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）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]
```

シンタックスの説明

interface interface-id	（任意）指定されたインターフェイスのポート 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は物理ポート（タイプ、スタック メンバー、モジュール、ポート番号を含む）を含みます。
 begin	（任意） <i>expression</i> と一致する行から表示を開始します。
 exclude	（任意） <i>expression</i> と一致する行を表示から除外します。
 include	（任意）指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 dtp** コマンドの出力を示します。

```
Switch# show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  21 interfaces using DTP
```

次の例では、**show dtp interface** コマンドの出力を示します。

```
Switch# show dtp interface gigabitethernet1/0/1
DTP information for GigabitEthernet1/0/1:
  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, 3160 software encap isl, 0 isl hardware 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 トランク情報を表示します。

show env

アクセスするスイッチ（スタンドアロン スイッチ、スタック マスター、スタック メンバー）のファン、温度、Redundant Power System（RPS; 冗長電源システム）の可用性、および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。**stack** キーワードを使用することで、スタックまたはスタック内で指定されるスイッチのすべての情報を表示します。

```
show env {all | fan | power | rps | stack [switch-number] | temperature [status]} [| {begin | exclude | include} expression]
```

シンタックスの説明

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	スイッチの電源のステータスを表示します。
rps	RPS 300 がスイッチに接続されているかどうか表示します。
stack [switch-number]	スタック内の各スイッチまたは指定のスイッチに関するすべての環境状態を表示します。指定できる範囲は 1 ～ 9 です（スタックのスイッチ メンバー番号に対応）。
temperature	スイッチの温度ステータスを表示します。
status	（任意）スイッチの内部温度（外部温度ではなく）およびスレッシュホールド値を表示します。このキーワードは、Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、および 3750G-24PS スイッチでのみ使用できます。
begin	（任意） <i>expression</i> と一致する行から表示を開始します。
exclude	（任意） <i>expression</i> と一致する行を表示から除外します。
include	（任意）指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE3	temperature status キーワードが追加されました。

使用上のガイドライン

マスター以外の特定のスイッチから情報にアクセスするには、**action** イネーブル EXEC コマンドを使用します。

任意のメンバー スイッチからスタック内のすべてのスイッチに関する情報を表示するには、**show env stack** [switch-number] コマンドを使用します。

show env temperature status コマンドはすべてのスイッチ上で表示されますが、Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、および 3750G-24PS スイッチに対してのみ有効です。これらのスイッチでこのコマンドを入力すると、コマンド出力ではスイッチの温度ステータスおよびスレッシュホールド レベルが表示されます。上記の 4 つのスイッチ以外でこのコマンドを入力すると、出力フィールドでは *Not Applicable* が表示されます。

また、Catalyst 3750G-48PS または 3750G-24PS スイッチでは、**show env temperature** コマンドを使用してスイッチの温度ステータスも表示できます。コマンド出力では、グリーンおよびイエロー ステータスが *OK* として、レッドステータスが *FAULTY* として表示されます。スイッチ上で **show env all** コマンドを入力した場合、そのコマンド出力は **show env temperature status** コマンド出力と同じです。

スレッショールド レベルの詳細については、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、マスター スイッチまたはスタンドアロン スイッチから入力した **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
```

次の例では、**show env stack** コマンドの出力を示します。

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 2
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 4
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 5
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 6
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

次の例では、マスター スイッチからスタック メンバー 3 に関する情報を表示する方法を示します。

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

次の例では、温度の値、ステート、およびスレッシュホールド値を表示する方法を示します。表 2-23 に、コマンド出力の温度ステータスの説明を示します。

```
Switch> show env temperature status
Temperature Value:28 Degree Celsius
Temperature State:GREEN
Yellow Threshold :70 Degree Celsius
Red Threshold    :75 Degree Celsius
```

表 2-23 show env temperature status コマンド出力のステート

State	説明
GREEN	スイッチの温度は正常な動作範囲内です。
YELLOW	温度が警告範囲にあります。スイッチ周辺の外部温度を確認してください。
RED	温度が危険範囲にあります。温度がこの範囲にある場合、スイッチは正常に稼働しない可能性があります。

show errdisable detect

errdisable の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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid のエラーの理由は、無効な Small Form-Factor Pluggable (SFP) モジュールであることを示します。

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 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
l2ptguard            Enabled
link-flap             Enabled
gbic-invalid          Enabled
dhcp-rate-limit      Enabled
unicast-flood         Enabled
storm-control         Enabled
ilpower               Enabled
arp-inspection        Enabled
```



(注)

ilpower、storm-control、および unicast-flood フィールドは、出力に表示はされますが、有効ではありません。

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
show errdisable flap-values	認識されている状態のエラー情報を表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	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

ある原因をエラーとして認識させる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*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

表示の *Flaps* カラムは指定された時間の間隔内でステートが何回変化したかを表示しています。この回数によって、エラーが検出されてポートがディセーブルになります。たとえば、Dynamic Trunking Protocol (DTP) ステート (ポートモードがアクセス / トランク) または Port Aggregation Protocol (PAgP) のフラップが 30 秒間に 3 回変化した場合、またはリンク ステート (リンク アップ / ダウン) が 10 秒間に 5 回変化した場合は、エラーとみなされ、ポートがシャットダウンされたことを示します。

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に対して errdisable 検出をイネーブルにします。
show errdisable detect	errdisable の検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	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**]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid の *ErrDisable Reason* は、無効な Small Form-Factor Pluggable (SFP) モジュール インターフェイスであることが原因です。

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 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
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
-----
Gi1/0/2      link-flap            279
```



(注)

unicast-flood フィールドは、出力に表示はされますが、有効ではありません。

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 の検出ステータスを表示します。
show errdisable flap-values	認識されている状態のエラ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 etherchannel

チャンネルの 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]
```

シンタックスの説明

channel-group-number	(任意) チャンネル グループの番号です。指定できる範囲は 1 ～ 48 です。
detail	EtherChannel の詳細を表示します。
load-balance	ポート チャン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	ポートチャン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	各チャンネルグループのサマリーを 1 行で表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	protocol キーワードが追加されました。
12.2(25)SE	<i>channel-group-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

channel-group を指定しない場合は、すべてのチャンネル グループが表示されます。

出力では、Passive ポート リストのフィールドはレイヤ 3 のポート チャンネルのみに対して表示されます。このフィールドは、起動していない物理ポートがチャンネル グループ内になるように設定されていることを意味します（間接的にチャンネル グループ内で唯一のポート チャンネル）。

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: Gi1/0/1
-----

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 LACPDU      F - Device is sending fast LACPDU
        A - Device is in active mode.           P - Device is in passive mode.

Local information:

Port      Flags   State      LACP port   Admin   Oper   Port   Port
Port      Flags   State      Priority    Key     Key     Number State
Gi1/0/1   SA      bndl      32768       0x1     0x1     0x101  0x3D
Gi1/0/2   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   Gi1/0/1  Active        0
    0    00   Gi1/0/2  Active        0

Time since last port bundled:    01d:20h:20m:20s    Gi1/0/2
```

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        Gi1/0/1(P) Gi1/0/2(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    Gi1/0/1   Active         0
    0     00    Gi1/0/2   Active         0

Time since last port bundled:    01d:20h:24m:44s    Gi1/0/2
```

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ため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。

show flowcontrol

フロー制御のステータスと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*]

シンタックスの説明

interface interface-id	(任意) 特定のインターフェイスのフロー制御のステータスおよび統計情報を表示します。
module number	(任意) 指定のスタック メンバー上のすべてのインターフェイスのフロー制御のステータスと統計情報を表示します。指定できる範囲は、1～9です。特定のインターフェイス ID を入力した場合は、このオプションを使用できません。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> 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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

スイッチまたは特定のインターフェイスにおけるフロー制御の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。

すべてのスイッチ インターフェイスの情報を表示するには、**show flowcontrol** コマンドを使用します。スタンドアロンスイッチでは、**show flowcontrol** コマンドの出力結果は、**show flowcontrol module number** コマンドの出力結果と同じになります。

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

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

```
Switch> show flowcontrol
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper      admin    oper
-----
Gi2/0/1       Unsupp.  Unsupp.   off       off         0         0
Gi2/0/2       desired  off       off       off         0         0
Gi2/0/3       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 gigabitethernet2/0/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper      admin    oper
-----
Gi2/0/2       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 idprom

指定されたインターフェイスの IDPROM 情報を表示するには、**show idprom** ユーザ EXEC コマンドを使用します。

show idprom {interface interface-id} [detail] [| {begin | exclude | include} expression]

シンタックスの説明

interface interface-id	指定された 10 ギガビット イーサネット インターフェイスの IDPROM 情報を表示します。
detail	(任意) IDPROM の詳細情報 (16 進数) を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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(20)SE1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは 10 ギガビット イーサネット インターフェイスにだけ適用されます。

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、10 ギガビット イーサネット インターフェイスの **show idprom interface tengigabitethernet1/0/1** コマンドの出力を示します。XENPAK モジュール シリアル Electrically Erasable Programmable Read-Only Memory (EEPROM; 電氣的消去再書き込み可能 ROM) の内容が表示されます。

EEPROM マップおよび出力のフィールド説明の詳細については、次のサイトの XENPAK Multisource Agreement (MSA) を参照してください。

http://www.xenpak.org/MSA/XENPAK_MSA_R2.1.pdf

http://www.xenpak.org/MSA/XENPAK_MSA_R3.0.pdf

どのバージョンの XENPAK マニュアルを読むべきか判断するには、出力の *XENPAK MSA Version supported* フィールドを確認してください。バージョン 2.1 は 15 (16 進数) で、バージョン 3.0 は 1E (16 進数) です (例示なし)。

```
Switch# show idprom interface tengigabitethernet1/0/1
TenGigabitEthernet1/0/1 (gpn:472, port-number:1)
-----
XENPAK Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
  XENPAK MSA Version supported      :0x15
  NVR Size in bytes                 :0x100
  Number of bytes used              :0xD0
  Basic Field Address               :0xB
  Customer Field Address            :0x77
  Vendor Field Address              :0xA7
  Extended Vendor Field Address     :0x100
  Reserved                          :0x0
  Transceiver type                  :0x1 =XENPAK
  Optical connector type            :0x1 =SC
  Bit encoding                      :0x1 =NRZ
  Normal BitRate in multiple of 1M b/s :0x2848
  Protocol Type                    :0x1 =10GgE

Standards Compliance Codes :
  10GbE Code Byte 0                :0x2 =10GBASE-LR
  10GbE Code Byte 1                :0x0
  SONET/SDH Code Byte 0            :0x0
  SONET/SDH Code Byte 1            :0x0
  SONET/SDH Code Byte 2            :0x0
  SONET/SDH Code Byte 3            :0x0
  10GFC Code Byte 0                :0x0
  10GFC Code Byte 1                :0x0
  10GFC Code Byte 2                :0x0
  10GFC Code Byte 3                :0x0
  Transmission range in 10m        :0x3E8
Fibre Type :
  Fibre Type Byte 0                :0x40 =NDSF only
  Fibre Type Byte 1                :0x0 =Unspecified

Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
Package Identifier OUI :0x41F420
Transceiver Vendor OUI :0x3400871
Transceiver vendor name :CISCO-OPNEXT,INC
Part number provided by transceiver vendor :800-24558-01
Revision level of part number provided by vendor :01
Vendor serial number :ONJ0735003U
Vendor manufacturing date code :2003082700

Reserved1 :00 00 00 00 00 00 00
Basic Field Checksum :0x6C

Customer Writable Area :
  0x00:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Vendor Specific :
  0x00:41 00 20 F4 88 84 28 94 C0 00 30 14 06 39 00 D9
  0x10:03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30:00 00 00 00 11 5E 19 E9 BF 1B AD 98 03 9B DF 87
  0x40:CC F6 45 FF 99 00 00 00 00 00 00 00 00 00 C0 48
  0x50:46 D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

関連コマンド

コマンド	説明
show controllers ethernet-controller	ハードウェア、インターフェイス内部レジスタ、またはポート Application Specific Integrated Circuit (ASIC; 特定用途向け IC) 情報から読み込まれる、各インターフェイスの送受信の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 | private-vlan mapping | pruning | stats | status
[err-disabled] | switchport [backup | module number] | transceiver [properties | detail] [module
number] | trunk] [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) 有効なインターフェイスは、物理ポート (タイプ、スタック メンバー、モジュール、およびポート番号を含む) やポート チャネルなどです。ポートチャネルに指定できる範囲は 1 ～ 48 です。
vlan <i>vlan-id</i>	(任意) VLAN (仮想 LAN) ID です。指定できる範囲は 1 ～ 4094 です。
accounting	(任意) インターフェイスのアカウント情報 (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) を表示します。
capabilities	(任意) すべてのインターフェイスまたは指定のインターフェイスの性能 (機能、インターフェイス上で設定可能なオプションを含む) 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は表示されていますが、VLAN ID には使用できません。
<i>module number</i>	(任意) 指定のスタック メンバーのすべてのインターフェイスの性能、スイッチ ポート コンフィギュレーション、またはトランシーバの特性 (上記のキーワードに対応) を表示します。指定できる範囲は 1 ～ 9 です。特定のインターフェイス ID を入力した場合は、このオプションを使用できません。
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) インターフェイスのフロー制御情報を表示します。
private-vlan mapping	(任意) VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) のプライベート VLAN マッピング情報を表示します。このキーワードは、スイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。
pruning	(任意) インターフェイス トランク VLAN Trunking Protocol (VTP; VLAN トランッキング 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 <i>unsupported</i> ステータスは、他社製の Small Form-Factor Pluggable (SFP) モジュールがモジュール スロットに搭載されていることを示します。

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 (非ルーティング) 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) スタック上の指定のインターフェイスまたはすべてのインターフェイスの 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 SFP モジュール インターフェイスの物理的特性を表示します。キーワードの意味は次のとおりです。 detail — (任意) 数の大小、およびあらゆるアラーム情報を含む、調整の特性を表示します。 properties — (任意) インターフェイスの速度、デュプレックス、インラインパワーの設定を表示します。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

1. Coarse Wavelength-Division Multiplexer : 低密度波長分割多重

2. Dense Wavelength-Division Multiplexer : 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tring 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	capabilities キーワードのサポートが追加されました。
12.2(20)SE	private-vlan mapping 、 backup 、 transceiver calibration 、 detail 、および properties キーワードが追加されました。
12.2(25)SEA	calibration キーワードが削除されました。

使用上のガイドライン

show interfaces capabilities コマンドに異なるキーワードを指定することで、次のような結果になります。

- スタックのスイッチ上におけるすべてのインターフェイスの性能を表示するには、**show interface capabilities module number** コマンドを使用します。スタックに指定されたモジュール番号のスイッチがない場合、その出力は空白になります。
- 指定のインターフェイスの性能を表示するには、**show interfaces interface-id capabilities** を使用します。
- スタック内のすべてのインターフェイスの性能を表示するには、**show interfaces capabilities** (モジュール番号またはインターフェイス ID の指定なし) を使用します。

- スタックのスイッチ上のすべてのインターフェイスのスイッチ ポートの性能を表示するには、**show interface switchport module number** コマンドを使用します。スタックに指定されたモジュール番号のスイッチがない場合、その出力は空白になります。

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

次の例では、スタック番号3のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 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 runts, 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.

GigabitEthernet1/0/1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
      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 gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model: WS-C3750G-24TS
  Type: 10/100/1000BaseTX
  Speed: 10,100,1000,auto
  Duplex: full,auto
  Trunk encap. type: 802.1Q,ISL
  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
```

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、インターフェイスの記述が *Connects to Marketing* として指定してある場合の **show interfaces interface description** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status      Protocol Description
Gi1/0/2      up          down      Connects to Marketing
```

次の例では、スイッチにポート チャン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、プライベート VLAN のプライマリ VLAN が VLAN 10 で、セカンダリ VLAN が VLAN 501 および 502 である場合の、**show interfaces private-vlan mapping** コマンドの出力を示します。

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan10    501      isolated
vlan10    502      community
```

次の例では、VTP ドメイン内でブ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 gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

次の例では、指定の VLAN 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
Fa1/0/1   Fa1/0/1             connected   routed    a-half  a-100  10/100BaseTX
Fa1/0/2   Fa1/0/2             notconnect  121,40    auto    auto   10/100BaseTX
Fa1/0/3   Fa1/0/3             notconnect  1         auto    auto   10/100BaseTX
Fa1/0/4   Fa1/0/4             notconnect  18        auto    auto   Not Present
Fa1/0/5   Fa1/0/5             connected   121       a-full  a-1000 10/100BaseTX
Fa1/0/6   Fa1/0/6             connected   122,11    a-full  a-1000 10/100BaseTX

(テキスト出力は省略)
Gi1/0/1   Gi1/0/1             notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/2   Gi1/0/2             notconnect  1         auto    auto   unsupported
```

次の例では、プライベート VLAN が設定されている場合の特定のインターフェイスの **show interfaces status** コマンドの出力を示します。ポート 22 は、プライベート VLAN のホストポートとして設定されています。これは、プライマリ VLAN 20 およびセカンダリ VLAN 25 と関連付けられています。

```
Switch# show interfaces fastethernet1/0/22 status
Port      Name                Status      Vlan      Duplex  Speed Type
Fa1/0/22   Fa1/0/22            connected   20,25     a-full  a-100  10/100BaseTX
```

この例では、ポート 20 はプライベート VLAN のプロミスキャスポートとして設定されています。表示されるのは、プライマリ VLAN 20 だけです。

```
Switch# show interfaces fastethernet1/0/20 status
Port      Name                Status      Vlan      Duplex  Speed Type
Fa1/0/20   Fa1/0/20            connected   20        a-full  a-100  10/100BaseTX
```

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が表示されます。

```
Switch# show interfaces status err-disabled
Port      Name                Status      Reason
Gi2/0/26   Gi2/0/26            err-disabled gbic-invalid
```

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 2-24 に、この出力で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 トランクはこのリリースではサポートされていないため、これらのフィールドを適用することはできません。

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
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 2-24 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。この出力の場合、ポートはスイッチポートモードです。
Administrative Mode	管理モードおよび動作モードを表示します。
Operational Mode	
Administrative Trunking Encapsulation	管理上および動作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。
Operational Trunking Encapsulation	
Negotiation of Trunking	
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN	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。
Trunking VLANs Enabled	
Trunking VLANs Active	
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 2-24 show interfaces switchport のフィールドの説明（続き）

フィールド	説明
Unknown unicast blocked	不明なマルチキャストおよび不明なユニキャストトラフィックがインターフェイス上でブロックされているかどうかを表示します。
Unknown multicast blocked	
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Administrative private-vlan host-association	プライベート VLAN のホストポートに対する管理 VLAN のアソシエーションを表示します。
Administrative private-vlan mapping	プライベート VLAN のプロミスキヤスポートに対する管理 VLAN のマッピングを表示します。
Operational private-vlan	プライベート VLAN の動作ステータスを表示します。
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、プライベート VLAN のプロミスキヤスポートとして設定されたポートの **show interfaces switchport** コマンド出力を示します。プライマリ VLAN 20 は、セカンダリ VLAN 25、30、および 35 にマッピングされます。

```
Switch# show interface gigabitethernet1/0/2 switchport
Name: Gi1/0/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 20 (VLAN0020) 25 (VLAN0025) 30 (VLAN0030) 35 (VLAN0035)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
30 (VLAN0030)
35 (VLAN0035)
```

(テキスト出力は省略)

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
  -----
  Fa1/0/1             Fa1/0/2            Active Up/Backup Standby
  Fa3/0/3             Fa4/0/5            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 gigabitethernet1/0/2 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。ポートのトランッキング情報が表示されます。

```
Switch# show interfaces gigabitethernet1/0/1 trunk
Port          Mode          Encapsulation  Status        Native vlan
Gi1/0/1       auto          negotiate      trunking      1

Port          Vlans allowed on trunk
Gi1/0/1       1-4094

Port          Vlans allowed and active in management domain
Gi1/0/1       1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi1/0/1       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 gigabitethernet1/0/1 transceiver properties
Name : Gi1/0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

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 gigabitethernet2/0/3 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.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi2/0/3	41.5	110.0	103.0	-8.0	-12.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi2/0/3	3.20	4.00	3.70	3.00	2.95

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi2/0/3	31.0	84.0	70.0	4.0	2.0

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/0/3	-0.0 (-0.0)	-0.0	-0.0	-0.0	-0.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/0/3	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不明なユニキャストまたは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 1 組のレイヤ 2 インターフェイスである、Flex Link を設定します。
switchport mode	ポートの VLAN メンバーシップ モードを設定します。
switchport mode private-vlan	ポートを、プライベート VLAN のホストまたはプロミスキャスポートとして設定します。
switchport private-vlan	ホスト ポートに対するプライベート VLAN のアソシエーション、またはプロミスキャスポートに対するプライベート VLAN のマッピングを定義します。
switchport protected	同じスイッチの他の保護されたポートからレイヤ 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

スイッチまたは特定の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** | **module** *switch- number* | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>interface-id</i>	(任意) 物理インターフェイスの ID (タイプ、スタック メンバー、モジュール、ポート番号を含む)。
errors	(任意) エラー カウンタを表示します。
etherchannel	(任意) EtherChannel のカウンタ情報 (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 パケットを含む) を表示します。
module <i>switch- number</i>	(任意) 指定のスタック メンバーのカウンタを表示します。指定できる範囲は 1 ～ 9 です (スタックのスイッチ番号に対応)。
 (注) このコマンドでは、 module キーワードはスタック メンバー番号 (1 ～ 9) を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。	
protocol status	(任意) インターフェイス上でイネーブルであ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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring 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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	etherchannel および protocol status キーワードが追加されました。 broadcast 、 multicast 、および unicast キーワードが削除されました。

使用上のガイドライン

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
Gi1/0/1       0           0             0             0
Gi1/0/2       0           0             0             0
```

(テキスト出力は省略)

次の例では、スタック メンバー 2 の **show interfaces counters module** コマンドの出力の一部を示します。スタック内の指定のスイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters module 2
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Fa2/0/1       520         2             0             0
Fa2/0/2       520         2             0             0
Fa2/0/3       520         2             0             0
Fa2/0/4       520         2             0             0
Fa2/0/5       520         2             0             0
Fa2/0/6       520         2             0             0
Fa2/0/7       520         2             0             0
Fa2/0/8       520         2             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の **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
FastEthernet1/0/1: Other, IP, ARP, CDP
FastEthernet1/0/2: Other, IP
FastEthernet1/0/3: Other, IP
FastEthernet1/0/4: Other, IP
FastEthernet1/0/5: Other, IP
FastEthernet1/0/6: Other, IP
FastEthernet1/0/7: Other, IP
FastEthernet1/0/8: Other, IP
FastEthernet1/0/9: Other, IP
FastEthernet1/0/10: 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
Gi1/0/1              0              0              0
Gi1/0/2              0              0              0
Gi1/0/3          80678          4155          0
Gi1/0/4          82320          126          0
Gi1/0/5              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*]

シンタックスの説明

<i>entity-name</i>	(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) モジュールのインストール先となるインターフェイス (gigabitethernet1/0/1 など) を入力します。
raw	(任意) 装置内のすべてのエンティティを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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)SEC	このコマンドが導入されました。

使用上のガイドライン

コマンドは大文字と小文字を区別します。**show inventory** コマンドには引数がないので、PID を持つ識別可能なすべてのエンティティの簡易ダンプが生成されます。簡易ダンプには、エンティティの位置 (スロット ID)、エンティティの内容、エンティティの Unique Device Identifier (UDI) (PID、VID、および SN) が表示されます。



(注)

PID がない場合、**show inventory** コマンドを入力しても何も出力されません。

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 inventory** コマンドの出力を示します。

```
Switch> show inventory
NAME: "5", DESCR: "WS-C3750G-12S"
PID: WS-C3750G-12S-S , VID: E0 , SN: CAT0749R204
```

show ip arp inspection

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査の設定および動作ステータス、またはすべての VLAN (仮想 LAN) または指定のインターフェイスか VLAN のこの機能に関するステータスを表示するには、**show ip arp inspection** イネーブル EXEC コマンドを使用します。

```
show ip arp inspection [interfaces [interface-id] | log | statistics [vlan vlan-range] | vlan vlan-range]
[ | {begin | exclude | include} expression]
```

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

interfaces <i>[interface-id]</i>	(任意) 指定のインターフェイス、またはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。指定できるインターフェイスは、物理ポートおよびポート チャネルです。
log	(任意) ダイナミック ARP 検査のロギング バッファの設定および内容を表示します。
statistics [vlan <i>vlan-range</i>]	(任意) 指定された VLAN の、転送、廃棄、MAC (メディア アクセス制御) 検証の障害、IP 検証の障害、許可および拒否された Access Control List (ACL; アクセス制御リスト)、許可および拒否された Dynamic Host Configuration Protocol (DHCP) のパケットに関する統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合、ダイナミック ARP 検査がイネーブル (アクティブ) である VLAN に関する情報のみを表示します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
vlan <i>vlan-range</i>	(任意) 指定された VLAN のダイナミック ARP 検査の設定および動作ステータスを表示します。VLAN が指定されていない場合、または範囲が指定されている場合、ダイナミック ARP 検査がイネーブル (アクティブ) である VLAN に関する情報のみを表示します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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(20)SE	このコマンドが導入されました。

使用上のガイドライン

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 arp inspection interfaces** コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces
Interface      Trust State    Rate (pps)    Burst Interval
-----
Gi1/0/1        Untrusted      15            1
Gi1/0/2        Untrusted      15            1
Gi1/0/3        Untrusted      15            1
```

次の例では、**show ip arp inspection interfaces interface-id** コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces gigabitethernet1/0/1
Interface      Trust State    Rate (pps)    Burst Interval
-----
Gi1/0/1        Untrusted      15            1
```

次の例では、**show ip arp inspection log** コマンドの出力を示します。これは、バッファがクリアされる前に、ロギング バッファの内容を示すものです。

```
Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.
```

Interface	Vlan	Sender MAC	Sender IP	Num Pkts	Reason	Time
Gi1/0/1	5	0003.0000.d673	192.2.10.4	5	DHCP Deny	19:39:01
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.0000.d774	128.1.9.25	6	DHCP Deny	19:39:02
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1111	10.10.10.1	7	DHCP Deny	19:39:03
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1112	10.10.10.2	8	DHCP Deny	19:39:04
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1114	173.1.1.1	10	DHCP Deny	19:39:06
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1115	173.1.1.2	11	DHCP Deny	19:39:07
UTC Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1116	173.1.1.3	12	DHCP Deny	19:39:08
UTC Mon Mar 1 1993						

ロギング バッファがオーバーフローの場合は、ログ イベントがロギング バッファのサイズに適合していないことを意味し、**show ip arp inspection log** イネーブル EXEC コマンドの表示が影響されます。表示中の A -- は、パケット カウントおよび時間以外のすべてのデータの変わりに表示されます。エントリには、その他の統計情報は提供されません。このエントリが表示される場合は、ロギング バッファのエントリ数を増やすか、または **ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドのロギング レートを上げてください。

次の例では、**show ip arp inspection statistics** コマンドの出力を示します。これは、すべてのアクティブ VLAN のダイナミック ARP 検査で処理されたパケットの統計情報を示しています。

```
Switch# show ip arp inspection statistics
Vlan      Forwarded    Dropped    DHCP Drops    ACL Drops
-----
5         3            4618       4605          4
2000      0            0          0             0

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
-----
5         0              12            0
2000      0              0             0

Vlan      Dest MAC Failures    IP Validation Failures
-----
5         0                    9
2000      0                    0
```

show ip arp inspection statistics コマンドでは、スイッチは、信頼性のあるダイナミック ARP 検査のポート上の各 ARP 要求および応答パケットで、転送されるパケット数を増やします。スイッチは、送信元 MAC、宛先 MAC、または IP の妥当性検査により拒否された各パケットで、ACL または DHCP に許可されるパケット数を増やします。また、適切な障害カウントを増やします。

次の例では、**show ip arp inspection statistics vlan 5** コマンドの出力を示します。これは、VLAN 5 のダイナミック ARP により処理されたパケットの統計情報を示しています。

```
Switch# show ip arp inspection statistics vlan 5
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
5          3          4618          4605            4

Vlan      DHCP Permits      ACL Permits      Source MAC Failures
----      -
5          0          12              0

Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
----      -
5          0              9              3
```

次の例では、**show ip arp inspection vlan 5** コマンドの出力を示します。これは、VLAN 5 のダイナミック ARP 検査の設定および動作ステートを示しています。

```
Switch# show ip arp inspection vlan 5
Source Mac Validation      :Enabled
Destination Mac Validation :Enabled
IP Address Validation      :Enabled

Vlan      Configuration      Operation      ACL Match      Static ACL
----      -
5          Enabled          Active          second          No

Vlan      ACL Logging      DHCP Logging
----      -
5          Acl-Match          All
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査のロギング バッファをクリアします。
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報をクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査のロギング バッファを設定します。
ip arp inspection vlan logging	VLAN 単位で記録されたパケット タイプを制御します。
show arp access-list	ARP アクセス リストに関する詳細情報を表示します。

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*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

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)
-----
GigabitEthernet1/0/1      yes         unlimited
GigabitEthernet1/0/2      yes         unlimited
GigabitEthernet2/0/3      no          2000
GigabitEthernet2/0/4      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

スイッチ上のすべてのインターフェイスに対する 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]
```

シンタックスの説明

<i>ip-address</i>	(任意) バインディング エントリ IP アドレスを指定します。
<i>mac-address</i>	(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。
<i>interface interface-id</i>	(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。
<i>vlan vlan-id</i>	(任意) バインディング エントリ VLAN (仮想 LAN) を指定します。
begin	<i>expression</i> と一致する行から表示を開始します。
exclude	<i>expression</i> と一致する行を表示から除外します。
include	指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(19)EA1	このコマンドが導入されました。
12.2(18)SE	dynamic および static キーワードが削除されました。

使用上のガイドライン

show ip dhcp snooping binding コマンドの出力は、ダイナミックに設定されたバインディングのみを示します。DHCP スヌーピング バインディング データベースのダイナミックおよびスタティック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 ステートに変更した場合、スイッチはスタティック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    GigabitEthernet2/0/1
00:D0:B7:1B:35:DE  10.1.2.151    237           dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 2
```

■ show ip dhcp snooping binding

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
GigabitEthernet2/0/1
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
GigabitEthernet2/0/2
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 gigabitethernet2/0/2
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290           dhcp-snooping  20
GigabitEthernet2/0/2
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
GigabitEthernet2/0/1
00:00:00:00:00:02  10.1.2.151    65           dhcp-snooping  20
GigabitEthernet2/0/2
Total number of bindings: 2
```

表 2-25 に、show ip dhcp snooping binding コマンド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 ip dhcp snooping binding コマンドの出力

フィールド	説明
MacAddress	クライアント ハードウェア MAC アドレス
IpAddress	DHCP サーバから割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレスの残りのリース時間
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 2-25 show ip dhcp snooping binding コマンドの出力（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	スイッチ上で設定されたバインディングの総数
	 (注) コマンド出力ではバインディングの総数が表示されない場合もあります。たとえば、200 個のバインディングがスイッチ上に設定され、すべてのバインディングが表示される前に出力を停止する場合、その総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]

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

detail	(任意) ステータスおよび統計情報の詳細を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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(20)SE	このコマンドが導入されました。

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 Succeeded 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 Succeeded 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 (仮想 LAN) 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の 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*]

シンタックスの説明

<i>profile number</i>	(任意) 表示する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、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 コマンドの出力を示します。プロファイル番号が入力されていない場合、表示にはスイッチ上で設定されたすべてのプロファイルが含まれます。

```
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	指定の 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]
```

シンタックスの説明

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。指定できる範囲は 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です）。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	querier キーワードが追加されました。
12.2(18)SE	groups キーワードが追加されました。 show ip igmp snooping multicast コマンドは、 show ip igmp snooping groups コマンドに変更されました。

使用上のガイドライン

スイッチまたは特定の VLAN のスヌーピングの設定を表示するのに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 Fiber Distributed Data Interface（FDDI）VLAN 専用で、IGMP スヌーピングでは使用できません。

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。特定の VLAN のスヌーピング特性が表示されます。

```
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。スイッチのすべての VLAN のスヌーピング特性が表示されます。

```
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	スイッチ上または VLAN 上の IGMP スヌーピングを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	レイヤ 2 ネットワークで IGMP クエリー機能を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 トポロジ変更通知の動作としてマルチキャストフラッドを設定します。
ip igmp snooping vlan immediate-leave	VLAN 上で、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、またはマルチキャストの学習方式を設定します。
ip igmp snooping vlan static	マルチキャスト グループのメンバーとして、レイヤ 2 ポートをスタティックに追加します。
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のマルチキャスト 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	スイッチ上で設定される IGMP クエリアの設定情報および動作情報を表示します。

show ip igmp snooping groups

スイッチまたはマルチキャスト情報の Internet Group Management Protocol (IGMP) スヌーピング マルチキャスト テーブルを表示するには、**show ip igmp snooping groups** イネーブル EXEC コマンドを使用します。指定のマルチキャスト VLAN (仮想 LAN) のマルチキャスト テーブル、または指定のマルチキャストの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]
```

シンタックスの説明

count	(任意) 実エントリの代わりに、指定のコマンド オプションのエントリ総数を表示します。
dynamic	(任意) IGMP スヌーピングから学習し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 エントリのみ表示します。
ip_address	(任意) 指定のグループ IP アドレスのマルチキャスト グループの特性を表示します。
vlan vlan-id	(任意) VLAN 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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(18)SE	このコマンドが導入されました。 show ip igmp snooping multicast コマンドはこのコマンドに変更されました。

使用上のガイドライン

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 Fiber Distributed Data Interface (FDDI) VLAN 専用で、IGMP スヌーピングでは使用できません。

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、キーワードの指定をしない **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
-----
1         224.1.4.4    igmp
1         224.1.4.5    igmp
2         224.0.1.40   igmp      v2         Fa1/0/15
```

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 スヌーピングから学習し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         Gi2/0/1, Fa1/0/15
104       224.1.4.3    igmp      v2         Gi2/0/1, Fa1/0/15
```

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。指定の IP アドレスの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         Gi2/0/1, Fa1/0/15
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピング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 ポートを設定します。
ip igmp snooping vlan static	マルチキャスト グループのメンバーとして、レイヤ 2 ポートをスタティックに追加します。
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のマルチキャスト 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

ダイナミックに学習および手動で設定したスイッチまたは指定のマルチキャスト VLAN（仮想 LAN）の Internet Group Management Protocol（IGMP）スヌーピング 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*]

シンタックスの説明	
vlan <i>vlan-id</i>	(任意) VLAN 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン スイッチまたは特定の VLAN 上のマルチキャスト ルータ ポートを表示するには、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 Fiber Distributed Data Interface（FDDI）VLAN 専用で、IGMP スヌーピングでは使用できません。

Multicast VLAN Registration（MVR）がイネーブルの場合、**show ip igmp snooping mrouter** コマンドは MVR マルチキャスト ルータの情報および IGMP スヌーピング情報を表示します。

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 ip igmp snooping mrouter** 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 ルータ ポートを表示します。

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
1         Gi2/0/1(dynamic)
```

関連コマンド	コマンド	説明
	ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピング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 ポートを追加します。
	ip igmp snooping vlan static	マルチキャスト グループのメンバーとして、レイヤ 2 ポートをスタティックに追加します。
	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のパラメータの 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

スイッチ上で設定される Internet Group Management Protocol (IGMP) クエリアの設定情報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*]

シンタックスの説明

detail	(任意) IGMP クエリアの詳細情報を表示します。
vlan <i>vlan-id</i> [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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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)SEA	このコマンドが導入されました。

使用上のガイドライン

クエリアともいう IGMP クエリー メッセージを送信する検出されたデバイスの 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。サブネットは複数のマルチキャスト ルータを持つことができますが、IGMP クエリアは 1 つのみです。IGMPv2 を稼働するサブネットでは、マルチキャスト ルータのうち 1 つがクエリアとして選出されます。そのクエリアはレイヤ 3 スイッチになることができます。

show ip igmp snooping querier コマンド出力では、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。クエリアがスイッチの場合、出力では *Port* フィールドが *Router* として表示されます。クエリアがルータの場合、出力には *Port* フィールドにクエリアを学習する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** コマンドとほぼ同じです。ただし **show ip igmp snooping querier** コマンドは、スイッチクエリアで最後に検出された装置の IP アドレスのみを表示します。

show ip igmp snooping querier detail コマンドは、スイッチクエリアで最後に検出された装置の IP アドレスと次の追加情報を表示します。

- VLAN (仮想 LAN) で選出された IGMP クエリア
- VLAN で設定されたスイッチクエリア (存在する場合) に関する設定情報および動作情報

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                 Gi1/0/1
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                 Fa8/0/1

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 Fa8/0/1
-----
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	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにします。
ip igmp snooping querier	レイヤ 2 ネットワークで IGMP クエリア機能をイネーブルにします。
show ip igmp snooping	スイッチまたは指定のマルチキャスト 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 source binding

スイッチ上の IP 送信元バインディングを表示するには、**show ip source binding** ユーザ EXEC コマンドを使用します。

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*] [| **begin** | **exclude** | **include**] *expression*

このコマンドは、ご使用のスイッチで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。

シンタックスの説明

<i>ip-address</i>	(任意) 特定の IP アドレスの IP 送信元バインディングを表示します。
<i>mac-address</i>	(任意) 特定の MAC (メディア アクセス制御) アドレスの IP 送信元バインディングを表示します。
dhcp-snooping	(任意) Dynamic Host Configuration Protocol (DHCP) スヌーピングによって学習された IP 送信元バインディングを表示します。
static	(任意) スタティックな IP 送信元バインディングを表示します。
interface <i>interface-id</i>	(任意) 特定のインターフェイス上の IP 送信元バインディングを表示します。
vlan <i>vlan-id</i>	(任意) 特定の VLAN 上の IP 送信元バインディングを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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(20)SE	このコマンドが導入されました。

使用上のガイドライン

show ip source binding コマンドの出力は、DHCP スヌーピング バインディング データベースのダイナミックおよびスタティックに設定されたバインディングを表示します。ダイナミックに設定されたバインディングのみを表示するには、**show ip dhcp snooping binding** イネーブル EXEC 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

次の例では、**show ip source binding** コマンドの出力を示します。

```
Switch> show ip source binding
MacAddress          IpAddress          Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B   11.0.0.1           infinite    static         10
GigabitEthernet1/0/1
00:00:00:0A:00:0A   11.0.0.2           10000      dhcp-snooping  10
GigabitEthernet1/0/1
```

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 データベースを設定します。
ip source binding	スイッチ上のスタティックな IP 送信元バインディングを設定します。

show ip verify source

スイッチ上、または特定のインターフェイス上の IP ソース ガード コンフィギュレーションを表示するには、**show ip verify source** ユーザ EXEC コマンドを使用します。

```
show ip verify source [interface interface-id] [ | {begin | exclude | include} expression]
```

シンタックスの説明

interface interface-id	(任意) 特定のインターフェイス上の IP ソース ガード コンフィギュレーションを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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(20)SE	このコマンドが導入されました。

使用上のガイドライン

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 verify source** コマンドの出力を示します。

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
gi1/0/1    ip           active       10.0.0.1        -----
gi1/0/1    ip           active       deny-all       11-20
gi1/0/2    ip           inactive-trust-port
gi1/0/3    ip           inactive-no-snooping-vlan
gi1/0/4    ip-mac       active       10.0.0.2        aaaa.bbbb.cccc  10
gi1/0/4    ip-mac       active       11.0.0.1        aaaa.bbbb.cccd  11
gi1/0/4    ip-mac       active       deny-all       12-20
gi1/0/5    ip-mac       active       10.0.0.3        permit-all     10
gi1/0/5    ip-mac       active       deny-all       permit-all     11-20
```


上記の例は、IP ソース ガード コンフィギュレーションを示しています。

- Gigabit Ethernet 1/0/1 インターフェイス上の、VLAN（仮想 LAN）10 ～ 20 では Dynamic Host Configuration Protocol（DHCP）スヌーピングがイネーブルで、インターフェイス上で IP アドレス フィルタリングによる IP ソース ガードが設定され、またインターフェイスにバインディングが存在しています。VLAN 11 ～ 20 では、2 番目のエントリが、IP ソース ガードが設定されていない VLAN のインターフェイスで、デフォルト ポートの Access Control List（ACL; アクセス制御リスト）が適用されていることを示します。
- Gigabit Ethernet 1/0/2 インターフェイスは、信頼性のある DHCP スヌーピングとして設定されています。
- Gigabit Ethernet 1/0/3 インターフェイスでは、DHCP スヌーピングはインターフェイスが所属する VLAN 上でイネーブルではありません。
- Gigabit Ethernet 1/0/4 インターフェイスでは、送信元 IP および MAC（メディア アクセス制御）アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP 送信元 バインディングは、VLAN 10 および 11 で設定されます。VLAN 12 ～ 20 では、デフォルト ポートの ACL が、インターフェイス上で IP ソース ガードが設定されていない VLAN に適用されます。
- Gigabit Ethernet 1/0/5 インターフェイスでは、送信元 IP および MAC アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP バインディングで設定されていますが、ポート セキュリティはディセーブルです。スイッチは、送信元 MAC アドレスをフィルタリングできません。

次の例では、IP ソース ガードがディセーブルなインターフェイスでの出力を示します。

```
Switch> show ip verify source gigabitethernet1/0/6
IP source guard is not configured on the interface gil/0/6.
```

関連コマンド

コマンド	説明
ip verify source	インターフェイスの IP ソース ガードをイネーブルにします。

show ipc

スイッチ スタックまたはスタンドアロン スイッチ上のステータス、および Interprocess Communication (IPC) プロトコルの設定や、統計情報を表示するには、**show ipc** ユーザ EXEC コマンドを使用します。

```
show ipc {mcast {appclass | groups | status} | nodes | ports [open] | queue | rpc | session {all | rx | tx}
[verbose] | status [cumlulative] | zones} [| {begin | exclude | include} expression]
```

シンタックスの説明

mcast {appclass groups status}	IPC マルチキャスト ルーティング情報を表示します。キーワードの意味は次のとおりです。 appclass — IPC マルチキャスト アプリケーション クラスを表示します。 groups — IPC マルチキャスト グループを表示します。 status — IPC マルチキャスト ルーティングのステータスを表示します。
nodes	参加ノードを表示します。
ports [open]	ローカルの IPC ポートを表示します。キーワードの意味は次のとおりです。 open — (任意) オープン状態のポートのみを表示します。
queue	IPC 送信キューの内容を表示します。
rpc	IPC リモートプロシージャの統計情報を表示します。
session {all rx tx}	(任意) IPC セッションの統計情報を表示します (イネーブル EXEC モードの場合のみ使用可能)。キーワードの意味は次のとおりです。 all — すべてのセッション統計情報を表示します。 rx — スイッチが受信するトラフィックのセッション統計情報を表示します。 tx — スイッチが転送するトラフィックのセッション統計情報を表示します。
verbose	(任意) 詳細統計情報を表示します (イネーブル EXEC モードの場合のみ使用可能)。
status [cumlulative]	ローカル IPC サーバのステータスを表示します。キーワードの意味は次のとおりです。 cumlulative — (任意) スイッチが起動または再起動されてからのローカル IPC サーバのステータスを表示します。
zones	参加している IPC ゾーンを表示します。スイッチは単一 IPC ゾーンをサポートしています。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.2(18)SE	mcast {appclass groups status} 、 rpc 、 session {all rx tx} [verbose] 、および cumulative キーワードが追加されました。

使用上のガイドライン

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、IPC ルーティング ステータスを表示する方法を示します。

```
Switch> show ipc mcast status
                        IPC Mcast Status
                                Tx          Rx
Total Frames                0            0
Total control Frames        0            0
Total Frames dropped        0            0
Total control Frames dropped 0            0
Total Reliable messages      0            0
Total Reliable messages acknowledged 0            0
Total Out of Band Messages  0            0
Total Out of Band messages acknowledged 0            0
Total No Mcast groups        0            0
Total Retries                0 Total Timeouts                0
Total OOB Retries            0 Total OOB Timeouts            0
Total flushes                0 Total No ports                0
```

次の例では、参加ノードを表示する方法を示します。

```
Switch> show ipc nodes
There is 1 node in this IPC realm.
  ID      Type      Name          Last   Last
          Sent      Heard
10000 Local      IPC Master    0      0
```

次の例では、ローカル IPC ポートを表示する方法を示します。

```
Switch> show ipc ports
There are 8 ports defined.
Port ID      Type      Name                                     (current/peak/total)
There are 8 ports defined.
  10000.1    unicast   IPC Master:Zone
  10000.2    unicast   IPC Master:Echo
  10000.3    unicast   IPC Master:Control
  10000.4    unicast   IPC Master:Init
  10000.5    unicast   FIB Master:DFS.process_level.msgs
  10000.6    unicast   FIB Master:DFS.interrupt.msgs
  10000.7    unicast   MDFS RP:Statistics
    port_index = 0  seat_id = 0x10000  last sent = 0      last heard = 0
0/2/159
  10000.8    unicast   Slot 1 :MDFS.control.RIL
    port_index = 0  seat_id = 0x10000  last sent = 0      last heard = 0
0/0/0
RPC packets:current/peak/total
                                           0/1/4
```

次の例では、IPC 再送キューの内容を表示する方法を示します。

```
Switch> show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages currently on the IPC inboundQ.
Messages currently in use                :      3
Message cache size                       :    1000
Maximum message cache usage              :    1000

0 times message cache crossed          5000 [max]

Emergency messages currently in use      :      0

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0
Zone inbound message queue depth 0
```

次の例では、IPC セッションの全統計情報を表示する方法を示します。

```
Switch# show ipc session all
Tx Sessions:
Port ID      Type      Name
10000.7      Unicast   MDFS RP:Statistics
  port_index = 0  type = Unreliable    last sent = 0    last heard = 0
  Msgs requested = 180  Msgs returned = 180

10000.8      Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  type = Reliable      last sent = 0    last heard = 0
  Msgs requested = 0   Msgs returned = 0

Rx Sessions:
Port ID      Type      Name
10000.7      Unicast   MDFS RP:Statistics
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 180  Msgs returned = 180

10000.8      Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 0    Msgs returned = 0
```

次の例では、ローカル IPC サーバの状態を表示する方法を示します。

```
Switch> show ipc status cumulative
IPC System Status

Time last IPC stat cleared :never

This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.
```

	Rx Side	Tx Side
Total Frames	12916	608
0	0	
Total from Local Ports	13080	574
Total Protocol Control Frames	116	17
Total Frames Dropped	0	0

```
Service Usage

Total via Unreliable Connection-Less Service      12783      171
Total via Unreliable Sequenced Connection-Less Svc 0        0
Total via Reliable Connection-Oriented Service    17        116
(テキスト出力は省略)
```

関連コマンド

コマンド	説明
clear ipc	IPC マルチキャスト ルーティング統計情報をクリアします。

show ipv6 access-list

現在の IPv6 アクセス リストのすべての内容を表示するには、**show ipv6 access-list** ユーザ EXEC コマンドを使用します。

show ipv6 access-list [*access-list-name*]



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

access-list-name (任意) アクセス リスト名

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	このコマンドが導入されました。

使用上のガイドライン

show ipv6 access-list コマンドの出力内容は **show ip access-list** コマンドと同じですが、IPv6 専用です。デュアル IPv4 および IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6 {default | vlan}** グローバル コンフィギュレーション コマンドを入力して、スイッチをリロードします。

例

次の **show ipv6 access-list** コマンドの出力では、inbound および outbound という名前の IPv6 アクセス リストが表示されます。

```
Router# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
```

表 2-26 に、この出力で表示される重要なフィールドの説明を示します。

表 2-26 show ipv6 access-list フィールドの説明

フィールド	説明
IPv6 access list inbound	IPv6 アクセス リストの名前（例：inbound）
permit	指定のプロトコル タイプに一致するパケットを許可します。
tcp	Transmission Control Protocol。パケットが一致するべき高レベル（レイヤ 4）のプロトコル
any	::/0 と同等です。
eq	（任意）TCP または UDP パケットの送信元または宛先ポートを比較するための等号オペランド
bgp（一致）	Border Gateway Protocol。パケットが一致するプロトコルのタイプと一致した数
sequence 10	着信パケットがアクセス リストの行と比較される順序。アクセス リストの行はプライオリティの高いもの（10 など、数値の小さいもの）からプライオリティの低いものに（80 など、数値の大きいもの）順に並べられます。

関連コマンド

コマンド	説明
clear ipv6 access-list	IPv6 アクセス リスト一致カウンタをリセットします。
ipv6 access-list	IPv6 アクセス リストを定義して、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。

show ipv6 mld snooping

スイッチまたは VLAN（仮想 LAN）の IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング設定を表示するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping [vlan *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) VLAN 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	このコマンドが導入されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのに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 Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

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

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 ipv6 mld snooping vlan** コマンドの出力を示します。特定の VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000

Vlan 100:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000
```

次の例では、**show ipv6 mld snooping** コマンドの出力を示します。スイッチのすべての VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 1
Last listener query count    : 2
Last listener query interval : 1000
```

(テキスト出力は省略)

```
Vlan 951:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000
```


関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。

show ipv6 mld snooping address

Multicast Listener Discovery (MLD) スヌーピングによって取得された、すべてまたは指定の IP version 6 (IPv6) のマルチキャスト アドレス情報を表示するには、**show ipv6 mld snooping address** ユーザ EXEC コマンドを使用します。

```
show ipv6 mld snooping address [[vlan vlan-id] [ipv6 address]] [vlan vlan-id] [count | dynamic | user]
[ | {begin | exclude | include} expression]
```



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan vlan-id	(任意) MLD スヌーピング マルチキャスト アドレス情報を表示する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 1001 または 1006 ～ 4094 です。
ipv6-multicast-address	(任意) 指定の IPv6 マルチキャスト アドレスに関する情報を表示します。このキーワードは、VLAN ID を入力した場合のみ使用できます。
count	(任意) スイッチ上または指定の VLAN 内のマルチキャスト グループの数を表示します。
dynamic	(任意) MLD スヌーピングから学習したグループ情報を表示します。
user	(任意) MLD スヌーピングのユーザ設定グループ情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	このコマンドが導入されました。

使用上のガイドライン

IPv6 マルチキャスト アドレス情報を表示するには、このコマンドを使用します。

IPv6 マルチキャスト アドレスは、VLAN ID の入力後にのみ入力できます。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

学習されたグループに関する情報のみを表示するには、**dynamic** キーワードを使用します。設定されているグループに関する情報のみを表示するには、**user** キーワードを使用します。

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

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 snooping address** ユーザ EXEC コマンドの出力を示します。

Switch> show ipv6 mld snooping address

```
Vlan Group   Type Version Port List
-----
2      FF12::3 user           Fa1/0/2, Gi2/0/2, Gi3/0/1,Gi3/0/3
```

次の例では、**show snooping address count** ユーザ EXEC コマンドの出力を示します。

Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2

次の例では、**show snooping address user** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address user
Vlan Group   Type Version Port List
-----
2      FF12::3 user   v2      Fa1/0/2, Gi2/0/2, Gi3/0/1,Gi3/0/3
```

関連コマンド

コマンド	説明
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。

show ipv6 mld snooping mrouter

ダイナミックに学習され、手動で設定された、スイッチまたは VLAN（仮想 LAN）の IP version 6（IPv6）Multicast Listener Discovery（MLD）ルータ ポートを表示するには、**show ipv6 mld snooping mrouter** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping mrouter [*vlan vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management（SDM）テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) VLAN 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	このコマンドが導入されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピング ルータ ポートを表示するには、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 Fiber Distributed Data Interface（FDDI）VLAN 専用で、MLD スヌーピングでは使用できません。

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

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 ipv6 mld snooping mrouter** コマンドの出力を示します。MLD スヌーピングに参加しているすべての VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping mrouter
Vlan      ports
----      -
    2      Gi1/0/11 (dynamic)
   72      Gi1/0/11 (dynamic)
  200      Gi1/0/11 (dynamic)
```

■ show ipv6 mld snooping mrouter

次の例では、**show ipv6 mld snooping mrouter vlan** コマンドの出力を示します。特定の VLAN のマルチキャスト ルータ ポートが表示されます。

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan      ports
----      -
      2    Gi1/0/11 (dynamic)
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
ipv6 mld snooping vlan	VLAN のマルチキャスト ルータ ポートを設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。

show ipv6 mld snooping querier

スイッチまたは VLAN (仮想 LAN) から最後に受信した IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピング クエリア関連情報を表示するには、**show ipv6 mld snooping querier** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping querier [*vlan vlan-id*] [*detail*] [| {*begin* | *exclude* | *include*} *expression*]



(注)

このコマンドは、スイッチ スタックで拡張 IP サービス イメージが動作していて、スイッチにデュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている場合のみ利用できます。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) VLAN を指定します。指定できる範囲は、1 ～ 1001 および 1006 ～ 4094 です。
detail	(任意) スイッチまたは VLAN の MLD スヌーピング詳細クエリア情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	このコマンドが導入されました。

使用上のガイドライン

クエリアともいう MLD クエリー メッセージを送信する検出されたデバイスの MLD バージョンおよび IPv6 アドレスを表示するには、**show ipv6 mld snooping querier** コマンドを使用します。サブネットは複数のマルチキャスト ルータを持つことができますが、MLD クエリアは 1 つのみです。そのクエリアはレイヤ 3 スイッチになることができます。

show ipv6 mld snooping querier コマンド出力では、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。クエリアがスイッチの場合、出力では *Port* フィールドが *Router* として表示されます。クエリアがルータの場合、出力には *Port* フィールドにクエリアを学習するポート番号が表示されます。

show ipv6 mld snoop querier vlan コマンド出力には、外部または内部クエリアからのクエリー メッセージへの応答として受信した情報も表示されます。特定の VLAN でのスヌーピング信頼性変数など、ユーザ定義の VLAN 値は表示されません。このクエリア情報は、スイッチによって送信される MASQ メッセージでのみ使用されます。この情報が、クエリー メッセージに回答しないメンバーのエージングアウトに使用されるユーザ定義の信頼性変数を上書きすることはありません。

VLAN ID 1002 ～ 1005 はトークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用で、MLD スヌーピングでは使用できません。

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

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 ipv6 mld snooping querier** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address      MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi3/0/1
```

次の例では、**show ipv6 mld snooping querier detail** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address      MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi3/0/1
```

次の例では、**show ipv6 mld snooping querier vlan** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi3/0/1
Max response time : 1000s
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。
ipv6 mld snooping last-listener-query-count	MLD クライアントをエージングアウトとみなすまでにスイッチが送信するクエリーの最大回数を設定します。
ipv6 mld snooping last-listener-query-interval	クエリーを送出したあと、ポートをマルチキャストグループから削除するまでにスイッチが待ち合わせる最大応答時間を設定します。
ipv6 mld snooping robustness-variable	応答がない場合にマルチキャストアドレスをエージングアウトとみなすまでにスイッチが送信するクエリーの最大回数を設定します。
sdm prefer	スイッチの使用方法に基づいてシステム リソースを最適化するための SDM テンプレートを設定します。

show l2protocol-tunnel

レイヤ 2 プロトコル トンネル ポートに関する情報を表示するには、**show l2protocol-tunnel** ユーザ EXEC コマンドを使用します。プロトコル トンネリングがイネーブルであるインターフェイスに関する情報を表示します。

show l2protocol-tunnel [*interface interface-id*] [*summary*] [| *{begin | exclude | include}* *expression*]

シンタックスの説明

interface interface-id	(任意) プロトコル トンネリング情報が表示される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およびポート チャネルです。ポート チャネルの使用範囲は 1 ～ 48 です。
summary	(任意) レイヤ 2 プロトコルの要約情報のみを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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)SE	このコマンドが導入されました。

使用上のガイドライン

l2protocol-tunnel インターフェイス コンフィギュレーション コマンドを使用して、アクセスまたは IEEE（米国電気電子学会）802.1Q トンネル ポート上でレイヤ 2 プロトコル トンネリングをイネーブルにすると、次のパラメータの一部またはすべてを設定できます。

- トンネリングするプロトコル タイプ
- シャットダウン スレッシュホールド
- 廃棄スレッシュホールド

show l2protocol-tunnel [*interface interface-id*] コマンドを入力すると、すべてのパラメータが設定されているアクティブ ポートに関する情報のみが表示されます。

show l2protocol-tunnel summary コマンドを入力すると、一部またはすべてのパラメータが設定されているアクティブ ポートに関する情報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 l2protocol-tunnel** コマンドの出力を示します。

```
Switch> show l2protocol-tunnel
```

```
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa3/0/3	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
Fa3/0/4	udld	----	----	0	897960	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
Gi6/0/3	udld	----	----	0	897960	
	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	0	242500	
Gi6/0/4	lacp	500	----	0	485320	
	udld	300	----	44899	448980	
	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	1000	0	242700	
	lacp	----	----	0	485220	
	udld	300	----	44899	448980	

次の例では、**show l2protocol-tunnel summary** コマンドの出力を示します。

```
Switch> show l2protocol-tunnel summary
```

```
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Fa3/0/2	---	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa9/0/3	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/----/----	----/----/----	
Fa9/0/4	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/500/----	----/----/----	
Fa9/0/5	cdp stp vtp	----/----/----	----/----/----	down
	---	----/----/----	----/----/----	
Gi4/0/1	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	
Gi4/0/2	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	

関連コマンド

コマンド	説明
clear l2protocol-tunnel counters	プロトコル トンネリング ポートのカウンタをクリアします。
l2protocol-tunnel	インターフェイス上の Cisco Discovery Protocol (CDP)、Spanning-Tree Protocol (STP; スパニングツリー プロトコル)、VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) に対して、レイヤ 2 プロトコル トンネリングをイネーブルにします。
l2protocol-tunnel cos	トンネリングされたレイヤ 2 プロトコル パケットに、Class of Service (CoS; サービス クラス) 値を設定します。

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]
```

シンタックスの説明

<i>channel-group-number</i>	(任意) チャネル グループの番号です。指定できる範囲は 1 ～ 48 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 で使用されるシステム ID を表示します。システム ID は、LACP システム プライオリティおよびスイッチ MAC (メディア アクセス制御) アドレスで構成されています。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	<i>channel-group-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

show lacp コマンドを入力すると、アクティブな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 グループの情報が表示されます。

channel-group-number オプションを入力することで、**sys-id** 以外のすべてのキーワードでチャネル グループを指定できます。

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 2-27 に、表示されるフィールドの説明を示します。

```
Switch> show lacp counters
          LACPDU      Marker      Marker Response      LACPDU
Port      Sent   Recv   Sent   Recv   Sent   Recv   Pkts Err
-----
Channel group:1
Gi2/0/1    19     10      0      0      0      0      0
Gi2/0/2    14      6      0      0      0      0      0
```

表 2-27 show lacp counters のフィールドの説明

フィールド	説明
LACPDU Sent および Recv	ポートで送受信された LACP パケットの数
Marker Sent および Recv	ポートで送受信された LACP マーカ パケットの数
Marker Response Sent および Recv	ポートで送受信された LACP マーカ応答パケットの数
LACPDU Pkts および Err	ポートの LACP で受信した不明および不正パケットの数

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 LACPDU
        F - Device is requesting Fast LACPDU
        A - Device is in Active mode           P - Device is in Passive mode

Channel group 1
Port      Flags   State      LACP port   Admin   Oper   Port   Port
Gi2/0/1    SA      bndl      32768       0x3     0x3    0x4    0x3D
Gi2/0/2    SA      bndl      32768       0x3     0x3    0x5    0x3D
```

表 2-28 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 2-28 show lacp internal のフィールドの説明

フィールド	説明
State	特定のポートの状態。表示される値は次のとおりです。 — ポートが不明な状態です。 bndl — ポートがアグリゲータに接続され、他のポートとバンドルされています。 susp — ポートが中断されている状態で、アグリゲータには接続されていません。 hot-sby — ポートがホットスタンバイの状態です。 indiv — ポートが他のポートとバンドルできない状態にあります。 indep — ポートが独立した状態にあります（バンドルされていませんが、データ トラフィックをスイッチングできます。この場合、パートナーポート上で LACP は稼働していません）。 down — ポートがダウンしています。

表 2-28 show lacp internal のフィールドの説明（続き）

フィールド	説明
LACP Port Priority	ポートのプライオリティ設定。互換性のあるすべてのポートが集約しないよう、ハードウェアが制限されている場合、LACP はポート プライオリティによりポートをスタンバイ モードにします。
Admin Key	ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します（16 進数）。管理用のキーは、ポートが他のポートと集約できる能力を定義します。ポートが他のポートと集約する機能は、ポートの物理的な特性（たとえば、データ レート、デュプレックス機能など）および決められた設定制限によって決まります。
Oper Key	ポートで使用されるランタイムの操作キー。LACP は自動的にこの値を生成します（16 進数）。
Port Number	ポート番号
Port State	ポートの状態変数。1 つのオクテット内で個々のビットとしてエンコードされ、意味は次のようになります。 • bit0 : LACP のアクティビティ • bit1 : LACP のタイムアウト • bit2 : 集約 • bit3 : 同期 • bit4 : 収集 • bit5 : 配信 • bit6 : デフォルト • bit7 : 期限切れ  (注) 上記のリストで、bit7 は MSB、bit0 は 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 LACPDU  F - Device is sending Fast LACPDU
        A - Device is in Active mode        P - Device is in Passive mode
```

```
Channel group 3 neighbors
```

```
Partner's information:
```

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

```
Partner's information:
```

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner 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 ID は、システム プライオリティおよびシステム 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、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

関連コマンド

コマンド	説明
clear lacp	LACP チャンネルグループ情報をクリアします。
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

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*]

シンタックスの説明

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およびポート チャネルです。ポートチャネルの使用範囲は 1 ～ 48 です（イネーブル EXEC モードでのみ使用できます）。
begin	（任意） <i>expression</i> と一致する行から表示を開始します。
exclude	（任意） <i>expression</i> と一致する行を表示から除外します。
include	（任意）指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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。表示では、ポート 2 が MAC アクセス リスト *macl_e1* を適用し、他のインターフェイスには MAC ACL を適用していません。

```
Switch> show mac access-group
Interface GigabitEthernet1/0/1:
  Inbound access-list is not set
Interface GigabitEthernet1/0/2:
  Inbound access-list is macl_e1
Interface GigabitEthernet1/0/3:
  Inbound access-list is not set
Interface GigabitEthernet1/0/4:
  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 gigabitethernet1/0/1** コマンドの出力を示します。

```
Switch# show mac access-group interface gigabitethernet1/0/1
Interface GigabitEthernet1/0/1:
  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 テーブルのダイナミック / スタティック エントリ、または特定のインターフェイスや VLAN (仮想 LAN) 上の MAC アドレス テーブルのダイナミック / スタティック 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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table コマンド (ハイフンあり) は、 show mac address-table コマンド (ハイフンなし) に変更されました。

使用上のガイドライン

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   Gi6/0/4
Total Mac Addresses for this criterion: 12
```

関連コマンド

コマンド	説明
<code>clear mac address-table dynamic</code>	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。
<code>show mac address-table aging-time</code>	すべての VLAN または指定の VLAN のエージング タイムを表示します。
<code>show mac address-table count</code>	すべての VLAN または指定の VLAN に存在しているアドレス数を表示します。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table interface</code>	指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。
<code>show mac address-table notification</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table address

指定の 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*]

シンタックスの説明

<i>mac-address</i>	48 ビットの MAC アドレスを指定します。有効な形式は H.H.H です。
interface <i>interface-id</i>	(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は、物理ポートおよびポート チャネルです。
vlan <i>vlan-id</i>	(任意) 特定の VLAN（仮想 LAN）のみ、エントリを表示します。指定できる範囲は、1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table address コマンド（ハイフンあり）は、 show mac address-table address コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

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
<code>show mac address-table aging-time</code>	すべての VLAN または指定の VLAN のエージング タイムを表示します。
<code>show mac address-table count</code>	すべての VLAN または指定の VLAN で存在しているアドレス数を表示します。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table interface</code>	指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。
<code>show mac address-table notification</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の 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、指定の VLAN（仮想 LAN）上のすべてのアドレス テーブル インスタンス、または VLAN が指定されていない場合、すべての VLAN のアドレス テーブル インスタンスのエージング タイムを表示するには、**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*]

シンタックスの説明

vlan <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table aging-time コマンド（ハイフンあり）は、 show mac address-table aging-time コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

VLAN 番号を指定しない場合、すべての VLAN に対するエージング 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
<code>mac address-table aging-time</code>	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。
<code>show mac address-table address</code>	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
<code>show mac address-table count</code>	すべての VLAN または指定の VLAN で存在しているアドレス数を表示します。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table interface</code>	指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。
<code>show mac address-table notification</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の 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）または指定の VLAN に存在するアドレスの数を表示するには、**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*]

シンタックスの説明

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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table count コマンド（ハイフンあり）は、 show mac address-table count コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

VLAN 番号を指定しない場合、すべての VLAN に対するアドレス 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
<code>show mac address-table address</code>	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
<code>show mac address-table aging-time</code>	すべての VLAN または指定の VLAN のエージング タイムを表示します。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table interface</code>	指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。
<code>show mac address-table notification</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の 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 テーブルの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]
```

シンタックスの説明

address mac-address	(任意) 48 ビットの MAC アドレスを指定します。有効な形式は H.H.H です（イネーブル EXEC モードでのみ使用可能）。
interface interface-id	(任意) 照合する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、物理ポートおよびポート チャネルです。
vlan vlan-id	(任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ～ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table dynamic コマンド（ハイフンあり）は、 show mac address-table dynamic コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

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 Gi6/0/2
1       00b0.6496.2741   DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
<code>clear mac address-table dynamic</code>	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。
<code>show mac address-table address</code>	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
<code>show mac address-table aging-time</code>	すべての VLAN または指定の VLAN のエージング タイムを表示します。
<code>show mac address-table count</code>	すべての VLAN または指定の VLAN で存在しているアドレス数を表示します。
<code>show mac address-table interface</code>	指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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table interface

指定の VLAN（仮想 LAN）の指定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 EXEC コマンドを使用します。

show mac address-table interface *interface-id* [*vlan vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>interface-id</i>	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は、物理ポートおよびポート チャネルです。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table interface コマンド（ハイフンあり）は、 show mac address-table interface コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

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 gigabitethernet6/0/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi6/0/2
1       00b0.6496.2741   DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```


関連コマンド

コマンド	説明
<code>show mac address-table address</code>	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
<code>show mac address-table aging-time</code>	すべての VLAN または指定の VLAN のエージング タイムを表示します。
<code>show mac address-table count</code>	すべての VLAN または指定の VLAN で存在しているアドレス数を表示します。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table notification</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	指定の 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（メディア アクセス制御）アドレス テーブル移行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**]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	このコマンドが導入されました。

使用上のガイドライン

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 テーブル移行更新カウンタをクリアします。
mac address-table move update {receive transmit}	スイッチ上で MAC アドレス テーブル移行更新を設定します。

show mac address-table notification

すべてのインターフェイスまたは指定のインターフェイスの 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]
```

シンタックスの説明

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は、物理ポートおよびポート チャンネルです。
<i>interface-id</i>	(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は、物理ポートおよびポート チャンネルです。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table notification コマンド（ハイフンあり）は、 show mac address-table notification コマンド（ハイフンなし）に変更されました。

使用上のガイドライン

機能がイネーブルかディセーブルか、MAC 通知間隔、履歴テーブルに許可されたエントリの最大数、および履歴テーブルの内容を表示するには、キーワードを指定しないで **show mac address-table notification** コマンドを使用します。

すべてのインターフェイスのフラグを表示するには、**interface** キーワードを使用します。*interface-id* が含まれている場合、そのインターフェイスのフラグのみ表示されます。

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 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	指定の 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 (仮想 LAN) または指定の 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 または指定の VLAN で存在してい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	指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	指定の 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 テーブルの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]
```

シンタックスの説明

address mac-address	(任意) 48 ビットの MAC アドレスを指定します。有効な形式は H.H.H です (イネーブル EXEC モードでのみ使用可能)。
interface interface-id	(任意) 照合する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、物理ポートおよびポート チャネルです。
vlan vlan-id	(任意) 特定の VLAN (仮想 LAN) 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.1(19)EA1	show mac-address-table static コマンド (ハイフンあり) は、 show mac address-table static コマンド (ハイフンなし) に変更されました。

使用上のガイドライン

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
----    -
A11     0100.0ccc.cccc    STATIC  CPU
A11     0180.c200.0000    STATIC  CPU
A11     0100.0ccc.cccd    STATIC  CPU
A11     0180.c200.0001    STATIC  CPU
A11     0180.c200.0004    STATIC  CPU
A11     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て、スイッチで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設定します。
show mac address-table address	指定の 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 または指定の 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 または指定の VLAN で存在してい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	指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	指定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table vlan

特定の 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*]

シンタックスの説明	<i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
	exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
	include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
	<i>expression</i>	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
	12.1(11)AX	このコマンドが導入されました。
	12.1(19)EA1	show mac-address-table vlan コマンド（ハイフンあり）は、 show mac address-table vlan コマンド（ハイフンなし）に変更されました。

使用上のガイドライン 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	指定の 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 または指定の 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 または指定の VLAN で存在してい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	指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**]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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) トランスペアレンシー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 トランスペアレンシー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	スイッチ全体の 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 ポリサーの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送信レート、送信の最大バースト サイズ、および最大値を超えた場合にとられるアクションを定義します。

show mls qos aggregate-policer [*aggregate-policer-name*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>aggregate-policer-name</i>	(任意) 指定された名前のポリサー設定を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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	ポリサーのパラメータを定義します (ポリシー マップ内で複数のクラスが共有できます)。

show mls qos input-queue

入力キューの Quality of Service (QoS; サービス品質) 設定を表示するには、**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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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	入力キューに対し Shaped Round Robin (SRR; シェイプド ラウンド ロビン) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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て、CoS 値をキューおよびスレッショールド 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て、DSCP 値をキューおよびスレッショールド 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	入力キューに対し Weighted Tail-Drop (WTD) スレッショールドのパーセンテージを割り当てます。

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]
```

シンタックスの説明

<i>interface-id</i>	(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) キューイングの指針 (共有またはシェーピング) およびキューに対応したウェイトを表示します。
statistics	(任意) 送受信した Differentiated Services Code Point (DSCP) の統計、送受信した Class of Service (CoS; サービス クラス) 値の統計、出力キューごとにキューイングまたは廃棄されたパケット数、各ポリサーの適合パケット数および不適合パケット数を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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（仮想 LAN）ベースの 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 gigabitethernet1/0/1
GigabitEthernet1/0/1
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 ベースの 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 gigabitethernet1/0/2
GigabitEthernet1/0/2
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 gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
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; シェイプドラウンドロビン）ウェイトを上書きします。

```
Switch> show mls qos interface gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
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
```

■ show mls qos interface

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 2-29 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 mls qos interface gigabitethernet1/0/2 statistics
GigabitEthernet1/0/2

  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      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      0
  cos: incoming
-----
  0 - 4 :    132067      0      0      0      0
  5 - 9 :         0      0      0      0      0
  cos: outgoing
-----
  0 - 4 :    739155      0      0      0      0
  5 - 9 :         90      0      0      0      0

Policer: Inprofile:          0 OutofProfile:          0
```

表 2-29 show mls qos interface statistics のフィールドの説明

フィールド		説明
DSCP	incoming	各 DSCP 値の受信したパケット数
	outgoing	各 DSCP 値の送信したパケット数
CoS	incoming	各 CoS 値の受信したパケット数
	outgoing	各 CoS 値の送信したパケット数
Policer	Inprofile	各ポリサーの適合パケット数
	Outofprofile	各ポリサーの不適合パケット数

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
mls qos srr-queue input bandwidth	入力キューに対し SRR ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間に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、または 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、または 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	入力キューに対し WTD スレッシュホールドのパーセンテージを割り当てます。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよび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 値を出力キューにマッピング、または 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。
policy-map	ポリシー マップを作成または修正します。
priority-queue	ポートでの出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
srr-queue bandwidth limit	ポート上の最大出力を制限します。
srr-queue bandwidth shape	シェーピングしたウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有のウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

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。分類中、QoS はマッピング テーブルを使用し、トラフィックのプライオリティを表示します。また、このテーブルで、受信した Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP)、IP precedence 値から対応する CoS、または DSCP 値を抽出します。

```
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]
```

シンタックスの説明

cos-dscp	(任意) CoS/DSCP マップを表示します。
cos-input-q	(任意) CoS 入力キューのスレッシュホールド マップを表示します。
cos-output-q	(任意) CoS 出力キューの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 入力キューのスレッシュホールド マップを表示します。
dscp-mutation <i>dscp-mutation-name</i>	(任意) 指定の DSCP/DSCP 合成マップを表示します。
dscp-output-q	(任意) DSCP 出力キューの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) ポリシングされた DSCP マップを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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。

ポリシングされた DSCP、DSCP/CoS、および DSCP/DSCP 合成マップが行列で表示されます。d1 のカラムは DSCP の最上位のビットを示しています。d2 の行は DSCP の最下位のビットを示しています。d1 および d2 の値の交点がポリシングされた DSCP、CoS、または合成 DSCP の値になります。たとえば、DSCP/CoS マップでは、DSCP 値 43 は CoS 値の 5 に対応することになります。

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 マップは行列で表示されます。d1 のカラムは DSCP 番号の最上位のビットを示しています。d2 の行は DSCP 番号の最下位のビットを示しています。d1 および d2 の値の交点にキュー ID およびスレッシュホールド ID になります。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 およびスレッシュホールド 1 (02-01) に対応することになります。

CoS 入力キュー スレッシユホールドおよび CoS 出力キュー スレッシユホールド マップは、CoS 値を一番上の行、対応するキュー ID およびスレッシユホールド ID は 2 番めの行に表示しています。たとえば、CoS 入力キュー スレッシユホールド マップでは、CoS 値 5 はキュー 2 およびスレッシユホールド 1 (2-1) に対応することになります。

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
```

■ show mls qos maps

```

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 合成マップ、IP precedence/DSCP マップ、およびポリシングされた 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、または 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、または 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 output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよび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 値を出力キューにマッピング、または 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。

show mls qos queue-set

出力キューの Quality of Service (QoS; サービス品質) 設定を表示するには、**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*]

シンタックスの説明

<i>qset-id</i>	(任意) キューセットの ID。キューセットに属する各ポートの 4 つの出力キューのすべての特性を定義します。指定できる範囲は、1 ～ 2 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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	キューセットに対しバッファを割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットの最大メモリ割り当てを設定します。

show mls qos vlan

Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に適用されたポリシー 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 ]
```

シンタックスの説明

<i>vlan-id</i>	ポリシー マップを表示するには、SVI の VLAN (仮想 LAN) ID を指定します。指定できる範囲は、1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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)SE	このコマンドが導入されました。

使用上のガイドライン

show mls qos vlan コマンドの出力は、VLAN ベースの Quality of Service (QoS; サービス品質) がイネーブルであり、さらに階層型ポリシー マップが設定されている場合にだけ意味があります。

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

スイッチのすべての 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。コマンドにキーワードを指定することで、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、すべてのリモートセッションを表示できます。

```
show monitor [session {session_number | all | local | range list | remote} [detail]] [| {begin | exclude | include} expression]
```

シンタックスの説明

session	(任意) 指定の SPAN セッションの情報を表示します。
session_number	SPAN または RSPAN の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。
all	すべての SPAN セッションを表示します。
local	ローカルの 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 (<i>list</i> は有効なセッションの範囲) を表示します。1 つのセッション、またはセッション範囲は 2 つの番号で表示され、番号の低いほうが最初になります (ハイフンで区切られます)。カンマ区切りのパラメータの間、またはハイフンで指定した範囲の間にスペースは入力しません。
 (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	リモートの SPAN セッションのみを表示します。
detail	(任意) 指定のセッションの詳細情報を表示します。
 begin	<i>expression</i> と一致する行から表示を開始します。
 exclude	<i>expression</i> と一致する行を表示から除外します。
 include	指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	range list および detail キーワードが追加されました。

使用上のガイドライン

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 コマンドおよび **show monitor session all** コマンドの出力結果は同一になります。

例

次の例では、**show monitor** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa4/0/1
Both : Fa4/0/2-3,Fa4/0/5-6
Destination Ports : Fa4/0/20
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 : Fa4/0/1
Both : Fa4/0/2-3,Fa4/0/5-6
Destination Ports : Fa4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送がイネーブルの状態での **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 : Fa4/0/2
Destination Ports : Fa4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Both : Fa4/0/8
Destination Ports : Fa4/0/12
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、または修正します。

show mvr

現在の Multicast VLAN Registration (MVR) グローバル パラメータの値を表示するには、キーワードを指定しないで **show mvr** イネーブル EXEC コマンドを使用します。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)、最大クエリ応答時間、マルチキャスト グループ数、および MVR モード (dynamic または compatible) が含まれます。

show mvr [**| {begin | exclude | include}** *expression*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 で固定されています。MVR モードは、compatible (Catalyst 2900 XL および Catalyst 3500 XL スイッチと連動する場合) または dynamic (動作が Internet Group Management Protocol [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	interface および members キーワードを指定した場合、設定された MVR インターフェイス、指定の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すべてのマルチキャスト 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。メンバーがない場合、グループは Inactive として表示されます。

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 コマンドを使用します。特定のレシーバー ポートの MVR パラメータを表示するには、キーワードを指定してこのコマンドを使用します。

show mvr interface [*interface-id* [**members** [*vlan vlan-id*]]] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>interface-id</i>	(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は物理ポート (タイプ、スタック メンバー、モジュール、ポート番号を含む) を含みます。
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。
<i>vlan vlan-id</i>	(任意) VLAN (仮想 LAN) 上のすべての MVR グループ メンバーを表示します。指定できる範囲は、1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、ポート単位の状態、および即時脱退設定が表示されます。

members キーワードを入力した場合、インターフェイス上のすべての MVR グループ メンバーが表示されます。VLAN ID を入力した場合、VLAN 内のすべての MVR グループ メンバーが表示されます。

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 mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface
Port          Type          Status          Immediate Leave
----          -
Gi1/0/1      SOURCE        ACTIVE/UP        DISABLED
Gi1/0/2      RECEIVER      ACTIVE/DOWN      DISABLED
```


上記の出力の 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、指定のポートの **show mvr interfaces** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet1/0/2
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 gigabitethernet1/0/2 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

IP マルチキャスト グループの現行メンバー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*

シンタックスの説明

<i>ip-address</i>	(任意) IP マルチキャスト アドレスです。アドレスが入力されると、マルチキャスト グループ メンバーの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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

show 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 の compatible モードでは、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      Gi1/0/1(d), Gi1/0/5(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。IP マルチキャスト グループのメンバーとそのアドレスが表示されます。

```
Switch# show mvr members 239.255.0.2
239.255.003.--22    ACTIVE      Gi1/0/1(d), Gi1/0/2(d), Gi1/0/3(d),
                  Gi1/0/4(d), Gi1/0/5(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 キーワードを指定した場合、設定された MVR インターフェイス、指定の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すべてのマルチキャスト グループを表示します。

show pagp

Port Aggregation Protocol (PAgP) 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]
```

シンタックスの説明

<i>channel-group-number</i>	(任意) チャネル グループの番号です。指定できる範囲は 1 ～ 48 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	<i>channel-group-number</i> の範囲が、1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

show pagp コマンドを入力すると、アクティブなチャネルグループの情報が表示されます。非アクティブな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
Gi1/0/1   45     42         0       0
Gi1/0/2   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
Gi1/0/1   SC    U6/S7  H       30s      1      128    Any    16
Gi1/0/2   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
Port      Name      Partner      Partner      Partner
          Name      Device ID    Port         Age  Flags  Cap.
Gi1/0/1   switch-p2  0002.4b29.4600  Gi01//1      9s  SC     10001
Gi1/0/2   switch-p2  0002.4b29.4600  Gi1/0/2      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クリアします。

show parser macro

スイッチに設定されているすべてのマクロまたは 1 つのマクロ用の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]
```

シンタックスの説明

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) マクロ名で特定された 1 つのマクロに関する情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

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、スイッチのプラットフォームおよびスイッチで稼働するソフトウェア イメージに応じて異なります。

```
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

```

次の例では、**show parser macro name** コマンドの出力を示します。

```

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

```

次の例では、**show parser macro brief** コマンドの出力を示します。

```
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
```

次の例では、**show parser description** コマンドの出力を示します。

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Gi1/0/1        standard-switch10
Gi1/0/2        this is test macro
-----
```

次の例では、**show parser description interface** コマンドの出力を示します。

```
Switch# show parser macro description interface gigabitethernet1/0/2
Interface      Macro Description
-----
Gi1/0/2        this is test macro
-----
```

関連コマンド

コマンド	説明
macro apply	インターフェイスにマクロを適用するか、インターフェイスにマクロを適用して追跡します。
macro description	インターフェイスに適用されるマクロに関する記述を追加します。
macro global	スイッチにマクロを適用するか、スイッチにマクロを適用して追跡します。
macro global description	スイッチに適用されるマクロに関する記述を追加します。
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 policy-map

着信トラフィックの分類条件を定義する 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*]

シンタックスの説明

<i>policy-map-name</i>	(任意) 指定されたポリシーマップの名前を表示します。
class <i>class-map-name</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring には表示されていますが、サポートされていません。表示にある統計は無視してください。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 1000000000 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 ポリシーを指定できるポリシー マップを作成、または変更します。

show port-security

インターフェイスまたはスイッチの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*]

シンタックスの説明

interface interface-id	(任意) 指定されたインターフェイス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は物理ポート (タイプ、スタック メンバー、モジュール、ポート番号を含む) を含みます。
address	(任意) すべてのポートまたは指定されたポート上のすべてのセキュア MAC (メディア アクセス制御) アドレスを表示します。
vlan	(任意) 指定されたインターフェイスのすべての VLAN (仮想 LAN) のポートセキュリティ設定を表示します。このキーワードは、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上でのみ表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	vlan キーワードが追加されました (トランク ポート上でのみ表示)。

使用上のガイドライン

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 を入力した場合、コマンドは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。

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、インターフェイスのすべての 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。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すべての VLAN について、セキュア MAC アドレスの設定最大値と現在の数が表示されます。このオプションは、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上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)
-----
      Gil/0/1           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 gigabitethernet1/0/1
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   Gil/0/2      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 gigabitethernet1/0/2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/0/2 address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800   SecureConfigured   Gil/0/2      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 gigabitethernet1/0/2 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 power inline

指定された Power over Ethernet (PoE) ポートまたはすべての PoE ポートの PoE ステータスを表示するには、**show power inline** ユーザ EXEC コマンドを使用します。

```
show power inline [interface-id | consumption default | module switch-number] [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) 指定されたインターフェイスの PoE 関連の電源管理情報を表示します。
consumption default	(任意) PoE ポートに接続された装置に割り当てられる電力を表示します。
module switch-number	(任意) 指定のスタック メンバーのポートのみを表示します。スイッチ番号は 1 ～ 9 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(19)EA1	このコマンドが導入されました。
12.2(25)SEC	consumption default キーワードが追加されました。

使用上のガイドライン

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 power inline** コマンドの出力を示します。この出力では、ポート2はスタティックとして設定されているので、電力は事前にこのポートに割り当てられます。ただし、受電装置は接続されていません。最大ワット数は10 Wに設定されているので、ポート6は **power-deny** ステータスのスタティック ポートです。接続された受電装置には、クラス0またはクラス3 装置用の報告されたクラスの最大ワット数が割り当てられます。

```
Switch> show power inline
Module      Available      Used      Remaining
            (Watts)        (Watts)    (Watts)
-----
1           370.0         114.9      255.1
2           370.0         34.3       335.

Interface Admin  Oper      Power  Device      Class Max
            (Watts)
-----
Fa1/0/1    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/2    static off       15.4    n/a         n/a  15.4
Fa1/0/3    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/4    auto    on        6.3     IP Phone 7960  2    15.4
Fa1/0/5    static on       15.4    IP Phone 7960  2    15.4
Fa1/0/6    static power-deny 10.0    n/a         n/a  10.0
Fa1/0/7    auto    on        6.3     IP Phone 7910  n/a  15.4
(テキスト出力は省略)
```

次の例では、ポートでの **show power inline** コマンドの出力を示します。

```
Switch> show power inline fastethernet2/0/1
Interface Admin  Oper      Power  Device      Class Max
            (Watts)
-----
Fa2/0/1    auto    on        6.3     IP Phone 7910  n/a  15.4
```

次の例では、すべての PoE スイッチ ポートでの **show power inline consumption default** コマンドの出力を示します。

```
Switch> show power inline consumption default
Default PD consumption : 15400 mW
```

次の例では、スタック メンバー1 での **show power inline module switch-number** コマンドの出力を示します。

```
Switch> show power inline module 1
Module      Available      Used      Remaining
            (Watts)        (Watts)    (Watts)
-----
1           370.0         166.2      203.9
Interface Admin  Oper      Power  Device      Class Max
            (Watts)
-----
Fa1/0/1    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/2    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/3    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/4    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/5    auto    on        6.3     IP Phone 7910  n/a  15.4
Fa1/0/6    auto    on        6.3     IP Phone 7910  n/a  15.4
(テキスト出力は省略)
```

表 2-30 show power inline interface のフィールドの説明

フィールド	説明
Admin	管理モード : auto、off、static
Oper	動作モード : - on — 受電装置が検出され、電力が供給されている状態です。 - off — PoE が適用されていない状態です。 - faulty — 装置検出または受電装置が障害の状態です。 - power-deny — 受電装置は検出されていますが、PoE が利用できない、または最大ワット数が検出された受電装置の最大値を超えている状態です。
Power	PoE の供給ワット数
Device	検出されたデバイスのタイプ : n/a、unknown、Cisco PD、IEEE（米国電気電子学会）PD、< Cisco Discovery Protocol（CDP）による名前 >
Class	IEEE 分類 : n/a、Class <0 ~ 4>
Available	システム内の PoE の総量
Used	ポートに割り当てられている PoE の量
Remaining	システム内でポートに割り当てられていない PoE の量（Available – Used = Remaining）

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電源管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。

show sdm prefer

特定の機能のシステム リソースの割り当てを最大限に活用させることができる Switch Database Management (SDM) テンプレートの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。キーワードを指定しない場合は使用中のテンプレートを表示します。

```
show sdm prefer [access | default | dual-ipv4-and-ipv6 {default | vlan} |routing | vlan [desktop]]
[ | {begin | exclude | include} expression]
```

シンタックスの説明

access	(任意) ACL でシステム リソースを最大限活用するテンプレートを表示します。
default	(任意) 機能間でシステム リソースを均等にするテンプレートを表示します。
dual-ipv4-and-ipv6 {default vlan}	(任意) IPv4 および IPv6 の両方をサポートするテンプレートを表示します。 default — デフォルトのデュアルテンプレート コンフィギュレーションを表示します。 vlan — VLAN (仮想 LAN) デュアルテンプレート コンフィギュレーションを表示します。
 (注) このオプションはすべてのスイッチで表示されますが、スイッチスタックで拡張 IP サービス イメージが稼働している場合にのみサポートされます。	
routing	(任意) ルーティングでシステム リソースを最大限活用するテンプレートを表示します。
vlan	(任意) レイヤ 2 VLAN でシステム リソースを最大限活用するテンプレートを表示します。
desktop	(任意) Catalyst 3750-12S アグリゲータ スイッチ専用で、デスクトップのテンプレートを表示します。このスイッチでは、 desktop キーワードを入力しない場合、アグリゲータ テンプレートが表示されます。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	desktop キーワードが追加されました。
12.2(25)SE	dual-ipv4-and-ipv6 {default vlan} キーワードが追加されました。
12.2(25)SED	access キーワードが追加されました。

使用上のガイドライン

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、SDM テンプレートを変更した場合は、設定の変更を有効にするため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** コマンドを入力した場合、**show sdm prefer** により、現在使用している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が表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字によって、実際の数字とは異なる場合があります。

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 sdm prefer** コマンドの出力を示します。現在使用されているテンプレートが表示されます。

```
Switch# show sdm prefer
"default" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          12K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 0
number of qos aces:                       512
number of security aces:                  1K

Switch# show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          6K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 8K
  number of directly connected hosts:      6K
  number of indirect routes:               2K
number of policy based routing aces:       0
number of qos aces:                       512
number of security aces:                   1K
```

次の例では、アグリゲータ スイッチ上で入力された **show sdm prefer routing** コマンドの出力を示します。

```
Switch# show sdm prefer routing
"aggregate routing" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          6K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 20K
  number of directly connected hosts:      6K
  number of indirect routes:               14K
number of policy based routing aces:       512
number of qos aces:                       512
number of security aces:                   1K
```

次の例では、デスクトップスイッチ上で入力された **show sdm prefer routing** コマンドの出力を示します。

```
Switch# show sdm prefer routing
"desktop routing" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          3K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 11K
  number of directly connected hosts:      3K
  number of indirect routes:               8K
number of policy based routing aces:       512
number of qos aces:                       512
number of security aces:                  1K
```

次の例では、デスクトップスイッチ上で入力された **show sdm prefer dual-ipv4-and-ipv6 default** コマンドの出力を示します。

```
Switch# show sdm prefer dual-ipv4-and-ipv6 default
"desktop IPv4 and IPv6 default" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:            3K
  number of directly-connected IPv4 hosts:  2K
  number of indirect IPv4 routes:           1K
number of IPv6 multicast groups:          1K
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:    1K
number of IPv4 policy based routing aces:  0
number of IPv4/MAC qos aces:               512
number of IPv4/MAC security aces:          1K
number of IPv6 policy based routing aces:  0
number of IPv6 qos aces:                   510
number of IPv6 security aces:              510
```

次の例では、新しいテンプレートを設定し、まだリロードしていないスイッチ上での **show sdm prefer** コマンドの出力を示します。

```
Switch# show sdm prefer
The current template is "desktop routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          3K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 11K
  number of directly connected hosts:      3K
  number of indirect routes:               8K
number of qos aces:                       512
number of security aces:                  1K

On next reload, template will be "desktop vlan" template.
```


関連コマンド

コマンド	説明
sdm prefer	SDM テンプレートを、ルーティングまたは VLAN のリソースを最大限に活用するように設定、デフォルト テンプレートを使用するように設定、デュアル IPv4/IPv6 テンプレートを選択するように設定、またはデスクトップ、アグリゲータ テンプレートを選択するように設定します。

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]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(14)EA1	このコマンドが導入されました。

例

次の例では、**show setup express** コマンドの出力を示します。

```
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

スパニングツリー状態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]
```

シンタックスの説明

<i>bridge-group</i>	(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 の状態を表示します。
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 (オプション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)。
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 (active キーワードはイネーブル EXEC モードの場合のみ使用可能)。
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 <i>interface-id</i> [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すべてイネーブル EXEC モードの場合のみ使用可能)。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は、物理ポート、VLAN (仮想 LAN)、およびポート チャネルです。VLAN の使用範囲は 1 ～ 4094 です。ポートチャネルの使用範囲は 1 ～ 48 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 MSTConfiguration Identifier (MSTCI) に含まれる MD5 ダイジェストを表示します。異なる 2 つのダイジェストが表示されます。1 つはスタンダード スイッチ用、もう 1 つはプレスタンダード スイッチ用のダイジェストです (イネーブル EXEC モードでのみ使用できます)。 IEEE (米国電気電子学会) 標準を実装するために用語が更新され、<i>txholdcount</i> フィールドが追加されました。 新しいマスター ロールが境界ポートに表示されます。 <i>pre-standard</i> または <i>Pre-STD</i> は、IEEE スタンダードブリッジがポートでプレスタンダード Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) を送信する場合に表示されます。 <i>pre-standard (config)</i> または <i>Pre-STD-Cf</i> は、ポートでプレスタンダード BPDU を送信するように設定されており、そのポートでプレスタンダード BPDU が受信されていない場合に表示されます。 <i>pre-standard (rcvd)</i> または <i>Pre-STD-Rx</i> は、ポートでプレスタンダード BPDU が受信されており、そのポートがプレスタンダード BPDU を送信するように設定されていない場合に表示されます。 <i>dispute</i> フラグは、ポートがフォワーディングステートに戻るか指定を中止するまで Designated Port (DP; 指定ポート) が下位指定情報を受信する場合に表示されます。 • instance-id — 1 つのインスタンス ID、それぞれをハイフンで区切った ID の範囲、またはカンマで区切った一連の 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の数が表示されます。 • interface interface-id — (任意) 有効なインターフェイスは、物理ポート、VLAN、およびポートチャネルです。VLAN の使用範囲は 1 ～ 4094 です。ポートチャネルの使用範囲は 1 ～ 48 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がイネーブル 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状態セクションの総行数を表示します。IEEE Standard は、スイッチで実行中の MST のバージョンを示します。
uplinkfast	(任意) スパニングツリー UplinkFast のステータスを表示します。

■ show spanning-tree

vlan <i>vlan-id</i> [active [detail]	(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
backbonefast blockedports	(一部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)。
bridge [address detail	VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN
forward-time hello-time id	を指定できます。指定できる範囲は、1 ～ 4094 です。
max-age priority [system-id]	
protocol]	
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	mst キーワードおよびオプションが追加されました。
12.2(25)SEC	digest キーワードが追加され、新規ダイジェストおよび送信ホールド回数フィールドが追加されました。

使用上のガイドライン

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 (GigabitEthernet2/0/1)
              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
-----
Gi2/0/1       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 (GigabitEthernet2/0/1), 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 (GigabitEthernet2/0/1) 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 gigabitethernet2/0/1
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 gigabitethernet2/0/1
GigabitEthernet2/0/1 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 Gi1/0/1 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
-----
GigabitEthernet2/0/1 root FWD 200000 128 P2P bound(STP)
GigabitEthernet2/0/2 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 bpduguard	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。
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 リージョン内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 (仮想 LAN) 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のインターフェイス上で、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たり、ストーム制御履歴を表示したりするには、**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]
```

シンタックスの説明

<i>interface-id</i>	(任意) 物理ポートのインターフェイス ID (タイプ、スタック メンバー、モジュール、ポート番号を含む)
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

interface-id を入力した場合、指定の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、スイッチ上のすべてのポートの1つのトラフィック タイプの設定が表示されます。

トラフィック タイプを入力しない場合、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、キーワードを指定せずに入力した **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のキーワードが入力されていないため、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
-----
Gi1/0/1        Forwarding    20 pps     10 pps     5 pps
Gi1/0/2        Forwarding    50.00%     40.00%     0.00%
(テキスト出力は省略)
```


次の例では、指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のキーワードが入力されていないため、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 1/0/1
Interface      Filter State   Upper          Lower          Current
-----
Gi1/0/1        Forwarding     20 pps         10 pps         5 pps
```

表 2-31 に、**show storm-control** の出力で表示されるフィールドの説明を示します。

表 2-31 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 — ストーム制御がディセーブルです。
Upper	増加する抑制レベルを利用可能な合計帯域幅のパーセンテージとして、パケット / 秒またはビット / 秒で表示します。
Lower	減少する抑制レベルを利用可能な総帯域幅のパーセンテージとして、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のトラフィック タイプ (ブロードキャスト、マルチキャスト、ユニキャスト) の帯域幅の使用率を、全体で利用可能な帯域幅のパーセンテージで表示します。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	スイッチにブロードキャスト、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 switch

スタック メンバーまたはスイッチ スタックに関連した情報を表示するには、**show switch** ユーザ EXEC コマンドを使用します。

```
show switch [stack-member-number | detail | neighbors | stack-ports | stack-ring activity [detail]] [|  
{begin | exclude | include} expression]
```

シンタックスの説明

<i>stack-member-number</i>	(任意) 指定のスタック メンバーの情報を表示します。指定できる範囲は、1 ～ 9 です。
detail	(任意) スタック リングの詳細情報を表示します。
neighbors	(任意) スイッチ スタック全体のネイバを表示します。
stack-ports	(任意) スイッチ スタック全体のポート情報を表示します。
stack-ring activity [detail]	(任意) スタック リングに送信されたフレーム数を、スタック メンバー単位で表示します。Application Specific Integrated Circuit (ASIC; 特定用途向け IC)、受信キュー、およびスタック リングに送信されるスタック メンバー単位のフレーム数を表示するには、 detail キーワードを使用します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	表示が、Switch Database Management (SDM) のミスマッチも含むよう拡張されました。
12.2(20)SE	表示が、プロビジョニング情報も含むよう拡張されました。 stack-ring activity [detail] キーワードが追加されました。

使用上のガイドライン

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。

次に、このコマンドで表示されるステータスを示します。

- **Waiting** — スイッチが起動中で、スタック内にある他のスイッチからの通信を待っているステータス。スイッチはまだスタック マスターであるかどうかを判別していません。
スタック マスター選出に参加していないスタック メンバーは、スタック マスターが選出され準備ができるまで **Waiting** ステータスのままです。
- **Initializing** — スイッチがスタック マスターであるかどうかの判別を完了したステータス。スイッチがスタック マスターでない場合、このスイッチはスタック マスターからシステム レベルおよびインターフェイス レベルのコンフィギュレーションを受信してロードしています。
- **Ready** — スタック メンバーがシステムレベルおよびインターフェイスレベルのコンフィギュレーションのロードを完了し、トラフィックを転送する準備ができているステータス。
- **Master Re-Init** — スタック マスター再選出で、今までと異なるスタック メンバーがスタック マスターに選出された直後のステータス。新しいスタック マスターがそのコンフィギュレーションを再初期化しています。このステータスは、新しいスタック マスターにだけ適用されます。

- **Ver Mismatch** — Version Mismatch (VM) モードのスイッチのステート。VM モードは、スイッチ スタックに加入しているスイッチに、スタック マスターとは異なったスタック プロトコル マイナー バージョン番号がある場合です。
- **SDM Mismatch** — スイッチが SDM ミスマッチ モードにあるステート。SDM ミスマッチは、スタック メンバーがスタック マスターで実行している SDM テンプレートをサポートしていない状態のことです。
- **Provisioned** — 事前設定されたスイッチが、スイッチ スタックのアクティブ メンバーになる前のステート、またはスタック メンバーがスイッチ スタックから脱退したあとのステート。プロビジョニングされたスイッチでは、MAC (メディア アクセス制御) アドレスおよびプライオリティ番号は、常に 0 と表示されます。

スタック メンバー (スタック マスターを含む) の代表的なステート遷移は、Waiting -> Initializing -> Ready です。

スタック マスター選出後のスタック マスターになるスタック メンバーの代表的なステート遷移は、Ready -> Master Re-Init -> Ready です。

VM モードのスタック メンバーの代表的なステート遷移は、Waiting -> Ver Mismatch です。

スイッチ スタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** イネーブル EXEC コマンドでは、この情報が提供されません。

例

次の例では、スイッチ スタックに関する情報のサマリーを表示する方法を示します。

```
Switch> show switch
```

Switch#	Role	Mac Address	Priority	Current State
6	Member	0003.e31a.1e00	1	Ready
*8	Master	0003.e31a.1200	1	Ready
2	Member	0000.000.0000	0	Provisioned

次の例では、スイッチ スタックに関する詳細情報を表示する方法を示します。

```
Switch> show switch detail
```

Switch#	Role	Mac Address	Priority	Current State
2	Member	0000.000.0000	0	Provisioned
6	Member	0003.e31a.1e00	1	Ready
*8	Master	0003.e31a.1200	1	Ready

Switch#	Stack Port Status		Neighbors	
	Port A	Port B	Port A	Port B
6	Down	Ok	None	8
8	Ok	Down	6	None

次の例では、スタック メンバー 6 に関する情報のサマリーを表示する方法を示します。

```
Switch> show switch 6
```

Switch#	Role	Mac Address	Priority	Current State
6	Member	0003.e31a.1e00	1	Ready

次の例では、スイッチ スタックに関するネイバ情報を表示する方法を示します。

```
Switch> show switch neighbors
Switch #      Port A      Port B
-----
      6         None         8
      8          6         None
```

次の例では、スイッチ スタックに関するスタックポート情報を表示する方法を示します。

```
Switch> show switch stack-ports
Switch #      Port A      Port B
-----
      6       Down       Ok
      8        Ok       Down
```

次の例では、スイッチ スタックに関するスタックリングのアクティビティの詳細情報を表示する方法を示します。

```
Switch> show switch stack-ring activity detail
Switch  Asic  Rx Queue-1  Rx Queue-2  Rx Queue-3  Rx Queue-4  Total
-----
1         0    2021864    1228937    281510         0    3532311
1         1         52         0      72678         0     72730
-----
Switch 1 Total:    3605041
-----
2         0    2020901     90833    101680         0    2213414
2         1         52         0         0         0         52
-----
Switch 2 Total:    2213466
-----
```

Total frames sent to stack ring : 5818507

Note: these counts do not include frames sent to the ring
by certain output features, such as output SPAN and output
ACLs.

関連コマンド

コマンド	説明
reload	スタック メンバーをリロードし、設定の変更を有効にします。
remote command session	すべてまたは指定のスタック メンバーをモニタします。
switch priority	特定のスタック メンバーにアクセスします。
switch provision	スタック メンバーのプライオリティ値を変更します。
switch renumber	新しいスイッチがスイッチ スタックに加入する前に、プロビジョニングします。
switch renumber	スタック メンバー番号を変更します。

show system mtu

スイッチのグローバル Maximum Transmission Unit (MTU; 最大伝送ユニット) または最大パケットサイズ セットを表示するには、**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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 の設定を変更した場合、スイッチをリセットしないかぎり、新しい設定は有効になりません。

システムの MTU は、10/100 Mbps (メガビット / 秒) で動作しているポートを基準としています。システムのジャンボ MTU の場合、ギガビット ポートが基準となり、システム ルーティング MTU の場合、ルーテッド ポートが基準となります。

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
Routing MTU size is 1500 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) の管理上および運用上のステータスを表示するには、**show udld** ユーザ EXEC コマンドを使用します。

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>interface-id</i>	(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は、物理ポートおよび VLAN (仮想 LAN) です。指定できる VLAN 範囲は 1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

interface-id 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。ここでは、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 UDLD が検出します。表 2-32 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 udld gigabitethernet2/0/1
Interface gi2/0/1
---
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: Gi2/0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi2/0/2
    Message interval: 5
    CDP Device name: Switch-A
```

表 2-32 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装置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 非対応装置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 対応装置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	UDLD ステート マシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステート マシンはアダプタイズ フェーズです。
Message interval	ローカル装置からアダプタイズ 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。ローカル装置および近接装置の両方で UDLD が正常に稼働している場合、ネイバステートおよびローカルステートは bidirectional 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	ネイバの装置名またはシステム シリアル番号。装置名が設定されていない場合や、デフォルトの設定 (スイッチ) の場合、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近接装置名
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	ネイバがアダプタイズ メッセージを送信する速度 (秒)
CDP device name	Cisco Discovery Protocol (CDP) 装置名またはシステム シリアル番号。装置名が設定されていない場合や、デフォルトの設定 (スイッチ) の場合、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 のアグレッシブまたはノーマル モードをイネーブルにします。また、設定可能なメッセージ タイマー時間を設定します。
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されるのを防ぎます。
udld reset	UDLD により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*]

シンタックスの説明

 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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) *configuration register* 情報は **show version** の出力には表示されますが、スイッチではサポートされていません。

```
Switch> show version
Cisco Internetwork Operating System Software
IOS (tm) C3750 Software (C3750-IPSERVICES-M), Version 12.2(25)SEB, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Tues 15-Feb-05 21:09 by antonino
Image text-base: 0x00003000, data-base: 0x008E36A4
```

```
ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25)SEB,
```

```
Switch uptime is 2 days, 11 hours, 16 minutes
System returned to ROM by power-on
System image file is "flash:i5.709"
```

```
cisco WS-C3750-48TS (PowerPC405) processor with 120822K/10240K bytes of memory.
Last reset from power-on
Bridging software.
Target IOS Version 12.2(25)SEB
1 Virtual Ethernet/IEEE 802.3 interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
32 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is enabled.
```

```
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:09:43:A7:F2:00
Motherboard assembly number     : 73-7056-05
Motherboard serial number       : CSJ0638004U
Motherboard revision number     : 05
Model number                    : 73-7056-05
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
1	28	WS-C3750G-24TS	12.2(25)SEB	C3750-IPSERVICES-M
*	8 52	WS-C3750-48TS	12.2(25)SEB	C3750-IPSERVICES-M

```
Switch 01
-----
```

```
Switch Uptime                : 2 days, 11 hours, 17 minutes
Base ethernet MAC Address     : 00:0B:46:2E:35:80
Motherboard assembly number   : 73-7058-04
Power supply part number      : 341-0045-01
Motherboard serial number     : CSJ0640010L
Model number                  : WS-C3750-24TS-SMI
System serial number          : CSJ0642U00A
```

```
Configuration register is 0xF
```

(テキスト出力は省略)

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 | dot1q tag native | id vlan-id | internal usage | mtu | name vlan-name | private-vlan
[type] | remote-span | summary] [ {begin | exclude | include} expression]
```

シンタックスの説明

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。
dot1q tag native	(任意) IEEE（米国電気電子学会）802.1Q ネイティブ VLAN のタギングステータスを表示します。
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。 <i>vlan-id</i> では、指定できる範囲は 1 ～ 4094 です。
internal usage	(任意) スイッチが内部的に使用する VLAN のリストを表示します。内部的に使用されている VLAN は常に拡張範囲 VLAN (ID が 1006 ～ 4094) になります。 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、内部的に使用されている ID で VLAN を作成するには、まず内部的に使用されている VLAN を削除します。
mtu	(任意) VLAN のリスト、および VLAN 内のポートで設定された最小および Maximum Transmission Unit (MTU; 最大伝送ユニット) 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。
private-vlan	(任意) プライマリおよびセカンダリ VLAN ID、タイプ（コミュニティ、独立、またはプライマリ）、およびプライベート VLAN に属するポートを含む、設定済みのプライベート VLAN の情報を表示します。このキーワードは、スイッチで IP サービス イメージが稼働している場合に限りサポートされます。IP サービス イメージは、以前は Enhanced Multilayer Image (EMI) と呼ばれていました。
type	(任意) プライベート VLAN の ID およびタイプのみを表示します。
remote-span	(任意) Remote SPAN (RSPAN) 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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 キーワードは、コマンドラインのヘルプ スtring 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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	mtu および private-vlan キーワードが追加されました。
12.2(25)SE	dot1q tag native キーワードが追加されました。

使用上のガイドライン

show vlan mtu コマンドの出力では、MTU_Mismatch カラムは VLAN 内のすべてのポートで MTU が同じかどうかを示しています。このカラムで *yes* が表示される場合は、VLAN 内のポートで MTU が異なるという意味で、MTU サイズが大きい方のポートから小さい方のポートにスイッチされたパケットは、廃棄される可能性があります。VLAN に Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) がない場合は、SVI_MTU カラムにハイフン (-) が表示されます。MTU-Mismatch カラムで *yes* が表示される場合は、MinMTU というポート名および MaxMTU というポート名が表示されます。

プライベート VLAN のセカンダリ VLAN をプライマリ VLAN と関連付けてから、セカンダリ VLAN を定義する場合、**show vlan private-vlan** コマンドの出力にセカンダリ VLAN は含まれません。

show vlan private-vlan type コマンドの出力では、*normal* と表示されるタイプは、プライベート VLAN のアソシエーションはありますが、プライベート VLAN に含まれていないことを意味します。たとえば、2 つの VLAN をプライマリ VLAN とセカンダリ VLAN として定義し、関連付けてから、プライマリ VLAN のアソシエーションを削除せずにセカンダリ VLAN コンフィギュレーションを削除した場合、セカンダリ VLAN であった VLAN は、*normal* として表示されます。**show vlan private-vlan** の出力では、プライマリおよびセカンダリ VLAN のペアは *non-operational* として表示されます。

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 vlan** コマンドの出力を示します。表 2-33 に、表示される各フィールドの説明を示します。

```
Switch> show vlan
VLAN Name                Status    Ports
-----
1    default                active    Fa1/0/1, Fa1/0/2, Fa1/0/3
                                           Fa1/0/4, Fa1/0/5, Fa1/0/6
                                           Fa1/0/7, Fa1/0/8, Fa1/0/9
                                           Fa1/0/10, Fa1/0/11, Fa1/0/12
                                           Fa1/0/13, Fa1/0/14, Fa1/0/15
                                           Fa1/0/16, Fa1/0/17, Fa1/0/18
                                           Fa1/0/19, Fa1/0/20, Fa1/0/21
                                           Fa1/0/24, Gi1/0/1, Gi1/0/2

(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
-----

Primary Secondary Type Ports
-----
20      25      isolated Fa1/0/13, Fa1/0/20, Fa1/0/22, Gi1/0/1, Fa2/0/13, Fa2/0/22,
                                           Fa3/0/13, Fa3/0/14, Fa3/0/20, Gi3/0/1
20      30      community Fa1/0/13, Fa1/0/20, Fa1/0/21, Gi1/0/1, Fa2/0/13, Fa2/0/20,
                                           Fa3/0/14, Fa3/0/20, Fa3/0/21, Gi3/0/1
20      35      community Fa1/0/13, Fa1/0/20, Fa1/0/23, Fa1/0/33, Gi1/0/1, Fa2/0/13,
                                           Fa3/0/14, Fa3/0/20, Fa3/0/23, Fa3/0/33, Gi3/0/1

(テキスト出力は省略)
```

表 2-33 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（名前が設定されている場合）
Status	VLAN のステータス（active または suspend）
Ports	VLAN に属するポート
Type	VLAN のメディア タイプ

表 2-33 show vlan コマンドの出力フィールド (続き)

フィールド	説明
SAID	VLAN のセキュリティ アソシエーション ID 値
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)
BrdgNo	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
Trans2	トランスレーションブリッジ 2
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。
Primary/Secondary/Type/Ports	設定されている任意のプライベート VLAN (プライマリ VLAN ID、セカンダリ VLAN ID、セカンダリ VLAN のタイプ [コミュニティ または独立]、およびそれに属するポートを含む) を含みます。

次の例では、**show vlan dot1q tag native** コマンドの出力を示します。

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

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

```
Switch> show vlan private-vlan
Primary Secondary Type Ports
-----
10      501      isolated      Gi3/0/3
10      502      community     Fa2/0/11
10      503      non-operational3 -
20      25       isolated      Fa1/0/13, Fa1/0/20, Fa1/0/22, Gi1/0/1, Fa2/0/13,
Fa2/0/22, Fa3/0/13, Fa3/0/14, Fa3/0/20, Gi3/0/1
20      30       community     Fa1/0/13, Fa1/0/20, Fa1/0/21, Gi1/0/1, Fa2/0/13,
Fa2/0/20, Fa3/0/14, Fa3/0/20, Fa3/0/21, Gi3/0/1
20      35       community     Fa1/0/13, Fa1/0/20, Fa1/0/23, Fa1/0/33, Gi1/0/1,
Fa2/0/13, Fa3/0/14, Fa3/0/20, Fa3/0/23, Fa3/0/33,
Gi3/0/1
20      55       non-operational
2000    2500     isolated      Fa1/0/5, Fa1/0/10, Fa2/0/5, Fa2/0/10, Fa2/0/15
```

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

```
Switch> show vlan private-vlan type
Vlan Type
-----
10      primary
501     isolated
502     community
503     normal
```

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    Fa1/0/7, Fa1/0/8

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
2    enet    100002   1500    -      -      -      -      -      0      0

Remote SPAN VLAN
-----
Disabled
```

次の例では、**show vlan internal usage** コマンドの出力を示します。VLAN 1025 および 1026 は、スタック メンバー 1 上のファスト イーサネットのルーテッド ポート 23 および 24 で、内部 VLAN として使用されています。これらの VLAN ID のうちの 1 つを使用する場合、まずルーテッド ポートをシャットダウンする必要があります。これで内部の VLAN は解放されるため、拡張範囲 VLAN を作成できます。ルーテッド ポートを開始すると、他の内部 VLAN 番号が割り当てられます。

```
Switch> show vlan internal usage
VLAN Usage
-----
1025 FastEthernet1/0/23
1026 FastEthernet1/0/24
```

関連コマンド

コマンド	説明
private-vlan	VLAN をコミュニティ、独立、またはプライマリ VLAN として設定するか、またはプライマリ VLAN をセカンダリ VLAN と関連付けします。
switchport mode	ポートの VLAN 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 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 vlan access-map

特定の VLAN（仮想 LAN）アクセス マップまたはすべての VLAN アクセス マップの情報を表示するには、**show vlan access-map** イネーブル EXEC コマンドを使用します。

```
show vlan access-map [mapname] [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>mapname</i>	(任意) 特定の VLAN アクセス マップ名
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 access-map** コマンドの出力を示します。

```
Switch# show vlan access-map
Vlan access-map "SecWiz" 10
  Match clauses:
    ip address: SecWiz_Fa10_3_in_ip

  Action:
    forward
```

関連コマンド

コマンド	説明
show vlan filter	すべての VLAN フィルタリングの情報、特定の VLAN または VLAN アクセス マップの情報を表示します。
vlan access-map	VLAN パケット フィルタリング用の VLAN マップのエントリを作成します。
vlan filter	VLAN マップを 1 つまたは複数の VLAN に適用します。

show vlan filter

すべての VLAN（仮想 LAN）のフィルタリングの情報、特定の VLAN または VLAN アクセス マップの情報を表示するには、**show vlan filter** イネーブル EXEC コマンドを使用します。

show vlan filter [*access-map name* | *vlan vlan-id*] [| {*begin* | *exclude* | *include*} *expression*]

シンタックスの説明

access-map name	(任意) 指定の VLAN アクセス マップのフィルタリング情報を表示します。
vlan vlan-id	(任意) 指定の VLAN のフィルタリング情報を表示します。指定できる範囲は、1 ～ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 filter** コマンドの出力を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

関連コマンド

コマンド	説明
show vlan access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップの情報を表示します。
vlan access-map	VLAN パケット フィルタリング用の VLAN マップのエントリを作成します。
vlan filter	VLAN マップを 1 つまたは複数の VLAN に適用します。

show vmps

VLAN (仮想 LAN) Query Protocol (VQP) バージョン、再確認間隔、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** ユーザ 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]

シンタックスの説明

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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 2-34 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 2-34 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	VLAN Management Policy Server (VMPS; VLAN マネジメント ポリシー サーバ) 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 の応答がアドレスを拒否した場合、そのアドレスでワークステーションとのフレーム伝送は実行されません（ポートが VLAN に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 フレームがワークステーションに対して配信されます）。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 VMPS 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 VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) 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]

シンタックスの説明

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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	password キーワードが追加されました。

使用上のガイドライン

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 2-35 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
Fal1/0/47	0	0	0
Fal1/0/48	0	0	0
Gi2/0/1	0	0	0
Gi3/0/2	0	0	0

表 2-35 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、管理ドメイン名、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 (仮想 LAN) 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 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、管理ドメイン名、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 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ごとに、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ごとに、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。

表 2-35 show vtp counters のフィールドの説明（続き）

フィールド	説明
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、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。
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装置からの 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 2-36 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 2-36 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	ローカルでサポートされている VLAN の最大数
Number of Existing VLANs	既存の VLAN 数

表 2-36 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 (Server、Client、または Transparent) を表示します。 Server — 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。 Client — 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。 Transparent — 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、他の装置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装置の 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	ブ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 サーバでブルーニングをイネーブルにすると、管理ドメイン全体でブルーニングが有効になります。ブ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ドイ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 装置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
<code>clear vtp counters</code>	VTP およびプルーニング カウンタを消去します。
<code>vtp</code> (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。
<code>vtp</code> (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ディセーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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。ディセーブル状態のインターフェイスを再開するには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ポートはイネーブルです（シャット ダウンされていません）。

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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン ポートに **shutdown** コマンドを入力すると、転送が停止されます。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 コマンドは指定のインターフェイス上のすべての機能をディセーブルにします。

また、このコマンドはインターフェイスを利用できない状態としてマーキングします。インターフェイスがディセーブルかどうかを確認するには、**show interfaces** イネーブル EXEC コマンドを使用します。シャットダウンされたインターフェイスは、管理上のダウンとして画面に表示されます。

例 次の例では、ポートをディセーブルにし、次に再びイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet1/0/2
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に対する統計情報を表示します。

shutdown vlan

指定の VLAN（仮想 LAN）上のローカル トラフィックをシャットダウン（中断）するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 トラフィックを再開するには、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*

シンタックスの説明

<i>vlan-id</i>	ローカルにシャットダウンする VLAN の ID です。使用できる範囲は 2 ～ 1001 です。VLAN Trunking Protocol（VTP; VLAN トランクキング 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（ID が 1005 を超える VLAN）は、シャットダウンできません。デフォルトの 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

shutdown 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。ローカル トラフィックはシャットダウンされますが、スイッチは VTP 情報をアドバタイズします。

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 <i>vlan-id</i> 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

スイッチで、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）通知の送信、または Network Management System（NMS; ネットワーク管理システム）への要求の通知をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 [bgp | bridge [newroot] [topologychange] | cluster | config | copy-config | entity | envmon [fan | shutdown | status | supply | temperature] | flash [insertion | removal] | fru-ctrl | 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 [bgp | bridge [newroot] [topologychange] | cluster | config | copy-config | entity | envmon [fan | shutdown | status | supply | temperature] | flash [insertion | removal] | fru-ctrl | 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]

シンタックスの説明

bgp (任意) Border Gateway Protocol (BGP) ステータス変更トラップをイネーブルにします。



(注)

このキーワードは、IP サービス イメージがスタック マスターにインストールされている場合にのみ使用できます。

bridge [newroot]
[topologychange] (任意) Spanning-Tree Protocol (STP; スパニングツリー プロトコル) ブリッジ MIB（管理情報ベース）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 ブリッジ 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 ブリッジ 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) 環境モニタ電源装置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 [insertion removal]	(任意) SNMP FLASH 通知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。 insertion — (任意) スイッチ (フラッシュ) がスタックに挿入されると (物理的に、パワー サイクルが原因で、またはリロードを実行したため)、トラップを生成します。 removal — (任意) スイッチ (フラッシュ) がスタックから取り外されると (物理的に、パワー サイクルが原因で、またはリロードを実行したため)、トラップを生成します。
fru-ctrl	(任意) エンティティ Field-Replaceable Unit (FRU) 制御トラップを生成します。Catalyst 3750 スイッチ スタックでは、このトラップはスタックに対するスイッチの挿入または取り外しを意味します。
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) シスコ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) 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) パケット再送信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; ランデブーポイント) 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。秒単位で送信され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。デフォルトは 0 (制限はなく、トラップが発生するたびに送信) です。
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 <i>value</i>	(任意) ストーム制御トラップをイネーブルにします。秒単位で送信され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。デフォルトは 0 (制限はなく、トラップが発生するたびに送信) です。
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。デフォルトはイネーブルです。
vlan-membership	(任意) SNMP VLAN 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 トランッキング プロトコル) トラップをイネーブルにします。



(注)

cpu [threshold] キーワードは、コマンドラインのヘルプ スtring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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	bgp 、 copy-config 、 envmon 、 flash 、 port-security 、 stpx 、 syslog 、 vlancreate 、 vlandelete キーワードが追加されました。
12.2(18)SE	ipmulticast 、 msdp 、 ospf [cisco-specific errors lsa rate-limit retransmit state-change]、 pim [invalid-pim-message neighbor-change rp-mapping-change]、 tty キーワードが追加されました。
12.2(25)SE	storm-control trap-rate value キーワードが追加されました。

使用上のガイドライン

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 コマンドがサポートされている場合、このコマンドを使用して、トラップまたは情報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** イネーブル EXEC コマンド、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、スイッチ スタックまたはスタンドアロン スイッチ上で **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
```

シンタックスの説明

<i>host-addr</i>	ホストの名前またはインターネット アドレス（ターゲットとなる受信側）です。
udp-port <i>port</i>	（任意）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。
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される SNMP のバージョン 次のキーワードがサポートされています。 1 — SNMPv1. informs を指定した場合は、このオプションを使用できません。 2c — SNMPv2C 3 — SNMPv3. 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） — DES（データ暗号化規格）によるパケット暗号化（<i>privacy</i> と呼ばれる）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のみ利用可能です。	
vrf <i>vrf-instance</i>	（任意）Virtual Private Network（VPN; 仮想私設網）ルーティング インスタンスおよびこのホストの名前

<i>community-string</i>	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tring です。 snmp-server host コマンドを使用してこの String を設定できますが、この String 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。
<i>notification-type</i>	(任意) ホストに送信する通知のタイプ。タイプを指定しない場合、すべての通知が送信されます。通知タイプは次のうち、1 つまたは複数のキーワードになることができます。 • bgp — Border Gateway Protocol (BGP) ステート変更トラップを送信します。このキーワードは、IP サービス イメージがスタック マスターにインストールされている場合にのみ使用できます。 • bridge — SNMP Spanning-Tree Protocol (STP; スパニングツリー プロトコル) ブリッジ MIB (管理情報ベース) 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 — 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。 • fru-ctrl — エンティティ Field-Replaceable Unit (FRU) 制御トラップを送信します。スイッチ スタックでは、このトラップはスタックに対するスイッチの挿入 / 取り外しを意味します。 • 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 (メディア アクセス制御) 通知トラップを送信します。 • msdp — SNMP Multicast Source Discovery Protocol (MSDP) トラップを送信します。 • ospf — Open Shortest Path First (OSPF) トラップを送信します。 • pim — SNMP Protocol-Independent Multicast (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 トランッキング プロトコル) トラップを送信します。



(注)

cpu キーワードは、コマンドラインのヘルプ スtring 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

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	bgp 、 copy-config 、 flash 、 port-security 、 stpx 、 syslog 、 vlancreate 、 vlandelete キーワードが追加されました。
12.2(18)SE	ipmulticast 、 msdp 、 ospf 、 pim キーワードが追加されました。コマンドの構文が変更されました。
12.2(25)SE	storm-control および vrf vrf-instance キーワードが追加されました。

使用上のガイドライン

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断できません。ただし、情報要求を受信した SNMP エンティティは、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) 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、再び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できます。

ローカル ユーザがリモート ホストに関連付けられていない場合、スイッチからは、**auth** (authNoPriv) および **priv** (authPriv) 認証レベルの情報は送信されません。

同じホストおよび同じ種類の通知に対して複数の **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 番目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。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。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tring *comaccess* を設定し、この String 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* という名前が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 String 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 String *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のインターフェイスで、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、スイッチ スタックまたはスタンドアロン スイッチ上で **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}

シンタックスの説明

added	MAC アドレスがインターフェイスに追加されるたびに、MAC 通知トラップをイネーブルにします。
removed	MAC アドレスがインターフェイスから削除されるたびに、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、アドレス追加および削除に対するトラップは両方ディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、MAC アドレスがポートに追加されたときに 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 gigabitethernet1/0/2
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ると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+)、または Multiple Spanning-Tree (MST) モードの BackboneFast 機能を設定できますが、この機能はスパニングツリー モードを PVST + に変更するまでは、ディセーブル (非アクティブ) のままです。

スイッチ上のルート ポートまたはブロックド ポートが指定のスイッチから下位 Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) を受信すると、BackboneFast が開始されます。下位 BPDU は、1 台のスイッチがルート ブリッジと指定スイッチの両方を宣言しているとして識別します。スイッチが下位 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、下位 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。その後、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設定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 bpdupfilter

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、スイッチ スタックまたはスタンドアロン スイッチ上で **spanning-tree bpdupfilter** インターフェイス 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 bpdupfilter {disable | enable}

no spanning-tree bpdupfilter

シンタックスの説明

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スイッチが 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 bpdupfilter 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 bpdupfilter 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 bpdupfilter** インターフェイス 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 gigabitethernet2/0/1
Switch(config-if)# spanning-tree bpdupfilter 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
<code>show running-config</code>	現在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。
<code>spanning-tree portfast</code> (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。
<code>spanning-tree portfast</code> (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 (仮想 LAN) 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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ンニングツリー トポロジ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 gigabitethernet2/0/1
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。
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 (仮想 LAN) 上で、PortFast 機能をイネーブルにします。

spanning-tree cost

スパニングツリーの計算に使用するパス コストを設定するには、スイッチ スタックまたはスタン
ドアロン スイッチ上で **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 コストを考慮して、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

シンタックスの説明

vlan <i>vlan-id</i>	(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。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
<i>cost</i>	パス コスト。使用できる範囲は 1 ～ 2000000000 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 (米国電気電
子学会) 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	<i>vlan-id</i> 変数の値が変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

spanning-tree vlan *vlan-id* cost *cost* コマンドおよび **spanning-tree cost *cost*** コマンドの両方を使用して
インターフェイスを設定する場合、**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、ポート上でパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ～ 15、20 にパス コストとして 300 を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
<code>show spanning-tree</code> <code>interface</code> <i>interface-id</i>	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。
<code>spanning-tree port-priority</code>	インターフェイス プライオリティを設定します。
<code>spanning-tree vlan</code> <i>priority</i>	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

スイッチで EtherChannel の設定不良が検出された場合にエラー 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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト EtherChannel ガードはスイッチ上でイネーブルです。

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
	12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン スイッチで EtherChannel の設定不良が検出されると、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.
```

設定不良の EtherChannel 内にあるスイッチ 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。リモート装置で EtherChannel の設定を確認するには、リモート装置上で **show etherchannel summary** イネーブル EXEC コマンドを使用します。

EtherChannel の設定不良のためにポートが errdisable ステートとなっている場合は、**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、手動で再びイネーブルにできます。

例 次の例では、EtherChannel ガード設定不良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 設定不良 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	チャネルの EtherChannel 情報を、チャネルグループごとに 1 行のサマリーで表示します。
	show interfaces status err-disabled	errdisable ステートのインターフェイスを表示します。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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tring 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。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スイッチは IEEE（米国電気電子学会）802.1t スパニングツリー拡張をサポートしています。スイッチのプライオリティで以前使用されていたビットの一部は、現在拡張システム ID として使用されています（Per-VLAN Spanning-Tree Plus [PVST+] および Rapid-PVST の VLAN（仮想 LAN）ID、または Multiple Spanning-Tree [MST] のインスタンス ID）。

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。Catalyst 3750 スイッチ スタックは他のネットワークからは単一のスイッチとして認識されるため、スタック内のすべてのスイッチは、指定のスパニングツリーに対して同一のブリッジ ID を使用します。スタック マスターに障害が発生した場合、スタック メンバーはスタック マスターの新しい MAC アドレスに基づいて、実行しているスパニングツリーすべてのブリッジ ID を再計算します。

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とんどありません。拡張システム ID によって、接続された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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スイッチが 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 ガード機能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。ただし、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 ステート（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+ 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+ 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のみ、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、指定の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 gigabitethernet2/0/2
Switch(config-if)# spanning-tree guard root
```

次の例では、指定の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 gigabitethernet2/0/2
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。
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、フォワーディング ステートへの Rapid Spanning-Tree (RST) 移行をイネーブルにするには、スイッチスタックまたはスタンドアロンスイッチ上で **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

シンタックスの説明

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見なされ、半二重インターフェイスは共有リンクであると見なされます。

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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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、Multiple Spanning-Tree Protocol (MSTP) や Rapid Per-VLAN Spanning-Tree Plus (Rapid-PVST+) プロトコルが動作するリモート スイッチ上の単一インターフェイスに半二重リンクを物理的にポイントツーポイントで接続し、高速移行をイネーブルにできます。

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び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状態の情報を表示します。
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、単方向リンクを発生させる障害が原因で指定ポートになることを防ぐには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン スイッチが 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+ 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のみ、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する方法を示します。

```
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
<code>show running-config</code>	現在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。
<code>spanning-tree guard loop</code>	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 (仮想 LAN) 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

mst	MST および Rapid Spanning-Tree Protocol (RSTP) をイネーブルにします (IEEE [米国電気電子学会] 802.1s および IEEE 802.1w に準拠)。
pvst	PVST+ をイネーブルにします (IEEE 802.1D に準拠)。
rapid-pvst	Rapid-PVST+ をイネーブルにします (IEEE 802.1w に準拠)。

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	mst および rapid-pvst キーワードが追加されました。

使用上のガイドライン

スイッチは PVST+、Rapid-PVST+、および MSTP をサポートしています。ただし、アクティブにする場合、1 度に 1 つのバージョンのみ可能です (つまりすべての VLAN [仮想 LAN] が PVST+、Rapid-PVST+、または MSTP のいずれかを実行)。すべてのスタック メンバーは同一のスパニング ツリー バージョンを実行しています。

MST モードをイネーブルにした場合、RSTP が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を停止し、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 および 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。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SEC	指定できる <i>instance-id</i> の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

spanning-tree mst configuration コマンドを入力すると、MST コンフィギュレーション モードが開始されます。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**: コンフィギュレーションの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、すべてのコンフィギュレーションの変更を適用します。
- **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。*vlan-range* に指定できる範囲は 1 ～ 4094 です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。
- **name *name***: コンフィギュレーション名を設定します。*name* スtring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** コマンドを無効にするか、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tringには表示されていますが、サポートされていません。
- **revision *version***: コンフィギュレーション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 MST または変更適用前の MST リージョン コンフィギュレーションを表示します。

MST モードでは、スイッチ スタックは最大 65 の MST インスタンスまでサポートします。特定の MST インスタンスにマッピング可能な 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場合、マッピングは徐々に実行され、コマンドで指定された VLAN が以前マッピングされた VLAN に対して追加または削除されます。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、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。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、同じコンフィギュレーション 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、コンフィギュレーション リビジョンを 1 に設定し、変更適用前のコンフィギュレーションを表示し、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  Vlan  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) の計算に使用するパス コストを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 コストを考慮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

シンタックスの説明

<i>instance-id</i>	スパニングツリー インスタンスの範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切っ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。
<i>cost</i>	パス コストの範囲は 1 ～ 2000000000 です。値が大きいくほど、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（米国電気電子学会）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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SEC	指定できる <i>instance-id</i> の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいく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 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 gigabitethernet1/0/2
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、スイッチ スタックまたはスタンドアロン スイッチ上で、**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決定します。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

シンタックスの説明	<i>seconds</i>	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
	12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン	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、スイッチ スタックまたは スタンドアロン スイッチ上で **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

シンタックスの説明

<i>seconds</i>	ルート スイッチ コンフィギュレーション メッセージで送信される 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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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、指定された間隔以内でルート 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

<i>seconds</i>	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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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、指定された間隔以内でルート 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 MST インスタンスについて、スパニングツリー有効期限を 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) が廃棄されて、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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明	<i>hop-count</i>	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
	12.1(14)EA1	このコマンドが導入されました。
	12.2(25)SEC	指定できる <i>hop-count</i> が範囲は 1 ～ 255 に変更されました。

使用上のガイドライン	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 プライオリティを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

<i>instance-id</i>	スパニングツリー インスタンスの範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切っ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。
<i>priority</i>	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、240 です。それ以外の値はすべて拒否されます。数値が低ければ低いほど、プライオリティは高くなります。

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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SEC	指定できる <i>instance-id</i> の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

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。

スイッチがスイッチ スタックのメンバーの場合、**spanning-tree mst [instance vlan-id] port-priority priority** インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst [instance-id] cost 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、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なければなりません。低いコスト値を最初に選択する必要があるインターフェイスに割り当て、高いコスト値を最後に選択させるインターフェイスに割り当てます。

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 gigabitethernet2/0/2
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
<code>show spanning-tree mst interface interface-id</code>	特定のインターフェイスの MST 情報を表示します。
<code>spanning-tree mst cost</code>	MST の計算に使用するパス コストを設定します。
<code>spanning-tree mst priority</code>	指定したスパンニングツリー 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

ポートがプレスタンダード Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) だけを送信するように設定するには、**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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト設定 デフォルト状態は、プレスタンダード 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)SEC	このコマンドが導入されました。

使用上のガイドライン

ポートでは、プレスタンダードおよびスタンダード BPDU のいずれも受け付けます。ネイバ タイプが一致しない場合、Common and Internal Spanning Tree (CIST) だけがこのインターフェイス上で実行されます。



(注)

スイッチ ポートがプレスタンダード Cisco IOS ソフトウェアを実行するスイッチに接続されている場合、そのポートで **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。ポートでプレスタンダード BPDU だけを送信するように設定していない場合、Multiple Spanning Tree Protocol (MSTP) の性能が低下することもあります。

ポートでプレスタンダード ネイバを自動検出するように設定している場合、**show spanning-tree mst** コマンドには常に *prestandard* フラグが表示されます。

例 次の例は、プレスタンダード BPDU だけ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	指定したインターフェイスの Multiple Spanning-Tree (MST) 情報を、 <i>prestandard</i> フラグも含めて表示されます。

spanning-tree mst priority

指定のスパニングツリーのインスタンスにスイッチのプライオリティを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

<i>instance-id</i>	スパニングツリー インスタンスの範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切っ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、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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SEC	指定できる <i>instance-id</i> 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 および 21 に対し、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 <i>instance-id</i>	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た Multiple Spanning-Tree (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 **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
```

シンタックスの説明

<i>instance-id</i>	スパニングツリー インスタンスの範囲。1つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切っ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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

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 プライオリティを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

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。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
priority	使用できる番号は 0 ～ 240 で、16 ずつ増加します。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。数値が低ければ低いほど、プライオリティは高くなります。

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	<i>vlan-id</i> 変数の値が変更されました。プライオリティ範囲の値が変更されました。

使用上のガイドライン

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。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。

インターフェイスを、**spanning-tree vlan vlan-id port-priority priority** コマンドおよび **spanning-tree port-priority priority** コマンドを両方使用して設定する場合、**spanning-tree vlan vlan-id port-priority priority** コマンドが有効になります。

スイッチがスイッチ スタックのメンバーの場合、**spanning-tree [vlan vlan-id] port-priority priority** インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree [vlan vlan-id] cost 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、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なければなりません。低いコスト値を最初を選択する必要があるインターフェイスに割り当て、高いコスト値を最後に選択させるインターフェイスに割り当てます。

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 ステートになる確率を高める方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

次の例では、VLAN 20 ～ 25 の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 <i>interface interface-id</i>	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 対応の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) のフィルタリングおよび BPDU ガード機能をグローバルにイネーブルにしたり、また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 **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 {bpdupfilter default | bpduguard default | default}

no spanning-tree portfast {bpdupfilter default | bpduguard default | default}

シンタックスの説明

bpdupfilter 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。その場合に、中間のスパニングツリー ステートには変わりません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

スイッチが 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に、これらの機能をイネーブルにできます。

spanning-tree portfast bpdupfilter 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 bpdupfilter 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 bpdupfilter** インターフェイス 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。

spanning-tree portfast default グローバル コンフィギュレーション コマンドは、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 ループが原因でデータ 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ポート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 bpduguard 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
<code>show running-config</code>	現在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。
<code>spanning-tree bpduguard</code>	インターフェイスが BPDU を送受信しないようにします。
<code>spanning-tree bpduguard</code>	BPDU を受信したインターフェイスを、errdisable ステートにします。
<code>spanning-tree portfast (インターフェイス コンフィギュレーション)</code>	対応するすべての VLAN (仮想 LAN) 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)

関連するすべての VLAN (仮想 LAN) 内の特定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、スイッチ スタックまたはスタンドアロン スイッチ上で **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。その場合に、中間のスパニングツリー ステートには変わりません。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

シンタックスの説明

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

この機能は、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 ループが原因でデータ 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 ポート上で 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 コマンドを使用します。トランク ポートでは、**spanning-tree portfast** コマンドはサポートされていません。

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に、こ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 機能をディセーブルにできます。

例

次の例では、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 gigabitethernet2/0/2
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。
spanning-tree bpdupfilter	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

1 秒間に送信される Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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*]

シンタックスの説明	<i>value</i>	(任意) 1 秒間に送信される 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)SEC	このコマンドが導入されました。

使用上のガイドライン	スイッチが rapid-per-VLAN spanning-tree plus (rapid-PVST+) モードの場合、transmit hold-count の値を増やすと CPU 使用率が大きな影響を受けます。値を小さくするとコンバージェンスが緩やかになります。デフォルト設定の使用を推奨します。

例	次の例では、送信ホールド回数を 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	Multiple Spanning-Tree (MST) のリージョン設定およびステータスを、送信ホールド回数も含めて表示します。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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*]

シンタックスの説明

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	max-update-rate キーワードが追加されました。

使用上のガイドライン

このコマンドは、アクセス スイッチ上だけで使用します。

Rapid PVST+、または MST モードの UplinkFast 機能を設定できますが、この機能はスパニングツリー モードを PVST+ に変更するまでは、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 をイネーブルまたはディセーブルにすると、すべての非スタック ポートのインターフェイス上で、Cross-Stack UplinkFast (CSUF) も自動的にイネーブルまたはディセーブルになります。CSUF は、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。

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、すべての VLAN のスイッチ プライオリティとすべての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 ポートに切り替えて、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 機能を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。ただし、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 機能を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** ステート（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) ベースでスパニングツリーを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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]
```

シンタックスの説明

<i>vlan-id</i>	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。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は、1 ～ 4094 です。
forward-time <i>seconds</i>	(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決定します。指定できる範囲は 4 ～ 30 秒です。
hello-time <i>seconds</i>	(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 <i>seconds</i>	(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 <i>priority</i>	(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、スタンドアロン スイッチまたはスタック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、61440 です。それ以外の値はすべて拒否されます。
root <i>primary</i>	(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 <i>secondary</i>	(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 <i>net-diameter</i>	(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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	<i>vlan-id</i> 変数の値が変更されました。

使用上のガイドライン

Spanning-Tree Protocol (STP; スパニングツリー プロトコル) 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 はループの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 をディセーブルまたは再びイネーブルにする場合、ディセーブルまたはイネーブルにする VLAN の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できます。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。

max-age seconds を設定すると、指定された間隔以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 および 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 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

10/100 Mbps（メガビット / 秒）ポートまたは 10/100/1000 Mbps ポートの速度を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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** または **default** 形式を使用します。

```
speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}
```

```
no speed
```

シンタックスの説明

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 ポート上でのみ有効で、表示されます。
auto	ポートが自動的に、もう一方のリンクの終端ポートを基準にして速度を検出します。 auto キーワードと一緒に 10 、 100 、または 1000 キーワードを使用する場合、ポートは指定された速度でのみオートネゴシエートします。
nonegotiate	自動ネゴシエーションはディセーブルになり、ポートは 1000 Mbps で動作します。

デフォルト

デフォルトの設定は **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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE1	auto キーワードと一緒に 10 、 100 、 1000 キーワードのサポートが追加されました。

使用上のガイドライン

10 ギガビット イーサネット ポートでは速度を設定できません。

1000BASE-T SFP モジュールをのぞき、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ない装置に接続されている場合、速度をネゴシエートしない (**nonegotiate**) に設定できます。

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にある終端の装置と速度設定についてネゴシエートし、ネゴシエートされた値に強制的に速度を設定します。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。

回線の両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、サポートされている側で **auto** の設定を使用し、もう一方のインターフェイス上でデュプレックスと速度を設定してください。



注意

インターフェイスの速度およびデュプレックス モードの設定を変更することで、再設定の間、インターフェイスのシャットダウンとインターフェイスの再イネーブル化が発生する場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、ポートの速度を 100 Mbps に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

次の例では、ポートが 10 Mbps のみでオートネゴシエートするよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10
```

次の例では、ポートが 10 Mbps または 100 Mbps のみでオートネゴシエートするよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
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	動作のデュプレックス モードを指定します。
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に対する統計情報を表示します。

srr-queue bandwidth limit

ポートの最大出力を制限するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 *weightl*

no srr-queue bandwidth limit

シンタックスの説明

weightl 制限されるポートの速度のパーセンテージ。指定できる範囲は、10 ～ 90 です。

デフォルト

ポートの速度に制限はなく、100% 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドで 80% を設定した場合、ポート時間の 20% はアイドル状態になります。ライン レートの接続速度は 80% まで落ち込みます。ただし、ライン レートはハードウェアが 6 ずつ調整しているため、これらの値は正確ではありません。

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



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更できます。

例

次の例では、ポートを 800 Mbps (メガビット / 秒) に制限する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
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	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	Class of Service (CoS; サービスクラス) 値を出力キューにマッピング、または 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 output dscp-map	Differentiated Services Code Point (DSCP) 値を出力キューにマッピング、または 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 queue-set output threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、キューセットに最大のメモリ割り当てを設定します。
queue-set	キューセットに対し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	シェーピングしたウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有のウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth shape

シェーピング ウェイトを割り当てることで、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

weight1 weight2 weight3 weight4 ウェイトを指定し、シェーピングするポートのパーセンテージを決定します。比率を逆にすることで ($1/\text{weight}$)、キューの帯域幅のシェーピングを指定します。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

ウェイト 1 は 25 に設定されています。ウェイト 2、ウェイト 3、ウェイト 4 は 0 に設定され、共有モードにあります。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

シェーピング モードでは、キューは帯域幅の一部（パーセンテージ）を保証されており、その値に対しレート制限されています。シェーピングされたトラフィックは、リンクがアイドル状態であったとしても、割り当てられた以上の帯域幅を使用しません。シェーピングを使用することで、バースト性のあるトラフィックを円滑にし、またより速く出力を実行できます。

シェーピング モードは共有モードを上書きします。

シェーピング キューのウェイトを **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドで 0 に設定した場合、このキューは共有モードになります。**srr-queue bandwidth shape** コマンドで指定されたウェイトは無効となり、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドでキューに指定したウェイトが有効になります。

同一のポートにシェーピングおよび共有モードの両方を設定する場合、一番低い番号のキューをシェーピング用に設定していることを確認してください。

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



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更してください。

例

次の例では、同一のポートにシェーピングおよび共有のキューを設定する方法を示します。キュー 2、3、4 のウェイトの比率に 0 が設定されるため、これらのキューは共有モードで動作します。キュー 1 の帯域幅のウェイトは 1/8 (12.5%) になります。キュー 1 はこの帯域幅が保証され、それに制限されます。他のキューにトラフィックがなく、アイドル状態でも、スロットの制限が拡張されることはありません。キュー 2、3 および 4 は共有モードにあり、キュー 1 の設定は無視されます。共有モードにあるキューに割り当てられる帯域幅の比率は 4/ (4+4+4) で、33% になります。

```
Switch(config)# interface gigabitethernet2/0/1
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	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	Class of Service (CoS; サービス クラス) 値を出力キューにマッピング、または 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 output dscp-map	Differentiated Services Code Point (DSCP) 値を出力キューにマッピング、または 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 queue-set output threshold	Weighted Tail-Drop (WTD) スレッシュホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
priority-queue	ポートでの出力緊急キューをイネーブルにします。
queue-set	キューセットに対し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	共有のウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth share

共有のウェイトを割り当てて、ポートにマッピングされた 4 つの出力キューの帯域幅の共有をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。ウェイトの比率は、Shaped Round Robin (SRR; シェイプド ラウンド ロビン) スケジューラが各キューからパケットをデキューする頻度の比率です。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。

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

シンタックスの説明

<i>weight1 weight2 weight3 weight4</i>	<i>weight1</i> 、 <i>weight2</i> 、 <i>weight3</i> 、および <i>weight4</i> の比率は、SRR スケジューラがパケットをデキューする頻度の比率を規定します。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

ウェイト 1、ウェイト 2、ウェイト 3、およびウェイト 4 は 25 に設定されています（各キューに帯域幅の 1/4 を割り当て）。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

各ウェイトの絶対値は無意味で、使用されるのはパラメータの比率だけです。

共有モードでは、キューは設定されたウェイトに従ってキュー間の帯域幅を共有します。帯域幅はこのレベルでは保証されますが、制限されるわけではありません。たとえば、キューが空で、リンクの共有が必要ない場合、残りのキューは未使用の帯域幅まで拡張され、キュー間で共有されます。

シェーピング キューのウェイトを **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドで 0 に設定した場合、このキューは SRR 共有モードになります。**srr-queue bandwidth shape** コマンドで指定されたウェイトは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドでキューに指定したウェイトが有効になります。

同一のポートにシェーピングおよび共有モードの両方を設定する場合、一番低い番号のキューをシェーピング用に設定していることを確認してください。



(注)

出力キューのデフォルト設定はほとんどの場合に適切になっています。これらの設定がご使用の Quality of Service (QoS; サービス品質) ソリューションに合わない場合は、出力キューについての詳細な知識がある場合に限り設定を変更してください。

例

次の例では、出力ポートで動作する SRR スケジューラのウェイト比率を設定する方法を示します。4 つのキューは使用されています。共有モードにある各キューに割り当てられた帯域幅の比率は、 $1/(1+2+3+4)$ 、 $2/(1+2+3+4)$ 、 $3/(1+2+3+4)$ 、および $4/(1+2+3+4)$ です（キュー 1、2、3、4 はそれぞれ 10%、20%、30%、40%）。これはキュー 4 に、キュー 1 の 4 倍、キュー 2 の 2 倍、キュー 3 の 1.3 倍の帯域幅が割り当てられていることを意味します。

```
Switch(config)# interface gigabitethernet2/0/1
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	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	Class of Service (CoS; サービス クラス) 値を出力キューにマッピング、または CoS 値をキューおよびスレッシホールド ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Services Code Point (DSCP) 値を出力キューにマッピング、または DSCP 値をキューおよびスレッシホールド ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) スレッシホールドを設定し、バッファの可用性を保証し、そしてキューセットに最大のメモリ割り当てを設定します。
priority-queue	ポートでの出力緊急キューをイネーブルにします。
queue-set	キューセットに対し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	シェーピングしたウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅シェーピングをイネーブルにします。

stack-mac persistent timer

永続的 MAC（メディア アクセス制御）アドレス機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **stack-mac persistent 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。この機能がイネーブルでスタック マスターが変更された場合、スタックの MAC アドレスは約 4 分間変更されません。この間に以前スタック マスターであったスイッチがスタックに再加入すると、スイッチが現在はスタック メンバーであっても、スタックはこのスイッチの MAC アドレスをスタックの MAC アドレスとして引き続き使用します。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。

stack-mac persistent timer

no stack-mac persistent timer

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

永続的 MAC アドレスはディセーブルに設定されています。スタックの MAC アドレスは常に、スタック マスターの MAC アドレスです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックの MAC アドレスは、スタック マスターの MAC アドレスにより決定します。デフォルト ステート（永続的 MAC アドレスがディセーブル）で、新しいスイッチがスタック マスターになると、スタックの MAC アドレスは新しいスタック マスターの MAC アドレスに変更されます。

永続的 MAC アドレスがイネーブルの場合、スタックの MAC アドレスは約 4 分間変更されません。この間に以前のスタック マスターがスタック メンバーとしてスタックに再加入した場合、スタックではこの MAC アドレスを持つスイッチがスタック内に存在するかぎり、以前のスタック マスターの MAC アドレスを保有します。以前のスタック マスターがスタックに再加入しない場合は、スイッチ スタックは新しいスタック マスターの MAC アドレスをスタックの MAC アドレスとします。

スタック全体がリロードする場合、このスタックが復元すると、スタック マスターの MAC アドレスがスタックの MAC アドレスとなります。

例

次の例では、永続的 MAC アドレスをイネーブルにする方法を示します。

```
Switch(config)# stack-mac persistent timer
```

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。イネーブルである場合は、**stack-mac persistent timer** が出力に表示されます。

関連コマンド

コマンド	説明
show running-config	現在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。

storm-control

インターフェイス上でブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御をイネーブルにし、スレッシュホールドのレベルを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}}
```

シンタックスの説明

broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level level [level-low]	増加および減少する抑制レベルを、ポートの合計帯域幅に対するパーセンテージとして指定します。 <i>level</i> — 増加する抑制レベル、最大で小数第 2 位まで。指定できる範囲は、0.00 ～ 100.00 です。<i>level</i> で指定された値に達した場合、ストーム パケットのフラッディングをブロックします。 <i>level-low</i> — (任意) 減少する抑制レベル、最大で小数第 2 位まで。指定できる範囲は、0.00 ～ 100.00 です。この値は増加する抑制値以下である必要があります。減少する抑制レベルを設定しない場合、増加する抑制レベルに設定されます。
level bps bps [bps-low]	増加および減少する抑制レベルを、トラフィックがポート上で受信されるビット / 秒単位の速度として指定します。 <i>bps</i> — 増加する抑制レベル、最大で小数第 1 位まで。指定できる範囲は、0.0 ～ 10000000000.0 です。<i>bps</i> で指定された値に達した場合、ストーム パケットのフラッディングをブロックします。 <i>bps-low</i> — (任意) 減少する抑制レベル、最大で小数第 1 位まで。指定できる範囲は、0.0 ～ 10000000000.0 です。この値は増加する抑制値以下である必要があります。 k、m、g などのメトリック サフィックスを大きな数字のスレッシュホールドに使用できます。
level pps pps [pps-low]	増加および減少する抑制レベルを、トラフィックがポート上で受信されるパケット / 秒単位の速度として指定します。 <i>pps</i> — 増加する抑制レベル、最大で小数第 2 位まで。指定できる範囲は、0.0 ～ 10000000000.0 です。<i>pps</i> で指定された値に達した場合、ストーム パケットのフラッディングをブロックします。 <i>pps-low</i> — (任意) 減少する抑制レベル、最大で小数第 2 位まで。指定できる範囲は、0.0 ～ 10000000000.0 です。この値は増加する抑制値以下である必要があります。 k、m、g などのメトリック サフィックスを大きな数字のスレッシュホールドに使用できます。

action {shutdown | trap} ポート上でストームが発生した場合に実行すべきアクション。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、SNMP（簡易ネットワーク管理プロトコル）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** — ストーム中のポートをディセーブルにします。
- **trap** — ストームが発生したときに 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、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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SE	level level [.level] オプションは、 level {level [level-low] pps pps [pps-low] bps bps [bps-low]} action {shutdown trap} オプションに変更されました。

使用上のガイドライン

ストーム制御は物理インターフェイス上でのみサポートされます。CLI（コマンドライン インターフェイス）で使用可能でも、EtherChannel ポートのチャンネルではサポートされません。

ストーム制御の抑制レベルは、ポートの合計帯域幅に対するパーセンテージとして、トラフィックを受信するパケット / 秒単位の速度として、またはトラフィックを受信するビット / 秒単位の速度として入力できます。

合計帯域幅に対するパーセンテージとして入力した場合、抑制値が 100% であれば、指定されたトラフィック タイプに対して制限が課せられていないということです。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、ユニキャスト トラフィックがブロックされることを意味します。増加する抑制レベルが 100% 未満の場合にのみ、ストーム制御はイネーブルになります。他のストーム制御設定が指定されていない場合、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ストームを発生させ、SNMP トラップを送信しません。



(注)

マルチキャスト トラフィックがストーム制御のスレッシュホールドに到達すると、Bridge Protocol Data Unit (BDPU; ブリッジプロトコルデータユニット)、Cisco Discovery Protocol (CDP) フレームなどの制御トラフィック以外のすべてのマルチキャスト トラフィックがブロックされます。ただし、スイッチは、Open Shortest Path First (OSPF) および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のトラフィックがブロックされます。

trap および **shutdown** オプションは相互に独立しています。

シャットダウンなどの実行すべきアクションを設定する（ストーム中にポートが **errdisable** ステートである）場合で、パケット ストームが削除されている場合、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 コマンドを使用します。**shutdown** アクションを指定しない場合、このアクションを **trap** として指定します（ストームが検出されると、スイッチはトラップを生成します）。

ストームが発生してアクションがトラフィックをフィルタリングする場合、減少する抑制レベルが指定されていないと、トラフィック伝送速度が増加する抑制レベルを下回るまで、スイッチはすべてのトラフィックをブロックします。減少する抑制レベルが指定されている場合、トラフィック伝送速度がそのレベルを下回るまで、スイッチはトラフィックをブロックします。

ブロードキャスト ストームが発生してアクションがトラフィックをフィルタリングする場合、スイッチはブロードキャスト トラフィックのみをブロックします。

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

次の例では、ブロードキャスト ストーム制御を 75.5% の増加する抑制レベルでイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、ポートのユニキャスト ストーム制御を、87% の増加する抑制レベルおよび 65% の減少する抑制レベルでイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、ポートのマルチキャスト ストーム制御を、2000 パケット / 秒の増加する抑制レベルおよび 1000 パケット / 秒の減少する抑制レベルでイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、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上、または指定のインターフェイス上で、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。

switch priority

スタック メンバーのプライオリティ値を変更するには、スタック マスター上から **switch 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。

switch *stack-member-number* **priority** *new-priority-value*

シンタックスの説明

<i>stack-member-number</i>	現行のスタック メンバー番号を指定します。指定できる範囲は、1 ～ 9 です。
priority <i>new-priority-value</i>	新しいスタック メンバーのプライオリティ値を指定します。指定できる範囲は、1 ～ 15 です。

デフォルト

デフォルトのプライオリティ値は 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

新しいプライオリティ値はスタックマスターの再選出にとって重要な要素になります。そのため、プライオリティ値の変更がただちにスタック マスターを変更するわけではありません。

例

次の例では、スタック メンバー 6 のプライオリティ値を 9 に変更する方法を示します。

```
Switch(config)# switch 6 priority 9
Changing the Switch Priority of Switch Number 6 to 9
Do you want to continue?[confirm]
```

関連コマンド

コマンド	説明
reload	スタック メンバーをリロードし、設定の変更を有効にします。
session	特定のスタック メンバーにアクセスします。
switch renumber	スタック メンバー番号を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

switch provision

新しいスイッチがスイッチ スタックに加入する前に、プロビジョニングするには（設定を提供する）、スタック マスターから **switch provision** グローバル コンフィギュレーション コマンドを使用します。削除されたスイッチ（スタックを脱退したスタック メンバー）に関連付けられたすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch stack-member-number provision type

no switch stack-member-number provision

シンタックスの説明

<i>stack-member-number</i>	スタック メンバー番号を指定します。指定できる範囲は、1 ～ 9 です。
provision type	新しいスイッチがスタックに加入する前に、このスイッチのタイプを指定します。
	<i>type</i> には、コマンドライン ヘルプ スtringに示されたサポート対象のスイッチのモデル番号を入力します。

デフォルト

スイッチは、プロビジョンされていません。

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(20)SE	このコマンドが導入されました。

使用上のガイドライン

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチ スタックから指定のスイッチを削除する必要があります。

スイッチ タイプを変更する場合も、スイッチ スタックから指定のスイッチを削除する必要があります。スイッチ タイプを変更しない場合でも、スイッチ スタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバー番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチ タイプと一致しない場合、スイッチ スタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチ スタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチ スタックの実行コンフィギュレーションで表示されます。**copy running-config startup-config** イネーブル EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチ スタックのスタートアップ コンフィギュレーション ファイルに保存されます。



注意

このコマンドを使用する場合、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチ タイプが設定される場合、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドを 200 回以上は使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

例 次の例では、スイッチ スタックにスタック メンバー番号が 2 の Catalyst 3750G-12S スイッチをプロビジョニングする方法を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
Switch(config)# switch 2 provision WS-C3750G-12S
Switch(config)# end
Switch# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
(テキスト出力は省略)
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバー 5 についてのすべての設定情報が削除される方法を示します。

```
Switch(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**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 switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

switch renumber

スタック メンバーの番号を変更するには、スタック マスター上から **switch renumber** グローバル コンフィギュレーション コマンドを使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

シンタックスの説明

<i>current-stack-member-number</i>	現行のスタック メンバー番号を指定します。指定できる範囲は、1 ～ 9 です。
renumber	スタック メンバーに新しいスタック メンバー番号を指定します。指定できる範囲は、1 ～ 9 です。
<i>new-stack-member-number</i>	

デフォルト

デフォルトのスタック メンバー番号は 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

他のスタック メンバーがすでに指定したメンバー番号を使用している場合、スタック マスターは、スタック メンバーをリロードする場合に、使用可能な一番低い番号を割り当てます。



(注)

スタック メンバー番号を変更し、新しいスタック メンバー番号がどの設定にも関連付けされていない場合、そのスタック メンバーは現行の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。スタック メンバー番号および設定に関する詳細については、ソフトウェア コンフィギュレーション ガイドを参照してください。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタック メンバーをリロードし、設定変更を適用するには、**reload slot current stack member number** イネーブル EXEC コマンドを使用します。

例

次の例では、スタック メンバー 6 のメンバー番号を 7 に変更する方法を示しています。

```
Switch(config)# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that
switch.
The interface configuration associated with the old switch number will remain as a
provisioned configuration.
Do you want to continue?[confirm]
```

関連コマンド

コマンド	説明
reload	スタック メンバーをリロードし、設定の変更を有効にします。
session	特定のスタック メンバーにアクセスします。
switch priority	スタック メンバーのプライオリティ値を変更します。
show switch	スイッチ スタックおよびスタック メンバーの情報を表示します。

switchport

レイヤ 3 のモードにあるインターフェイスを、レイヤ 2 の設定のためレイヤ 2 モードに変更するには、スイッチ スタックまたはスタンドアロン スイッチ上でキーワードを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを使用します。レイヤ 3 モードにインターフェイスを戻す場合は、このコマンドの **no** 形式を使用します。

switchport

no switchport

インターフェイスをルーテッドインターフェイスの状態に設定することで、レイヤ 2 の設定をすべて削除するには、**no switchport** コマンド (パラメータの指定なし) を使用します。このコマンドは、ルーテッド ポートに IP アドレスを割り当てる前に使用する必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	インターフェイスがレイヤ 2 モードからレイヤ 3 モード間、またはその逆に変更されると、インターフェイス上の以前の設定情報は削除されます。

使用上のガイドライン

no switchport コマンドは、ポートをシャットダウンし、再びイネーブルにします。ポートに接続されている装置上ではメッセージが生成される可能性があります。

Release 12.2(20)SE 以降で、インターフェイスをレイヤ 2 モードからレイヤ 3 モードに (またはその逆に) 設定する場合、影響を受けるインターフェイスに関連する以前の設定情報が削除され、インターフェイスがデフォルト設定に戻る場合があります。



(注)

インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、まず **switchport** コマンドをキーワードを指定しないで入力し、インターフェイスをレイヤ 2 ポートとして設定します。その後、ここで記載されているようなキーワードを指定した別の **switchport** コマンドを入力できます。

例

次の例では、インターフェイスをレイヤ 2 ポートとして動作することを止め、Cisco ルーテッド ポートにする方法を示します。

```
Switch(config-if)# no switchport
```

次の例では、ポート インターフェイスを Cisco ルーテッド ポートとして動作することを止め、レイヤ 2 のスイッチング インターフェイスに変更する方法を示します。

```
Switch(config-if)# switchport
```



(注)

キーワードを指定しない **switchport** コマンドは、Cisco ルーテッド ポートをサポートしないプラットフォーム上では使用することができません。このようなプラットフォーム上の物理ポートは、レイヤ 2 のスイッチング インターフェイスとして想定されます。

インターフェイスの上のスイッチ ポートのステータスを確認するには、**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 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 (非ルーティング) 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。
show running-config	現在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。

switchport access

ポートをスタティックアクセス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、スイッチ スタックまたはスタンドアロン スイッチ上で **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 ポートのモードが、**access** に設定されている場合、ポートは指定の 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場合、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

シンタックスの説明

vlan vlan-id	インターフェイスを、アクセス モード VLAN の VLAN ID を持つスタティック 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。スイッチは受信した新しい 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

デフォルトのアクセス 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したデフォルト VLAN です。

ダイナミックアクセス ポートは最初は何の 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

no switchport access コマンドは、アクセス モード VLAN を装置に対して適切なデフォルト 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 VMPS をクエリーできる VLAN Query Protocol (VQP) クライアントを実装します。Catalyst 3750 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接続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。
- Spanning-Tree Protocol (STP; スパニングツリープロトコル) 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してい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 で動作するよう変更する方法を示します。

```
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 (非ルーティング) 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 メンバーシップモードを設定します。

switchport backup interface

1 組のインターフェイスで、相互にバックアップを提供する Flex Link を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上のレイヤ 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 の設定を削除する場合は、このコマンドの **no** 形式を使用します。

switchport backup interface {*interface-id*}

no switchport backup

シンタックスの説明

<i>interface-id</i>	レイヤ 2 インターフェイスを指定して、設定されるインターフェイスのバックアップ リンクとして動作します。インターフェイスは、物理インターフェイスでもポート チャネルでもかまいません。ポートチャネルに指定できる範囲は 1 ～ 48 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tring 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

デフォルトでは、Flex Link は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

Flex Link が設定されている場合、1 つのリンクがプライマリ インターフェイスとして動作し、トラフィックを転送する間、もう 1 つのインターフェイスはスタンバイ モードで、プライマリ リンクがシャット ダウンした場合に備えてトラフィックの転送を開始する準備をします。設定されるインターフェイスはアクティブ リンクとみなされ、指定されるインターフェイスはバックアップ リンクとして識別されます。この機能により、Spanning-Tree Protocol (STP; スパニングツリー プロトコル) の代替が提供され、ユーザが STP をオフにしても基本的なリンク冗長性を保持できます。

- このコマンドは、レイヤ 2 インターフェイスでのみ使用できます。
- 任意のアクティブ リンクに設定できる Flex Link のバックアップ リンクは 1 つのみで、これはアクティブ インターフェイスとは別のインターフェイスである必要があります。
- インターフェイスが所属できるのは、1 組の Flex Link 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 リンクとなれます。アクティブ リンクは、他の Flex Link の組には所属できません。
- バックアップ リンクは、アクティブ リンクと必ずしも同じタイプである必要はありません (ファストイーサネットまたはギガビット イーサネットなど)。ただし、スタンバイ リンクがトラフィックの転送を引き継ぐ場合に、ループまたは動作の変更が発生しないように、両方の Flex Link には同様の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りません。ただし、ポート チャネルまたは物理インターフェイスのいずれかをプライマリ リンクと設定する場合は、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、また 1 つのポート チャネルおよび 1 つの物理インターフェイスを Flex Link として設定できます。

- スイッチ上で STP が設定されている場合は、すべての有効な VLAN で Flex Link は STP に加入しません。STP が稼働していない場合は、設定されたトポロジーにループがないことを確認してください。

例

次の例では、2 つのインターフェイスを Flex Link として設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
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 <i>[interface-id]</i> switchport backup	スイッチ上または指定のインターフェイスで設定された Flex Link およびそのステータスを表示します。

switchport block

不明なマルチキャストまたはユニキャストのパケットが転送されることを回避するには、スイッチスタックまたはスタンドアロンスイッチ上で **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。不明なマルチキャスト、またはユニキャスト パケットの転送を許可する場合は、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}

シンタックスの説明

multicast	不明なマルチキャスト トラフィックをブロックするよう指定します。
unicast	不明なユニキャスト トラフィックをブロックするよう指定します。

デフォルト

不明な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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、不明な MAC（メディア アクセス制御）アドレスを持ったすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックはブロックできます。保護ポートで、不明な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ない場合、セキュリティ上の問題が発生します。

不明な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クは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックの詳細については、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、インターフェイス上で不明なマルチキャスト 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（非ルーティング）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

レイヤ 2 ポートのホスト接続を最適化するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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、システム上では無効です。

switchport host

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートのデフォルトは、ホストへの接続が最適化されていません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

ポートのホスト接続を最適化する場合、**switchport host** コマンドを使用することで、ポート モードをアクセスにし、スパニングツリー PortFast をイネーブルにします（チャンネルのグループ化もディセーブルにします）。エンドステーションのみこの設定を適用できます。

スパニングツリー PortFast がイネーブルのため、**switchport host** コマンドを入力します（1 つのホストに接続しているポート上でのみ可能）。高速開始ポートに他のスイッチ、ハブ、コンセントレータ、またはブリッジを接続すると、一時的にスパニングツリーのループが発生する可能性があります。

switchport host コマンドをイネーブルにし、パケット転送の開始における遅延時間を減少させることができます。

例

次の例では、ポートのホスト接続の設定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 モードを含む、スイッチング（非ルーティング）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、スイッチ スタックまたはスタンドアロン スイッチ上で **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。モードを装置の適切な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 | dot1q-tunnel | dynamic {auto | desirable} | private-vlan | trunk}
no switchport mode {access | dot1q-tunnel | dynamic | trunk}
```

シンタックスの説明

access	ポートにアクセス 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。
dot1q-tunnel	ポートを IEEE (米国電気電子学会) 802.1Q トンネル ポートとして設定します。
dynamic auto	インターフェイス トランッキング モード ダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチ ポート モードになります。
dynamic desirable	インターフェイス トランッキング モード ダイナミック パラメータを desirable に設定して、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するように指定します。
private-vlan	switchport mode private-vlan コマンドを参照してください。
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ッキングします。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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	private-vlan キーワードが追加されました。
12.2(25)SE	dot1q-tunnel キーワードが追加されました。

使用上のガイドライン

access、**dot1q-tunnel**、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固定非トランッキング 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固定トランキング 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トするには、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) 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によって 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。

- これらのリンクを介して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へ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。

dot1q-tunnel を入力すると、ポートは IEEE 802.1Q トンネル ポートとして無条件に設定されます。

アクセス ポート、トランク ポート、トンネル ポートは相互に排他的な関係にあります。

トンネル ポート上で受信された IEEE 802.1Q カプセル化 IP パケットは、IP Access Control List (ACL; アクセス制御リスト) ではなく、MAC (メディア アクセス制御) ACL によってフィルタリングされます。これは、スイッチが IEEE 802.1Q ヘッダー内のプロトコルを認識しないためです。この制限事項はルータ ACL、ポート ACL、および VLAN マップに適用されます。

ポートを IEEE 802.1Q トンネル ポートとして設定する場合、次の制限事項があります。

- IP ルーティングおよびフォールバック ブリッジングはトンネル ポート上でサポートされません。
- トンネル ポートは IP ACL をサポートしません。
- IP ACL がトンネル ポートを含む VLAN のトランク ポートに適用された場合、または VLAN マップがトンネル ポートを含む VLAN に適用された場合、トンネル ポートから受信したパケットは非 IP パケットとして処理され、MAC アクセス リストでフィルタリングされます。
- レイヤ 3 の Quality of Service (QoS; サービス品質) ACL 機能、およびレイヤ 3 情報に関連するその他 QoS 機能は、トンネル ポートではサポートされません。

IEEE 802.1Q トンネル ポートの設定に関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

IEEE 802.1x 機能は次の方法でスイッチ ポート モードと連動します。

- 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。
- dynamic auto** または **dynamic desirable** に設定されているポートで 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 **dynamic auto** または **dynamic desirable** 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、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 gigabitethernet2/0/1
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 gigabitethernet2/0/1
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 gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

次の例では、IEEE ポートを 802.1Q トンネル ポートとして設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dot1q-tunnel
```

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（非ルーティング）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 モードの場合、トランクの特性を設定します。

switchport mode private-vlan

ポートをプロミスキャス ポートまたはホストのプライベート VLAN（仮想 LAN）ポートとして設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **switchport mode private-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。モードを装置の適切な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 private-vlan {host | promiscuous}
```

```
no switchport mode private-vlan
```

シンタックスの説明

host	インターフェイスを、プライベート VLAN のホスト ポートとして設定します。ホスト ポートはプライベート VLAN のセカンダリ VLAN に所属し、所属する VLAN に応じてコミュニティ ポートまたは独立ポートになります。
promiscuous	インターフェイスを、プライベート VLAN のプロミスキャス ポートとして設定します。プロミスキャス ポートは、プライベート VLAN のプライマリ VLAN のメンバーです。

デフォルト

プライベート VLAN のデフォルト モードは、ホストでもプロミスキャスでもありません。スイッチ ポートのデフォルト 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(20)SE	このコマンドが導入されました。

使用上のガイドライン

プライベート VLAN のホスト ポートまたはプロミスキャス ポートは、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 宛先ポートにはなれません。SPAN 宛先ポートをプライベート VLAN のホスト ポートまたはプロミスキャス ポートとして設定すると、ポートは非アクティブになります。

ポート上のプライベート VLAN に次のその他の機能を設定しないでください。

- ダイナミックアクセス ポートの VLAN メンバーシップ
- Dynamic Trunking Protocol (DTP)
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- Voice VLAN

プライベート VLAN ポートは、SPAN 宛先ポートとして設定できません。

ポートが、プライベート VLAN コンフィギュレーションに含まれている間は、その EtherChannel のコンフィギュレーションは非アクティブです。

プライベート VLAN ポートは、セキュア ポートとして設定できません。また、保護ポートとして設定しないでください。

プライベート VLAN と他の機能との相互作用の詳細については、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。

設定の矛盾による STP ループを防止するため、および STP コンバージェンスを高速化するために、独立またはコミュニティ ホスト上でスパニングツリー PortFast および Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) をイネーブルにすることを強く推奨します。

switchport private-vlan host-association インターフェイス コンフィギュレーション コマンドを使用して、ポートをプライベート VLAN のホスト ポートとして設定したり、有効なプライベート VLAN アソシエーションを設定しない場合は、インターフェイスが非アクティブになります。

switchport private-vlan mapping インターフェイス コンフィギュレーション コマンドを使用して、ポートをプライベート VLAN のプロミスキヤス ポートとして設定したり、有効なプライベート VLAN マッピングを設定しない場合は、インターフェイスが非アクティブになります。

例

次の例では、インターフェイスをプライベート VLAN のホスト ポートとして設定し、これをプライマリ VLAN 20 に関連付けする方法を示します。インターフェイスはセカンダリ独立 VLAN 501 およびプライマリ VLAN 20 のメンバーです。



(注)

ポートをプライベート VLAN のホスト ポートとして設定する場合は、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドおよび **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、BPDU ガードおよび PortFast もイネーブルにする必要があります。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

次の例では、インターフェイスをプライベート VLAN のプロミスキヤス ポートとして設定し、これをプライベート VLAN にマッピングする方法を示します。インターフェイスは、プライマリ VLAN 20 のメンバーで、セカンダリ VLAN 501 ~ 503 はこれにマッピングされます。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-503
Switch(config-if)# end
```

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
private-vlan	VLAN をコミュニティ、独立、またはプライマリ VLAN として設定するか、またはプライマリ VLAN をセカンダリ VLAN と関連付けします。
show interfaces switchport	プライベート VLAN の設定を含む、スイッチング（非ルーティング）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 private-vlan	プライベート VLAN のアソシエーション、およびインターフェイスのプライマリ VLAN およびセカンダリ VLAN 間のマッピングを設定します。

switchport nonegotiate

レイヤ 2 インターフェイス上で Dynamic Trunking Protocol (DTP) ネゴシエーション パケットが送信されないように指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトでは、トランキング ステータスを判別するために、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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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 ポート 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装置では、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。装置は **mode** パラメータ (**access** または **trunk**) に従って、トランクを実行します。

- これらのリンクを介して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、(モードの設定に応じて) 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 gigabitethernet2/0/1
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（非ルーティング）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 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のポート セキュリティをイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上でキーワードを指定せずに **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、スティッキー 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 [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}]
```

シンタックスの説明

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 アドレスを追加できます。
vlan vlan-id	(任意) トランク ポート上でのみ、VLAN (仮想 LAN) ID および MAC アドレスを指定します。VLAN ID が指定されない場合、ネイティブ VLAN が使用されます。
vlan access	(任意) アクセス ポート上でのみ、VLAN をアクセス VLAN として指定します。
vlan voice	(任意) アクセス ポート上でのみ、VLAN を音声 VLAN として指定します。



(注)

voice キーワードは、ポート上で音声 VLAN が設定されており、そのポートがアクセス VLAN ではない場合にだけ指定できます。

mac-address sticky [<i>mac-address</i>]	(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スティッキー ラーニングをイネーブルにします。スティッキー ラーニングをイネーブルにすると、インターフェイスはダイナミック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ー セキュア MAC アドレスに変換します。 (任意) <i>mac-address</i> を入力し、スティッキー セキュア MAC アドレスを指定します。
maximum value	(任意) インターフェイスのセキュア MAC アドレスの最大数を設定します。スイッチ スタックで設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。sdm prefer コマンドを参照してください。この数字は使用可能な MAC アドレスの総数を意味します (他のレイヤ 2 機能およびインターフェイス上に設定された他のセキュア MAC アドレスを含む)。 デフォルトの設定は 1 です。
vlan [<i>vlan-list</i>]	(任意) トランク ポートに対して、VLAN のセキュア MAC アドレスの最大数を設定できます。vlan キーワードが入力されていない場合、デフォルト値が使用されます。 • vlan — VLAN ごとに最大値を設定します。 • vlan vlan-list — VLAN 範囲、または一連の VLAN で VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
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。このモードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットは廃棄されます。廃棄することでセキュア MAC アドレス数を下げるか、許可するアドレスの最大数を増やさないかぎり、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。
 (注) トランク ポート上に保護モードを設定することは推奨しません。保護モードでは、VLAN がその制限に到達した場合、たとえポートが制限に到達していなくても、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、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除するか、許可するアドレスの最大数を増やさないかぎり、この状態が続きます。SNMP (簡易ネットワーク管理プロトコル) トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

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、ポートの LED がオフになると、インターフェイスが errdisable の状態になります。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、 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、手動で再びイネーブルにできます。

デフォルト

デフォルト設定では、ポート セキュリティをディセーブルにします。

セキュリティがイネーブルの場合に、キーワードを入力しないと、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。

スティッキー 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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	sticky および vlan キーワードが追加されました。
12.2(25)SEB	access および voice キーワードが追加されました。

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートになることができます。ダイナミック アクセス ポートにはなれません。
- セキュア ポートはルーテッド 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 ポートは、プライベート VLAN ポートにはなれません。
- 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ー セキュア MAC アドレスを設定できません。
- 音声 VLAN を設定し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、アクセス VLAN 上のポートの最大セキュア アドレス許容数に 2 を加えた設定に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 2 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上から学習でき、アクセス VLAN 上からも学習できる可能性があります。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 ポート上のみでサポートされます。トランク ポート上ではサポートされません。
- インターフェイスの最大セキュア アドレス値を入力した場合、新しい値が古い値より大きい場合、新しい値は古い設定の値を上書きします。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。

- スイッチはスティッキー 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 アドレスの最大数がアドレス テーブルにあり、アドレス テーブルにない 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した場合、または他のセキュア ポート上のセキュア MAC アドレスとして設定されている MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、セキュリティ違反が発生します。

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びイネーブルにできます。

アドレスの最大数を 1 に設定し、接続された装置の MAC アドレスを設定することは、装置がポートの帯域幅を完全に使用できる保証となります。

最大セキュア アドレスの値をインターフェイスに入力した場合、次の事柄が発生します。

- 新しい値が古い値より大きい場合、新しい値が古い設定値を上書きします。
- 新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。

スティッキー 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、インターフェイス上でスティッキー ラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミック セキュア MAC アドレスを（スティッキー ラーニングがイネーブルになる前にダイナミックに学習されたアドレスも含め）、スティッキー セキュア MAC アドレスに変換し、すべてのスティッキー セキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドでスティッキー ラーニングをディセーブルにした場合、または実行コンフィギュレーションを削除した場合、スティッキー セキュア MAC アドレスは実行コンフィギュレーションに一部を残しますが、アドレス テーブルからは削除されます。削除されたアドレスはダイナミックに再設定でき、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** インターフェイス コンフィギュレーション コマンドを使用し、スティッキー セキュア MAC アドレスを設定する場合、これらのアドレスはアドレス テーブルおよび、実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキー セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキー 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すみす。スティッキー 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。スティッキー ラーニングをディセーブルにした場合、スティッキー 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。
- スティッキー ラーニングをディセーブルにし、**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、スティッキー セキュア MAC アドレスは実行コンフィギュレーションには追加されません。

例

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

```
Switch(config)# interface gigabitethernet 2/0/2
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 2/0/2
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、ポートでスティッキー ラーニングをイネーブルにして、2 つのスティッキー 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 2/0/2
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すべてのセキュア アドレスを表示します。
show port-security interface interface-id	スイッチまたは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。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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}

シンタックスの説明

static	このポートにスタティック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	完全なエージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間（分）が経過した直後に期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	非アクティビティ エージング タイプを設定します。指定された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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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

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

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

セキュア アドレス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、スタティック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、ポートの全セキュア アドレスの絶対エージングについて、エージング タイムを 2 時間に設定します。

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

次の例では、ポートで設定されたセキュア アドレスに対してエージングがイネーブルになっている非アクティビティ エージング タイプについて、エージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet1/0/2
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 gigabitethernet1/0/2
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、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

cos value	PC または指定の 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 (米国電気電子学会) 802.1p プライオリティを上書きするように IP Phone のポートを設定します。指定できる範囲は 0 ～ 7 です。7 が最高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

デフォルトのポート プライオリティは、ポート上で受信されたタグなしフレームの CoS 値が 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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

音声 VLAN (仮想 LAN) がイネーブルの場合、スイッチが Cisco Discovery Protocol (CDP) パケットを送信するよう設定し、IP Phone に、Cisco IP Phone のアクセス ポートに接続されている装置からデータ パケットを送信する方法を指示できます。Cisco IP Phone に接続しているスイッチ ポート上の CDP をイネーブルにし、Cisco IP Phone に設定を送信する必要があります (すべてのスイッチのインターフェイス上で、CDP はデフォルトの状態です)。

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 は、レイヤ 2 ポート上でのみ設定できます。

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 コマンドをスイッチ上で入力して、Quality of Service (QoS; サービス品質) をイネーブルにすることを推奨します。また、**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、ポート ステータスが信頼されるよう設定することも推奨します。

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 gigabitethernet1/0/2
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（非ルーティング）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 private-vlan

独立ポートまたはコミュニティ ポートへのプライベート VLAN（仮想 LAN）アソシエーション、またはプロミスキャス ポートへのマッピングを定義するには、スイッチ スタックまたはスタンドアロン スイッチ上で **switchport private-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。ポートからプライベート VLAN のアソシエーションまたはマッピングを削除する場合は、このコマンドの **no** 形式を使用します。

```
switchport private-vlan {association {host primary-vlan-id secondary-vlan-id | mapping
primary-vlan-id {add | remove} secondary-vlan-list} | host-association primary-vlan-id
secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}
```

```
no switchport private-vlan {association {host | mapping} | host-association | mapping}
```

このコマンドは、スタック マスターで IP サービス イメージが稼働している場合に限り使用できます。IP サービス イメージは、以前は Enhanced Multilayer Image（EMI）と呼ばれていました。プライベート VLAN が設定されている場合は、スタック メンバーでも EMI を稼働することを強く推奨します。

シンタックスの説明

association	ポートのプライベート VLAN アソシエーションを定義します。
host	コミュニティまたは独立ホスト ポートのプライベート VLAN アソシエーションを定義します。
<i>primary-vlan-id</i>	プライベート VLAN のプライマリ VLAN の VLAN ID。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。
<i>secondary-vlan-id</i>	プライベート VLAN のセカンダリ（独立またはコミュニティ）VLAN の VLAN ID。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。
mapping	プロミスキャス ポートのプライベート VLAN マッピングを定義します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN 間のアソシエーションをクリアします。
<i>secondary-vlan-list</i>	プライマリ VLAN にマッピングされる、1 つまたは複数のセカンダリ（独立またはコミュニティ）VLAN
host-association	コミュニティまたは独立ホスト ポートのプライベート VLAN アソシエーションを定義します。

デフォルト

デフォルトでは、プライベート VLAN のアソシエーションまたはマッピングは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが導入されました。

使用上のガイドライン

switchport mode private-vlan {host | promiscuous} インターフェイス コンフィギュレーション コマンドにより、ポートがプライベート VLAN のホスト ポートまたはプロミスキャス ポートとして設定されないかぎり、プライベート VLAN のアソシエーションまたはマッピングはポートで有効になりません。

ポートはプライベート VLAN のホスト モードまたはプロミスキャス モードですが、VLAN が存在しない場合、コマンドは許可されますが、ポートは非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めません。カンマで区切られた複数の項目を含めます。各項目は、単一の VLAN ID またはハイフンで連結したプライベート VLAN ID の範囲です。リストには、1 つの独立型 VLAN および複数のコミュニティ VLAN を含めます。

プロミスキャス ポートをマッピングできるのは、プライマリ VLAN に対してのみです。プライマリおよびセカンダリ VLAN にすでにマッピングされているプロミスキャス ポートで **switchport private-vlan mapping** コマンドを入力すると、プライマリ VLAN のマッピングが上書きされます。

プロミスキャス ポートのプライベート VLAN マッピングで、セカンダリ VLAN を追加または削除するには、**add** および **remove** キーワードを使用します。

switchport private-vlan association host コマンドを入力すると、**switchport private-vlan host-association** 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のと同じ効果があります。

switchport private-vlan association mapping コマンドを入力すると、**switchport private-vlan mapping** インターフェイス コンフィギュレーション コマンドを入力するのと同じ効果があります。

例

次の例は、インターフェイスをプライベート VLAN のホスト ポートとして設定し、プライマリ VLAN 20 およびセカンダリ VLAN 501 に関連付ける方法を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

次の例では、インターフェイスをプライベート VLAN のプロミスキャス ポートとして設定し、これをプライマリ VLAN およびセカンダリ VLAN にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-502
Switch(config-if)# end
```

プライベート VLAN のマッピングを確認するには、**show interfaces private-vlan mapping** イネーブル EXEC コマンドを入力します。スイッチ スタック上で設定されたプライベート VLAN およびインターフェイスを確認するには、**show vlan private-vlan** イネーブル EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) のプライベート VLAN マッピング情報を表示します。
show vlan private-vlan	スイッチ スタックで設定されたすべてのプライベート VLAN 関係およびタイプを表示します。

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 **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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン スイッチ ポート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 装置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、他の保護ポートにあらゆるトラフィック（ユニキャスト、マルチキャスト、またはブロードキャスト）を転送しません。レイヤ 2 の保護ポート間で、データ トラフィックを転送できません。そのパケットが CPU で処理され、ソフトウェアに転送される PIM など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 装置を経由して転送される必要があります。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックはスタック内の同一のスイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

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 gigabitethernet1/0/2
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
<code>show interfaces switchport</code>	ポート ブロッキング、ポート保護設定など、スイッチング（非ルーティング）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。
<code>switchport block</code>	インターフェイス上で不明なユニキャストまたは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、スイッチ スタックまたはスタンドアロン スイッチ上で **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。トランクの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 | encapsulation {dot1q | isl | negotiate} | native vlan vlan-id
| pruning vlan vlan-list}
no switchport trunk {allowed vlan | encapsulation | native vlan | {pruning vlan}}
```

シンタックスの説明

allowed vlan <i>vlan-list</i>	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 <i>vlan-list</i> 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。
encapsulation dot1q	トランク ポートのカプセル化形式を IEEE（米国電気電子学会）802.1Q に設定します。この形式を使用すると、スイッチはポート上で、タグ付きおよびタグなしトラフィックを同時にサポートします。
encapsulation isl	トランク ポートのカプセル化形式を ISL（スイッチ間リンク）に設定します。スイッチはすべての送受信のパケットを ISL ヘッダーでカプセル化し、ISL トランク ポートから受信するネイティブ フレームをフィルタリングします。
encapsulation negotiate	Dynamic Inter-Switch Link (DISL) および Dynamic Trunking Protocol (DTP) のネゴシエーションがカプセル化形式を解決しない場合に、ISL が形式として選択されるよう指定します。
native vlan <i>vlan-id</i>	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 <i>vlan-list</i>	トランキング モードの場合に、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) プルーニングに適格である VLAN のリストを設定します。 all キーワードは無効です。

vlan-list の形式は、**all | none | [add | remove | except] *vlan-atom* [,*vlan-atom*...]** です。各キーワードの意味は、次のとおりです。

- **all** は、1 ～ 4094 のすべての VLAN を指定します。このキーワードは、リスト内のすべての VLAN を同時に設定することを許可しないコマンド上では使用できません。
- **none** は、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** は、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 ID（VLAN ID が 1005 より上）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 リストには追加できません。

カンマで、連続しない VLAN ID を区切ります。一定範囲の ID を指定するにはハイフンを使用します。

- **remove** は、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。

カンマで、連続しない VLAN ID を区切ります。一定範囲の ID を指定するにはハイフンを使用します。

- **except** は、定義済み VLAN リスト以外の、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 の範囲は 1 ～ 1005 です。カンマで、連続しない VLAN ID を区切ります。一定範囲の ID を指定するにはハイフンを使用します。
- **vlan-atom** は、1 ～ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、より小さい値が最初になります（ハイフン区切り）。

デフォルト

デフォルトのカプセル化形式はネゴシエートです。

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
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	allowed vlan <i>vlan-list</i> add 、 remove 、および except キーワードが修正され、VLAN 1 および VLAN 1002 ～ 1005 の値が使用できるようになりました。

使用上のガイドライン

カプセル化

- **switchport trunk encapsulation** コマンドは ISL と IEEE 802.1Q の両方をサポートできるプラットフォーム、およびインターフェイス ハードウェアでのみサポートされます。
- トランクの一方の終端を IEEE 802.1Q トランクに、もう一方の終端を ISL、または非トランクポートに設定することはできません。ただし、1 つのポートを ISL トランクとして設定し、同一のスイッチ上の異なるポートに IEEE 802.1Q トランクを設定することはできます。
- **negotiate** キーワードを入力し、DTP ネゴシエーションがカプセル化形式を解決しない場合、ISL が形式として選択されます。このコマンドの **no** 形式は、トランクのカプセル化形式をデフォルトに戻します。

- **encapsulation** コマンドの **no** 形式は、トランクのカプセル化形式をデフォルトに戻します。

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、装置に適したデフォルト VLAN にリセットします。

許可 VLAN

- スパニングツリーのループまたはストームのリスクを軽減するため、許可リストから VLAN 1 を削除することで、個々の VLAN トランク ポート上で VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除すると、インターフェイスは管理トラフィックの送受信を続けます。たとえば、Cisco Discovery Protocol (CDP)、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)、Dynamic Trunking Protocol (DTP)、および VTP がこれに該当します。
- **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、フラグディング 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、トランキンング モードのデフォルトのトランク形式にかかわらず、スイッチング インターフェイスとして設定されたポートを、IEEE 802.1Q トランク形式でカプセル化を行うようにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk encapsulation dot1q
```

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ポートのデフォルトとして設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
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 gigabitethernet1/0/2
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 gigabitethernet1/0/2
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
<code>show interfaces switchport</code>	ポートブロッキング、ポート保護設定など、スイッチング（非ルーティング）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。
<code>switchport mode</code>	ポートの VLAN 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、スイッチ スタックまたはスタンドアロン スイッチ上で **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
```

シンタックスの説明

<i>vlan-id</i>	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（米国電気電子学会）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 プライオリティのタグおよび VLAN 0（ネイティブ VLAN）を使用するよう電話を設定します。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	音声 VLAN に関して IP Phone に指示しません。IP Phone は、電話キーパッドから入力された設定を使用します。
untagged	電話をタグなしの音声トラフィックを送信するよう設定します。これが電話のデフォルト設定になります。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

スイッチの Cisco IP Phone に接続しているスイッチ ポート上の Cisco Discovery Protocol（CDP）をイネーブルにし、Cisco IP Phone に設定情報を送信する必要があります。インターフェイス上で CDP は、デフォルトの状態です。

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、スイッチで Quality of Service（QoS; サービス品質）をイネーブルにすることを推奨します。また、**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、ポート ステータスが信頼されるよう設定することも推奨します。

VLAN ID を入力した場合、IP Phone は音声トラフィックを IEEE 802.1Q のフレームで、指定の VLAN ID のタグ付きで転送します。スイッチは、音声 VLAN 内に IEEE 802.1Q 音声トラフィックを入れます。

dot1q、**none** または **untagged** を選択した場合、スイッチは指定の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 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 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 上で、ポート セキュリティのいずれかのタイプがイネーブルになっている場合、ダイナミック ポートのセキュリティが自動的に音声 VLAN 上で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 ポートは、プライベート VLAN ポートとして設定できません。

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 をポートの音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet1/0/2
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（非ルーティング）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装置が、着信ポートで受信されたプライオリティ トラフィックを処理する方法を規定します。

system env temperature threshold yellow

イエロー スレッシュホールドの値を決定するイエローとレッドの温度スレッシュホールドの差を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **system env temperature threshold yellow** グローバル 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値に戻す場合は、このコマンドの **no** 形式を使用します。

system env temperature threshold yellow value

no system env temperature threshold yellow value

シンタックスの説明

value イエローとレッドのスレッシュホールド値の差（摂氏）を指定します。指定できる範囲は 10 ～ 25 です。デフォルト値は 10 です。

デフォルト

デフォルト値は次のとおりです。

表 2-37 温度スレッシュホールドのデフォルト値

スイッチ	イエローとレッドの差	レッド ¹
Catalyst 3750G-48TS	10°C	66°C
Catalyst 3750G-48PS	10°C	68°C
Catalyst 3750G-24TS-1U	10°C	65°C
Catalyst 3750G-24PS	10°C	61°C

1. レッドの温度スレッシュホールドは設定できません。

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)SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべてのスイッチで表示されますが、次のスイッチに対してのみ有効です。

- Catalyst 3750G-48TS
- Catalyst 3750G-48PS
- Catalyst 3750G-24TS-1U
- Catalyst 3750G-24PS

グリーンおよびレッドのスレッシュホールドは設定できませんが、イエローのスレッシュホールドは設定できます。イエローとレッドのスレッシュホールドの差を指定し、イエローのスレッシュホールドを設定するには、**system env temperature threshold yellow value** グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドのスレッシュホールドが 66°C で、イエローのスレッシュホールドを 51°C に設定する場合、**system env temperature threshold yellow 15** コマンドを使用してスレッシュホールドの差を 15 に設定します。



(注)

スイッチの内部温度センサは、内部システム温度を計測します。変動は ±5°C です。

例

次の例では、イエローとレッドのスレッシュホールドの差を 15 に設定します。

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

関連コマンド

コマンド	説明
show env temperature status	温度ステータスおよびスレッシュホールド レベルを表示します。

system mtu

ギガビットイーサネットポート、ルーテッドポート、またはファストイーサネット (10/100) ポートに最大パケットサイズ、または Maximum Transmission Unit (MTU; 最大伝送ユニット) を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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* | *routing bytes*}

no system mtu

シンタックスの説明

<i>bytes</i>	10 または 100 Mbps (メガビット / 秒) に設定されたポートのシステム 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 ポートで受信する最大 MTU です。
<i>jumbo bytes</i>	1000 Mbps 以上に動作するギガビット イーサネットポートには、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 ポートで受信する最大 MTU です。
<i>routing bytes</i>	ルーテッドパケットの最大 MTU を設定します。設定された MTU サイズをサポートするルーティングプロトコルで、最大 MTU をアダプタイズするように設定することもできます。指定できる範囲は、1500 バイトからシステム MTU 値までです。システム ルーティング MTU はルーテッドパケットの最大 MTU で、OSPF などのプロトコルのためにスイッチがルーティング更新でアダプタイズする最大 MTU でもあります。

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。ただし、システム MTU に別の値を設定した場合、スイッチのリセットによって適用すると、その設定値がルーテッドポートのデフォルト MTU サイズになります。

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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SEC	指定できる範囲は 1500 ~ 1998 バイトです。
12.2(25)SED	routing bytes キーワードが追加されました。

使用上のガイドライン

このコマンドでシステム MTU またはジャンボ MTU のサイズを変更した場合、新しい設定内容を反映させるには、スイッチをリセットする必要があります。**system mtu routing** コマンドの場合、変更内容を反映させるためにスイッチのリセットを行う必要はありません。

1000 Mbps で動作するギガビット イーサネット ポートは **system mtu** コマンドの影響を受けません。10/100 Mbps ポートは **system mtu jumbo** コマンドの影響を受けません。

ルーテッド ポートで MTU サイズを設定するには、**system mtu routing** コマンドを使用します。



(注)

システム MTU サイズを超えたルーティング MTU サイズを設定することはできません。システム MTU サイズを、現在設定されているルーティング MTU サイズより小さい値に変更した場合、設定した値が受け付けられますが、次にスイッチをリセットするまでは適用されません。設定変更が反映されると、ルーティング MTU サイズのデフォルトは新しいシステム MTU サイズになります。

特定のスイッチの許容範囲外の値を入力すると、値が拒否されます。



(注)

スイッチは、インターフェイスごとの MTU の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たフレームは、通常 CPU では受信されませんが、一部の packets (制御トラフィック、SNMP、Telnet、ルーティング プロトコルなど) は CPU に送信されます。

スイッチは packets をフラグメント化しないため、次の packets は廃棄されます。

- 出力インターフェイスでサポートされる packets サイズより大きいスイッチド packets
- ルーティング MTU 値より大きいルーテッド packets

たとえば、**system mtu** 値が 1998 バイトで **system mtu jumbo** 値が 5000 バイトの場合、1000 Mbps で動作するインターフェイスでは、5000 バイトまでの packets が受信できます。1998 バイトより大きい packets については、1000 Mbps で動作するインターフェイスでは受信できますが、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 ポートの最大ジャンボ packets 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、ギガビット イーサネット ポート、ルーテッド ポートに設定された packets サイズを表示します。

test cable-diagnostics tdr

インターフェイス上で Time Domain Reflector (TDR; タイム ドメイン反射率計) 機能を実行するには、スイッチ スタックまたはスタンドアロン スイッチで **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

シンタックスの説明

<i>interface-id</i>	TDR が動作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
12.1(19)EA1	このコマンドが導入されました。

使用上のガイドライン

TDR は、10/100/100 銅線イーサネット ポート上でのみサポートされます。10/100 ポート、10 ギガビット モジュール ポート、または Small Form-Factor Pluggable (SFP) モジュール ポートではサポートされていません。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、インターフェイスで TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

リンク ステータスがアップで速度が 10 または 100 Mbps (メガビット/秒) のインターフェイスで **test cable-diagnostics tdr interface interface-id** コマンドを入力すると、次のようなメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
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 結果を表示します。

tracert mac

指定の送信元 MAC（メディア アクセス制御）アドレスから指定の宛先 MAC アドレスまでを通過するパケットのレイヤ 2 パスを表示するには、スイッチ スタックまたはスタンドアロン スイッチ上で **tracert mac** イネーブル EXEC コマンドを使用します。

```
tracert mac [interface interface-id] {source-mac-address} [interface interface-id]
           {destination-mac-address} [vlan vlan-id] [detail]
```

シンタックスの説明

interface interface-id	（任意）送信元および宛先スイッチ上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 アドレスを指定します（16 進数）。
destination-mac-address	宛先スイッチの MAC アドレスを指定します（16 進数）。
vlan vlan-id	（任意）送信元スイッチから宛先スイッチを通過するパケットのレイヤ 2 パスを追跡する VLAN（仮想 LAN）を指定します。有効な VLAN ID は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 **tracert** を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにしないでください。

スイッチがパス内でレイヤ 2 **tracert** をサポートしていない装置を検知した場合、スイッチはレイヤ 2 追跡クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

レイヤ 2 **tracert** はユニキャスト トラフィックのみをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、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の MAC アドレスが同じ VLAN にある場合、**tracert mac** コマンド出力はレイヤ 2 パスを表示します。異なる VLAN にある送信元および宛先 MAC アドレスを指定しても、レイヤ 2 パスは識別されず、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 にある場合、送信元および宛先 MAC アドレス両方が属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを通じて 1 つのポートに接続されている場合（例えば、複数の CDP ネイバが 1 つのポートで検知される場合）、レイヤ 2 **tracert** の機能はサポートされません。1 つのポートで複数の CDP ネイバが検知される場合、レイヤ 2 パスは識別されず、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 アドレスを指定することで、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-C3750-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5 (2.2.5.5) : Gi0/0/3 => Gi0/0/1
con1 (2.2.1.1) : Gi0/0/1 => Gi0/0/2
con2 (2.2.2.2) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2 [WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、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-C3750-12T] (2.2.6.6)
con6/WS-C3750-12T/2.2.6.6 :
    Gi0/0/2 [auto, auto] => Gi0/0/3 [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することで、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-C3750-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5 (2.2.5.5) : Gi0/0/3 => Gi0/0/1
con1 (2.2.1.1) : Gi0/0/1 => Gi0/0/2
con2 (2.2.2.2) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2 [WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、送信元スイッチにスイッチが接続され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-C3750-12T] (2.2.5.5)
con5/WS-C3750-12T/2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [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、送信元 MAC アドレスの宛先ポートが見つからない場合のレイヤ 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異なる VLAN にある場合のレイヤ 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 にある場合のレイヤ 2 パスを示しています。

```
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	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名までを通過するパケットのレイヤ 2 パスを表示するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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]
```

シンタックスの説明

<i>source-ip-address</i>	送信元スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
<i>destination-ip-address</i>	宛先スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
<i>source-hostname</i>	送信元スイッチの IP ホスト名を指定します。
<i>destination-hostname</i>	宛先スイッチの IP ホスト名を指定します。
detail	（任意）詳細情報を表示するよう指定します。

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
12.1(14)EA1	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 traceroute を適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにしないでください。

スイッチがパス内でレイヤ 2 traceroute をサポートしていない装置を検知した場合、スイッチはレイヤ 2 追跡クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定した場合、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用し、IP アドレスとそれに対応する MAC (メディア アクセス制御) アドレスおよび VLAN (仮想 LAN) ID を関連付けます。

- 指定の IP アドレスの ARP のエントリが存在していた場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP の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、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを通じて 1 つのポートに接続されている場合（例えば、複数の CDP ネイバが 1 つのポートで検知される場合）、レイヤ 2 traceroute の機能はサポートされません。1 つのポートで複数の CDP ネイバが検知される場合、レイヤ 2 パスは識別されず、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て、送信元および宛先 IP アドレスを指定することで、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-C3750-12T/2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [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することで、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) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :    Gi0/0/3 => Gi0/1
con1          (2.2.1.1      ) :    Gi0/0/1 => Gi0/2
con2          (2.2.2.2      ) :    Gi0/0/2 => 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	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスを通過するパケットのレイヤ 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 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 コマンドで分類されたトラフィックの信頼状態を定義するには、スイッチ スタックまたはスタンドアロンスイッチ上で **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]

シンタックスの説明

cos	(任意) パケットの Class of Service (CoS; サービス クラス) 値を使用して、入力パケットを分類します。タグのないパケットの場合、デフォルト ポートの 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) を使用して、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。
ip-precedence	(任意) パケットの IP precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。

デフォルト

信頼性のない状態です。コマンド入力時、キーワードが指定されていない場合、デフォルトは **dscp** になります。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、特定のトラフィック間の Quality of Service (QoS; サービス品質) の信頼性を判別します。たとえば、特定の DSCP 値を持った着信トラフィックは信頼できます。クラス マップを設定し、着信トラフィックの DSCP 値を照合することで信頼できます。

このコマンドで設定された信頼性の値は、**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性の値を上書きします。

trust コマンドは、同一ポリシー マップ内の **set** ポリシーマップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

trust cos を指定した場合、QoS は受信した、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用し、パケットの DSCP 値を生成します。

trust dscp を指定した場合、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 パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

trust ip-precedence を指定した場合、QoS は入力パケットおよび IP precedence/DSCP マップから IP precedence 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルトポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

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、ポートの信頼状態を定義し、*class1* で分類されたトラフィックの着信 DSCP 値を信頼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	指定のクラスマップ名で、トラフィックの分類一致条件を定義します (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)。
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 タイマー時間を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}

シンタックスの説明

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 1 ～ 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
12.1(11)AX	このコマンドが導入されました。
12.2(25)SEC	<i>message-timer-interval</i> に指定できる範囲が、7 ～ 90 秒から 1 ～ 90 秒に変更されました。

使用上のガイドライン

UDLD は、2 つの動作モードをサポートしています。ノーマル モードとアグレッシブ モードです。ノーマル モードでは、UDLD は、光ファイバ接続でインターフェイスが誤接続されていること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 は光ファイバおよびツイストペア リンクの片方向トラフィックによる単一方向リンクと、光ファイバリンクでインターフェイスが誤接続されていることによる単一方向リンクも検出します。ノーマル モードおよびアグレッシブ モードに関する情報は、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」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。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **uddld reset** イネーブル EXEC コマンドは、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
- UDLD をグローバルに再びイネーブルにするには、**no uddld 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 **uddld {aggressive | 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。
- 指定したインターフェイスで UDLD を再びイネーブルにするには、**no uddld 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 **uddld port** または **uddld 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。
- 自動的に UDLD errdisable ステートから回復するには、**errdisable recovery cause uddld** および **errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを使用します。

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)# uddld enable
```

設定を確認するには、**show uddld** 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 uddld	すべてのポートまたは指定されたポートの UDLD 管理ステートまたは動作ステートを表示します。
uddld 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 uddld 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ぎます。
uddld 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。

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、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されるのを防ぐには、スイッチ スタックまたはスタンドアロン スイッチ上で **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 コマンドの設定に戻したり、光ファイバ以外のポートに対して入力された場合に 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]

シンタックスの説明

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 はイネーブルでなく、アグレッシブ モードでなく、ディセーブルでもありません。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したがい UDLD をイネーブルにします。

光ファイバ以外の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
12.1(11)AX	このコマンドが導入されました。
12.2(20)SE	disable キーワードが削除されました。

使用上のガイドライン

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、2 つの動作モードをサポートしています。ノーマル モードとアグレッシブ モードです。ノーマル モードでは、UDLD は、光ファイバ接続でインターフェイスが誤接続されていること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 は光ファイバおよびツイストペア リンクの片方向トラフィックによる単一方向リンクと、光ファイバリンクでインターフェイスが誤接続されていることによる単一方向リンクも検出します。ノーマル モードおよびアグレッシブ モードに関する情報は、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。

UDLD をノーマル モードで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。UDLD をアグレッシブ モードで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 を光ファイバ以外の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。

uddld enable または **uddld 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 **uddld 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 **uddld** 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 を光ファイバ以外の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。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **uddld reset** イネーブル EXEC コマンドは、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
- UDLD をグローバルに再びイネーブルにするには、**no uddld 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 **uddld {aggressive | 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。
- 指定したインターフェイスで UDLD を再びイネーブルにするには、**no uddld 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 **uddld port** または **uddld 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。
- 自動的に UDLD errdisable ステートから回復するには、**errdisable recovery cause uddld** および **errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、特定のポートで UDLD をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# uddld port
```

次の例では、**uddld** 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 gigabitethernet6/0/1
Switch(config-if)# no uddld port
```

設定を確認するには、**show running-config** または **show uddld 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 uddld	すべてのポートまたは指定されたポートの UDLD 管理ステートまたは動作ステートを表示します。
uddld	UDLD のアグレッシブまたはノーマル モードをイネーブルにします。また、設定可能なメッセージ タイマー時間を設定します。
uddld 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。

udld reset

(スパニングツリー、Port Aggregation Protocol [PAgP]、Dynamic Trunking Protocol [DTP] のような他の機能がイネーブルで通常動作をしている場合でも) UniDirectional Link Detection (UDLD; 単一方向リンク検出) によってディセーブルにされたすべてのインターフェイスをリセットし、トラフィックの通過を再開することを許可するには、**udld reset** イネーブル EXEC コマンドを使用します。

udld reset

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

インターフェイス コンフィギュレーションで、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 の実行を開始し、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 によってディセーブルにされたすべてのインターフェイスを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 管理ステートまたは動作ステートを表示します。
udld	UDLD のアグレッシブまたはノーマル モードをイネーブルにします。また、設定可能なメッセージ タイマー時間を設定します。
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されるのを防ぎます。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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) のコンフィギュレーション情報は、常に VLAN データベースに保存されます。VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) モードがトランスペアレントなときは、拡張範囲 VLAN (VLAN ID が 1006 以上) を作成できます。すると、VTP モード、VTP 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、コンフィギュレーションをスイッチ スタートアップ コンフィギュレーション ファイルに保存できます。

```

vlan vlan-id
no vlan vlan-id

```

シンタックスの説明	vlan-id	追加および設定する VLAN の ID。vlan-id に指定できる範囲は 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
	12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン	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 によって学習されませんし、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、VTP 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ますし、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 VLAN 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 VTP 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、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 モードを開始できません。

VLAN ID を指定して **vlan** コマンドを入力すると、**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 でサポートされる VLAN コンフィギュレーション コマンドは、**mtu mtu-size**、**private-vlan**、および **remote-span** のみです。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 All Route Explorer (ARE) 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 に対してのみ適用します。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 Concentrator Relay Function (CRF; コンセントレータ リレー機能) モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
 - この VLAN のバックアップ CRF モードを **enable** (イネーブル) にします。
 - この VLAN のバックアップ CRF モードを **disable** (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、Fiber Distributed Data Interface (FDDI) -Network Entity Title (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。FDDI-NET、TrBRF、およびトークンリング NET VLAN については、デフォルトのブリッジ番号は 0 (ソースルーティングブリッジなし) です。**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
- **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) を増加させ、**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 2-38 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の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 アドバタイズに限りて設定します。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 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 バージョン 2 (v) 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。デフォルト値は 1500 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 4 桁の数字 (先行ゼロを含む) で VLAN ID 番号と同じです。
- **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。
- **private-vlan** : VLAN をプライベート VLAN のコミュニティ、独立、またはプライマリ VLAN として設定するか、またはプライベート VLAN のプライマリ VLAN とセカンダリ VLAN 間でアソシエーションを設定します。詳細は、**private-vlan** コマンドを参照してください。
- **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 特性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 ポートも非アクティブとなります。VTP がイネーブルの場合、新しい RSPAN VLAN は、1024 より小さい番号の VLAN ID の VTP により伝播されます。学習は VLAN 上でディセーブルになります。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 ID は 1 ~ 4294967294 です。この数字は、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* : Spanning-Tree Explorer (STE) 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 Spanning-Tree Protocol (STP; スパニングツリー プロトコル) 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 にトランスレーショナルブリッジングが行われている 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 2-38 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 <i>vlan-name</i> 、 media <i>ethernet</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 remote-span 、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> 、 media <i>fddi</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 ring <i>ring-number</i> 、 parent <i>parent-vlan-id</i> 、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> 、 media <i>fd-net</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 bridge <i>bridge-number</i> 、 stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i> VTP v2 モードがディセーブルの場合、 stp type を <i>auto</i> 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 <i>vlan-name</i> 、 media <i>tokenring</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 ring <i>ring-number</i> 、 parent <i>parent-vlan-id</i> 、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
TrCRF	VTP v2 モードがイネーブルの場合 name <i>vlan-name</i> 、 media <i>tokenring</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 ring <i>ring-number</i> 、 parent <i>parent-vlan-id</i> 、 bridge type { <i>srb</i> <i>srt</i> }、 are <i>are-number</i> 、 ste <i>ste-number</i> 、 backupcrf { <i>enable</i> <i>disable</i> }、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
トークンリング NET	VTP v1 モードがイネーブルの場合 name <i>vlan-name</i> 、 media <i>tr-net</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 bridge <i>bridge-number</i> 、 stp type { <i>ieee</i> <i>ibm</i> }、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
TrBRF	VTP v2 モードがイネーブルの場合 name <i>vlan-name</i> 、 media <i>tr-net</i> 、 state { <i>suspend</i> <i>active</i> }、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 bridge <i>bridge-number</i> 、 stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>

表 2-39 では、VLAN の設定規則を説明します。

表 2-39 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にしないでください。 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 CRF だけをイネーブルにできます。
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。

表 2-39 VLAN 設定規則 (続き)

設定	規則
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にしないでください。
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 へのポイント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 *VLANxxxx* の *vlan-name* が含まれています。ここで、xxxx は 4 桁の数字 (先行ゼロを含む) で VLAN ID 番号と同じです。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、新しい VLAN をすべてデフォルト特性で作成し、**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	設定されたすべての VLAN または 1 つの VLAN (VLAN ID または名前が指定されている場合) のパラメータを管理ドメインに表示します。
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、スイッチ スタックまたはスタンドアロン スイッチ上で **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 ID 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 アドバタイズに限りて設定します。これらの VLAN はローカルに停止されます。

シンタックスの説明

<i>vlan-id</i>	設定された VLAN の ID。指定できる ID は、1 ~ 1005 です。この数字は、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。
<i>are are-number</i>	(任意) この VLAN の All-Route Explorer (ARE) ホップの最大数を指定します。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。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 Concentrator Relay Function (CRF; コンセントレータ リレー機能) モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。 - この VLAN のバックアップ CRF モードを enable (イネーブル) にします。 - この VLAN のバックアップ CRF モードを disable (ディセーブル) にします。

bridge <i>bridge-number</i> type { <i>srb</i> <i>srt</i> }	(任意) 論理分散ソースルーティングブリッジ、すなわち Fiber Distributed Data Interface (FDDI) - Network Entity Title (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 { <i>ethernet</i> <i>fddi</i> <i>fd-net</i> <i>tokenring</i> <i>tr-net</i> }	(任意) VLAN メディア タイプを指定します。表 2-40 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 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 <i>mtu-size</i>	(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 <i>vlan-name</i>	(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 <i>parent-vlan-id</i>	(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 <i>ring-number</i>	(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 <i>said-value</i>	(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 ID は 1 ～ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。
state { <i>suspend</i> <i>active</i> }	(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 <i>ste-number</i>	(任意) Spanning-Tree Explorer (STE) ホップの最大数を指定します。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。

stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }	(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 <i>tb-vlan1-id</i> および tb-vlan2 <i>tb-vlan2-id</i>	(任意) この VLAN にトランスレーショナルブリッジングが行われている 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 2-40 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 2-40 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 <i>vlan-id</i> [name <i>vlan-name</i>] media ethernet [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fddi [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI-NET	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fd-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] 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 <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
TrCRF	VTP v2 モードがイネーブルの場合 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [bridge type { <i>srb</i> <i>srt</i> }] [are <i>are-number</i>] [ste <i>ste-number</i>] [backupcrf { <i>enable</i> <i>disable</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
トークンリング NET	VTP v1 モードがイネーブルの場合 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
TrBRF	VTP v2 モードがイネーブルの場合 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]

表 2-41 では、VLAN の設定規則を説明します。

表 2-41 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にしないでください。 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 CRF だけをイネーブルにできます。
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にしないでください。
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する必要があります。 (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 4 桁の数字 (先行ゼロを含む) で VLAN ID 番号と同じです。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

このコマンド 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。VLAN モードがトランスペアレントの場合、VLAN 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 VLAN 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** も存在しない場合) 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 4 桁の数字 [先行ゼロを含む] で VLAN ID 番号と同じです)。
- **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-id tb-vlan2** 形式を使用すると、1 つまたは複数の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ナルブリッジ 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 **VLANxxxx** の **vlan-name** が含まれています。ここで、**xxxx** は 4 桁の数字 (先行ゼロを含む) で VLAN ID 番号と同じです。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
<code>show vlan</code>	設定されたすべての VLAN または 1 つの VLAN (VLAN ID または名前が指定されている場合) のパラメータを管理ドメインに表示します。
<code>vlan</code> (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 access-map

VLAN (仮想 LAN) パケット フィルタリング用の VLAN マップのエントリを作成または修正するには、スイッチ スタックまたはスタンドアロン スイッチ上で **vlan access-map** グローバル コンフィギュレーション コマンドを使用します。このエントリは VLAN アクセスマップ コンフィギュレーションにモードを変更します。VLAN マップのエントリを削除する場合は、このコマンドの **no** 形式を使用します。**vlan 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、VLAN マップを 1 つまたは複数の VLAN に適用します。

```
vlan access-map name [number]
```

```
no vlan access-map name [number]
```

シンタックスの説明

<i>name</i>	VLAN マップ名
<i>number</i>	(任意) 作成または修正するマップ エントリの一連の番号 (0 ~ 65535)。VLAN マップを作成し、一連の番号が指定されていない場合は、自動的に 10 から始まる番号が割り当てられます (10 ずつ増加)。この番号は、VLAN のアクセスマップ エントリに追加、または削除される順番です。

デフォルト

VLAN マップ エントリおよび VLAN に適用する VLAN マップはありません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードでは、このコマンドを使用して VLAN マップを作成または修正します。このエントリは VLAN アクセス マップ コンフィギュレーションにモードを変更します。アクセスマップ コンフィギュレーションでは、**match** アクセス マップ コンフィギュレーション コマンドを使用して、照合するための IP または非 IP トラフィックのアクセス リストを指定できます。また、**action** コマンドを使用して、パケットの転送と廃棄を決める条件を設定できます。

VLAN アクセスマップ コンフィギュレーション モードでは、次のコマンドを利用できます。

- **action** : 実行すべきアクションを設定します (転送または廃棄)。
- **default** : コマンドをそのデフォルトに設定します。
- **exit** : VLAN アクセスマップ コンフィギュレーション モードを終了します。

- **match** : 照合する変数を設定します (IP アドレスまたは MAC [メディア アクセス制御] アドレス)。
- **no** : コマンドを無効にするか、またはデフォルトに設定します。

エントリ番号 (一連の番号) を指定しない場合、マップの最後に追加されます。

VLAN マップは VLAN ごとに 1 つのみ可能で、パケットが VLAN に受信されると適用されます。

単一のエントリを削除するには、**no vlan access-map name [number]** コマンドを一連の番号を指定して使用します。

グローバル コンフィギュレーション モードでは、**vlan 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、マップを 1 つまたは複数の VLAN に適用します。

VLAN マップ エントリに関する詳細情報は、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、*vac1* という名前の VLAN マップを作成し、一致条件および処理を適用します。マップに他のエントリが存在していない場合、エントリは 10 になります。

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

次の例では、VLAN マップ *vac1* を削除する方法を示します。

```
Switch(config)# no vlan access-map vac1
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップ エントリのアクションを設定します。
match (アクセスマップ コンフィギュレーション)	1 つまたは複数のアクセス リストに対しパケットを照合する VLAN マップを設定します。
show vlan access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップの情報を表示します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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できます。コンフィギュレーション情報は、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。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンドモード

イネーブル EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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。

いったん 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 パラメータの変更が完了すると、次の編集バッファ処理コマンドを使用できます。

- **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 モードを続けます。



(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廃棄し、設定しようとしたデータベースをスイッチ上に実装されている 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 モードを続けます。
- **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ンになりません。

show vlan イネーブル EXEC コマンドを入力すれば、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の VLAN 7 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	管理ドメイン内の設定されたすべての 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。

vlan dot1q tag native

すべての 802.1Q トランク ポートでネイティブ VLAN（仮想 LAN）フレームのタグgingをイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **vlan dot1q tag native** グローバル 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。

vlan dot1q tag native

no vlan dot1q tag native

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IEEE（米国電気電子学会）802.1Q ネイティブ VLAN のタグging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)EA1	このコマンドが導入されました。

使用上のガイドライン

イネーブルの場合、すべての IEEE 802.1Q トランク ポートから発信するネイティブ VLAN パケットはタグ付けされます。

ディセーブルの場合、すべての IEEE 802.1Q トランク ポートから発信するネイティブ VLAN パケットはタグ付けされません。

このコマンドは IEEE 802.1Q トンネリング機能と一緒に使用できます。この機能は、サービスプロバイダー ネットワークのエッジスイッチで動作し、VLAN 階層内 VLAN を使用し、タグ付きパケットをタグリングすることで、VLAN スペースを拡張します。サービスプロバイダー ネットワークへパケットを送信するには、IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通るパケットは、IEEE 802.1Q トランク上でも伝送できます。IEEE 802.1Q トランクのネイティブ VLAN が、同じスイッチ上のトンネリング ポートのネイティブ VLAN と一致する場合、ネイティブ VLAN 上のトラフィックは送信トランク ポート上でタグ付けされません。このコマンドにより、すべての IEEE 802.1Q トランク ポート上のネイティブ VLAN パケットはタグ付けされます。

IEEE 802.1Q プロトコル トンネリングに関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例 次の例では、ネイティブ VLAN フレーム上で IEEE 802.1Q タグリングをイネーブルにする方法を示します。

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

設定を確認するには、**show vlan dot1q tag native** 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 dot1q tag native	IEEE 802.1Q ネイティブ VLAN のタグリング ステータスを表示します。

vlan filter

VLAN（仮想 LAN）マップを 1 つまたは複数の VLAN 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 **vlan filter** グローバル 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。

```
vlan filter mapname vlan-list {list | all}
```

```
no vlan filter mapname vlan-list {list | all}
```

シンタックスの説明

<i>mapname</i>	VLAN マップのエントリ名
<i>list</i>	1 つまたは複数の VLAN のリスト (tt、uu-vv、xx、yy-zz 形式)。カンマおよびダッシュの前後のスペースは任意に挿入できます。指定できる範囲は、1 ～ 4094 です。
all	すべての VLAN からフィルタを削除します。

デフォルト

VLAN フィルタはありません。

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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

誤って多くのパケットを廃棄、または設定処理の途中で接続をディセーブルにしてしまうことを回避するため、VLAN に VLAN アクセス マップを適用する前に、マップの定義を完成させておくことを推奨します。

VLAN マップ エントリに関する詳細情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、VLAN 20 および VLAN 30 に対して VLAN マップ エントリの *map1* を適用する方法を示します。

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

次の例では、VLAN マップ エントリ *mac1* を VLAN 20 から削除する方法を示します。

```
Switch(config)# no vlan filter map1 vlan-list 20
```

設定を確認するには、**show vlan filter** 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 access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップの情報を表示します。
show vlan filter	すべての VLAN フィルタリングの情報、特定の VLAN または VLAN アクセス マップの情報を表示します。
vlan access-map	VLAN パケット フィルタリング用の VLAN マップのエントリを作成します。

vmps reconfirm (イネーブル EXEC)

ただちに VLAN (仮想 LAN) 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 割り当てを再確認するには、スイッチ スタックまたはスタンドアロン スイッチ上で **vmps reconfirm** イネーブル EXEC コマンドを使用します。

vmps reconfirm

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンド モード イネーブル EXEC

コマンド履歴	リリース	変更内容
	12.1(11)AX	このコマンドが導入されました。

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
```

設定を確認するには、**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 行を調べます。**show vmps** コマンドは、再確認タイマー切れの結果または **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 (仮想 LAN) Query Protocol (VQP) クライアントの再確認間隔を変更するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明	<i>interval</i>	ダイナミック VLAN 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
	12.1(11)AX	このコマンドが導入されました。

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
```

設定を確認するには、**show vmps** イネーブル EXEC コマンドを入力して、Reconfirm Interval 行を調べます。

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（仮想 LAN）Query Protocol（VQP）クライアントのサーバあたりの再試行回数を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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

シンタックスの説明

<i>count</i>	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）に接続しようとする回数。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
12.1(11)AX	このコマンドが導入されました。

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
```

設定を確認するには、**show vmps** イネーブル EXEC コマンドを入力して、Server Retry Count 行を調べます。

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、スイッチ スタックまたはスタンドアロン スイッチ上で **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*]

シンタックスの説明

<i>ipaddress</i>	プライマリまたはセカンダリ VMPS サーバの IP アドレスまたはホスト名。ホスト名を指定する場合には、Domain Name System (DNS; ドメイン ネーム システム) サーバが設定されている必要があります。
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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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。その代わりに、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
```

設定を確認するには、**show vmps** イネーブル EXEC コマンドを入力して、VMPS Domain Server 行を調べます。

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修正するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}
```

シンタックスの説明

domain <i>domain-name</i>	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。ドメイン名では大文字と小文字が区別されません。
file <i>filename</i>	VTP VLAN 設定が保存されている Cisco IOS ファイルシステムのファイルを指定します。
interface <i>name</i>	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) VTP IP アップデータとしてこのインターフェイスの IP アドレスのみ使用します。
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 <i>password</i>	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。パスワードでは大文字と小文字が区別されます。
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 <i>number</i>	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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、つぎの条件によって VTP および VLAN 設定が選択されます。

- 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 VLAN 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 ファイルから選択されます。

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 ステートになります。非管理ドメイン ステートの間は、ローカル VLAN 設定に変更が生じててもスイッチは VTP アドバタイズを送信しません。スイッチは、トランッ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を再び開始す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、サーバのコンフィギュレーションを複製します。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、そのコンフィギュレーションは許可されません。
- 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。
- スイッチをパスワードがない状態に戻す場合は、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。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、装置ストレージ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ン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、プルーンング、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) の特性を設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **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}
```

シンタックスの説明

domain <i>domain-name</i>	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。ドメイン名では大文字と小文字が区別されます。
password <i>password</i>	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。パスワードでは大文字と小文字が区別されます。
pruning	VTP 管理ドメインでプルーンングをイネーブルにします。VTP プルーンングは、プルーンング適格 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。

プルーン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
12.1(11)AX	このコマンドが導入されました。

使用上のガイドライン

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、サーバのコンフィギュレーションを複製します。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 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)

VLAN 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 ステートになります。非管理ドメイン ステートの間は、ローカル VLAN 設定に変更が生じてスイッチは VTP アドバタイズを送信しません。スイッチは、トランッ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られません。

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。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に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) または Token Ring Concentrator Relay Function (TrCRF; トークンリングコンセンレータリレー機能) 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、VTP 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。

