CHAPTER 2

Cisco CGS 2520 の Cisco IOS コマンド

aaa accounting dot1x

認証、認可、およびアカウンティング（AAA）アカウンティングをイネーブルにして、IEEE 802.1x セッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に使用します。
start-stop	プロセスの開始時に start アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start アカウンティング通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • *name*：サーバ グループ名 • **radius**：全 RADIUS ホストのリスト • **tacacs+**：全 TACACS+ ホストのリスト **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードは、複数入力できます。

radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、RADIUS サーバへのアクセスが必要です。

（注）　インターフェイスに IEEE 802.1x RADIUS アカウンティングを設定する前に、**authentication periodic** インターフェイス コンフィギュレーション コマンドを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 accounting dot1x
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)#
```

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

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1x が動作しているインターフェイスで使用する 1 つ以上の AAA メソッドを指定します。
aaa-new-model	AAA アクセス コントロール モデルをイネーブルにします。構文情報については、『**Cisco IOS Security Command Reference, Release 12.2**』>「**Authentication, Authorization, and Accounting**」>「**Authentication Commands**」を参照してください。
authentication periodic	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。
authentication timer	再認証の試行の間隔（秒）を設定します。

aaa authentication dot1x

IEEE 802.1x に準拠するポートで認証、認可、およびアカウンティング（AAA）方式を使用するように指定するには **aaa authentication dot1x** グローバル コンフィギュレーション コマンドを使用します。認証をディセーブルにするには、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**}

構文の説明

default	この引数の後に続く、リストされた認証方式をログイン時のデフォルトの方式として使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。

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

デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために一定の順序で試みる方式を指定します。実際に IEEE 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。

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

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

例

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

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

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

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。構文情報については、『**Cisco IOS Security Command Reference, Release 12.2**』>「**Authentication, Authorization, and Accounting**」>「**Authentication Commands**」を参照してください。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

action

VLAN アクセス マップ エントリに対してアクションを設定するには、**action** アクセスマップ コンフィギュレーション コマンドを使用します。このアクションをデフォルト値である forward に設定するには、このコマンドの **no** 形式を使用します。

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

no action

構文の説明

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

デフォルト

デフォルトのアクションは、パケットの転送です。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

例

次の例では、VLAN アクセス マップ *vmap4* を指定し VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップは、パケットがアクセス リスト *al2* に定義された条件に一致する場合に、VLAN がその IP パケットを転送するように指定します。

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

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

関連コマンド

コマンド	説明
access-list {deny | permit}	番号付き標準 ACL を設定します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
ip access-list	名前付きアクセス リストを作成します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
match（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	スイッチで作成された VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

alarm contact

外部アラームのトリガーおよび重大度を設定するには、**alarm contact** グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

alarm contact {*contact-number* {**description** *string* | **severity** {**critical** | **major** | **minor**} | **trigger** {**closed | open**}} | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}

no alarm contact {*contact-number* {**description** | **severity** | **trigger**} | **all** {**severity** | **trigger**}

contact-number	特定のアラーム接点番号を設定します。指定できる範囲は 1 ～ 4 です。
description *string*	アラーム接点番号の説明を追加します。説明の文字列の長さは 80 文字以下の英数字にすることができます。この文字列は、アラームのトリガー時に生成されるシステム メッセージに含まれます。
all	すべてのアラーム接点を設定します。
severity	アラームがトリガーされたときに設定される重大度を設定します。重大度はアラーム通知に含まれます。**no alarm contact severity** を入力すると、重大度がマイナーに設定されます。
critical	重大度をクリティカルに設定します。
major	重大度をメジャーに設定します。
minor	重大度をマイナーに設定します。
trigger	アラームをトリガーする状態を設定します（接続回線がオープンか、またはクローズか）。**no alarm contact trigger** を入力すると、トリガーがクローズに設定されます。
closed	接点がクローズの場合に、アラームがトリガーされることを指定します。
open	接点がオープンの場合に、アラームがトリガーされることを指定します。

デフォルト

アラーム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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

no alarm contact *contact-number* **description** は、説明を空の文字列に設定します。

no alarm contact {*contact-number* | **all**} **severity** は、アラーム接点の重大度をマイナーに設定します。

no alarm contact {*contact-number* | **all**} **trigger** は、外部アラーム接点のトリガーをクローズに設定します。

例

次の例は、接点がオープンのときにクリティカル アラームを報告するようにアラーム接点番号 1 を設定する方法を示します。

```
Switch(config)# alarm contact 1 description main_lab_door
Switch(config)# alarm contact 1 severity critical
Switch(config)# alarm contact 1 trigger open
Dec  4 10:34:09.049: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm asserted:
main_lab_door
```

show env alarm-contact または **show running-config** 特権 EXEC コマンドを入力すると、設定を確認できます。

```
Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      asserted
   Description: main_lab_door
   Severity:    critical
   Trigger:     open
```

次の例は、クリア アラーム接点番号 1 と show のコマンド出力を設定する方法を示します。

```
Switch(config)# no alarm contact 1 description
Dec  4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared:
main_lab_door Dec  4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm contact 1 severity
Dec  4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1 Dec  4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm contact 1 trigger open
Dec  4 10:39:56.547: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1

Switch(config)# end
Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
Switch# show hard led
SWITCH: 1
SYSTEM: GREEN
MGMT: GREEN
ALARM 1: BLACK
ALARM 2: BLACK
ALARM 3: BLACK
ALARM 4: BLACK
```

関連コマンド

コマンド	説明
show env alarm-contact	スイッチのアラーム設定およびステータスを表示します。

alarm facility fcs-hysteresis

フレーム チェック シーケンス（FCS）エラー ヒステリシスしきい値を FCS ビットエラー レートの変動率として設定するには、**alarm facility fcs-hysteresis** グローバル コンフィギュレーション コマンドを使用します。FCS エラー ヒステリシスしきい値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

alarm facility fcs-hysteresis *percentage*

no alarm facility fcs-hysteresis *percentage*

構文の説明

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

デフォルト

デフォルトのしきい値は 10% 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

FCS ヒステリシスしきい値はスイッチすべてのポートで設定します。ポートごとに FCS エラー レートを設定するには、**fcs-threshold** インターフェイス コンフィギュレーション コマンドを使用します。

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

例

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

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

関連コマンド

コマンド	説明
fcs-threshold	インターフェイスの FCS エラー レートを設定します。
show running-config	FCS ヒステリシスしきい値（デフォルト値以外の場合）を含むスイッチの実行コンフィギュレーションを表示します。

alarm facility power-supply

システムがデュアル電源モードで稼動している場合に、電源の欠落または障害を検出するアラーム オプションを設定するには、**alarm facility power-supply** グローバル コンフィギュレーション コマンドを使用します。指定した設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

disable	電源アラームをディセーブルにします。
notifies	電源装置アラーム トラップを SNMP サーバに送信します。
relay major	リレー回路にアラームを送信します。
Syslog	電源装置アラーム トラップを Syslog サーバに送信します。

デフォルト

電源アラーム メッセージは保存されますが、SNMP サーバ、リレー、または syslog サーバに送信されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

電源アラームは、システムがデュアル電源モードの場合にのみ生成されます。2 つ目の電源が接続された場合、**power-supply dual** グローバル コンフィギュレーション コマンドを使用してデュアル電源モードの動作を設定します。

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

例

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

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

関連コマンド

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

alarm facility temperature

プライマリ温度モニタリング アラームの設定または上限値が低いセカンダリ温度アラームしきい値を設定するには、**alarm facility temperature** グローバル コンフィギュレーション コマンドを使用します。温度モニタリング アラームの設定を削除またはセカンダリ温度アラームをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

high	プライマリ温度アラームまたはセカンダリ温度アラームの高温しきい値を設定します。指定できる範囲は、–238 ～ 572 ºF（–150 ～ 300 ºC）です。
low	プライマリ温度アラームまたはセカンダリ温度アラームの低温しきい値を設定します。指定できる範囲は、-328 ～ 482 ºF（-200 ～ 250 ºC）です。
notifies	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを SNMP サーバに送信します。
relay major	プライマリ温度アラームまたはセカンダリ温度アラームがリレー回路に送信されます。
Syslog	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを Syslog サーバに送信します。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

温度が最大プライマリ温度のしきい値よりも小さいしきい値に達した場合に高温アラームをトリガーするには、セカンダリ温度アラームを使用します。温度しきい値とアラーム オプションを設定できます。

notifies キーワードを使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

例

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

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

次の例では、セカンダリ温度アラームをディセーブルにする方法を示します。

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

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

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

関連コマンド

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

alarm profile（グローバル コンフィギュレーション）

アラーム プロファイルを作成し、アラーム プロファイル コンフィギュレーション モードを開始するには、**alarm profile** グローバル コンフィギュレーション コマンドを使用します。アラーム プロファイルを削除するには、このコマンドの **no** 形式を使用します。

alarm profile *name*

no alarm profile *name*

構文の説明

name	アラームのプロファイル名です。

デフォルト

アラーム プロファイルは作成されません。

プロファイルを作成しても、アラームは 1 つもイネーブルになりません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラームプロファイル モードの使用可能なコマンド：

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

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

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

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

表 2-1　AlarmList ID 番号とアラームの説明

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

アラーム プロファイルを作成すると、**alarm-profile** インターフェイス コンフィギュレーション コマンドを使用して、プロファイルをインターフェイスに関連付けられます。

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

例

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

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

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

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

関連コマンド

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

alarm profile（インターフェイス コンフィギュレーション）

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

alarm profile *name*

no alarm profile

構文の説明

name	アラームのプロファイル名です。

デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラーム プロファイルを作成して、アラームを 1 つ以上イネーブルにし、アラーム オプションを指定するには、**alarm profile** グローバル コンフィギュレーション コマンドを使用します。

インターフェイスに関連付けられるアラーム プロファイルは 1 つのみです。

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

例

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

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

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

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

関連コマンド.

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

alarm relay-mode

スイッチのアラーム リレー モードをポジティブまたはネガティブに設定するには、**alarm relay-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。アラーム リレー モードをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

alarm relay-mode {*negative*}

no alarm relay-mode {*negative*}

構文の説明

negative	アラーム リレー モードをネガティブに設定します。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラーム リレーの動作を元に戻すには、このコマンドを使用します。アラーム リレー モードがネガティブに設定されている場合、アラーム リレーは通常クローズされています。アラーム イベントが 1 つ以上検出されると、該当するアラーム リレーがオープンされます。

例

次の例では、アラーム リレーをネガティブ モードに設定する方法を示します。

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

関連コマンド

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

archive download-sw

新しいイメージを TFTP サーバからスイッチにダウンロードし、既存のイメージを上書きまたは保持するには、**archive download-sw** 特権 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** | **/overwrite** | **/reload** | **/safe** | **/warm**} *source-url*

構文の説明

/force-reload	ソフトウェア イメージのダウンロードが成功した後で無条件にシステムのリロードを強制します。
/imageonly	ソフトウェア イメージだけをダウンロードし、組み込みデバイス マネージャに関連する HTML ファイルはダウンロードしません。既存のバージョンの HTML ファイルは、既存のバージョンが上書きまたは削除されている場合にだけ削除されます。
/leave-old-sw	ダウンロードに成功した後で古いソフトウェア バージョンを保存します。
/no-set-boot	新しいソフトウェア イメージのダウンロードに成功した後に、BOOT 環境変数の設定が新しいソフトウェア イメージを指定するように変更されません。
/no-version-check	互換性のないイメージをインストールしないように確認せずに、ソフトウェア イメージをダウンロードします。
/overwrite	ダウンロードされたイメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	変更された設定が保存されていない場合を除き、イメージのダウンロードに成功した後でシステムをリロードします。
/safe	現在のソフトウェア イメージを保存します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。

/warm	イメージをダウンロードしたら、ストレージからイメージを読み取らずにスイッチをリロードします。
source-url	ローカルまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文：**flash:** • FTP の構文：**ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文：**http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文：**https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文：**rcp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、スイッチにダウンロードし、インストールするソフトウェア イメージです。

デフォルト

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

ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。

新しいイメージは flash: ファイル システムにダウンロードされます。

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

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

ダウンロードするイメージでのバージョンの互換性がチェックされます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマン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** オプションを指定すると、十分なフラッシュ メモリがない場合には新しいイメージのダウンロードが行われないようにすることができます。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合に、エラーが発生します。

/leave-old-sw オプションを使用し、新しいイメージをダウンロードしたときに古いイメージが上書きされなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。詳細については、「delete」（P.2-116）を参照してください。

（注）　**/no-version-check** オプションの使用には注意が必要です。このオプションを使用すると、最初にイメージにスイッチとの互換性があることを確認せずにイメージをダウンロードできます。

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と同じではないことを確認します。イメージが同じである場合は、ダウンロードは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがダウンロードされます。

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

例

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

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

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

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

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

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

関連コマンド

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

archive tar

archive tar 特権 EXEC コマンドを使用して、tar ファイルの作成、tar ファイル内のファイルの一覧表示、または tar ファイルからのファイルの抽出を行います。

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

構文の説明

/create *destination-url* **flash:**/*file-url*	ローカルまたはネットワーク ファイル システムに新しい tar ファイルを作成します。 *destination-url* には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスおよび作成する tar ファイルの名前を指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文：**flash:** • FTP の構文：**ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • Remote Copy Protocol（RCP）の構文：**rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、作成する tar ファイルです。 **flash:**/*file-url* には、新しい tar ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。 送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。
/table *source-url*	既存の tar ファイルの内容を画面に表示します。 *source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文：**flash:** • FTP の構文：**ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • RCP の構文：**rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、表示する tar ファイルです。

/xtract *source-url* **flash:**/*file-url* [*dir/file...*]	tar ファイルからローカル ファイル システムにファイルを抽出します。 *source-url* には、ローカル ファイル システムの*送信元* URL エイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文：**flash:** • FTP の構文：**ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • RCP の構文：**rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、抽出される tar ファイルです。 **flash:**/*file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

イメージ名では、大文字と小文字が区別されます。

例

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

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

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

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
info (219 bytes)
image_name-mz.122-release/(directory)
image_name-mz.122-release(610856 bytes)
image_name-mz.122-release/info (219 bytes)
info.ver (219 bytes)
```

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

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
image_name-mz.122-release/html
image_name-mz.122-release/html/ (directory)
image_name-mz.122-release/html/const.htm (556 bytes)
image_name-mz.122-release/html/xhome.htm (9373 bytes)
image_name-mz.122-release/html/menu.css (1654 bytes)
<output truncated>
```

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

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

関連コマンド

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

archive upload-sw

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

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

構文の説明

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

デフォルト

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

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

イメージ名では、大文字と小文字が区別されます。

例

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

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

関連コマンド

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

arp access-list

Address Resolution Protocol（ARP; アドレス解決プロトコル）Access Control List（ACL; アクセス コントロール リスト）を定義する場合、または以前定義したリストの最後にコマンドを追加する場合は、**arp access-list** グローバル コンフィギュレーション コマンドを使用します。指定された ARP アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

arp access-list *acl-name*

no arp access-list *acl-name*

構文の説明

acl-name	ACL の名前

デフォルト

ARP アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

- **default**：コマンドをデフォルト設定に戻します。
- **deny**：パケットを拒否するように指定します。詳細については、「deny（ARP アクセス リスト コンフィギュレーション）」（P.2-117）を参照してください。
- **exit**：ARP アクセス リスト コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。
- **permit**：パケットを転送するように指定します。詳細については、「permit（ARP アクセス リスト コンフィギュレーション）」（P.2-357）を参照してください。

指定された一致条件に基づいて ARP パケットを転送またはドロップするには、**permit** または **deny** アクセス リスト コンフィギュレーション コマンドを使用します。

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

例

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

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

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

関連コマンド

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

authentication control-direction

authentication control-direction インターフェイス コンフィギュレーション コマンドを使用して、ポート モードを単一方向または双方向に設定します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication control-direction {both | in}

no authentication control-direction

構文の説明

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

デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、双方向モードをイネーブルにする方法を示します。

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

次の例では、単一方向モードをイネーブルにする方法を示します。

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

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

関連コマンド

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

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

authentication critical recovery delay

Auth Manager のクリティカルな回復遅延を設定するには、グローバル コンフィギュレーション モードで **authentication critical recovery delay** コマンドを使用します。以前に設定した回復遅延を削除するには、このコマンドの **no** 形式を使用します。

authentication critical recovery delay *milliseconds*

no authentication critical recovery delay

構文の説明

milliseconds	使用不可になっていた RADIUS サーバが使用可能になったときに、クリティカル ポートの再初期化を Auth Manager が待機する時間（ミリ秒単位）です。有効な値は 1 ～ 10000 です。

コマンド デフォルト

デフォルト遅延は 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例は、クリティカルな回復遅延時間を 1500 ミリ秒に設定する方法を示します。

```
Switch(config)# authentication critical recovery delay 1500
```

authentication event

authentication event インターフェイス コンフィギュレーション コマンドを使用して、ポートの特定の認証イベントに関するアクションを設定します。

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

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

構文の説明

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

イベント応答はポートに設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドに **fail**、**no-response**、または **event** キーワードを付けて使用して、特定のアクションのスイッチ応答を設定します。

server-dead イベントの場合：

- スイッチが critical-authentication ステートに移ると、認証を試行している新しいホストが critical-authentication VLAN（または*クリティカル VLAN*）に移動されます。ポートがシングルホスト モード、マルチホスト モード、マルチ認証モード、または MDA モードの場合、これが適用されます。認証済みホストは認証済み VLAN に残り、再認証タイマーはディセーブルになります。

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

  Windows XP クライアントに DHCP が設定されており、DHCP サーバからの IP アドレスが設定されている場合に、クリティカル ポートで EAP 認証成功メッセージを受信しても、DHCP 設定プロセスは再初期化できません。

no-response イベントの場合：

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

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

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

authentication-fail イベントの場合：

- サプリカントが認証に失敗すると、ポートは制限 VLAN に移動され、EAP 成功メッセージがサプリカントに送信されます。これは、サプリカントには実際の認証の失敗が通知されないためです。
  - EAP の成功メッセージが送信されない場合、サプリカントは 60 秒ごと（デフォルト）に EAP 開始メッセージを送信して認証を行おうとします。
  - 一部のホスト（たとえば、Windows XP を実行中のデバイス）は、EAP の成功メッセージを受け取るまで DHCP を実装できません。

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

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

  制限 VLAN による再認証をイネーブルにしてください。再認証がディセーブルにされていると、制限 VLAN に含まれているポートでは、ディセーブルにされている場合に再認証要求を受け取りません。

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

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

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

例

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

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

次の例では、応答なしアクションの設定方法を示します。

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

次の例では、サーバ応答アクションの設定方法を示します。

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

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。

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

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。ポートをマルチホスト モードまたはマルチ認証モードにするには、このコマンドを使用します。

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication fallback

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

authentication fallback ***name***

no authentication fallback ***name***

構文の説明

name	Web 認証のフォールバック プロファイルを指定します。

デフォルト

フォールバックはイネーブルではありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

フォールバック方式を設定する前に **authentication port-control auto** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

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

例

次の例では、ポートのフォールバック プロファイルを指定する方法を示します。

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication host-mode

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

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

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

構文の説明

multi-auth	ポートのマルチ認証モード（multiauth モード）をイネーブルにします。
multi-host	ポートのマルチホスト モードをイネーブルにします。
single-host	ポートのシングルホスト モードをイネーブルにします。

デフォルト

シングルホスト モードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ハブ越しの 8 台までのデバイスに、個別の認証を通じて保護されたポート アクセスの取得を許可するには、マルチ認証モードを設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

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

例

次の例では、ポートの**マルチ認証**モードをイネーブルにする方法を示します。

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

次の例では、ポートの**マルチホスト** モードをイネーブルにする方法を示します。

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

次の例では、ポートの**シングルホスト モードをイネーブルにする方法を示します。**

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication mac-move permit

スイッチ上で MAC 移動をイネーブルにするには、**authentication mac-move permit** グローバル 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。

authentication mac-move permit

no authentication mac-move permit

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

MAC 移動はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

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

関連コマンド

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

コマンド	説明
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication open

authentication open インターフェイス コンフィギュレーション コマンドを使用して、ポートでオープン アクセスをイネーブルまたはディセーブルにします。オープン アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication open

no authentication open

デフォルト

オープン アクセスはディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

例

次の例では、ポートのオープン アクセスをイネーブルにする方法を示します。

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

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication order

authentication order インターフェイス コンフィギュレーション コマンドを使用して、ポートで使用する認証方式の順序を設定します。

authentication order [dot1x | mab] {webauth}

no authentication order

構文の説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	認証方式の順序に MAC Authentication Bypass（MAB; MAC 認証バイパス）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトの認証順序は **dot1x**、**mab**、および **webauth** の順です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。リスト内の方式の 1 つで成功しないと、次の方式が試行されます。

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

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

例

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

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

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

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication periodic

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

authentication periodic

no authentication periodic

コマンド デフォルト

再認証はディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

定期的に再認証を行う間隔の時間を設定するには、**authentication timer reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポートの定期的再認証をイネーブルにする方法を示します。

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

次の例では、ポートの定期的再認証をディセーブルにする方法を示します。

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。

コマンド	説明
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication port-control

authentication port-control インターフェイス コンフィギュレーション コマンドを使用して、ポート許可ステートの手動制御をイネーブルにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

例

次の例では、ポート ステートを自動に設定する方法を示します。

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

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

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

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

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication priority

authentication priority インターフェイス コンフィギュレーション コマンドを使用して、ポート プライオリティ リストに認証方式を追加します。

auth priority [dot1x | mab] {webauth}

no auth priority [dot1x | mab] {webauth}

構文の説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	認証方式の順序に MAC Authentication Bypass（MAB; MAC 認証バイパス）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

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

例

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

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

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

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication timer

authentication timer インターフェイス コンフィギュレーション コマンドを使用して、802.1x 対応ポートのタイムアウトと再認証のパラメータを設定します。

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

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

構文の説明

inactivity	この時間間隔を過ぎてもアクティビティがない場合に、クライアントが無許可にされる秒数です。
reauthenticate	自動再認証の試行が開始されるまで時間（秒）です。
restart	無許可ポートの認証の試行が行われるまでの間隔（秒）です。
value	1 から 65535 までの値（秒）を入力します。

デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

次の例では、再認証タイマーを 120 秒に設定する方法を示します。

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

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

関連コマンド

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

コマンド	説明
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication violation

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

authentication violation {protect | restrict | shutdown | replace}

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

構文の説明

protect	予期しない着信 MAC アドレスがドロップされます。syslog エラーは生成されません。
restrict	違反エラーが発生し、着信 MAC アドレスがドロップされると、Syslog エラーが生成されます。
shutdown	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。
replace	古いセッションを切断し、着信 MAC アドレスを使用して認証シーケンスを開始します。

デフォルト

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

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

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

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

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

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

次の例は、新しいデバイスがポートに接続された場合に、古いセッションを切断して、新しいデバイスを認証する単一ホスト モードである IEEE 802.1x 対応ポートを設定する方法を示します。

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

bandwidth

ポリシーマップ クラスの出力帯域幅を設定して、クラスベース均等化キューイング（CBWFQ）を設定するには、**bandwidth** 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。クラスの帯域幅設定を削除するには、このコマンドの **no** 形式を使用します。

bandwidth {*rate* | **percent** *value* | **remaining percent** *value*}

no bandwidth [*rate* | **percent** *value* | **remaining percent** *value*]

構文の説明

rate	クラスの帯域幅レートをキロビット/秒（kb/s）単位で設定します。指定できる範囲は 64 ～ 1000000 です。
percent *value*	合計帯域幅の割合としてクラスの帯域幅を設定します。指定できる範囲は 1 ～ 100% です。
remaining percent *value*	残りの帯域幅の割合としてクラスの帯域幅を設定します。指定できる範囲は 1 ～ 100% です。

デフォルト

帯域幅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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

出力トラフィックを制御するには、**bandwidth** ポリシーマップ クラス コマンドを使用します。**bandwidth** コマンドは、そのクラス内のトラフィックの帯域幅を指定します。CBWFQ はクラスに割り当てられた帯域幅から、クラスに属するパケットの重み付けを取得し、この重み付けを使用して、このクラスのキューが適正に処理されるようにします。帯域幅設定は、入力ポリシー マップでサポートされません。

トラフィックのクラスの帯域幅を絶対レート（kb/s）または帯域幅に対する割合（**percent** *value*）として設定すると、その帯域幅はそのトラフィック クラスの最小帯域幅保証または認定情報レート（CIR）を表します。つまり、トラフィック クラスは最低でもコマンドにより指定された帯域幅を取得しますが、その帯域幅に制限されるわけではありません。ポートの超過帯域幅はすべて、設定済み CIR レートと同じ比率で各クラスに割り当てられます。

bandwidth remaining percent コマンドを入力すると、絶対帯域幅が保証されず、相対帯域幅のみが確認されます。クラスの帯域幅は、常に、ポートに設定された指定帯域幅の割合に比例します。

出力ポリシーで帯域幅を設定する場合、各帯域幅設定で同じ単位を指定する必要があります。つまり、すべての絶対値（レート）にするか、またはパーセントにします。

ポリシーの各キューにおける最小帯域幅保証の合計速度は、インターフェイスの合計速度を上回ることはできません。**percent** キーワードが使用されている場合、クラスの帯域幅の割合の合計が 100% を超えることはできません。

queue-limit コマンドを使用してデフォルトのキュー制限を変更すると、インターフェイスに必要な最小帯域幅保証を満たすことができるため、高速のインターフェイスで特に重要です。

bandwidth 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 CBWFQ を設定したり、**shape average** コマンドを使用してポリシー マップの同じクラスのクラスベース シェーピングを設定したりすることはできません。

プライオリティ キューイング（**priority** 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設定）を含むクラスの帯域幅は設定できません。

例

次に、帯域幅（kbps）を設定することにより、出力キューの優先順位を設定する例を示します。クラス *outclass1*、*outclass2*、および *outclass3* は、それぞれ 50000、20000、および 10000 kb/s の最小帯域幅を取得します。クラス **class-default** は、最低限として、残りの帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、各トラフィック クラスに、使用可能な合計帯域幅の割合を割り当てることで、出力キューの優先順位を設定する例を示します。クラス *outclass1*、*outclass2* および *outclass3* は、それぞれ 50、20、および 10% の最小帯域幅を取得します。クラス **class-default** は、最低限 20% の帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、プライオリティ キューとして *outclass1* を設定し、プライオリティ キューが処理された後に *outclass2* および *outclass3* がそれぞれ残りの帯域幅の 50% および 20% を取得するように設定する例を示します。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

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

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。

boot config-file

Cisco IOS がシステム設定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するには、**boot config-file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no boot config-file

構文の説明

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

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot enable-break

自動ブート プロセスの中断をイネーブルにするには、**boot enable-break** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot enable-break

no boot enable-break

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力すると、フラッシュ ファイル システムが初期化された後にブレーク キーを押して、自動ブート プロセスを中断できます。ブレーク キーは、オペレーティング システムごとに異なります。

- UNIX を実行している SUN ワークステーションでは、Ctrl+C が ブレーク キーです。
- Windows 2000 を実行する PC では、Ctrl+Break がブレーク キーとなります。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper

boot helper グローバル コンフィギュレーション コマンドを使用して、ブート ローダー初期化中に動的にファイルをロードして、ブート ローダーの機能を拡張したり、パッチを当てたりします。このコマンドをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no boot helper

構文の説明

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper-config-file

boot helper-config-file グローバル コンフィギュレーション コマンドを使用して、Cisco IOS ヘルパー イメージが使用するコンフィギュレーション ファイルの名前を指定します。このコマンドが設定されていない場合は、CONFIG_FILE 環境変数によって指定されたファイルが、ロードされたすべてのバージョンの Cisco IOS に使用されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no boot helper-config file

構文の説明

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER_CONFIG_FILE 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot manual

次回のブート 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、**boot manual** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot manual

no boot manual

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

手動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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot private-config-file

Cisco IOS がプライベート設定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するには、**boot private-config-file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot private-config-file *filename*

no boot private-config-file

構文の説明

filename	プライベート コンフィギュレーション ファイルの名前

デフォルト

デフォルトのコンフィギュレーション ファイルは、*private-config* です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ファイル名は、大文字と小文字を区別します。

例

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

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

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot system

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

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

no boot system

構文の説明

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

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

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

このコマンドは、BOOT 環境変数の設定を変更します。詳細については、付録 A「Cisco CGS 2520 スイッチのブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

channel-group

EtherChannel グループにイーサネット ポートを割り当てるには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用します。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**

（注） Link Aggregation Control Protocol（LACP）およびポート集約プロトコル（PAgP）は、ネットワーク ノード インターフェイス（NNI）または拡張ネットワーク インターフェイス（ENI）でだけ使用できます。**active**、**auto**、**desirable**、および **passive** キーワードは、ユーザ ネットワーク インターフェイス（UNI）では表示されません。

構文の説明

channel-group-number	チャネル グループ番号を指定します。指定できる範囲は 1 ～ 48 です。
mode	EtherChannel モードを指定します。
active	無条件に LACP をイネーブルにします active モードは、ポートをネゴシエーション ステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポート グループで形成されます。
auto	PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。 auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。チャネルは、desirable モードの別のポート グループでだけ形成されます。**auto** がイネーブルの場合、サイレント動作がデフォルトになります。
desirable	無条件に PAgP をイネーブルにします。 desirable モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。相手側のポート グループが desirable または auto モードの場合にチャネルが形成されます。**desirable** がイネーブルの場合は、デフォルトでサイレント動作となります。
non-silent	（任意）他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。

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

デフォルト

チャネル グループは割り当てることができません。

モードは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ポートが UNI または ENI の場合、**channel-group** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。NNI はデフォルトでイネーブルです。

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

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

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

auto モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント モードを設定するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にスイッチを接続する場合です。サイレント パートナーの例は、トラフィッ

クを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、物理ポート上で稼動している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネル グループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

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

注意　モードを **on** に設定（手動設定）する場合は、慎重に実行する必要があります。**on** モードに設定したすべてのポートは、同じグループにバンドルされており、同様の特性を持つようになります。グループの設定を誤ると、パケット損失またはスパニング ツリー ループが発生することがあります。

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

（注）　PAgP および LACP は、NNI および ENI 上でだけ使用できます。

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

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

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

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

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

例

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

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

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

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
```

```
Switch(config-if-range)# end
```

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

関連コマンド

コマンド	説明
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

channel-protocol

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

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

no channel-protocol

構文の説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	Port Aggregation Protocol（PAgP; ポート集約プロトコル）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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

（注） PAgP および LACP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

ポートがユーザ ネットワーク インターフェイス（UNI）または ENI の場合、**channel-protocol** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。NNI はデフォルトでイネーブルです。

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

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

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

例

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

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

設定を確認するには、**show etherchannel** [*channel-group-number*] **protocol** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel protocol	EtherChannel のプロトコル情報を表示します。

class

ポリシーを作成、変更、またはポリシーを設定する前にポリシーにシステムのデフォルト クラスを指定するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始するには、**class** ポリシーマップ コンフィギュレーション コマンドを使用します。ポリシー マップからクラスを削除するには、このコマンドの **no** 形式を使用します。

class {*class-map-name*| **class-default**}

no class {*class-map-name*| **class-default**}

構文の説明

class-map-name	**class-map** グローバル コンフィギュレーション コマンドを使用して作成されたクラス マップの名前。
class-default	システムのデフォルト クラス。このクラスは、すべての分類されないトラフィックと一致します。デフォルト クラスは作成または削除できません。

デフォルト

ポリシー マップ クラス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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポリシーマップ コンフィギュレーション モードで **class** *class-map-name* コマンドを使用する前に、**class-map** *class-map-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、クラスを作成する必要があります。**class-default** クラスは、トラフィックが設定されているクラス マップのいずれの一致基準とも一致しない場合に、そのトラフィックが送られるクラスです。

ポリシー マップを指定し、ポリシーマップ コンフィギュレーション モードを開始するには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。ポリシー マップを指定すると、ポリシー マップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。

入力ポリシー マップの最大クラス数は 64 + **class-default** です。

service-policy インターフェイス コンフィギュレーション コマンドを使用して、ポリシー マップをポートへ添付することができます。

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

- **bandwidth**：ポリシー マップに属しているクラスに割り当てる帯域幅を指定します。詳細については、**bandwidth** コマンドを参照してください。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。

- **police**：分類したトラフィックにそれぞれポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** および **police aggregate**（ポリシーマップ クラス コンフィギュレーション）ポリシーマップ クラス コマンドを参照してください。
- **priority**：このクラスに厳密なスケジューリング プライオリティを設定します。または、**police** キーワードと併用して、ポリシングを含むプライオリティを設定します。詳細については、**priority** ポリシーマップ クラス コマンドを参照してください。
- **queue-limit**：重み付きテール ドロップ（WTD）のキューの最大しきい値を設定します。詳細については、**queue-limit** コマンドを参照してください。
- **service-policy**：QoS サービス ポリシーを設定して、入力ポリシーまたは出力ポリシーの親ポリシー マップに適用します。詳細については、**service-policy**（ポリシーマップ クラス コンフィギュレーション）コマンドを参照してください。
- **set**：分類したトラフィックに割り当てる値を指定します。詳細については、**set** コマンドを参照してください。
- **shape average**：平均トラフィック シェーピング レートを指定します。詳細については、**shape average** コマンドを参照してください。

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

例

次に、ポリシー マップ *policy1* を作成し、クラス *class1* を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始してクラスの基準を設定する例を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	QoS ポリシー マップを表示します。
show policy-map interface [*interface-id*]	（任意）指定したインターフェイスまたはすべてのインターフェイスに設定されているポリシー マップを表示します。

class-map

指定した基準とパケットのマッチングに使用されるクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始するには、**class-map** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

match-all	（任意）このクラス マップ内のすべての一致ステートメントの論理積をとります。パケットがすべての一致基準を満たす必要があります。
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。パケットが 1 つまたは複数の一致基準を満たす必要があります。
class-map-name	クラス マップ名です。

デフォルト

クラス マップは定義されていません。

match-all または **match-any** のいずれのキーワードも指定しない場合、デフォルトは **match-all** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

スイッチでは、最大 1024 の一意のクラス マップをサポートしています。

ポート単位で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分類を定義するには、**class-map** コマンドとクラスマップ コンフィギュレーション モードを使用します。クラス マップを設定したら、1 つまたは複数の **match** コマンドを使用して一致基準を指定できます。入力インターフェイスまたは出力インターフェイスのいずれかに到達（**service-policy** インターフェイス コンフィギュレーション コマンドの設定によって決定されます）するパケットは、クラスマップの一致基準に照らしてチェックされ、パケットがそのクラスに属しているかどうかが判断されます。

match-all クラス マップは、パケットがすべてのエントリと一致する必要があり、他の一致ステートメントがない可能性があることを意味します。

クラスマップ コンフィギュレーション モードを開始すると、次のコンフィギュレーション コマンドが利用できます。

- **description**：クラス マップを説明します（最大 200 文字）。**show class-map** 特権 EXEC コマンドを実行すると、クラス マップの説明と名前が表示されます。
- **exit**：QoS クラスマップ コンフィギュレーション モードを終了します。

- **match**：分類基準を設定します。詳細については、**match** クラスマップ コンフィギュレーション コマンドを参照してください。
- **no**：クラス マップから一致ステートメントを削除します。

例

次の例は、*class1* というクラス マップの設定方法を示します。デフォルトでは、クラス マップは **match-all** であるため、他の一致基準が含まれない場合があります。

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
```

次の例は、一致基準が 1 つの match-any クラス マップ（アクセス リスト *103*）を設定する方法を示します。このクラス マップ（ACL に一致）は、入力ポリシー マップでだけサポートされます。

```
Switch(config)# class-map class2
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次の例では、クラス マップ ***class1*** を削除する方法を示します。

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

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

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
match access-group	指定したアクセス コントロール リスト（ACL）に基づいて、クラス マップの一致基準を設定します
match cos	レイヤ 2 サービス クラス（CoS）マーキングに基づいて、クラス マップの一致基準を設定します。
match ip dscp	特定の IPv4 の DiffServ コード ポイント（DSCP）値に基づいて、クラス マップの一致基準を設定します。
match ip precedence	IPv4 precedence 値に基づいて、クラス マップの一致基準を設定します。
match qos-group	特定の Quality of Service（QoS）グループ値に基づいて、クラス マップの一致基準を設定します。
match vlan	VLAN ID または一連の VLAN ID に基づいて、階層型ポリシー マップの親ポリシーのクラス マップの一致基準を設定します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show class-map	QoS クラス マップを表示します。

clear ip arp inspection log

ダイナミック アドレス解決プロトコル（ARP）インスペクション ログ バッファを消去するには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

clear ip arp inspection log

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

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

ログがクリアされたかどうかを確認するには、**show ip arp inspection log** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP Access Control List（ACL; アクセス コントロール リスト）を定義します。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show ip arp inspection log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

clear ip arp inspection statistics

ダイナミック Address Resolution Protocol（ARP; 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、**clear ip arp inspection statistics** 特権 EXEC コマンドを使用します。

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

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、VLAN 1 の統計情報をクリアする方法を示します。

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

統計情報が削除されたかどうかを確認するには、**show ip arp inspection statistics vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip arp inspection statistics	すべての VLAN または指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、および IP 検証に失敗したパケットの統計情報を表示します。

clear ip dhcp snooping

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

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

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

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

次の例では、DHCP スヌーピング統計カウンタをクリアする方法を示します。

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

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

関連コマンド

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

clear ipc

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

clear ipc {queue-statistics | statistics}

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、すべての統計情報をクリアする方法を示します。

```
Switch# clear ipc statistics
```

次の例では、キューの統計情報だけをクリアする方法を示します。

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

統計情報が削除されたかどうかを確認するには、**show ipc rpc** または **show ipc session** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ipc {**rpc** | **session**}	IPC マルチキャスト ルーティングの統計情報を表示します。

clear ipv6 dhcp conflict

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

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

（注）　このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

関連コマンド

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

clear l2protocol-tunnel counters

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

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

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみサポートされます。

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

```
Switch# clear l2protocol-tunnel counters gigabitethernet0/2
```

関連コマンド

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

clear lacp

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

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

（注）　LACP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear lacp counters
```

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

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

情報が削除されたかどうかを確認するには、**show lacp counters** または **show lacp 4 counters** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show lacp	LACP チャネル グループ情報を表示します。

clear logging onboard

フラッシュ メモリに保存されている稼働時間と CLI コマンド情報以外のすべてのオンボード障害ロギング（OBFL）を消去するには、**clear logging onboard** 特権 EXEC コマンドを使用します。

clear logging onboard [**module** {*slot-number* | **all**}]

構文の説明

module {*slot-number* | **all**}	（任意）スロット番号は常に 1 で、CGS 2520 には関連しません。**clear logging onboard module 1** または **clear logging onboard all** を入力した結果は、**clear logging onboard** を入力した結果と同じになります。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

例

次の例に、稼働時間と CLI コマンド情報以外のすべての OBFL 情報を消去する方法を示します。

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
PID: CGS-2520-24TC , VID: 03 , SN: FOC1225U4CY

Switch# clear logging onboard module all
Clear logging onboard buffer [confirm]
PID: CGS-2520-24TC , VID: 03 , SN: FOC1225U4CY
```

情報が消去されたかどうかを確認するには、**show logging onboard onboard** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
hw-module module logging onboard	OBFL をイネーブルにします。
show logging onboard	OBFL 情報を表示します。

clear mac address-table

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

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

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
dynamic address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
dynamic interface *interface-id*	（任意）指定された物理ポートまたはポート チャネル上のすべてのダイナミック MAC アドレスを削除します。
dynamic vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4096 です。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

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

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

関連コマンド

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

clear mac address-table move update

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

clear mac address-table move update

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみサポートされます。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

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

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

関連コマンド

コマンド	説明
mac address-table move update	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

clear pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）チャネル グループ情報を表示するには、**clear pagp** 特権 EXEC コマンドを使用します。

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

（注）　PAgP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear pagp counters
```

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

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

情報が削除されたかどうかを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show pagp	PAgP チャネル グループ情報を表示します。

clear policer cpu uni-eni counters

コントロール プレーン ポリサー統計情報を消去するには、**clear policer cpu uni-eni counters** 特権 EXEC コマンドを使用します。コントロール プレーン ポリサーは、ユーザ ネットワーク インターフェイス（UNI）および拡張ネットワーク インターフェイス（ENI）から制御パケットをドロップまたはレート制限して、CPU を過負荷から保護します。

clear policer cpu uni-eni counters {**classification** | **drop**}

構文の説明

classification	機能によって統計情報を維持するコントロールプレーン ポリサー分類カウンタを消去します。
drop	コントロールプレーン ポリサーで維持されるすべてのフレーム ドロップ統計情報を消去します。

コマンド 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

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、機能またはドロップされたフレームに関する統計情報ごとに維持される統計情報を消去できます。

clear コマンドを使用する前後に機能の統計情報またはドロップされたフレームを表示するには、**show platform policer cpu classification** コマンドまたは **show policer cpu uni drop** コマンドを入力します。

関連コマンド

コマンド	説明
show platform policer cpu classification	機能ごとの CPU ポリサー統計情報を表示します。
show policer cpu uni-eni	スイッチの CPU ポリサー情報を表示します。

clear port-security

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定のタイプ（設定済み、ダイナミック、またはスティッキ）のすべてのセキュア アドレスを削除するには、**clear port-security** 特権 EXEC コマンドを使用します。

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

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

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

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

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

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

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

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

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

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

関連コマンド

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

clear rep counters

指定したインターフェイスまたはすべてのインターフェイスの Resilient Ethernet Protocol（REP; レジリエント イーサネット プロトコル）カウンタをクリアするには、**clear rep counters** 特権 EXEC コマンドを使用します。

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

構文の説明

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

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

例

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

```
Switch# clear rep counters
```

REP 情報が削除されたかどうかを確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep detail	REP の設定およびステータス情報の詳細を表示します。

clear scada modbus tcp server statistics

MODBUS TCP サーバおよびクライアントの統計情報を消去するには、**clear scada modbus tcp server statistics** グローバル コンフィギュレーション コマンドを使用します。

clear scada modbus tcp server statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

```
Switch# clear scada modbus tcp server statistics
```

統計情報が消去されたかどうかを確認するには、**show scada modbus tcp server** [**connections**] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
scada modbus tcp server	スイッチ上で MODBUS TCP をイネーブルにします。スイッチは、MODBUS TCP サーバとして機能します。
show scada modbus tcp server [**connections**]	サーバ情報および統計情報を表示します。クライアント情報および統計情報を表示するには、connection キーワードを使用します。

clear spanning-tree counters

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

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

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニング ツリー カウンタをすべてクリアします。有効なインターフェイスは、物理ネットワーク ノード インターフェイス（NNI）、スパニング ツリーがイネーブルになっている拡張ネットワーク インターフェイス（ENI）、VLAN、スパニング ツリー ポート チャネルなどです。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** スパニング ツリー プロトコル（STP）は、ユーザ ネットワーク インターフェイス（UNI）ではサポートされていません。このコマンドは、コマンドラインのヘルプには表示されますが、STP を実行していない UNI または ENI では無効です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

interface-id が指定されていない場合は、すべての STP ポートのスパニング ツリー カウンタが消去されます。

例

次の例は、すべての STP ポートのスパニング ツリー カウンタを消去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

すべてのスパニング ツリー 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（ネイバー スイッチと強制的に再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

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

構文の説明

interface *interface-id*	（任意）指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスは、物理ネットワーク ノード インターフェイス（NNI）、スパニング ツリーがイネーブルになっている拡張ネットワーク インターフェイス（ENI）、VLAN、ポート チャネルなどです。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 **（注）** スパニング ツリー プロトコル（STP）は、ユーザ ネットワーク インターフェイス（UNI）ではサポートされていません。このコマンドは、コマンドラインのヘルプには表示されますが、STP を実行していない UNI または ENI では無効です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ただし、それ以上 IEEE 802.1D BPDU を受信しなければ、スイッチが自動的に Rapid-PVST+ または MSTP モードに戻ることはありません。レガシー スイッチが指定スイッチでない限り、スイッチはレガシー スイッチがリンクから削除されたことを検出できません。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

例

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

関連コマンド

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

clear vmps statistics

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

clear vmps statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

```
Switch# clear vmps statistics
```

情報が削除されたかどうかを確認するには、**show vmps statistics** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vmps	VQP バージョン、再確認間隔、再試行回数、VMPS IP アドレス、および現在のサーバとプライマリ サーバを表示します。

conform-action

レートを適合バーストよりも小さくすることによって、認定情報レート（CIR）または最大情報レート（PIR）に適合するパケットのポリシーマップ クラスのアクションを複数設定するには、**conform-action** ポリシーマップ クラス ポリシング コンフィギュレーション コマンドを使用します。アクションをキャンセルしたり、デフォルト アクション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。

conform-action {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

no conform-action {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

構文の説明

drop	パケットをドロップします。
set-cos-transmit *new-cos-value*	パケットの新しいサービス クラス（CoS）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit *new-dscp-value*	パケットの新しい DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit *new-precedence-value*	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit *qos-group-value*	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	（任意）着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
dscp	（任意）着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
precedence	（任意）着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
table *table-map name*	（任意）上記の *from-type* キーワードとともに使用します。拡張パケット マーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの *from-type* パラメータに基づき、アクションの *to-type* がマーキングされます。
transmit	（任意）パケットを変更せずに送信します。

デフォルト

デフォルトの適合アクションは、パケットの送信です。

コマンド モード

ポリシーマップ クラス ポリシング設定

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

パケット レートが設定されている適合バーストよりも少ない場合に、パケットの適合アクションを設定します。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。

適合アクション マーキングを設定するには、拡張パケット マーキングを使用して、任意の着信 QoS マーキングおよびテーブル マップに基づき QoS マーキングを変更します。また、スイッチは、同じクラスの複数の QoS パラメータの同時マーキングと適合アクション、超過アクション、および違反アクション マーキングをサポートします。

ポリシーマップ クラス ポリシング コンフィギュレーション モードにアクセスするには、**police** ポリシーマップ クラス コマンドを入力します。詳細については、**police** ポリシーマップ クラス コンフィギュレーション コマンドを参照してください。

トラフィック クラスに 1 つ以上の適合アクションを設定するには、このコマンドを使用します。

例

次の例は、23000 ビット/秒（bps）の認定情報レートおよび 10000 bps の適合バースト レートを設定するポリシー マップの複数の適合アクションを設定する方法を示します。このポリシー マップには、複数の適合アクション（DSCP 用およびレイヤ 2 CoS 用）および超過アクションが含まれます。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
```

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

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
exceed-action	CIR を超過するトラフィックに対して実行するアクションを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
police	分類したトラフィックにポリサーを定義します。
show policy-map	QoS ポリシー マップを表示します。
violate-action	適合レートに超過バーストを加えたレートよりも大きいレートのトラフィックで実行されるアクションを定義します。

copy logging onboard module

オンボード障害ロギング（OBFL）データをローカル ネットワークまたは特定のファイル システムにコピーするには **copy logging onboard module** 特権 EXEC コマンドを使用します。

copy logging onboard module [*slot-number*] *destination*

構文の説明

slot-number	（任意）スロット番号は常に 1 で、CGS 2520 には関連しません。
destination	ローカル ネットワーク上またはファイル システム上にある、システム メッセージのコピー先とする場所を指定します。 *destination* には、ローカルまたはネットワーク ファイル システム上のコピー先の場所とファイル名を指定します。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:***/filename* • FTP の構文：**ftp:**//*username***:***password*@*host*/*filename* • HTTP サーバの構文：**http:**//[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*filename* • null ファイル システムの構文：**null:**/*filename* • NVRAM の構文：**nvram:**/*filename* • Remote Copy Protocol（RCP）の構文：**rcp:**//*username***@***host*/*filename* • スイッチ ファイル システムの構文：**system:***filename* • TFTP の構文：**tftp:**[[//*location*]/*directory*]/*filename* • 一時ファイル システムの構文：**tmpsys:**/*filename*

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

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL については、**hw-module module logging onboard** グローバル コンフィギュレーション コマンドを参照してください。

例

次の例は、フラッシュ ファイル システムの *obfl_file* ファイルに OBFL データ メッセージをコピーする方法を示します。

```
Switch# copy logging onboard module flash:obfl_file
OBFL copy successful
```

関連コマンド

コマンド	説明
hw-module module logging onboard	OBFL をイネーブルにします。
show logging onboard	OBFL 情報を表示します。

cpu traffic qos cos

コントロール プレーン トラフィックのサービス クラス（CoS）に基づいて Quality of Service（QoS）マーキングを設定するには、グローバル コンフィギュレーション モードで **cpu traffic qos cos** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cpu traffic qos cos {*cos_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

no cpu traffic qos cos {*cos_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

構文の説明

cos-value	CoS 値を指定します。指定できる範囲は 0 ～ 7 です。CoS 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。
cos	テーブルマップを使用して、パケットの CoS 値に基づく CoS 値を設定します。
table-map *table-map-name*	パケットの CoS 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
dscp	テーブルマップを使用して、パケットの DSCP 値に基づく CoS 値を設定します。
table-map *table-map-name*	パケットの DSCP 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
precedence	precedence 値を設定します。指定できる範囲は 0 ～ 7 です。
table-map *table-map-name*	パケットの IP-precedence 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。

コマンド デフォルト

コントロール プレーン（CPU）トラフィックは QoS ではマーキングされません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

必要なテーブルマップを設定してから、CPU トラフィックのマーキングまたはキューイングを設定します。

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキング アクションを入力します。

cpu traffic qos cos グローバル コンフィギュレーション コマンドは、特定の CoS 値またはテーブルマップの両方ではなく、いずれかを使用して、CPU 生成トラフィックの CoS マーキングを設定します。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 2 つの **map from** 値（CoS と DSCP または precedence のいずれか）を設定できます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが IP-DSCP または IP-precedence の **map from** 値だけで設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの IP-DSCP（または IP-precedence）値および設定されたテーブル マップを使用してマッピングされます。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は変わりません。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが CoS の **map from** 値で設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが DSCP または precedence および CoS の **map from** 値で設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの DSCP または precedence 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

例

次に、パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の CoS をマーキングし、CoS 値に基づいて出力キューイングを設定する例を示します。

この設定例の結果は次のとおりです。

- CPU によって生成されたすべての IP トラフィックは、DSCP 値および *output-policy* という設定済み出力ポリシー マップに基づいて出力ポートのキューに格納される。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プローブが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が 48 および 56 のすべての IP 制御プロトコル トラフィックが *network-internetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルト クラスに割り当てられている。
- CoS 5 のすべての CPU 生成非 IP トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CPU 生成非 IP トラフィックが *video* クラスに割り当てられている。
- CoS 6 および 7 のすべての CPU 生成非 IP トラフィックが *network-internetwork-control* クラスに割り当てられている。
- CoS 5 のすべての CFM トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CFM トラフィックが *video* クラスに割り当てられている。

- CoS 6 および 7 のすべての CFM トラフィックが *network-internetwork-control* クラスに割り当てられている。

テーブル マップ：

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# map from af41 to 3
Switch(config-tablemap)# map from af42 to 3
Switch(config-tablemap)# map from af43 to 3
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS：

```
Switch(config)# cpu traffic qos cos dscp table-map dscp-to-cos
Switch(config)# cpu traffic qos cos cos
```

クラス：

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match cos 6 7
Switch(config-cmap)# exit
```

ポリシー：

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

インターフェイス

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos dscp	コントロール プレーン トラフィックの DSCP に基づく Quality of Service（QoS）マーキングを設定します。
cpu traffic qos precedence	コントロール プレーン トラフィックの優先順位に基づく Quality of Service（QoS）マーキングを設定します。
cpu traffic qos qos-group	サービス クラス（CoS）、IP DiffServ コード ポイント（DSCP）、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service（QoS）マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

cpu traffic qos dscp

コントロール プレーン トラフィックの DiffServ コード ポイント（DSCP）値に基づいて Quality of Service（QoS）マーキングを設定するには、グローバル コンフィギュレーション モードで **cpu traffic qos dscp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cpu traffic qos dscp {*dscp_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

no cpu traffic qos dscp {*dscp_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

構文の説明

dscp-value	IP-DSCP 値を指定します。指定できる範囲は 0 ～ 63 です。IP-DSCP 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。
cos	テーブル マップを使用して、パケットの IP-DSCP 値に基づく CoS 値を設定します。
table-map *table-map-name*	パケットの CoS 値に基づく CPU トラフィック IP-DSCP のマーキングに使用するテーブルマップを指定します。
dscp	テーブル マップを使用して、パケットの IP-DSCP に基づく IP-DSCP 値を設定します。
table-map *table-map-name*	パケットの IP-DSCP 値に基づく CPU トラフィック IP-DSCP のマーキングに使用するテーブルマップを指定します。
precedence	テーブル マップを使用して、パケットの IP-precedence 値に基づく IP-precedence 値を設定します。
table-map *table-map-name*	パケットの IP-precedence 値に基づく CPU トラフィック IP-DSCP 値のマーキングに使用するテーブルマップを指定します。

コマンド デフォルト

コントロール プレーン（CPU）トラフィックは QoS ではマーキングされません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキング アクションを入力します。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドは、特定の DSCP 値またはテーブル マップの両方ではなく、いずれかを使用して、CPU 生成 IP トラフィックの IP-DSCP マーキングを設定します。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドと **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドは相互に排他的です。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 1 つの **map from** 値（DSCP、precedence、または CoS）しか設定できません。新しく設定を行うと、既存の設定は置き換えられます。このコマンドでマーキングされたパケットは、マーキングされた DSCP 値または precedence 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

DSCP および precedence 両方の **map from** 値は設定できません。新しく設定を行うと、既存の設定は置き換えられます。

例

次に、CPU 生成 IP パケットの DSCP 値に基づいて出力キューイングを設定する例を示します。

この設定例の結果は次のとおりです。

- IP DSCP 値および設定済み出力ポリシー マップ *output-policy* に基づく、出力ポート上のすべての CPU 生成 IP トラフィック キュー。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プローブが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が *48* および *56* のすべての IP 制御プロトコル トラフィックが *network-internetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルト クラスに割り当てられている。
- すべての CPU 生成非 IP トラフィックが、スタティックに出力ポートの固定キューにマッピングされている。
- CoS に基づくクラスが存在しないため、すべての CFM トラフィックがデフォルト クラスにキューイングされている。

```
Switch(config)# cpu traffic qos dscp dscp
```

クラス：

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match ip dscp af41 af42 af43
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match ip dscp 48 56
Switch(config-cmap)# exit
```

ポリシー：

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class network-internetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

インターフェイス

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

次の例を示します。

- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の DSCP 値をマーキングする。
- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック（IP-SLA および TWAMP を含む）の CoS をマーキングする。
- パケットの CoS 値に基づいて CPU 生成非 IP トラフィックの CoS をマーキングする。
- QoS グループが付いたすべての CPU 生成トラフィックをマーキングする。
- QoS グループに基づいて出力キューイングを設定する。

この例の結果は次のとおりです。

- DSCP 値が *46*、*48*、および *56* のすべての CPU 生成 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成 IP パケットについては、DSCP 値は *0* にリセットされる。
- DSCP 値が *46*、*48*、および *56* のすべての CPU 生成 IP トラフィックは、それぞれ対応する CoS 値 *5*、*6*、および *7* にマッピングされる。
- その他のすべての CPU 生成 IP パケットについては、CoS 値は *0* にリセットされる。
- CoS 値が *5*、*6*、および *7* のすべての CPU 生成非 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成非 IP パケットについては、CoS 値は *0* にリセットされる。
- すべての CPU 生成トラフィックは、*cpu-traffic* という 1 つのクラスを通過する。*user-voice* クラスである *user-voice* および *user-video* は、ユーザ トラフィック用に確保されています。その結果、CPU トラフィックおよびユーザ トラフィックは出力ポートのさまざまなキューに分割されています。

テーブルマップ

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end

Switch(config)# table-map dscp-to-dscp
Switch(config-tablemap)# map from 46 to 46
Switch(config-tablemap)# map from 48 to 48
Switch(config-tablemap)# map from 56 to 56
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

```
Switch(config)# table-map cos-to-cos
Switch(config-tablemap)# map from 5 to 5
Switch(config-tablemap)# map from 6 to 6
Switch(config-tablemap)# map from 7 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS：

```
Switch(config)# cpu traffic qos dscp dscp table-map dscp-to-dscp
Switch(config)# cpu traffic qos cos dscp table dscp-to-cos
Switch(config)# cpu traffic qos cos cos table cos-to-cos
Switch(config)# cpu traffic qos qos-group 50
```

クラス：

```
Switch(config)# class-map match-any cpu-traffic
Switch(config-cmap)# match qos-group 50
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

ポリシー：

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class user-voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class user-video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cpu-traffic
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

インターフェイス：

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロール プレーン トラフィックのサービス クラス（CoS）マーキングを設定します。
cpu traffic qos precedence	コントロール プレーン トラフィックの優先順位に基づく Quality of Service（QoS）マーキングを設定します。

コマンド	説明
cpu traffic qos qos-group	サービス クラス（CoS）、IP DiffServ コード ポイント（DSCP）、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service（QoS）マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

cpu traffic qos precedence

コントロール プレーン トラフィックの Quality Of Service（QoS）を設定するには、グローバル コンフィギュレーション モードで **cpu traffic qos precedence** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cpu traffic qos precedence {*precedence_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

no cpu traffic qos precedence {*precedence_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

構文の説明

precedence-value	precedence 値を設定します。指定できる範囲は 0 ～ 7 です。IP-precedence 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。 **（注）**　次のキーワードを 0 ～ 7 の数字に置き換えることができます。 • routine（0） • priority（1） • immediate（2） • flash（3） • flash-override（4） • critical（5） • internet（6） • network（7）
cos	テーブルマップを使用して、パケットの CoS 値に基づく CoS 値を設定します。
table-map *table-map-name*	パケットの CoS 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
dscp	テーブルマップを使用して、パケットの IP-DSCP 値に基づく DiffServ コード ポイント（DSCP）値を設定します。
table-map *table-map-name*	パケットの DSCP 値に基づく CPU トラフィック precedence のマーキングに使用するテーブルマップを指定します。
precedence	テーブルマップを使用して、パケットの IP-precedence 値に基づく IP-precedence 値を設定します。
table-map *table-map-name*	パケットの precedence 値に基づく CPU トラフィック precedence のマーキングに使用するテーブルマップを指定します

コマンド デフォルト

コントロール プレーン（CPU）トラフィックは QoS ではマーキングされません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキング アクションを入力します。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドと **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドは相互に排他的です。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos precedence グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に 1 つの **map from** 値（DSCP、precedence、または CoS）しか設定できません。新しく設定を行うと、既存の設定は置き換えられます。このコマンドでマーキングされたパケットは、マーキングされた precedence 値または DSCP 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

DSCP および precedence 両方の **map from** 値は設定できません。新しく設定を行うと、既存の設定は置き換えられます。

例

次の例は、DSCP 値に基づいて precedence をマーキングし、precedence 値に基づいて出力キューイングを設定する方法を示します。

この例の結果は次のとおりです。

- DSCP 値が *48* の CPU 生成 IP トラフィックが precedence 値 *7* にマーキングされる。
- その他の CPU 生成 IP トラフィックが precedence 値 *0* にマーキングされる。
- その他すべての CPU 生成非 IP トラフィックがデフォルト クラスによって処理される。
- クラスの優先順位 *7* を使用して precedence 値 *7* の CPU 生成 IP トラフィックがキューに格納される。
- その他すべての CPU 生成 IP トラフィックがデフォルト クラスによって処理される。

テーブルマップ：

```
switch(config)# table-map dscp-to-prec
switch(config-tablemap)# map from 48 to 7
switch(config-tablemap)# default 0
switch(config-tablemap)# end
```

CPU QoS

```
switch(config)# cpu traffic qos precedence dscp table-map dscp-to-prec
```

クラスマップ：

```
switch(config)# class-map prec7
switch(config-cmap)# match ip precedence 7
switch(config-cmap)# end
```

ポリシーマップ：

```
switch(config)# policy-map output-policy
switch(config-pmap)# class prec7
switch(config-pmap-c)# priority
switch(config-pmap-c)# end
```

インターフェイス：

```
switch(config)# interface g1/0/1
switch(config-if)# service-policy output output-policy
switch(config-if)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロール プレーン トラフィックのサービス クラス（CoS）マーキングを設定します。
cpu traffic qos dscp	コントロール プレーン トラフィックの DSCP に基づく Quality of Service（QoS）マーキングを設定します。
cpu traffic qos qos-group	サービス クラス（CoS）、IP DiffServ コード ポイント（DSCP）、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service（QoS）マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

cpu traffic qos qos-group

サービス クラス（CoS）、IP DiffServ コード ポイント（DSCP）、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングするには、グローバル コンフィギュレーション モードで **cpu traffic qos qos-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cpu traffic qos qos-group *qos-group-value*

no cpu traffic qos qos-group *qos-group-value*

構文の説明

qos-group-value	QoS グループ番号を指定します。有効な値は 0 ～ 99 です。

コマンド デフォルト

コントロール プレーン（CPU）トラフィックは QoS ではマーキングされません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキング アクションを入力します。

cpu traffic qos qos-group グローバル コンフィギュレーション コマンドを使用して、特定の QoS グループの CPU 生成トラフィックだけの QoS グループ マーキングを設定できます。table-map オプションは使用できません。

例

次の例は、すべての CPU 生成トラフィックを QoS グループでマーキングし、その QoS グループに基づいて出力キューイングを設定する方法を示します。

CPU QoS

```
switch(config)# cpu traffic qos qos-group 40
```

クラスマップ：

```
switch(config)# class-map group40
switch(config-cmap)# match qos-group 40
switch(config-cmap)# end
```

ポリシーマップ：

```
switch(config)# policy-map output-policy
switch(config-pmap)# class group40
switch(config-pmap-c)# bandwidth percent 50
switch(config-pmap-c)# end
```

インターフェイス：

```
Switch(config)# interface g1/0/1
Switch(config-if)# service-policy output output-policy
Switch(config-if)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロール プレーン トラフィックのサービス クラス（CoS）マーキングを設定します。
cpu traffic qos dscp	コントロール プレーン トラフィックの DSCP に基づく Quality of Service（QoS）マーキングを設定します。
cpu traffic qos precedence	コントロール プレーン トラフィックの優先順位に基づく Quality of Service（QoS）マーキングを設定します。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service（QoS）マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

define interface-range

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

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

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

構文の説明

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

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

マクロ名は、最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。

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

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

- *type* {*first-interface*} - {*last-interface*}
- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gabitethernet 0/1 - 2** であれば範囲は指定されますが、**gigabitethernet 0/1-2** では指定されません。

type および *interface* の有効値は次のとおりです。

- **vlan** *vlan-id*。ここで、*vlan-id* の範囲は 1 ～ 4094 です。

  VLAN インターフェイスは、**interface vlan** コマンドで設定する必要があります（**show running-config** 特権 EXEC コマンドは、設定された VLAN インターフェイスを表示します）。**show running-config** コマンドで表示されない VLAN インターフェイスは、*interface-range* では使用できません。
- **port-channel** *port-channel-number*、ここで、*port-channel-number* は 1 ～ 48 です。
- **fastethernet** *module*/{*first port*} - {*last port*}

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

物理インターフェイス

- モジュールは常に 0 です。
- 指定できる範囲は、*type* **0**/*number* - *number* です（例：**gigabitethernet 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。

gigabitethernet0/1 - 2

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

fastethernet0/3, gigabitethernet0/1 - 2

fastethernet0/3 -4, gigabitethernet0/1 - 2

例

次の例では、複数インターフェイスのマクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

delete

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

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

構文の説明

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

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

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

関連コマンド

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

deny（ARP アクセス リスト コンフィギュレーション）

DHCP バインディングとの照合に基づいて 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、**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 コントロール エントリ）を削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

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

コマンド モード

ARP アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

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

関連コマンド

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

deny（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 モードで **deny** コマンドを使用します。拒否条件を削除するには、このコマンドの **no** 形式を使用します。

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

インターネット制御メッセージ プロトコル

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

伝送制御プロトコル

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

ユーザ データグラム プロトコル

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*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/*prefix-length*	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	拒否条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。

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

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

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

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

（注） すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 ネイバー探索を許可します。ICMPv6 ネイバー探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な**拒否**エントリが ACL 内にある必要があります。3 つの暗黙的なステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

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

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

このスイッチは、すべての範囲のプレフィクス長で IPv6 アドレス マッチングをサポートしています。

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

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request

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

例

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

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

関連コマンド

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

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 トラフィックが転送されないようにするには、**deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拒否条件を名前付き MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
host *src MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または SNAP カプセル化を使用して、パケットのプロトコルを識別します。 *type* には、0 ～ 65535 の 16 進数を指定できます。 *mask* は、照合を行う前に Ethertype に適用される *don't care* ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を選択します。
amber	（任意）EtherType DEC-Amber を選択します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までの Class of Service（CoS; サービス クラス）値を選択します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを選択します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	（任意）EtherType DEC-Diagnostic を選択します。
dsm	（任意）EtherType DEC-DSM を選択します。
etype-6000	（任意）EtherType 0x6000 を選択します。
etype-8042	（任意）EtherType 0x8042 を選択します。
lat	（任意）EtherType DEC-LAT を選択します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を選択します。

lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と IEEE 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *mask* は、照合を行う前に LSAP 番号に適用される *don't care* ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を選択します。
mop-dump	（任意）EtherType DEC-MOP Dump を選択します。
msdos	（任意）EtherType DEC-MSDOS を選択します。
mumps	（任意）EtherType DEC-MUMPS を選択します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を選択します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を選択します。

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

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。表 2-2 に、Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を一覧表示します。

表 2-2　IPX フィルタ基準

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

デフォルト

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

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

host キーワードを使用した場合、アドレス マスクは入力できません。**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 コントロール エントリ）がアクセス コントロール リストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

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

例

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

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

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

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

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

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

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

関連コマンド

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

diagnostic monitor

ヘルス モニタリング診断テストを設定するには、**diagnostic monitor** グローバル コンフィギュレーション コマンドを使用します。テストをディセーブルにし、デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

diagnostic monitor test {***name*** | *test-id* | *test-id-range* | **all**}

diagnostic monitor syslog

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

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

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

no diagnostic monitor syslog

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

構文の説明

interval test	テストの間隔を設定します。
test	実行するテストを指定します。
name	テスト名を指定します。テスト ID のリストのテスト名を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id	テストの ID 番号を指定します。指定できる範囲は 1 ～ 6 です。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id-range	複数のテストをテストの ID 番号の範囲で指定します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
hh:mm:ss	モニタリング間隔を時、分、秒で設定します。 • *hh*：時間（0 ～ 24）を入力します。 • *mm*：分（0 ～ 60）を入力します。 • *ss*：秒（0 ～ 60）を入力します。
milliseconds	モニタリング間隔（テスト時間）をミリ秒（ms）単位で設定します。指定できる範囲は 0 ～ 999 ミリ秒です。
day	モニタリング間隔をテストとテストの間の日数で設定します。指定できる範囲は 0 ～ 20 日です。
Syslog	ヘルス モニタ診断テストが失敗した場合に Syslog メッセージを生成します。
threshold test	障害しきい値を設定します。
failure count *count*	障害しきい値のカウントを設定します。*count* に指定できる範囲は 0 ～ 99 です。

デフォルト

モニタリングはディセーブルで、障害しきい値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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

- 診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。
- 診断モニタリングイネーブルにするには、**diagnostic monitor test 1** コマンドを入力します。
- **diagnostic monitor** test {*name* | *test-id* | *test-id-range* | **all**} コマンドを入力する場合は、接続されているすべてのポートをディセーブルにしてネットワーク トラフィックを分離する必要があります。
- テスト中はテスト パケットを送信しないでください。

例

次に、ヘルス モニタリング テストを設定する例を示します。

```
Switch(config)# diagnostic monitor threshold test 1 failure count 20
Switch(config)# diagnostic monitor interval test 1 12:30:00 750 5
```

関連コマンド

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

diagnostic schedule test

診断テストのスケジュールを設定するには、**diagnostic schedule test** グローバル コンフィギュレーション コマンドを使用します。スケジュー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。

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

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

構文の説明

name	テスト名を指定します。テスト ID のリストのテスト名を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id	テストの ID 番号を指定します。指定できる範囲は 1 ～ 6 です。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id-range	複数のテストをテストの ID 番号の範囲で指定します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
basic	基本的なオンデマンドの診断テストを指定します。
non-disruptive	ノンディスラプティブ ヘルス モニタリング テストを指定します。
daily *hh*:*mm*	診断テストのスケジューリング（日単位）を指定します。 *hh*:*mm*：2 桁の数字（24 時間表記）で時間および分を入力します。コロン（:）が必要です（例：12:30）。
on *mm dd yyyy hh*:*mm*	特定の日時の診断テストのスケジューリングを指定します。 *mm dd yyyy*： • *mm*：January、February のように、月を大文字または小文字で入力します。 • *dd*：2 桁の数字で日を入力します（例：03、16）。 • *yyyy*：4 桁の数字で年を入力します（例：2008）。
weekly *day-of-week hh*:*mm*	診断テストのスケジューリング（週単位）を指定します。 *day-of-week*：Monday、Tuesday のように、曜日を大文字または小文字で入力します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次に、特定の日時に診断テストをスケジューリングする例を示します。

```
Switch(config)# diagnostic schedule test 1,2,4-6 on november 3 2006 23:10
```

次に、毎週特定の時間に診断テストを行うようスケジューリングする例を示します。

```
Switch(config)# diagnostic schedule test TestPortAsicMem weekly friday 09:23
```

関連コマンド

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

diagnostic start test

オンライン診断テストを実行するには、**diagnostic start test** 特権 EXEC コマンドを使用します。

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

構文の説明

name	テスト名を指定します。テスト ID のリストのテスト名を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id	テストの ID 番号を指定します。指定できる範囲は 1 ～ 6 です。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
test-id-range	複数のテストをテストの ID 番号の範囲で指定します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。テスト ID のリストのテスト番号を表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
basic	基本的なオンデマンドの診断テストを指定します。
non-disruptive	ノンディスラプティブ ヘルス モニタリング テストを指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

diagnostic start コマンドを使用してテストを開始したら、テスト プロセスの停止はできません。

スイッチは、次のテストをサポートしています。

```
ID   Test Name [On-Demand Test Attributes]
---  ----------------------------------------
1    TestPortAsicStackPortLoopback    [B*N****]
2    TestPortAsicLoopback             [B*D*R**]
3    TestPortAsicCam                  [B*D*R**]
4    TestPortAsicRingLoopback         [B*D*R**]
5    TestMicRingLoopback              [B*D*R**]
6    TestPortAsicMem                  [B*D*R**]
---  ----------------------------------------
```

テスト名を確認するには、**show diagnostic content** 特権 EXEC コマンドを使用してテスト ID リストを表示します。テスト名を使用してテスト 3 を指定するには、**diagnostic start switch** *number* **test TestPortAsicCam** 特権 EXEC コマンドを入力します。

複数のテストを指定するには、*test-id-range* パラメータを使用し、カンマとハイフンで区切られた整数を入力します。 たとえば、テスト 2、3、および 4 を指定するには、**diagnostic start test 2-4** コマンドを入力します。テスト 1、3、4、5、および 6 を指定するには、**diagnostic start test 1,3-6** コマンドを入力します。

例

次に、診断テスト 1 を開始する例を示します。

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

次に、診断テスト 2 を開始する例を示します。このテストを実行すると、通常のシステム動作が中断され、スイッチがリロードされます。

```
Switch# diagnostic start test 2
Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]: y
Switch#
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console
00:00:30: %DIAG-6-TEST_RUNNING : Running TestPortAsicLoopback{ID=2} ...
00:00:30: %DIAG-6-TEST_OK: TestPortAsicLoopback{ID=2} has completed successfully
```

関連コマンド

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

dot1x credentials

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

dot1x credentials *profile*

no dot1x credentials *profile*

構文の説明

profile	サプリカント スイッチのプロファイルを指定します。

デフォルト

スイッチにプロファイルは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、スイッチをサプリカントとして設定する方法を示します。

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

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

関連コマンド

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

dot1x critical eapol（グローバル コンフィギュレーション）

スイッチによりクリティカルなポートが critical-authentication ステートに置かれた場合、スイッチが EAPOL-Success メッセージを送信するよう指定するには、**dot1x critical eapol** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x critical eapol

no dot1x critical eapol

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートのアクセス不能認証バイパスをイネーブルにするか、またはスイッチがクリティカルなポートを割り当てるアクセス VLAN を設定するには、**authencation event** インターフェイス コンフィギュレーション コマンドを使用します。

関連コマンド

コマンド	説明
authentication event	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
show dot1x	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x default

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

dot1x default

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト値は次のとおりです。

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

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

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

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

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x guest-vlan supplicant

スイッチでオプションの IEEE 802.1x ゲスト VLAN 動作をグローバルに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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ゲスト VLAN 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチのゲスト VLAN を設定する方法については、**authentication event no-response action authorize vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを参照してください。

例

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

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

関連コマンド

コマンド	説明
authentication event	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
show authentication [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x initialize

ポート上で新しく認証セッションを初期化する前に、指定の IEEE 802.1x 対応ポートを、手動で無許可ステートに戻すには、**dot1x initialize** 特権 EXEC コマンドを使用します。

dot1x initialize interface *interface-id*

構文の説明

interface *interface-id*	ポートを初期化します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IEEE 802.1x ステート マシンを初期化し、新たな認証環境を設定します。このコマンドを入力した後、ポートの状態は無許可になります。

このコマンドの **no** 形式はありません。

例

次の例では、ポートを手動で初期化する方法を示します。

```
Switch# dot1x initialize interface gigabitethernet0/2
```

show dot1x [**interface** *interface-id*] 特権 EXEC コマンドを入力することにより、ポート ステータスが無許可になっていることを確認できます。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-reauth-req

ポートが無許可ステートに移行するまでスイッチが認証プロセスを再起動する上限回数を設定するには、**dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *count*

no dot1x max-reauth-req

構文の説明

count	ポートが無許可ステートに移行する前に、スイッチが EAPOL-Identity-Request フレームを再送信して認証プロセスを開始する回数を設定します。ポートに 802.1x 非対応のデバイスが接続されている場合、スイッチは、デフォルトでは 2 回の認証試行を行います。ポートにゲスト VLAN が設定されている場合は、2 回の再認証試行後にポートはデフォルトでゲスト VLAN で許可されます。指定できる範囲は 1 ～ 10 です。デフォルトは 2 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

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

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

関連コマンド

コマンド	説明
dot1x max-req	スイッチが認証プロセスを再起動する前に、EAP フレームを認証サーバに送信する最高回数を設定します（応答を受信しないと仮定）。
authentication timer	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。

コマンド	説明
show authentication	指定されたポートの認証ステータスを表示します。
show dot1x [**interface** *interface-id*]	指定されたポートの 802.1x の状態を表示します。

dot1x max-req

スイッチが認証プロセスを再起動する前に、拡張認証プロトコル（EAP）フレームを認証サーバからクライアントに送信する最大回数を設定するには（応答を受信しないことが前提）、**dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req *count*

no dot1x max-req

構文の説明

count	スイッチが、認証プロセスを再起動する前に、EAPOL DATA パケットの再送信を試行する回数です。たとえば、認証プロセス中にサプリカントに問題が発生した場合、オーセンティケータがデータ要求を 2 回再送信し、応答がなければプロセスを中止します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、認証プロセスを再起動する前に、スイッチが EAP フレームを認証サーバから送信する回数を 5 回に設定する方法を示します。

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

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

関連コマンド

コマンド	説明
authentication timer	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 authentication	指定されたポートの認証ステータスを表示します。

dot1x pae

IEEE 802.1x ポート アクセス エンティティ（PAE）タイプを設定するには、**dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。設定されている PAE タイプ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 pae [supplicant | authenticator | both]

no dot1x pae [supplicant | authenticator | both]

構文の説明

supplicant	（任意）インターフェイスは、IEEE 802.1x サプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	（任意）インターフェイスは、IEEE 802.1x オーセンティケータとしてだけ機能し、サプリカント向けのメッセージに応答しません。
both	（任意）インターフェイスは、IEEE 802.1x サプリカントおよび IEEE 802.1x オーセンティケータとして動作するため、すべての dot1x メッセージに応答します。

デフォルト

IEEE 802.1x PAE タイプは設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

dot1x system-auth-control コマンドが設定されていない場合、**supplicant** キーワードがこのコマンドで使用できる唯一のキーワードとなります （つまり、**dot1x system-auth-control** コマンドが設定されていない場合、インターフェイスをオーセンティケータとして設定できません）。

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

例

次に、インターフェイスをサプリカントとして動作するように設定する例を示します。

```
Router (config-if)# dot1x pae supplicant
```

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

関連コマンド

コマンド	説明
dot1x system-auth-control	スイッチ上で IEEE 802.1x 認証をグローバルにイネーブルにします。
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。
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

dot1x supplicant force-multicast

マルチキャストまたはユニキャスト Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合、常にサプリカント スイッチにマルチキャスト EAPOL *だけ*を送信させるようにするには、**dot1x supplicant force-multicast** グローバル 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 supplicant force-multicast

no dot1x supplicant force-multicast

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカントのクレデンシャルを設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x system-auth-control

IEEE 802.1x をグローバルにイネーブルにするには、**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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x system-auth-control

no dot1x system-auth-control

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IEEE 802.1x はディセーブル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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

IEEE 802.1x をグローバルにイネーブルにする前に、認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

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

例

次の例では、スイッチで 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
```

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

関連コマンド

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
show authentication	指定されたポートの認証ステータスを表示します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、**dot1x test eapol-capable** 特権 EXEC コマンドを使用します。

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

構文の説明

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

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1x 機能をテストするには、このコマンドを使用します。

このコマンドには、**no** 形式はありません。

例

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

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

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

関連コマンド

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

dot1x test timeout

IEEE 802.1x の準備が整っているかどうかを確認するためにクエリーが実行されるポートからの EAPOL 応答の待機に使用するタイムアウトを設定するには、**dot1x test timeout** グローバル コンフィギュレーション コマンドを使用します。

dot1x test timeout *timeout*

構文の説明

timeout	EAPOL 応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。

デフォルト

デフォルト設定は 10 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、**no** 形式はありません。

例

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

```
Switch# dot1x test timeout 27
```

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

関連コマンド

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

dot1x timeout

IEEE 802.1x のタイマーを設定するには、**dot1x timeout** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **reauth-period** {*seconds* | **server**} | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

構文の説明

auth-period *seconds*	サプリカント（クライアント）がオーセンティケータからの応答（Extensible Authentication Protocol over LAN（EAPOL）-Start 以外のパケット）を何秒待機するとタイムアウトとなるかを設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルト値は 60 です。
quiet-period *seconds*	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数。指定できる範囲は 1 ～ 65535 です。
ratelimit-period *seconds*	この期間中に認証に成功したクライアントからの Extensible Authentication Protocol over LAN（EAPOL）パケットをスイッチが無視した秒数。指定できる範囲は 1 ～ 65535 です。
reauth-period {*seconds* | **server**}	再認証の試行の間隔（秒）を設定します。 キーワードの意味は次のとおりです。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : セッションタイムアウト RADIUS 属性（属性 [27]）の値として秒数を設定します。
server-timeout *seconds*	認証サーバに対して、スイッチのパケット再送信を待機する秒数。 指定できる範囲は 1 ～ 65535 です。30 の最小設定を推奨します。
start-period *second*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 指定できる値は 1 ～ 65535 です。デフォルトは 30 です。
supp-timeout *seconds*	スイッチが IEEE 802.1x クライアントへパケットを再送信する前に待機する秒数。指定できる範囲は 30 ～ 65535 です。
tx-period *seconds*	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

auth-period は 30 秒です。

held-period は 60 秒です。

quiet-period は 60 秒です。

rate-limit は 1 秒です。

reauth-period は 3600 秒です。

server-timeout は 30 秒です。

start-period は 30 秒です。

supp-timeout は 30 秒です。

tx-period は 5 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

dot1x timeout コマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

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

例

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

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

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

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

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

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

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

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

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

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

次の例では、EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

次の例では、認証に成功したクライアントからの EAPOL パケットをスイッチが無視する秒数を 30 と設定する方法を示します。

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

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

関連コマンド

コマンド	説明
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
dot1x max-req	スイッチが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最高回数を設定します。
authentication periodic	クライアントの定期的再認証をイネーブルにします。
show dot1x	すべてのポートの IEEE 802.1x ステータスを表示します。

duplex

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

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	自動によるデュプレックス設定をイネーブルにします（接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードかを判断します）。
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 Mb/s または 100 Mb/s で動作するインターフェイスに限る）。1000 Mb/s または 10,000 Mb/s で動作するインターフェイスに対しては半二重モードを設定できません。

デフォルト

ファスト イーサネット ポート、ギガビット イーサネット ポート、および 1000BASE-T 小型フォーム ファクタ（SFP）モジュールのデフォルトは **auto** です。

100BASE-x（-x は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **half** 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、1000BASE-T SFP モジュールまたは 100BASE-FX MMF SFP モジュールが SFP モジュール スロットに挿入されている場合のみ使用できます。他のすべての SFP モジュールは全二重モードだけで動作します。

1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックス モードを **auto** または **full** に設定できます。

100BASE-FX MMF SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックス モードを **half** または **full** に設定できます。100BASE-FX MMF SFP モジュールでは、**auto** キーワードを使用できますが、自動ネゴシエーションがサポートされていないため、インターフェイスは半デュプレックス モード（デフォルト）になります。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

ファスト イーサネット ポートでは、接続された装置がデュプレックス パラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**half** を指定するのと同じ効果があります。

ギガビット イーサネット ポートでは、接続装置がデュプレックス パラメータを自動ネゴシエートしないときにポートを **auto** に設定すると、**full** を指定する場合と同じ効果があります。

（注）　デュプレックス モードが **auto** で、接続されている装置が半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

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

速度が **auto** に設定されている場合、スイッチはリンクの反対側のデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

（注）　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 ガイドを参照してください。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

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

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

関連コマンド

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

errdisable detect cause

特定の原因、またはすべての原因に対して、errdisable 検出をイネーブルにするには、**errdisable detect cause** グローバル コンフィギュレーション コマンドを使用します。errdisable 検出機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

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

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

（注） コマンドライン インターフェイスでは表示されますが、既存のブロードキャスト ストーム ディセーブル機能が小さなフレームを正しく制御できるので、**small-frame** キーワードは必要ありません。

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック 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）スヌーピング用のエラー検出をイネーブルにします。
gbic-invalid	無効な Gigabit Interface Converter（GBIC; ギガビット インターフェイス コンバータ）モジュール用のエラー検出をイネーブルにします。 **（注）** このエラーは、無効な小型フォーム ファクタ（SFP）モジュールを意味します。
inline-power	Power over Ethernet（PoE）の errdisable 原因に対して、エラー検出をイネーブルにします。
l2ptguard	レイヤ 2 プロトコル トンネルの errdisable 原因に対して、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; ポート集約プロトコル）フラップの errdisable 原因のエラー検出をイネーブルにします。
small-frame	スイッチでは、この機能は不要です。

デフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

原因（**all**、**dhcp-rate-limit** など）は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、リンクダウン ステートに類似した動作ステートとなります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因に対して **errdisable recovery** グローバル コンフィギュレーション コマンドを入力して、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、インターフェイスを手動で errdisable ステートから回復させる必要があります。

例

次の例では、リンクフラップ errdisable 原因に対して 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** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

errdisable recovery

回復メカニズムの変数を設定するには、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **gbic-invalid** | **inline-power** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **small-frame** | **udld** |**unicast-flood** | **vmps**} | {**interval** *interval*}

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

（注） **storm-control** キーワードおよび **unicast-flood** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。**small-frame** キーワードは、ブロードキャスト ストーム ディセーブル機能が小さなフレームを処理するため、使用されません

構文の説明

cause	特定の原因から回復するように errdisable メカニズムをイネーブルにします。
all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
bpduguard	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）検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
channel-misconfig	EtherChannel の設定矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	Gigabit Interface Converter（GBIC; ギガビット インターフェイス コンバータ）モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 **（注）** このエラーは無効な小型フォーム ファクタ（SFP）の errdisable ステートを意味します。
inline-power	Power over Ethernet（PoE）の errdisable ステートから回復するタイマーをイネーブルにします。
l2ptguard	レイヤ 2 プロトコル トンネルによる errdisable ステートから回復するためのタイマーをイネーブルにします。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	Port Aggregation Protocol（PAgP; ポート集約プロトコル）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。

security-violation	IEEE 802.1x 違反ディセーブル ステートから回復するタイマーをイネーブルにします。
small-frame	このキーワードは使用されません。
udld	UniDirectional Link Detection（UDLD; 単方向リンク検出）errdisable ステートから回復するタイマーをイネーブルにします。
unicast-flood	ユニキャスト フラッディング 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。
vmps	VLAN 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 recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

デフォルト

すべての原因に対して回復はディセーブルです。

デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

原因（**all**、**bpduguard** など）は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート（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。その原因の errdisable 回復をイネーブルにしない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するまで、インターフェイスは errdisable ステートのままです。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 ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でインターフェイスを errdisable ステートから回復させる必要があります

例

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

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

次の例では、タイマーを 500 秒に設定する方法を示します。

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

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

関連コマンド

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

ethernet evc

イーサネット仮想接続（EVC）を定義し、EVC コンフィギュレーション モードを開始するには、**ethernet evc** グローバル コンフィギュレーション コマンドを使用します。EVC を削除するには、このコマンドの **no** 形式を使用します。

ethernet evc *evc-id*

no ethernet evc *evc-id*

構文の説明

evc-id	EVC の ID。1 ～ 100 文字の文字列を設定できます。

デフォルト

EVC 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ethernet evc *evc-id* コマンドを入力すると、スイッチは、EVC コンフィギュレーション モードを開始して、次のコンフィギュレーション コマンドを使用できるようになります。

- **default**：EVC をデフォルト ステートに設定します。
- **exit**：EVC 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**：コマンドを無効にするか、コマンドをデフォルト設定に戻します。
- **oam protocol cfm svlan**：イーサネットの運用管理および保守（OAM）プロトコルを IEEE 802.1ag の接続障害管理（CFM）として設定し、パラメータを設定します。**oam protocol cfm svlan** コマンドを参照してください。
- **uni count**：EVC の UNI カウントを設定します。**uni count** コマンドを参照してください。

例

次の例では、EVC を定義して EVC 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)# ethernet evc test1
Switch(config-evc)#
```

関連コマンド

コマンド	説明
service instance *id* **ethernet** *evc-id*	イーサネット サービス インスタンスを設定し、EVC を適用します。
show ethernet service evc	設定された EVC に関する情報を表示します。

ethernet lmi

イーサネット ローカル管理インターフェイス（E-LMI）としてイネーブルにする設定を行ったり、スイッチをプロバイダー エッジ（PE）デバイスまたはカスタマー エッジ（CE）デバイスとして設定したりするには、**ethernet lmi** グローバル コンフィギュレーション コマンドを使用します。E-LMI をグローバルにディセーブルにしたり、E-LMI CE をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

ethernet lmi {**ce** | **global**}

no ethernet lmi {**ce** | **global**}

構文の説明

ce	スイッチを E-LMI CE デバイスとしてイネーブルにします。 **（注）** イーサネット LMI はデフォルトでディセーブルです。E-LMI は CE モードでイネーブルにするだけではなく、グローバルにまたはインターフェイスでもイネーブルにする必要があります。
global	スイッチで E-LMI をグローバルにイネーブルにします。デフォルトでは、スイッチは PE デバイスです。

デフォルト

イーサネット LMI はディセーブルです。global キーワードを使用してイネーブルにされた場合、デフォルトでは、スイッチは PR デバイスです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

E-LMI をグローバルにイネーブルにするには、**ethernet lmi global** コマンドを使用します。E-LMI CE デバイスとしてスイッチをイネーブルにするには、**ethernet lmi ce** コマンドを使用します。

イーサネット LMI はインターフェイスではデフォルトでディセーブルであり、**ethernet lmi interface** インターフェイス コンフィギュレーション コマンドを入力して、明示的にイネーブルにする必要があります。**ethernet lmi global** コマンドはデバイス全体のすべてのインターフェイスにおいて、PE モードでイーサネット LMI をイネーブルにします。このコマンドの利点は、各インターフェイスでイーサネット LMI を個別にイネーブルにする代わりに 1 種類のコマンドですべてのインターフェイスのイーサネット LMI をイネーブルにできることです。CE モードでインターフェイスをイネーブルにするには、**ethernet lmi ce** グローバル コンフィギュレーション コマンドも入力する必要があります。

ethernet lmi global コマンドを入力したあとで、特定のインターフェイスで E-LMI をディセーブルにするには、**no ethernet lmi interface** インターフェイス コンフィギュレーション コマンドを入力します。

ethernet lmi interface インターフェイス コンフィギュレーション コマンドと **ethernet lmi global** 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順序が重要です。入力された最新のコマンドが前のコマンドを上書きします。

（注）　**ethernet lmi** インターフェイス コンフィギュレーション コマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080690f2d.html#wp1166797

スイッチを E-LMI CE デバイスとしてイネーブルにするには、**ethernet lmi global** コマンドおよび **ethernet lmi ce** コマンドの両方を入力します。デフォルトでは E-LMI はディセーブルです。E-LMI をイネーブルにしても **ethernet lmi ce** コマンドを入力しない限り、スイッチは PE モードです。

スイッチを E-LMI CE デバイスとして設定すると、次のインターフェイス コンフィギュレーション コマンドとキーワードが表示されますが、サポートされていません。

- **service instance**
- **ethernet uni**
- **ethernet lmi t392**

例

次の例では、スイッチを E-LMI CE デバイスとして設定する方法を示します。

```
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
```

関連コマンド

コマンド	説明
ethernet lmi インターフェイス コンフィギュレーション コマンド	ユーザネットワーク インターフェイスの E-LMI をイネーブルにします。

ethernet lmi ce-vlan map

イーサネット ローカル管理インターフェイス（ELMI）パラメータを設定するには、**ethernet lmi ce-vlan map** のイーサネット サービス コンフィギュレーション コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ethernet lmi ce-vlan map {*vlan-id* | **any** | **default** | **untagged**}

no ethernet lmi ce-vlan map {*vlan-id* | **any** | **default** | **untagged**}

構文の説明

vlan-id	マッピングする 1 つ以上のカスタマー VLAN ID を入力します。単一の VLAN ID（範囲は 1 ～ 4094）、ハイフンで区切られた VLAN ID の範囲、またはカンマで区切った一連の VLAN ID を入力できます。
any	すべての VLAN（タグ付けされていない VLAN および 1 ～ 4094 の VLAN）をマッピングします。
default	デフォルトのサービス インスタンスにマッピングします。**default** キーワードは、すでにサービス インスタンスを 1 つの VLAN または VLAN のグループにマッピングしている場合にだけ使用できます。
untagged	タグ付けされていない VLAN のみをマッピングします。

デフォルト

E-LMI マッピング パラメータは定義されていません。

コマンド モード

イーサネット サービス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

特定の User-Network Interface（UNI; ユーザネットワーク インターフェイス）の E-LMI カスタマー VLAN から EVC へのマッピングを設定するには、このコマンドを使用します。

ethernet uni {**bundle** [**all-to-one**] | **multiplex**} 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設定されたバンドル特性に E-LMI マッピング パラメータが関連付けられます。

- デフォルト UNI 属性（バンドルおよび多重化）の使用では、複数の EVC および複数の VLAN がサポートされます。
- **ethernet uni bundle** コマンドの入力では、1 つ以上の VLAN を持つ 1 つの EVC だけがサポートされます。
- **ethernet uni bundle all-to-one** コマンドの入力では、複数の VLAN がサポートされますが、EVC は 1 つだけサポートされます。**ethernet lmi ce-vlan map any** イーサネット サービス コンフィギュレーション コマンドを使用する場合、事前に **all-to-one** バンドルをインターフェイスで設定する必要があります。
- **ethernet uni multiplex** コマンドの入力では、EVC ごとに VLAN を 1 つだけ持つ、複数の EVC がサポートされます。

例

次の例では、E-LMI カスタマー VLAN から EVC へのマッピングを設定し、インターフェイスのサービス インスタンス 333 にあるカスタマー VLAN 101 に EVC *test* をマッピングする方法を示します。

```
Switch(config-if)# service instance 333 ethernet test
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
```

関連コマンド

コマンド	説明
service instance *id* **ethernet**	イーサネット サービス インスタンスを定義し、イーサネット サービス コンフィギュレーション モードを開始します。
show ethernet service instance	設定されたイーサネット サービス インスタンスに関する情報を表示します。

ethernet loopback（イーサネット コンフィギュレーション）

複数のスイッチ間での接続をテストするためのポート単位のループバックを設定するには、**ethernet loopback facility** インターフェイス コンフィギュレーション コマンドを使用します。Quality of Service（QoS）をテストするには、**ethernet loopback terminal** インターフェイス コンフィギュレーション コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ethernet loopback facility [**vlan** *vlan-list*] [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**

ethernet loopback terminal [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**

no ethernet loopback

構文の説明

facility	接続テスト用のファシリティ ループバックを設定します。
vlan *vlan-list*	中断のないループバック テストの VLAN のループバックを設定します。
terminal	QoS のテストのターミナル ループバックを設定します。
mac-address swap	ループバック処理のため送信元 MAC アドレスと宛先 MAC アドレスをスワップするようスイッチを設定します。
mac-address copy	ループバック処理のため送信元 MAC アドレスと宛先 MAC アドレスをコピーするようスイッチを設定します。
timeout *seconds*	秒単位でのループバック タイムアウト時間を設定します。指定できる範囲は 5 ～ 300 秒です。デフォルトは 60 秒です。
timeout none	ループバックがタイムアウトしないように設定します。
supported	設定されたループバックをサポートするように指定します。

デフォルト

ループバックは設定されません。**mac-address** オプションが設定されていない場合、デフォルトでは、送信元アドレスおよび宛先アドレスがコピーされます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット ループバックは、VLAN またはポート チャネルではなく、物理ポートでだけ設定できます。

ファシリティ ループバックにより、ポートでは、通常のトラフィックに対してリンクはアップ状態になりますが、ライン プロトコルはダウン状態になります。スイッチにより、すべての受信トラフィックはループバックされます。

キーワード **vlan** *vlan-list* を入力して VLAN ループバックを設定すると、ポートのその他の VLAN では引き続き正常にスイッチが行われるため、処理を中断させずにループバック テストできます。

ループバックは、ポートのシャットダウンやスイッチ ポートからルーテッド ポートへの変更などのポート イベント後に終了します。

ターミナル ループバックの場合、ソフトウェアでは、ポートはアップ状態であるがリンクはダウン状態であると認識され、パケットは送信されません。ポートの設定変更は、ループバックされているトラフィックに即座に影響を与えます。

ポート 1 つにつきループバックを 1 つ設定でき、スイッチ 1 つにつきループバックを 2 つまで設定できます。スイッチ 1 つにつきターミナル ループバックは 1 つだけ設定できます。そのため、スイッチには 1 つのファシリティ ループバックおよび 1 つのターミナル ループバック、または 2 つのファシリティ ループバックが存在する可能性があります。

他の機能とのイーサネット ループバックの相互作用：

- SPAN とループバックは同じスイッチで同時に設定できません。いずれかのポートにループバックが設定されている場合に任意のポートに SPAN を設定しようとすると、エラー メッセージが表示されます。
- ポート ループバック機能は、VLAN マッピング機能とハードウェア リソースを共有します。ループバックを設定しようとするとき、VLAN マッピング設定のために十分な TCAM リソースが使用できない場合、エラー メッセージを受信し、設定は許可されません。
- ループバックがポート上でアクティブな場合、このポートを Flex Link ペアまたは EtherChannel に追加できません。

イーサネット ループバックを設定したら、ループバックを開始するために **ethernet loopback start** *interface-id* 特権 EXEC コマンドを入力します。ループバックを停止するには、**ethernet loopback stop** {*interface-id* | **all**} コマンドを入力します。

例

次に、宛先 MAC アドレスおよび送信元 MAC アドレスをスワップし、30 秒後にタイムアウトし、ループバック プロセスを開始して、設定を確認するようイーサネット ループバックを設定する方法の例を示します。設定する前に処理を確認する必要があります。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback?[confirm]

Switch# show ethernet loopback
=====================================
Loopback Session 0  : Interface GI0/1
Direction           : facility
Type                : port
Status              : active
MAC Mode            : swap
Time out            : 30
Time remaining      : 25 seconds
```

また、2 番めのインターフェイスに中断のないループバックを設定する例を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ethernet loop facility mac-address swap timeout none supported
Switch(config-if)# exit
Switch(config-if)# interface fastethernet0/2
```

```
Switch(config-if)# ethernet loop facility vlan 3 mac-address copy timeout 100 supported
switch(config-if)# switch mode trunk
Switch(config-if)# exit
switch(config)# vlan 3
switch(config-vlan)# end

Switch# show ethernet loopback
=====================================
Loopback Session 0  : Interface Fa0/1
Direction           : facility
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : none
=====================================
Loopback Session 1  : Interface Fa0/2
Direction           : facility
Type                : vlan
Status              : configured
MAC Mode            : copy
Vlan                : 3
Time out            : 100
```

次に、2 つのインターフェイスでイーサネット ループバック機能設定を削除して、1 つのインターフェイスでイーサネット ターミナル ループバックを設定する例を示します。

```
Switch(config)# interface fastethernet 0/1
switch(config-if)# no ethernet loopback
switch(config-if)# interface fastethernet 0/2
switch(config-if)# no ethernet loopback
switch(config-if)# exit
switch(config)# default interface range fastethernet 0/1-2
switch(config)# interface fastethernet 0/1
switch(config-if)# ethernet loop terminal mad-address swap timeout 300 supported
switch(config-if)# end

Switch# show ethernet loopback
=====================================
Loopback Session 0  : Interface Fa0/1
Direction           : terminal
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : 300
```

関連コマンド

コマンド	説明
ethernet loopback（特権 EXEC）	インターフェイス上のイーサネット ループバック操作を開始または停止します。
show ethernet loopback	スイッチまたは指定したインターフェイスに設定されているイーサネット ループバックを表示します。

ethernet loopback（特権 EXEC）

インターフェイスでイーサネット ループバック機能を開始または停止するには、**ethernet loopback** 特権 EXEC コマンドを使用します。

ethernet loopback {**start** *interface-id* | **stop** {*interface-id* | **all**}}

構文の説明

start	インターフェイスに設定されているイーサネット ループバック操作を開始します。
stop	イーサネット ループバック操作を停止します。
interface-id	ループバック操作を開始または停止するインターフェイスを指定します。
all	スイッチ上のすべてのイーサネット ループバック操作を停止します。このキーワードは、**stop** キーワードの後にのみ使用できます。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット ループバック操作を開始または停止する前に、**ethernet loopback** インターフェイス コンフィギュレーション コマンドを入力して、インターフェイスでイーサネット ループバックを設定する必要があります。ループバックを開始すると、警告メッセージが表示されます。

物理ポートに対してのみ、イーサネット ループバックを設定して **ethernet loopback start** コマンドまたは **ethernet loopback stop** コマンドを入力できます。VLAN やポート チャネルに対してはこれらを行うことはできません。

非トランク インターフェイスでは VLAN ループバックを開始できません。ルーテッド インターフェイスではターミナル ループバックを開始できません。

ポート 1 つにつきループバックを 1 つのみ設定でき、スイッチ 1 つにつきループバックを 2 つまで設定できます。スイッチ 1 つにつきターミナル ループバックは 1 回だけ設定できます。

例

次に、ファシリティ ポート ループバック プロセスを開始し、確認して、停止する例を示します。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback?[confirm]
```

```
Switch# show ethernet loopback
====================================
Loopback Session 0  : Interface Gi0/1
Direction           : facility
Type                : port
Status              : active
MAC Mode            : swap
Time out            : 30
Time remaining      : 25 seconds

Switch# ethernet loop stop all

Dec  4 11:18:44.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Switch# show ethernet loopback
====================================
Loopback Session 0  : Interface Gi0/1
Direction           : facility
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : 30
```

次に、VLAN の非侵入型ループバック プロセスを開始する例を示します。

```
Switch# ethernet loop start fastethernet 0/2
This is a non-intrusive loopback.
Therefore, while you test Ethernet connectivity on vlan 3, you will be unable to pass
traffic across it, however, other vlans will be unaffected.
Proceed with Local Loopback?[confirm]

Switch# show ethernet loopback
====================================
Loopback Session 1  : Interface Fa0/2
Direction           : facility
Type                : vlan
Status              : active
MAC Mode            : copy
Vlan                : 3
Time out            : 100
Time remaining      : 94 seconds
```

関連コマンド

コマンド	説明
ethernet loopback（イーサネット コンフィギュレーション）	インターフェイス上のイーサネット ループバック操作を設定します。
show ethernet loopback	スイッチまたは指定したインターフェイスに設定されているイーサネット ループバックを表示します。

ethernet oam remote-failure

Ethernet Operation, administration, and Maintenance（EOM）リモート障害表示を設定するには、**ethernet oam remote-failure** インターフェイス コンフィギュレーションまたはコンフィギュレーション テンプレート コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action error-disable-interface**

no ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action**

構文の説明

critical-event	未指定のクリティカルなイベントが発生したとき、インターフェイスを errdisable モードにするようにスイッチを設定します。
dying-gasp	回復不能な状態が発生したとき、インターフェイスを errdisable モードにするようにスイッチを設定します。
link-fault	レシーバが電力の損失を検出すると errdisable モードにインターフェイスを変更するようにスイッチを設定します。

デフォルト

設定テンプレート

インターフェイス コンフィギュレーション

コマンド モード

イーサネット サービス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、イーサネット OAM テンプレートおよびインターフェイスに適用できます。インターフェイス設定は、テンプレートの設定よりも優先されます。OAM テンプレート コンフィギュレーション モードを開始するには、**template** template-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。

Cisco CGS 2520 スイッチは、Link Fault と Critical Event OAM PDU を生成しません。ただし、スイッチがこれらの PDU をリンクの相手方から受信した場合は処理します。イーサネット OAM がディセーブルのとき、インターフェイスがシャットダウンしたとき、インターフェイスが errdisable ステートになったとき、またはスイッチがリロードしているときに、スイッチは Dying Gasp OAM PDU の生成と受信をサポートします。また、スイッチは電源喪失に基づいた Dying Gasp PDU を生成し、受信できます。PDU には、PDU が送信された理由を示す原因コードが含まれています。リモート デバイスがディセーブルの場合、またはリモート デバイスがインターフェイス上のイーサネット OAM をディセーブルにした場合に、errdisable アクションを発生させるように設定できます。

イーサネット OAM プロトコルのコマンドと設定の詳細については、次の URL の Cisco IOS フィーチャ モジュールを参照してください。
http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008067344c.html

CFM およびイーサネット OAM コマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6922/products_command_reference_book09186a0080699104.html

例

次に、回復不能なエラーが発生した場合のためのリモート障害表示のイーサネット OAM テンプレート設定方法、およびインターフェイスへの適用方法の例を示します。

```
Switch(config)# template oam1
Switch(config-template)# ethernet oam remote-failure dying-gasp action error-disable
interface
Switch(config-template)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# source template oam1
Switch(config-if)# exit
```

次に、回復不能なエラーが発生した場合のイーサネット OAM リモート障害表示を 1 つのインターフェイスに設定する例を示します。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp action error-disable interface
Switch(config-if)# exit
```

関連コマンド

コマンド	説明
show ethernet oam status [**interface** *interface-id*]	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上に設定済みのイーサネット OAM リモート障害条件を表示します。

ethernet uni

UNI バンドル属性を設定するには、**ethernet uni** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトのバンドル設定に戻すには、このコマンドの **no** 形式を使用します。

ethernet uni {**bundle** [**all-to-one**] | **multiplex**}

no ethernet uni {**bundle** | **multiplex**}

構文の説明

bundle	多重化しないでバンドルをサポートするように UNI を設定します。このサービスでは、UNI において、1 つまたは複数のカスタマー エッジ（CE）VLAN ID がマッピングされた 1 つのイーサネット仮想接続（EVC）のみがサポートされます。
all-to-one	（任意）UNI において、すべての CE VLAN がマッピングされた 1 つの EVC によるバンドルをサポートするように UNI を設定します。
multiplex	バンドルしないで多重化をサポートするように UNI を設定します。UNI には、それぞれに 1 つの CE VLAN ID がマッピングされた 1 つ以上の EVC を設定できます。

デフォルト

バンドルまたは多重化属性が設定されていない場合、デフォルトは多重化を使用したバンドリングです。その場合、UNI には、それぞれに 1 つ以上の CE VLAN VLAN がマッピングされた 1 つ以上の EVC を設定できます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

UNI 属性によって、VLAN のバンドル、EVC の多重化、およびこれらの組み合わせについてのインターフェイスの機能が決定されます。

UNI にバンドルと多重化両方のサービスを行わせたい場合、バンドルまたは多重化を設定する必要はありません。バンドルまたは多重化だけする場合、これを適切に設定する必要があります。

UNI サービス タイプを設定、変更、削除する場合、EVC および CE-VLAN ID 設定をチェックして、コンフィギュレーションと UNI サービス タイプが一致していることを確認します。設定が一致しない場合、コマンドは拒否されます。

ethernet lmi ce-vlan map any サービス コンフィギュレーション コマンドを使用する場合、事前に **all-to-one** バンドルをインターフェイスで設定する必要があります。詳細については、**ethernet lmi ce-vlan map** の項を参照してください。

例

次に、多重化しないでバンドルを設定する例を示します。

```
Switch(config-if)# ethernet uni bundle
```

UNI サービス タイプを確認するには、**show ethernet service interface detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ethernet service interface	サービス タイプなど、インターフェイスのイーサネット サービス インスタンスに関する情報を表示します。

ethernet uni id

ユーザ ネットワーク インターフェイス（UNI）ID を作成するには、**ethernet uni** インターフェイス コンフィギュレーション コマンドを使用します。UNI ID を削除するには、このコマンドの **no** 形式を使用します。

ethernet uni id *name*

no ethernet uni id

構文の説明

name	イーサネット UNI ID を識別します。同じサービス インスタンスに属するすべての UNI の名前はそれぞれ、一意である必要があります。名前の長さは 64 文字までです。

デフォルト

UNI ID は作成されません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートに UNI ID を設定すると、その ID はポートに設定されたすべてのメンテナンス エンド ポイント（MEP）のデフォルトの名前として使用されます。

カスタマー エッジ（CE）デバイスに直接接続されているすべてのポートで **ethernet uni id** *name* コマンドを入力する必要があります。指定された ID がデバイス上で一意でない場合は、エラー メッセージが表示されます。

例

次に、一意の UNI を識別する方法を示します。

```
Switch(config-if)# ethernet uni id test2
```

関連コマンド

コマンド	説明
show ethernet service interface	サービス タイプなど、インターフェイスのイーサネット サービス インスタンスに関する情報を表示します。

exceed-action

認定情報レート（CIR）または最大情報レート（PIR）の適合レートと、適合レートに超過バーストを加えたレートの間のレートのパケットに対するポリシーマップ クラスに複数のアクションを設定するには、**exceed-action** ポリシーマップ クラス ポリシング コンフィギュレーション コマンドを使用します。アクションをキャンセルしたり、デフォルト アクション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。

exceed-action {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

no exceed-action {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

構文の説明

drop	パケットをドロップします。
set-cos-transmit *new-cos-value*	パケットの新しいサービス クラス（CoS）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit *new-dscp-value*	パケットの新しい DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit *new-precedence-value*	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit *qos-group-value*	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	（任意）着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
dscp	（任意）着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
precedence	（任意）着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
table *table-map name*	（任意）上記の *from-type* キーワードとともに使用します。拡張パケット マーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの *from-type* パラメータに基づき、アクションの *to-type* がマーキングされます。
transmit	（任意）パケットを変更せずに送信します。

デフォルト

デフォルトのアクションは、パケットのドロップです。

コマンド モード

ポリシーマップ クラス ポリシング設定

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

パケット レートが、設定された適合レートと、適合レートに超過バーストを加えたレートの間である場合のパケットに対する超過アクションを設定します。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

超過アクションは、パケットの変更なしでの送信、明示値を使用したマーキング、および拡張パケット マーキングのすべての組み合わせの使用に設定できます。拡張パケット マーキングによって、任意の着信 QoS マーキングおよびテーブル マップに基づいて QoS マーキングを変更できます。スイッチでは、同じクラスに複数の QoS パラメータをマーキングし、同時に conform-action、exceed-action、violate-action マーキングを行う機能もサポートされています。

ポリシーマップ クラス ポリシング コンフィギュレーション モードにアクセスするには、**police** ポリシーマップ クラス コマンドを入力します。詳細については、**police** コマンドを参照してください。

このコマンドを使用して、トラフィック クラスに対して 1 つ以上の超過アクションを設定できます。

例

次に、情報レートを 23000 ビット/秒に、バースト レートを 10000 ビット/秒に設定するポリシー マップで複数のアクションを設定する例を示します。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# exit
```

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

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
conform-action	CIR に適合するトラフィックに対して実行するアクションを定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	QoS ポリシー マップを表示します。
violate-action	適合レートに超過バーストを加えたレートよりも大きいレートのトラフィックで実行されるアクションを定義します。

fcs-threshold

フレーム チェック シーケンス（FCS）ビットエラー レートを設定するには、**fcs-threshold** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

fcs-threshold *value*

no fcs-threshold *value*

構文の説明

value	値範囲は 6 ～ 11 で、10^{-6} ～ 10^{-11} ビットエラー レートを示します。

デフォルト

デフォルトは 8 です。これは、イーサネット標準の 10^{-8} ビット エラー レートを示します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット標準の上限ビット エラー レートは 10^{-8} です。CGS 2520 スイッチで設定可能なビット エラー レートの範囲は 10^{-6} ～ 10^{-11} です。スイッチのビット エラー レートは自然数です。ビット エラー レートに 10^{-9} を設定する場合は、係数に 9 を入力します。

スイッチに FCS エラー ヒステリシスしきい値を設定して、実際のビット エラー レートの変動が設定したビット エラー レートに接近した場合のアラームを防止するには、**alarm facility fcs hysteresis** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、ポートの FCS ビット エラー レートを 10^{-10} に設定する方法を示します。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# fcs-threshold 10
```

関連コマンド

コマンド	説明
alarm facility fcs-hysteresis	スイッチの FCS ヒステリシスしきい値をポートに設定された FCS ビット エラー レートの許容変動率で設定します。
show fcs-threshold	インターフェイスそれぞれの FCS エラー ビット レート設定を正数の係数として表示します。

flowcontrol

インターフェイスの受信フロー制御ステート を設定するには、**flowcontrol** インターフェイス コンフィギュレーション コマンドを使用します。ある装置に対してフロー制御 **send** が動作可能でオンになっていて、接続のもう一方の側で輻輳が少しでも検出された場合は、休止フレームを送信することによって、リンクの相手側またはリモート装置に輻輳を通知します。ある装置に対してフロー制御 **receive** がオンで、休止フレームを受信した場合、データ パケットの送信は停止します。こうすることにより、輻輳期間中にデータ パケットの損失を防ぎます。

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

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

（注）　Cisco CGS 2520 スイッチはポーズ フレームのみを受信できます。

構文の説明

receive	インターフェイスがリモート装置からフロー制御パケットを受信できるかどうかを設定します。
desired	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼動させることができます。
off	接続装置がフロー制御パケットをインターフェイスへ送信する機能をオフにします。
on	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼動させることができます。

デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このスイッチでは、送信フロー制御の休止フレームはサポートされません。ポートがユーザ ネットワーク インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）の場合、**flowcontrol** コマンドを使用する前に **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してインターフェイスをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス（NNI）はデフォルトでイネーブルです。

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

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

- **receive on** または **desired**：ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要がある装置、または送信可能な接続装置と連動できます。ポートでは、ポーズ フレームを受信できます。
- **receive off**：フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

表 2-3 は、各設定の組み合わせによるローカル ポートおよびリモート ポート上のフロー制御の結果を示したものです。表は **receive desired** キーワードの使用時と **receive on** キーワードの使用時の結果が同一になることを前提としています。

表 2-3　フロー制御設定およびローカル/リモート ポート フロー制御解決

フロー制御設定		フロー制御解決	
ローカル デバイス	**リモート デバイス**	**ローカル デバイス**	**リモート デバイス**
send off/receive on	**send on/receive on**	受信だけ行います。	送受信を行います。
	send on/receive off	受信だけ行います。	送信だけ行います。
	send desired/receive on	受信だけ行います。	送受信を行います。
	send desired/receive off	受信だけ行います。	送信だけ行います。
	send off/receive on	受信だけ行います。	受信だけ行います。
	send off/receive off	送受信を行いません。	送受信を行いません。
send off/receive off	**send on/receive on**	送受信を行いません。	送受信を行いません。
	send on/receive off	送受信を行いません。	送受信を行いません。
	send desired/receive on	送受信を行いません。	送受信を行いません。
	send desired/receive off	送受信を行いません。	送受信を行いません。
	send off/receive on	送受信を行いません。	送受信を行いません。
	send off/receive off	送受信を行いません。	送受信を行いません。

例

次の例では、リモート ポートによってフロー制御がサポートされないようにローカル ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive off
```

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

関連コマンド

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

hw-module module logging onboard

オンボード障害ロギング（OBFL）をイネーブルにするには、**hw-module module logging onboard** グローバル コンフィギュレーション コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hw-module module [*slot-number*] **logging onboard** [**message level** *level*]

no hw-module module [*slot-number*] **logging onboard** [**message level**]

構文の説明

slot-number	（任意）スロット番号は常に 1 で、CGS 2520 には関連しません。
message level *level*	（任意）フラッシュ メモリに保存されるハードウェア関連のメッセージの重大度を指定します。指定できる範囲は 1 ～ 7 です。1 が最も高い重大度です。

デフォルト

OBFL はイネーブルになっており、すべてのメッセージが表示されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

OBFL データ ログ内のタイム スタンプを正確にするには、システム クロックを手動で設定するか、またはネットワーク タイム プロトコル（NTP）を使用して設定します。

message level *level* パラメータを入力しなければ、ハードウェア関連のすべてのメッセージがスイッチによって生成され、フラッシュ メモリに保存されます。

任意のスロット番号は常に 1 です。**hw-module module** [*slot-number*] **logging onboard** [**message level** *level*] コマンドを入力することは、**hw-module module logging onboard** [**message level** *level*] コマンドを入力することと同じです。

例

次に、スイッチ上で OBFL をイネーブルにし、ハードウェア関連のメッセージがフラッシュ メモリに保存されるように指定する例を示します。

```
Switch(config)# hw-module module logging onboard
```

次に、スイッチ上で OBFL をイネーブルにし、重大度 1 のハードウェア関連のメッセージだけがフラッシュ メモリに保存されるように指定する例を示します。

```
Switch(config)# hw-module module logging onboard message level 1
```

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

関連コマンド

コマンド	説明
clear logging onboard	フラッシュ メモリ内の OBFL データを削除します。
show logging onboard	OBFL 情報を表示します。

interface port-channel

ポート チャネルの論理インターフェイスにアクセスしたり、作成したりするには、**interface port-channel** グローバル コンフィギュレーション コマンドを使用します。ポート チャネルを削除する場合は、このコマンドの **no** 形式を使用します。

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

構文の説明

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを獲得すると、ポートチャネル インターフェイスは自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

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

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

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

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

- Cisco Discovery Protocol（CDP）を使用する場合には、これを物理ポートでだけ設定してください。ポート チャネル インターフェイスでは設定できません。

（注）　CDP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。

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

例

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

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

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

interface range

インターフェイス範囲コンフィギュレーション モードを開始し、複数のポートでコマンドを同時に実行するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス範囲を削除する場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイス範囲コンフィギュレーション モードを開始して入力した、すべてのインターフェイスのパラメータは、その範囲内のすべてのインターフェイスに対する属性になります。

VLAN については、既存の VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）でだけ **interface range** コマンドを使用することができます。VLAN の SVI を表示する場合は、**show running-config** 特権 EXEC コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用することはできません。**interface range** コマンドのもとで入力したコマンドは、この範囲のすべての既存の VLAN SVI に適用されます。

あるインターフェイス範囲に対して行われた設定変更は、すべて NVRAM に保存されますが、インターフェイス範囲自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力できます。

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

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

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

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

- **gigabitethernet** module/{*first port*} - {*last port*}　(*module は常に* ***0***)

  物理インターフェイス

  - モジュールは常に 0 です。
  - 指定できる範囲は、*type* **0**/*number* - *number* です（例：**gigabitethernet0/1 - 2**）。
- **port-channel** *port-channel-number* - *port-channel-number*（*port-channel-number* は 1 ～ 48）

（注） ポート チャネルの **interface range** コマンドを使用した場合、範囲内の最初と最後のポート チャネル番号はアクティブなポート チャネルである必要があります。

範囲を定義するときは、最初の入力とハイフン（-）の間にスペースが必要です。

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

範囲を複数定義するときでも、最初のエントリとカンマ（,）の間にスペースを入れる必要があります。

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

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

port-range では単一のインターフェイスも指定できます（この場合、**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）。

（注） インターフェイス範囲の設定の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、**interface range** コマンドを使用して、インターフェイス範囲コンフィギュレーション モードを開始し、2 つのポートにコマンドを入力する方法を示します。

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

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

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイス範囲のマクロを作成します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

interface vlan

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

interface vlan *vlan-id*

no interface vlan *vlan-id*

構文の説明

vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

（注）　VLAN 1 インターフェイスを削除することはできません。

削除した SVI は、削除したインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力することで、元に戻すことができます。インターフェイスは復元しますが、以前の設定の大半は失われます。

スイッチ上で設定された 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 使用率に影響が出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ることができます。詳細については、**sdm prefer** コマンドを参照してください。

例

次に、VLAN ID 23 を作成し、インターフェイス コンフィギュレーション モードを開始する例を示します。

```
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* 特権 EXEC コマンドを入力します。

関連コマンド

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

ip access-group

レイヤ 2 またはレイヤ 3 インターフェイスへのアクセスを制御するには、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスからすべてまたは指定のアクセス グループを削除するには、このコマンドの **no** 形式を使用します。スイッチでメトロ IP アクセス イメージが稼動している場合、レイヤ 3 インターフェイスへのアクセスを制御することもできます。

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

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

構文の説明

access-list-number	IP Access Control List（ACL; アクセス コントロール リスト）の番号です。指定できる範囲は、1 ～ 199 または 1300 ～ 2699 です。
name	**ip access-list** グローバル コンフィギュレーション コマンドで指定された IP ACL 名です。
in	入力パケットに対するフィルタリングを指定します。
out	発信パケットに対するフィルタリングを指定します。このキーワードは、レイヤ 3 のインターフェイス上に限り有効です。

デフォルト

アクセス リストは、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

スイッチでは、レイヤ 3 をサポートするため、メトロ IP アクセス イメージが稼動している必要があります。

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

- ACL は受信方向に対してだけ適用できます。**out** キーワードはレイヤ 2 のインターフェイスでサポートされていません。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC ACL だけを適用できます。
- ポート ACL はロギングをサポートしていないため、IP ACL で **log** キーワードを指定しても無視されます。

- レイヤ 2 のインターフェイスに適用された IP ACL は、IP パケットだけをフィルタにかけます。非 IP パケットをフィルタリングするには、MAC 拡張 ACL とともに **mac access-group** インターフェイス コンフィギュレーション コマンドを使用します。

ユーザは同一のスイッチ上で、ルータ ACL、入力ポート ACL、VLAN マップを使用できます。ただし、ポート ACL が常に優先されます。入力ポートの ACL と VLAN マップが両方適用されている場合、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。その他のパケットは、VLAN マップによってフィルタリングされます。

- 入力ポートの ACL がインターフェイスに適用され、さらにインターフェイスがメンバとなっている VLAN に VLAN マップが適用された場合、ACL のポート上で受信した着信パケットは、そのポート ACL でフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- 入力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- VLAN マップ、出力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

IP の ACL は、送信側または受信側のレイヤ 3 インターフェイス両方に適用できます。

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

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

標準入力アクセス リストでは、スイッチは、パケットを受信すると、パケットの送信元アドレスをアクセス リストに比較して検査します。IP 拡張アクセス リストでは、任意で、宛先 IP アドレス、プロトコル タイプ、ポート番号などのパケット内の他のフィールドを検査することができます。アクセス リストがパケットを許可する場合に、スイッチはパケットの処理を続行します。アクセス リストがパケットを拒否する場合は、スイッチはそのパケットをドロップします。アクセス リストがレイヤ 3 のインターフェイスに適用された場合、パケットのドロップにともない（デフォルト設定）、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の Host Unreachable のメッセージが生成されます。ICMP Host Unreachable メッセージは、レイヤ 2 インターフェイスでドロップされたパケットに対しては生成されません。

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

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

例

次の例では、ポートの入力パケットに IP アクセス リスト 101 を適用する方法を示します。

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

show ip interface、**show access-lists**、または **show ip access-lists** 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
access list	番号付き ACL を設定します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
ip access-list	名前付き ACL を設定します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
show access-lists	スイッチで設定された ACL を表示します。
show ip access-lists	スイッチで設定された IP ACL を表示します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
show ip interface	インターフェイスのステータスと設定に関する情報を表示します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。

ip address

レイヤ 2 スイッチの IP アドレスを設定したり、レイヤ 3 スイッチの各スイッチ仮想インターフェイス（SVI）またはルーテッド ポートの IP アドレスを設定したりするには、**ip address** インターフェイス コンフィギュレーション コマンドを使用します。IP アドレスを削除したり、IP 処理をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

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

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

（注） スイッチでメトロ IP アクセス イメージが稼動している場合にだけルーテッド ポートおよび SVI を設定できます。

構文の説明

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

デフォルト

IP アドレスは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ホストは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）Mask Request メッセージを使用して、サブネット マスクを判別できます。ルータは、この要求に対して ICMP Mask Reply メッセージで応答します。

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

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定することができます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストと ARP 要求は、IP ルーティング テーブル内のインターフェイス ルートと同様に、適切に処理されます。

（注）　ネットワーク セグメント上のすべてのルータがセカンダリのアドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。

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

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

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

例

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

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

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

関連コマンド

コマンド	説明
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

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に、スタティック IP アドレスが設定されたホストからの ARP 要求および応答を許可または拒否するには、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

arp-acl-name	ARP Access Control List（ACL; アクセス コントロール リスト）の名前
vlan-range	VLAN の番号または範囲。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
static	（任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、**static** を指定します。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。

デフォルト

VLAN には、定義された ARP ACL が適用されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ARP ACL を VLAN に適用してダイナミック ARP 検査を行う場合は、IP/MAC バインディングを含む ARP パケットだけが ACL と比較されます。ACL がパケットを許可すると、スイッチがパケットを転送します。それ以外のすべてのパケット タイプは、検証されずに、入力 VLAN 内でブリッジングされます。

スイッチが ACL 内の明示的な拒否ステートメントによってパケットを拒否すると、パケットがドロップされます。スイッチが暗黙の拒否ステートメントによってパケットを拒否すると、パケットは DHCP バインディングのリストと照合されます。ただし、ACL がスタティック（パケットがバインディングと比較されない）である場合を除きます。

ARP ACL を定義、または定義済みのリストの末尾に句を追加するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

例

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

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

設定を確認するには、**show ip arp inspection vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
permit（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection limit

インターフェイス上の着信 Address Resolution Protocol（ARP; 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、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。DoS 攻撃が発生した場合にダイナミック ARP 検査によってスイッチ リソースのすべてが消費されないようにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no ip arp inspection limit

構文の説明

rate *pps*	1 秒間に処理される着信パケット数の上限を指定します。範囲は、0 ～ 2048 pps です。
burst interval *seconds*	（任意）インターフェイスで高速 ARP パケットをモニタリングするインターバルを秒単位で指定します。範囲は 1 ～ 15 秒です。
none	処理可能な着信 ARP パケットのレートに上限を指定しません。

デフォルト

1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチド ネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。

信頼できるすべてのインターフェイスでは、レートは無制限です。

バースト インターバルは 1 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

レートは、信頼できるインターフェイスおよび信頼できないインターフェイスの両方に適用されます。複数のダイナミック ARP 検査対応 VLAN でパケットを処理するようにトランクに適切なレートを設定するか、**none** キーワードを使用してレートを無制限にします。

スイッチが、設定されているレートを超えるレートのパケットを、バーストの秒数を超える連続する秒数受信すると、インターフェイスが errdisable ステートになります。

インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートは、集約が反映されるように、より大きいレートに設定する必要があります。着信パケットのレートが、ユーザが定義したレートを超えると、スイッチはインターフェイスを errdisable ステートにします。errdisable 回復機能により、回復設定に従ってポートが errdisable ステートから自動的に解除されます。

EtherChannel ポートの着信 ARP パケットのレートは、すべてのチャネル メンバの着信 ARP パケット レートの合計と同じです。EtherChannel ポートのレート制限は、必ずすべてのチャネル メンバの着信 ARP パケットのレートを調べてから設定してください。

例

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

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

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip arp inspection 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、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

entries *number*	バッファに記録されるエントリ数。指定できる範囲は 0 ～ 1024 です。
logs *number* **interval** *seconds*	システム メッセージを生成するために、指定された間隔で必要なエントリ数 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値 0 は、エントリはログ バッファに配置されるものの、システム メッセージは生成されないことを意味します。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。値が 0 の場合、システム メッセージがただちに生成され、ログ バッファは常に空の状態です。

デフォルト

ダイナミック ARP がイネーブル化されると、拒否またはドロップされた ARP パケットが記録されます。

ログ エントリ数は、32 です。

システム メッセージ数は、1 秒あたり 5 に制限されています。

ロギングレート インターバルは、1 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

0 の値は、**logs** および **interval** キーワードの両方で許可されていません。

logs および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、X 割る Y（X/Y）のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y 割る X（Y/X）秒ごとに送信されます。たとえば、**logs** *number* が 20 で、**interval** *seconds* が 4 の場合、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

ログ バッファ エントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同一の VLAN 上のパケットを同一の ARP パラメータで多数受信すると、スイッチは、ログ バッファ内の 1 つのエントリとしてパケットを結合し、1 つのエントリとしてシステム メッセージを生成します。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリには、これ以外の統計情報が提供されません。出力にこのようなエントリが表示される場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

例

次の例では、最大 45 のエントリを保持できるようにロギング バッファを設定する方法を示します。

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

次の例では、ロギング レートを 4 秒あたり 20 のログ エントリに設定する方法を示します。この設定では、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

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

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

関連コマンド

コマンド	説明
arp access-list	ARP Access Control List（ACL; アクセス コントロール リスト）を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ バッファをクリアします。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show ip arp inspection log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

ip arp inspection trust

検査対象の着信 Address Resolution Protocol（ARP; 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、**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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

インターフェイスは、信頼できない状態です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチは、信頼できるインターフェイス上で受信した ARP パケットを確認せず、単純にパケットを転送します。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。

例

次の例では、ポートを信頼できる状態に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
show ip arp inspection 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 ip arp inspection log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

ip arp inspection validate

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査の特定のチェックを実行するには、**ip arp inspection validate** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip [allow zeros]**]

構文の説明

src-mac	イーサネット ヘッダー内の送信元 MAC アドレスと、ARP 本体内の送信側 MAC アドレスを比較します。このチェックは、ARP 要求と応答の両方に対して行われます。 このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。
dst-mac	イーサネット ヘッダー内の宛先 MAC アドレスと、ARP 本体内のターゲット MAC アドレスを比較します。このチェックは、ARP 応答に対して行われます。 このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。
ip	ARP 本体内で、無効な予期しない IP アドレスを比較します。このようなアドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信側 IP アドレスは、すべての ARP 要求および応答と比較されます。ターゲット IP アドレスは ARP 応答でだけチェックされます。
allow-zeros	送信側アドレスが 0.0.0.0（ARP プローブ）である ARP が拒否されないように、IP 検証テストを変更します。

デフォルト

チェックは行われません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが **src-mac** および **dst-mac** の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって **src-mac** および **dst-mac** の検証がディセーブルになります。

allow-zeros キーワードは、次の方法で ARP Access Control List（ACL; アクセス コントロール リスト）と連動します。

- ARP ACL が ARP プローブを拒否するように設定されている場合は、**allow-zero** キーワードが指定されていても、ARP プローブはドロップされます。

- ARP プローブを明確に許可する ARP ACL を設定し、**ip arp inspection validate ip** コマンドを設定する場合、**allow-zeros** キーワードを入力しない限り、ARP プローブはドロップされます。

このコマンドの **no** 形式を使用すると、指定されたチェックだけがディセーブルになります。どのオプションもイネーブルにしない場合は、すべてのチェックがディセーブルになります。

例

次の例では、送信元 MAC の検証をイネーブルにする方法を示します。

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

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

関連コマンド

コマンド	説明
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection vlan

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

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

構文の説明

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ダイナミック ARP 検査は、アクセス ポート、トランク ポート、EtherChannel ポートおよびプライベート VLAN ポートでサポートされます。

例

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

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

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

関連コマンド

コマンド	説明
arp access-list	ARP Access Control List（ACL; アクセス コントロール リスト）を定義します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection vlan logging

VLAN 単位でロギングされるパケットのタイプを制御するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。このロギング制御をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

vlan-range	ロギングに対して設定された VLAN を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
acl-match {**matchlog** | **none**}	Access Control List（ACL; アクセス コントロール リスト）との一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **matchlog**：Access Control Entry（ACE; アクセス コントロール エントリ）に指定されたロギング設定に基づいてパケットを記録します。このコマンドに **matchlog** キーワード、**permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットが記録されます。 • **none**：ACL に一致するパケットを記録しません。
dhcp-bindings {**permit** | **all** | **none**}	Dynamic Host Configuration Protocol（DHCP）バインディングとの一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **all**：DHCP バインディングに一致するすべてのパケットを記録します。 • **none**：DHCP バインディングに一致するパケットを記録しません。 • **permit**：DHCP バインディングに許可されたパケットを記録します。
arp-probe	具体的に許可されたパケットが ARP プローブである場合に、パケットのロギングを指定します。

デフォルト

拒否またはドロップされたパケットは、すべて記録されます。ARP プローブ パケットは記録されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

acl-match キーワードと **dhcp-bindings** キーワードは連携しています。ACL の一致を設定すると、DHCP バインディングの設定はディセーブルになりません。ロギング基準をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。いずれのオプションも指定しない場合は、ARP パケットが拒否されたときに、すべてのロギング タイプが記録されるようにリセットされます。使用できるオプションは、次の 2 つです。

- **acl-match**：拒否されたパケットが記録されるように、ACL との一致に関するロギングがリセットされます。
- **dhcp-bindings**：拒否されたパケットが記録されるように、DHCP バインディングとの一致に関するロギングがリセットされます。

acl-match キーワードと **dhcp-bindings** キーワードのどちらも指定されないと、拒否されたすべてのパケットが記録されます。

ACL の末尾にある暗黙の拒否には、**log** キーワードが含まれません。つまり、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドで **static** キーワードを使用した場合、ACL は DHCP バインディングを上書きします。ARP ACL の末尾で明示的に **deny ip any mac any log** ACE を指定しない限り、拒否された一部のパケットが記録されない場合があります。

例

次の例では、ACL 内の **permit** コマンドと一致するパケットを記録するように、VLAN 1 の ARP 検査を設定する方法を示します。

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

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

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
show ip arp inspection log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。
show ip arp inspection vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip device tracking maximum

レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにするには、**ip device tracking maximum** コマンドを使用します。信頼できないレイヤ 2 インターフェイスで IP ポート セキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking maximum {*number*}

no ip device tracking maximum {*number*}

構文の説明

number	ポートの IP デバイス トラッキング テーブルに作成するバインディングの数を指定します。有効値の範囲は 0 ～ 2048 です。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティ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)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

関連コマンド

コマンド	説明
ip verify source	信頼できないレイヤ 2 インターフェイスで IP ソース ガードをイネーブルにします。
show ip verify source	特定のインターフェイス上の IP ソース ガード設定とフィルタを表示します。

ip dhcp snooping

DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping

no ip dhcp snooping

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピングは、ディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ip dhcp snooping vlan *vlan-id* グローバル コンフィギュレーション コマンドを使用して VLAN 上でスヌーピングをイネーブルにするまで DHCP スヌーピングはアクティブになりません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

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

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

関連コマンド

コマンド	説明
ip dhcp snooping vlan	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping binding

DHCP スヌーピング バインディング データベースを設定して、バインディング エントリをデータベースに追加するには、**ip dhcp snooping binding** 特権 EXEC コマンドを使用します。バインディング データベースからエントリを削除するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 4904 です。
ip-address	IP アドレスを指定します。
interface *interface-id*	バインディング エントリを追加または削除するインターフェイスを指定します。
expiry *seconds*	バインディング エントリが無効になるまでのインターバル（秒）を指定します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

デフォルトのデータベースは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP スヌーピング バインディング データベースでは、各データベース エントリ（別名、バインディング）には、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進数）、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、8192 のバインディングを含めることができます。

ダイナミックに設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。動的および静的に設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポートに、有効期限が 1000 秒の DHCP バインディング設定を生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1 expiry 1000
```

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

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングおよび設定情報を表示します。
show ip source binding	DHCP スヌーピング バインディング データベース内の動的および静的に設定されたバインディングを表示します。

ip dhcp snooping database

DHCP スヌーピング バインディング データベース エージェントを設定するには、**ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。エージェントのディセーブル化、タイムアウト値のリセット、または書き込み遅延値のリセットを行うには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

flash:/*filename*	データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。
ftp://*user*:*password*@*host*/*filename*	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
http://*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar**	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
rcp://*user@host/filename*	データベース エージェントまたはバインディング ファイルが Remote Copy Protocol（RCP; リモート コピー プロトコル）サーバにあることを指定します。
tftp://*host/filename*	データベース エージェントまたはバインディング ファイルが TFTP サーバにあることを指定します。
timeout *seconds*	DHCP スヌーピングのバインディング データベースが変更されたあとのデータベース転送プロセスを停止する時間（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。無期限を定義するには 0 を使用します。
write-delay *seconds*	バインディング データベースが変更された後に、転送を遅らせる期間（秒）を指定します。デフォルト値は 300 秒です。指定できる範囲は 15 ～ 86400 です。

デフォルト

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

タイムアウト値は、300 秒（5 分）です。

書き込み遅延値は、300 秒（5 分）です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング バインディング データベースには、8192 のバインディングを含めることができます。

データベース内のリース時間を正確な時間にするには、Network Time Protocol（NTP; ネットワーク タイム プロトコル）をイネーブルにし、次の機能を設定することを強く推奨します。

- NTP 認証
- NTP ピアおよびサーバ アソシエーション
- NTP ブロードキャスト サービス
- NTP アクセス制限
- NTP パケット送信元 IP アドレス

NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。

NVRAM とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを TFTP サーバ上に保存することを推奨します。スイッチがネットワークベースの URL（TFTP や FTP など）の設定済み URL 内のバインディング ファイルにバインディングを初めて書き込む前に、この URL に空のファイルを作成しておく必要があります。

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

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

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

例

次の例では、IP アドレス 10.1.1.1 の *directory* という名前のディレクトリ内にバインディング ファイルを保存する方法を示します。TFTP サーバに *file* という名前のファイルが存在しなければなりません。

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

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

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping information option

DHCP オプション 82 データ挿入をイネーブルにするには、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。DHCP オプション 82 データ挿入をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option

no ip dhcp snooping information option

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP オプション 82 データ挿入はイネーブルです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

オプション 82 機能がイネーブルの場合、スイッチがホストからの DHCP 要求を受信すると、オプション 82 情報がパケットに追加されます。オプション 82 情報には、スイッチ MAC アドレス（リモート ID サブオプション）、およびパケットが受信された **vlan-mod-port**（回線 ID サブオプション）のポート ID が含まれます。スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

DHCP サーバがパケットを受信する場合、リモート ID、回線 ID、または両方を使用して IP アドレスを割り当てるとともに、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数の制限などのポリシーを適用することができます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。

スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同一サブネットにある場合、サーバは応答をブロードキャストします。スイッチは、リモート ID または回線 ID フィールドを検査し、オプション 82 データが最初から挿入されていたかを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP ホストに接続するスイッチ ポートにパケットを転送します。

例

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

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

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

関連コマンド

コマンド	説明
show ip dhcp 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 allowed-untrusted

エッジ スイッチに接続されている信頼できないポートで受信するか、オプション 82 情報を持つ DHCP パケットを受け入れるようにアグリゲーション スイッチを設定するには、アグリゲーション スイッチで **ip dhcp snooping information option allowed-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。スイッチがエッジ スイッチからのこれらのパケットをドロップするよう設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、エッジ スイッチに接続されている信頼できないポートで受信する、オプション 82 情報を持つ DHCP パケットをドロップします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ホストに接続されたエッジ スイッチが、ネットワークのエッジで DHCP オプション 82 情報を挿入するように設定したい場合があります。また集約スイッチでは、DHCP スヌーピング、IP ソース ガード、またはダイナミック Address Resolution 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こともできます。ただし、アグリゲーション スイッチで DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないポートで受信されたオプション 82 情報を持つパケットをドロップし、信頼できるインターフェイスに接続されたデバイスの DHCP スヌーピング バインディングを学習しません。

ホストに接続されたエッジ スイッチがオプション 82 情報を挿入する場合に、アグリゲーション スイッチで DHCP スヌーピングを使用するには、アグリゲーション スイッチで **ip dhcp snooping information option allowed-untrusted** コマンドを入力します。アグリゲーション スイッチは信頼できないポートで DHCP スヌーピング パケットを受信しますが、ホストのバインディングを学習できます。アグリゲーション スイッチで DHCP セキュリティ機能をイネーブルにすることも可能です。アグリゲーション スイッチが接続されているエッジ スイッチ上のポートは、信頼できるポートとして設定する必要があります。

（注）　**ip dhcp snooping information option allowed-untrusted** コマンドを、信頼できないデバイスが接続されている集約スイッチに入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

例

次の例では、アクセス スイッチが、エッジ スイッチからの信頼できないパケットのオプション 82 情報を確認せずに、パケットを受け入れるように設定する方法を示します。

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

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

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping information option format remote-id

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

ip dhcp snooping information option format remote-id [**string** *ASCII-string* | **hostname**]

no ip dhcp snooping information option format remote-id

構文の説明

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

デフォルト

スイッチの MAC アドレスは、リモート ID です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping vlan information option format-type circuit-id string	オプション 82 サーキット ID サブオプションを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping limit rate

インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数を設定するには、**ip dhcp snooping limit rate** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

構文の説明

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

デフォルト

DHCP スヌーピング レート制限は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

通常、レート制限は信頼できないインターフェイスに適用されます。信頼できるインターフェイスのレート制限を設定する場合、信頼できるインターフェイスはスイッチ内の複数の VLAN 上（一部はスヌーピングされない場合があります）の DHCP トラフィックを集約するので、インターフェイス レート制限を高い値に調整する必要があることに注意してください。

レート制限を超えた場合、インターフェイスが errdisable になります。**errdisable recovery dhcp-rate-limit** グローバル コンフィギュレーション コマンドを入力してエラー回復をイネーブルにした場合、インターフェイスはすべての原因が時間切れになった際に動作を再試行します。エラー回復メカニズムがイネーブルでない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するまでインターフェイスは errdisable ステートのままです。

例

次の例は、インターフェイス上でメッセージ レート制限を 1 秒あたり 150 メッセージに設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

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

関連コマンド

コマンド	説明
errdisable recovery	回復メカニズムを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping trust

DHCP スヌーピングを実行するためにポートを信頼できるポートとして設定するには、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp snooping trust

no ip dhcp snooping trust

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピング信頼は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

DHCP サーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCP クライアントに接続されたポートを信頼できないポートとして設定します。

例

次の例では、ポート上で DHCP スヌーピング信頼をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

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

関連コマンド

コマンド	説明
show ip dhcp 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 mac-address

信頼性のないポート上で DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスと一致することを確認す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 **ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドを使用します。スイッチが MAC アドレスを確認しないように設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

サービスプロバイダー ネットワークで、スイッチが信頼できないポートの DHCP クライアントからパケットを受信した場合、スイッチは自動的に送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致するかを確認します。アドレスが一致する場合、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

例

次の例では、MAC アドレス確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

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

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

DHCP スヌーピングを VLAN 上でイネーブルにするには、**ip dhcp snooping vlan** グローバル コンフィギュレーション コマンドを使用します。DHCP スヌーピングを VLAN 上でディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

構文の説明

vlan *vlan-range*	DHCP スヌーピングをイネーブルにする VLAN ID または VLAN 範囲を指定します。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。

デフォルト

すべての VLAN 上で DHCP スヌーピングがディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

VLAN 上で DHCP スヌーピングをイネーブルにする前に、まず DHCP スヌーピングをグローバルにイネーブルにする必要があります。

例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

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

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping vlan information option format-type circuit-id string

オプション 82 回線 ID サブオプションを設定するには、**ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトのサーキット ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*

no ip dhcp snooping vlan *vlan* **information option format-type circuit-id** [**override**] **string**

構文の説明

vlan *vlan*	VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
override	（任意）3 ～ 63 の ASCII 文字（スペースなし）を使用して、上書き文字列を指定します。
string *ASCII-string*	3 ～ 63 の ASCII 文字（スペースなし）を使用して、サーキット ID を指定します。

デフォルト

vlan-mod-port 形式のスイッチ VLAN およびポート ID は、デフォルトのサーキット ID です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

オプション 82 機能がイネーブルの場合、デフォルトのサーキット ID サブオプションは、**vlan-mod-port** 形式のスイッチ VLAN およびポート ID です。このコマンドを使用すると、サーキット ID となる ASCII 文字列を設定できます。**vlan-mod-port** フォーマット タイプを無効にし、その代わりにサーキット ID を使用して、加入者情報を定義する場合、**override** キーワードを使用します。

（注） スイッチ上で文字数の多いサーキット ID を設定する場合、NVRAM またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。

例

次の例では、オプション 82 サーキット ID サブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

次の例では、オプション 82 サーキット ID 上書きサブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

（注）　**show ip dhcp snooping ユーザ EXEC** コマンドでは、リモート ID 設定を含むグローバル コマンド出力だけが表示されます。サーキット ID として設定したインターフェイス単位または VLAN 単位の文字列は表示されません。

関連コマンド

コマンド	説明
ip dhcp snooping information option format remote-id	オプション 82 リモート ID サブオプションを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip igmp filter

インターフェイスにインターネット グループ管理プロトコル（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、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*

no ip igmp filter

構文の説明

profile number	適用する 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

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 物理インターフェイスにだけ IGMP フィルタを適用できます。

ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、または EtherChannel グループに属するポートに対しては IGMP フィルタを適用できません。

IGMP のプロファイルは 1 つまたは複数のポート インターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

例

次の例では、IGMP プロファイル 22 をポートに適用する方法を示します。

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

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
ip igmp profile	指定された IGMP プロファイル番号を設定します。
show ip dhcp snooping statistics	指定された IGMP プロファイルの特性を表示します。
show running-config interface *interface-id*	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、『**Cisco IOS 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インターネット グループ管理プロトコル（IGMP）グループの最大数を設定したり、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、**ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリング アクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

number	インターフェイスが参加できる IGMP グループの最大数。指定できる範囲は 0 ～ 4294967294 です。デフォルトの設定に制限はありません。
action deny	エントリの最大数が IGMP スヌーピング転送テーブルにある場合は、次の IGMP 加入レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが ICMP スヌーピング転送テーブルにある場合、IGMP レポートを受信した既存のグループを新しいグループに置き換えます。

デフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループ エントリの最大数があることをスイッチが学習した後の、デフォルトのスロットリング アクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。

ルーテッド ポート、Switch Virtual Interface（SVI; 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 IGMP 最大グループ数を設定することはできません。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- スロットリング アクションを **deny** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートをスイッチがドロップします。

- スロットリング アクションを **replace** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したマルチキャスト エントリを受信した IGMP レポートと置き換えます。
- 最大グループ制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups** {**deny** | **replace**} コマンドを入力しても無効です。

例

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

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

次の例では、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるように設定する方法を示します。

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

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
show running-config interface *interface-id*	インターフェイスが参加できる IGMP グループの最大数やスロットリング アクションなど、スイッチのインターフェイス上で実行コンフィギュレーションを表示します。構文情報については、『**Cisco IOS Configuration Fundamentals Command Reference, Release 12.2**』>「**File Management Commands**」>「**Configuration File Management Commands**」を選択してください。

ip igmp profile

インターネット グループ管理プロトコル（IGMP）プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始するには、**ip igmp profile** グローバル コンフィギュレーション コマンドを使用します。このモードで、スイッチポートからの IGMP メンバシップ レポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*

no ip igmp profile *profile number*

構文の説明

profile number	設定する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否します（デフォルト設定の状態）。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にする、またはデフォルトにリセットします。
- **permit**：一致するアドレスを許可します。
- **range**：プロファイルに対する IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

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

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

関連コマンド

コマンド	説明
ip igmp filter	指定のインターフェイスに対し、IGMP を適用します。
show ip dhcp snooping statistics	すべての IGMP プロファイルまたは指定の IGMP プロファイル番号の特性を表示します。

ip igmp snooping

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングをスイッチ上でグローバルにイネーブル、または VLAN ごとにイネーブルにするには、**ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

構文の説明

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

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

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1
```

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

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip 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 detail	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping last-member-query-interval

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）の設定可能な Leave タイマーをグローバルにまたは VLAN ベースごとにイネーブルにするには、**ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [vlan *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [vlan *vlan-id*] **last-member-query-interval**

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび Leave タイマーをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
time	秒単位のタイムアウト間隔。指定できる範囲は 100 ～ 32768 ミリ秒です。

デフォルト

デフォルトのタイムアウト設定は 1000 ミリ秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN 上に Leave タイマーを設定すると、グローバル設定を上書きします。

IGMP 設定可能な Leave タイムは、IGMP バージョン 2 を実行するデバイスでだけサポートされます。

設定は、NVRAM に保存されます。

例

次の例では、IGMP Leave タイマーを 2000 ミリ秒でグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

次の例では、VLAN 1 上で IGMP Leave タイマーを 3000 ミリ秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

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

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan immediate-leave	IGMP 即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをグループのメンバとして設定します。
show ip igmp snooping	IGMP スヌーピング設定を表示します。

ip igmp snooping querier

レイヤ 2 ネットワークの Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** グローバル コンフィギュレーション コマンドを使用します。キーワードとともにコマンドを入力すると、VLAN インターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping querier [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

no ip igmp snooping querier [**vlan** *vlan-id*] [**address** | **max-response-time** | **query-interval** | **tcn query** { **count** *count* | **interval** *interval*} | **timer expiry** | **version**]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
address *ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time *response-time*	（任意）IGMP クエリア レポートを待機する最長時間を設定します。指定できる範囲は 1 ～ 25 秒です。
query-interval *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
tcn query [count *count* | **interval** *interval*]	（任意）Topology Change Notification（TCN; トポロジ変更通知）に関連するパラメータを設定します。キーワードの意味は次のとおりです。 • **count** *count* : TCN 時間間隔に実行される TCN クエリーの数を設定します。指定できる範囲は 1 ～ 10 です。 • **interval** *interval* : TCN クエリーの時間間隔を設定します。指定できる範囲は 1 ～ 255 です。
timer expiry	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
version *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

デフォルト

IGMP スヌーピング クエリア機能は、スイッチでグローバルにイネーブルです。

イネーブルになっている場合、マルチキャスト対応デバイスから IGMP トラフィックを検出すると、IGMP スヌーピング クエリアはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリー メッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピング クエリアは、IGMP *バージョン 2*（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP *バージョン 1*（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time** 値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、**max-response-time** を設定できません （値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリー メッセージを拒否することがあります。デバイスで IGMP 一般クエリー メッセージを受け入れる場合、IGMP スヌーピング クエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピング クエリア機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピング クエリアの時間間隔を 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピング クエリアの TCN クエリー カウントを 25 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier version 2
```

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

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。

ip igmp snooping report-suppression

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）レポート抑制をイネーブルにするには、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャスト ルータへ転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャスト ルータに送信されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
Switch(config)# no ip igmp snooping report-suppression
```

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

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）Topology Change Notification（TCN; トポロジ変更通知）の動作を設定するには、**ip igmp snooping tcn** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping tcn {**flood query count** *count* | **query solicit**}

no ip igmp snooping tcn {**flood query count** | **query solicit**}

構文の説明

flood query count *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。
query solicit	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。

デフォルト

TCN フラッド クエリー カウントは 2 です。

TCN クエリー要求はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用することにより、トポロジの変更によって発生する可能性のあるマルチキャスト トラフィックの損失を防ぐことができます。**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッディング クエリー数を 1 に設定した場合、フラッディングは一般クエリーを 1 つ受信した時点で停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャスト トラフィックのフラッディングは、7 つの一般的クエリーを受信するまで継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

例

次の例では、マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を 7 に指定する方法を示します。

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

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

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn flood	インターフェイスのフラッディングを IGMP スヌーピング スパニング ツリー TCN 動作として指定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn flood

マルチキャスト フラッディングを Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング スパニングツリー Topology Change Notification（TCN; トポロジ変更通知）の動作として設定するには、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。マルチキャスト フラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

マルチキャスト フラッディングは、スパニング ツリー TCN のイベント中、インターフェイス上でイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチが TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングします。異なるマルチキャスト グループのホストに接続しているポートが複数ある場合、フラッディング トラフィックがリンクの容量を超え、パケット損失が発生する場合があるため、このフラッディング動作は適切でない可能性があります。

ip igmp snooping tcn flood query count *count* グローバル コンフィギュレーション コマンドを使用して、フラッディング クエリー カウントを変更できます。

例

次の例では、インターフェイス上でマルチキャスト フラッディングをディセーブルにする方法を示します。

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

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

関連コマンド

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

ip igmp snooping vlan immediate-leave

VLAN ごとにインターネット グループ管理プロトコル（IGMP）スヌーピング即時脱退処理をイネーブルにするには、**ip igmp snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

構文の説明

vlan-id	指定された VLAN で IGMP スヌーピングおよび即時脱退機能をイネーブルにします。指定できる範囲は 1 ～ 1001 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN の各ポート上で最大 1 つのレシーバが設定されている場合に限り、即時脱退処理の機能を設定してください。設定は、NVRAM に保存されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

例

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

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

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

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier detail	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan mrouter

マルチキャスト ルータ ポートを追加したり、マルチキャスト学習方式を設定したりするには、**ip igmp snooping vlan** *vlan-id* **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 pim-dvmrp**}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

構文の説明

vlan-id	IGMP スヌーピングをイネーブルにして、指定した VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
interface *interface-id*	ネクストホップ インターフェイスをマルチキャスト ルータに指定します。有効なインターフェイスは、物理インターフェイスおよびポート チャネルです。ポート チャネル範囲は 1 ～ 48 です。
learn pim-dvmrp	マルチキャスト ルータの学習方式を指定します。Cisco CGS 2520 スイッチでサポートされている学習方式は、IGMP クエリーおよびプロトコル独立型マルチキャスト ディスタンス ベクトル マルチキャスト ルーティング プロトコル（PIM-DVMRP）パケットのスヌーピングによってマルチキャスト ルータ ポートを学習するようにスイッチを設定する **pim-dvmrp** です。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM に保存されます。

例

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

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

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier detail	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan static

インターネット グループ管理プロトコル（IGMP）スヌーピングをイネーブルにし、レイヤ 2 ポートをマルチキャスト グループのメンバとしてスタティックに追加するには、**ip igmp snooping vlan** *vlan-id* **static** グローバル コンフィギュレーション コマンドを使用します。スタティックなマルチキャスト グループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	指定した VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
ip-address	指定のグループ IP アドレスを持ったマルチキャスト グループのメンバとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバ ポートのインターフェイスを指定します。キーワードの意味は次のとおりです。 • **fastethernet** *interface number*：ファスト イーサネット IEEE 802.3 インターフェイス • **gigabitethernet** *interface number*：ギガビット イーサネット IEEE 802.3z インターフェイス • **port-channel** *interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM 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 mrouter interface gigabitethernet0/2
```

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

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	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 detail	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip sla responder twamp

Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）レスポンダとしてスイッチを設定するには、**ip sla responder twamp** グローバル コンフィギュレーション コマンドを使用します。IP SLA TWAMP レスポンダ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 sla responder twamp [**timeout** *seconds*]

no ip sla responder twamp [**timeout** *seconds*]

構文の説明

timeout *seconds*	（任意）このセッションが非アクティブになってから TWAMP セッションを終了するまでの秒数を指定します。指定できる範囲は 1 ～ 604800 秒です。デフォルトは、900 秒です。

デフォルト

IP SLA TWAMP レスポンダ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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ip sla responder twamp コマンドを入力すると、IP SLA TWAMP リフレクタ 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**：コマンドをそのデフォルトに設定します。
- **exit**：IP SLA TWAMP リフレクタ 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。
- **timeout** *seconds*：セッションが非アクティブの場合に終了されるまでの最大時間を指定します。指定できる範囲は 1 ～ 604800 秒です。デフォルトは、900 秒です。

TWAMP サーバとリフレクタが機能するには、TWAMP 制御デバイスも設定する必要があります。制御デバイスはクライアントおよびセッション送信元として機能します。これらの機能は、シスコ デバイスでは設定されません。

例

次に、スイッチを IP SLA TWAMP レスポンダとして設定する例を示します。

```
Switch(config)# ip sla responder twamp
Switch(config-twamp-ref)# timeout inactivity 900
```

関連コマンド

コマンド	説明
ip sla responder	一般的な IP SLA 運用に対して Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）レスポンダをイネーブルにします。
ip sla server twamp	双方向アクティブ測定プロトコル（TWAMP）サーバとしてスイッチを設定します。
show ip sla standards	（任意）スイッチに設定されている IP SLA 標準を表示します。
show ip sla twamp connection {**detail** | **requests**}	（任意）現在の Cisco IOS IP Service Level Agreements（SLA; サービス レベル契約）の Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）接続を表示します。

ip sla server twamp

双方向アクティブ測定プロトコル（TWAMP）サーバとしてスイッチを設定するには、**ip sla server twamp** グローバル コンフィギュレーション コマンドを使用します。IP SLA TWAMP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip sla server twamp

no ip sla server twamp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IP SLA TWAMP サーバ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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ip sla server twamp コマンドを入力すると、IP SLA TWAMP サーバ 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**：コマンドをそのデフォルトに設定します。
- **exit**：IP SLA TWAMP サーバ 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。
- **port** *port-number*：TWAMP 制御トラフィックの送信元ポートを指定します。有効なポート番号は 1 ～ 65535 です。
- **timer inactivity** *seconds*：セッションが非アクティブの場合に終了されるまでの最大時間を指定します。指定できる範囲は 1 ～ 6000 秒です。デフォルト値は 900 秒です。

TWAMP サーバとリフレクタが機能するには、TWAMP 制御デバイスも設定する必要があります。制御デバイスはクライアントおよびセッション送信元として機能します。これらの機能は、シスコ デバイスでは設定されません。

例

次に、スイッチを IP SLA TWAMP サーバとして設定する例を示します。

```
Switch(config)# ip sla server twamp
Switch(config-twamp-srvr)# port 862
Switch(config-twamp-srvr)# timer inactivity 540
```

関連コマンド

コマンド	説明
ip sla responder	一般的な IP SLA 運用に対して Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）レスポンダをイネーブルにします。
ip sla responder twamp	Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）レスポンダとしてスイッチを設定します。
show ip sla standards	（任意）スイッチに設定されている IP SLA 標準を表示します。
show ip sla twamp connection {**detail** | **requests**}	（任意）現在の Cisco IOS IP Service Level Agreements（SLA; サービス レベル契約）の Two-Way Active Measurement Protocol（TWAMP; 双方向アクティブ測定プロトコル）接続を表示します。

ip source binding

スイッチ上のスタティックな IP 送信元バインディングを設定するには、**ip source binding** グローバル コンフィギュレーション コマンドを使用します。スタティック バインディングを削除するには、このコマンドの **no** 形式を使用します。

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

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

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 4094 です。
ip-address	IP アドレスを指定します。
interface *interface-id*	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スタティック IP 送信元バインディング エントリには、IP アドレス、関連付けられた MAC アドレス、および関連付けられた VLAN 番号が含まれます。エントリは、MAC アドレスおよび VLAN 番号に基づいています。IP アドレスだけの変更でエントリを変更する場合は、スイッチは新しいエントリを作成せずに、エントリを更新します。

例

次の例では、スタティック IP 送信元バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1
```

次の例では、スタティック バインディングを追加してから、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet0/1
```

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

関連コマンド

コマンド	説明
ip verify source	インターフェイス上の IP 送信元ガードをイネーブルにします。
show ip source binding	スイッチ上の IP 送信元バインディングを表示します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ip ssh

Secure Shell（SSH; セキュア シェル）version 1（SSHv1）または SSH version 2（SSHv2）を実行するようにスイッチを設定するには、**ip ssh** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、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**]

このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

構文の説明

1	（任意）スイッチが SSHv1 を実行するように設定します。
2	（任意）スイッチが SSH バージョン 2（SSHv1）を実行するように設定します。

デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力しない場合、またはキーワードを指定しないときは、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。また、SSHv1 クライアントもサポートします。SSH サーバおよび SSH クライアントの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

SSHv1 サーバによって生成された Rivest、Shamir、Adelman（RSA）キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。

例

次の例では、スイッチが SSH バージョン 2 を実行するように設定する方法を示します。

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

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

関連コマンド

コマンド	説明
show ip ssh	SSH サーバがイネーブルであるかどうかを表示すると同時に、SSH サーバのバージョンおよび設定情報を表示します。構文情報については、「**Cisco IOS Release 12.2 Configuration Guides and Command References**」>『**Cisco IOS Security Command Reference, Release 12.2**』>「**Other Security Features**」>「**Secure Shell Commands**」を選択してください。
show ssh	SSH サーバのステータスを表示します。構文情報については、「**Cisco IOS Release 12.2 Configuration Guides and Command References**」>『**Cisco IOS Security Command Reference, Release 12.2**』>「**Other Security Features**」>「**Secure Shell Commands**」を選択してください。

ip sticky-arp（グローバル コンフィギュレーション）

プライベート VLAN に属する Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上で sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにするには、**ip sticky-arp** グローバル コンフィギュレーション コマンドを使用します。sticky ARP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip sticky-arp

no ip sticky-arp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

sticky ARP はイネーブル化されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

sticky ARP エントリとは、プライベート VLAN SVI によって学習されるエントリです。これらのエントリは、期限切れになることはありません。

ip sticky-arp グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。

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

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

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

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

- スイッチをデバイスから取り外し、MAC アドレスは異なるが IP アドレスが同じである別のデバイスに接続する場合、ARP エントリは作成されず、次のメッセージが表示されます。

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* グローバル コンフィギュレーション コマンドを使用して、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。

- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP をディセーブルにするには、**no sticky-arp** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP がディセーブルのときに、インターフェイス上で sticky ARP をディセーブルにするには、**no sticky-arp** インターフェイス コンフィギュレーション コマンドを使用します。

例

sticky ARP をディセーブルにする方法：

```
Switch(config)# no ip sticky-arp
```

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

関連コマンド

コマンド	説明
arp	ARP テーブルに永続的エントリを追加します。構文情報については、『**Cisco IOS IP Addressing Services Command Reference, Release 12.4**』>「**ARP Commands**」を参照してください。
show arp	ARP テーブル内のエントリを表示します。構文情報については、『**Cisco IOS IP Addressing Services Command Reference, Release 12.4**』>「**ARP Commands**」を参照してください。

ip sticky-arp（インターフェイス コンフィギュレーション）

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）またはレイヤ 3 インターフェイス上で sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにするには、**ip sticky-arp** インターフェイス コンフィギュレーション コマンドを使用します。sticky ARP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip sticky-arp

no ip sticky-arp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

sticky ARP は、レイヤ 3 インターフェイスおよび標準 SVI 上でディセーブルになります。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。

ip sticky-arp インターフェイス コンフィギュレーション コマンドは、次の上でだけサポートされます。

- レイヤ 3 インターフェイス
- 標準 VLAN に属する SVI
- プライベート VLAN に属する SVI

レイヤ 3 インターフェイスまたは標準 VLAN に属する SVI 上で

- sticky ARP をイネーブルにするには、**sticky-arp** インターフェイス コンフィギュレーション コマンドを使用します。
- sticky ARP をディセーブルにするには、**no sticky-arp** インターフェイス コンフィギュレーション コマンドを使用します。

プライベート VLAN SVI 上で

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

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

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

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

- スイッチをデバイスから取り外し、MAC アドレスは異なるが IP アドレスが同じである別のデバイスに接続する場合、ARP エントリは作成されず、次のメッセージが表示されます。

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* グローバル コンフィギュレーション コマンドを使用して、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。
- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP をディセーブルにするには、**no sticky-arp** グローバル コンフィギュレーション コマンドを使用します。
- インターフェイス上で sticky ARP をディセーブルにするには、**no sticky-arp** インターフェイス コンフィギュレーション コマンドを使用します。

例

標準 SVI 上で sticky ARP をイネーブルにする方法：

```
Switch(config-if)# ip sticky-arp
```

レイヤ 3 インターフェイスまたは SVI 上で sticky ARP をディセーブルにする方法：

```
Switch(config-if)# no ip sticky-arp
```

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

関連コマンド

コマンド	説明
arp	ARP テーブルに永続的エントリを追加します。構文情報については、『**Cisco IOS IP Addressing Services Command Reference, Release 12.4**』>「**ARP Commands**」を参照してください。
show arp	ARP テーブル内のエントリを表示します。構文情報については、『**Cisco IOS IP Addressing Services Command Reference, Release 12.4**』>「**ARP Commands**」を参照してください。

ip verify source

インターフェイスで IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source {**vlan dhcp-snooping** | **tracking**} [**port-security**]

no ip verify source {**vlan dhcp-snooping** | **tracking**} [**port-security**]

構文の説明

vlan dhcp-snooping	信頼できないレイヤ 2 DHCP スヌーピング インターフェイスで IP ソース ガードをイネーブルにします。
tracking	ポートで固定 IP アドレス ラーニングを学習するために IP ポート セキュリティをイネーブルにします。
port-security	（任意）IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 **port-security** のキーワードを入力しない場合、IP アドレス フィルタリングがイネーブルになります。

デフォルト

IP 送信元ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスのポート セキュリティをイネーブルにする必要があります。

例

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

```
Switch(config-if)# ip verify source
```

次の例では、ポート単位で VLAN 10 ～ 20 で IP ソース ガード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)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
```

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface gigabitethernet0/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Gi0/1      ip-mac       active       10.0.0.1                            10
Gi0/1      ip-mac       active       deny-all                            11-20
Switch#
```

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティ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)# ip device tracking
Switch(config)# interface gigabitEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

関連コマンド

コマンド	説明
ip device tracking maximum	レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにします。
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping limit rate	インターフェイスが 1 秒間に受信できる DHCP メッセージの数を設定します。
ip dhcp snooping information option	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN で DHCP スヌーピングをイネーブルにします。
ip source binding	スイッチにスタティック バインディングを設定します。
show ip 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 エントリを表示します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ipv6 access-list

IPv6 アクセス リストを定義し、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにするには、**ipv6 access-list** グローバル コンフィギュレーション コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

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

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

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

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

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

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

IPv6 ACL を IPv6 インターフェイスに適用するには、**access-list-name** 引数を指定して *ipv6 traffic-filter* インターフェイス コンフィギュレーション コマンドを使用します。着信および発信 IPv6 ACL をレイヤ 3 物理インターフェイス、またはルーテッド ACL の Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に適用することはできますが、ポート ACL のレイヤ 2 インターフェイスに適用できるのは着信 IPv6 ACL だけです。

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

例

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

```
Switch(config)# ipv6 access-list list2
Switch(config-ipv6-acl)# deny FE80:0:0:2::/64 any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter list2 out
```

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

関連コマンド

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

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイスの IPv6 アドレスを取得するには、**ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address dhcp [**rapid-commit**]

no ipv6 address dhcp [**rapid-commit**]

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

rapid-commit	（任意）アドレス割り当てに 2 つのメッセージ交換方式を許可します。

デフォルト

デフォルトは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ipv6 address dhcp インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP を使用して IPv6 アドレスを動的に学習できます。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。これをイネーブルにすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

設定を確認するには、**show ipv6 dhcp interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ipv6 dhcp interface	DHCPv6 インターフェイス情報を表示します。

ipv6 dhcp client request vendor

DHCP for IPv6（DHCPv6）サーバからオプションを要求するよう IPv6 クライアントを設定するには、**ipv6 dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。要求を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp client request vendor

no ipv6 dhcp client request vendor

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ベンダー固有オプションを要求するには、**ipv6 dhcp client request vendor** インターフェイス コンフィギュレーション コマンドを使用します。イネーブルにすると、IPv6 アドレスを DHCP から取得するときにだけこのコマンドを確認します。インターフェイスが IPv6 アドレスを取得したあとでこのコマンドを入力しても、次回クライアントが DHCP から IPv6 アドレスを取得するまでこのコマンドは有効になりません。

例

次の例では、ベンダー固有オプションの要求をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 dhcp client request vendor-specific
```

関連コマンド

コマンド	説明
ipv6 address dhcp	DHCP からインターフェイスの IPv6 アドレスを取得します。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが、ping 動作の一部としてプール アドレスに送信するパケットの数を指定するには、**ipv6 dhcp ping packets** グローバル コンフィギュレーション コマンドを使用します。サーバがプール アドレスに ping を送信しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp ping packets *number*

no ipv6 dhcp ping packets

（注）　このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

number	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。指定できる範囲は 0 ～ 10 です。

デフォルト

デフォルト値は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプール アドレスに ping を送信します。ping の応答がない場合はアドレスが使用されていないことを示すため、サーバは要求元クライアントにそのアドレスを割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 操作がオフになります。

例

次の例では、DHCPv6 サーバによる 2 回の ping 試行を指定する方法を示します（その後、ping 試行を停止します）。

```
Switch(config)# ipv6 dhcp ping packets 2
```

関連コマンド

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

ipv6 dhcp pool

Dynamic Host Configuration Protocol for IPv6（DHCPv6）プール コンフィギュレーション モードを開始するには、**ipv6 dhcp pool** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

poolname	DHCPv6 プールのユーザ定義名。プール名には象徴的な文字列（*Engineering* など）または整数（0 など）を使用できます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

DHCPv6 プール コンフィギュレーション モードのコマンドは次のようになります。

- **address prefix** *IPv6-prefix* : アドレス割り当てのアドレス プレフィクスを設定します。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。
- **lifetime** ***t1 t2*** : IPv6 アドレスの*有効*間隔（秒）および*優先*間隔（秒）を設定します。指定できる範囲は 5 ～ 4294967295 秒です。有効なデフォルト値は 2 日です。優先されるデフォルト値は 1 日です。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。間隔を指定しない場合は、**infinite** を指定します。
- **link-address** *IPv6-prefix :* リンク アドレス IPv6 プレフィクスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィクスと一致する場合、サーバは設定情報プールを使用します。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。

- **vendor-specific**：次のコンフィギュレーション コマンドを使用して、DHCPv6 ベンダー固有のコンフィギュレーション モードをイネーブルにします。
  - *vendor-id*：ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
  - **suboption** *number*：ベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、16 進文字列を、サブオプション パラメータで定義されているとおりに入力します。

DHCPv6 設定情報プールを作成してから、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用してプールとインターフェイス上のサーバを関連付けます。ただし、情報プールを設定しない場合は、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用して DHCPv6 サーバ機能をインターフェイスでイネーブルにする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィクスを使用しないということは、プールは設定されているオプションだけを返すことを指します。

link-address キーワードを使用すると、必ずしもアドレスを割り当てなくてもリンク アドレスを照合できます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレス プール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィクスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次の例では、*engineering* という IPv6 アドレス プレフィクスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次の例では、*testgroup* という 3 つのリンク アドレス プレフィクスおよび 1 つの IPv6 アドレス プレフィクスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6 dhcp server	インターフェイスで DHCPv6 サービスをイネーブルにします。
show ipv6 dhcp pool	DHCPv6 設定プール情報を表示します。

ipv6 dhcp server

インターフェイスで Dynamic Host Configuration Protocol for IPv6（DHCPv6）サービスをイネーブルにするには、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで DHCPv6 サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp server [*poolname* | **automatic**] [**allow-hint**] [**rapid-commit**] [**preference** *value*]

no ipv6 dhcp server

（注） このコマンドは、メトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

poolname	（任意）IPv6 DHCP プールのユーザ定義名。プール名には象徴的な文字列（*Engineering* など）または整数（0 など）を使用できます。
automatic	（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。
allow-hint	（任意）サーバが SOLICIT メッセージ内のクライアント提案を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
preference *value*	（任意）サーバにより送信されるアドバタイズ メッセージのプリファレンス オプションで伝送されるプリファレンス値。有効な範囲は 0 ～ 255 です。デフォルト値は 0 です。
rapid-commit	（任意）2 つのメッセージ交換方式を許可します。

デフォルト

デフォルトでは、DHCPv6 パケットはインターフェイス上で処理されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ipv6 dhcp server インターフェイス コンフィギュレーション コマンドは、指定されたインターフェイスで DHCPv6 サービスをイネーブルにします。

automatic キーワードを入力すると、クライアントにアドレスを割り当てるときに使用するプールが自動的に決定されます。サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。サーバは、このリンク アドレスと、すべてのアドレス プレフィクスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィクス一致を探します。サーバは最長一致と関連付けられているプールを選択します。

パケットをクライアントから直接受信した場合、サーバは同じ照合を行いますが、照合を行うときに着信インターフェイスに設定されているすべての IPv6 アドレスを使用します。そして再度、サーバは最長のプレフィクス照合を選択します。

allow-hint のキーワードを入力した場合、サーバは送信請求メッセージおよび要求メッセージの有効なクライアント提案アドレスを割り当てます。プレフィクス アドレスは、関連付けられているローカル プレフィクス アドレス プール内にあり、デバイスに割り当てられていない場合は有効です。**allow-hint** キーワードを指定しない場合、サーバはクライアント ヒントを無視して、プール内のフリー リストにあるアドレスが割り当てられます。

preference キーワードを 0 以外の値に設定すると、サーバはアドバタイズ メッセージにプリファレンス オプションを追加して、プリファレンス値を伝送します。この動作は、クライアントによるサーバの選択に影響を与えます。プリファレンス オプションを含まないアドバタイズ メッセージのプリファレンス値は 0 であると見なされます。クライアントが、プリファレンス値が 255 であるアドバタイズ メッセージを受信する場合、クライアントはメッセージの送信元であるサーバに要求メッセージを即時に送信します。

rapid-commit キーワードを入力すると、2 つのメッセージ交換を使用できます。

DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイス上で相互に排他的です。これらの機能の 1 つがすでにイネーブルになっているときに同じインターフェイスで別の機能を設定しようとすると、スイッチは次のメッセージのいずれかを返します。

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

例

次の例では、testgroup というプールの DHCPv6 をイネーブルにします。

```
Switch(config-if)# ipv6 dhcp server testgroup
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	DHCPv6 プールを設定して、DHCPv6 プール コンフィギュレーション モードを開始します。
show ipv6 dhcp interface	DHCPv6 インターフェイス情報を表示します。

ipv6 mld snooping

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

no ipv6 mld snooping [**vlan** *vlan-id*]

（注）　このコマンドは、スイッチで IP Services イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で IPv6 MLD スヌーピングをイネーブルまたはディセーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD スヌーピングをグローバルにイネーブルにする必要があります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

MLD スヌーピングがグローバルにディセーブルである場合、すべての既存の VLAN インターフェイスで MLD スヌーピングがディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、デフォルトの状態（イネーブル）であるすべての VLAN インターフェイス上で MLD スヌーピングがイネーブルになります。VLAN 設定は、MLD スヌーピングがディセーブルのインターフェイス上のグローバル コンフィギュレーションを上書きします。

MLD スヌーピングがグローバルにディセーブルである場合、VLAN 上で MLD スヌーピングをイネーブルにできません。MLD スヌーピングがグローバルにイネーブルである場合、個々の VLAN 上で MLD スヌーピングをディセーブルにできます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、MLD スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping
```

次の例では、MLD スヌーピングを VLAN でディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 11
```

設定を確認するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントがエージング アウトになる前に送信される IP version 6（IPv6）Multicast Listener Discovery（MLD）Multicast Address Specific Queries（MASQ）を設定するには、**ipv6 mld snooping last-listener-query-count** グローバル コンフィギュレーション コマンドを使用します。クエリー カウントをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー カウントを設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 7 です。

コマンド デフォルト

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です（グローバル カウントを使用します）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

MLD スヌーピングでは、IPv6 マルチキャスト ルータはマルチキャスト グループに所属するホストにクエリーを定期的に送信します。ホストがマルチキャスト グループを脱退する場合、ホストは静かに脱退する、または Multicast Listener Done メッセージでクエリーに応答できます（IGMP Leave メッセージに相当）。即時脱退が設定されていない場合（1 つのグループに対し複数のクライアントが同じポート上に存在する場合は設定しない）、設定された last-listener クエリー カウントにより、MLD クライアントが期限切れになる前に送信する MASQ の数が決定します。

last-listener クエリー カウントが VLAN 用に設定されている場合、このカウントはグローバルに設定された値より優先されます。VLAN カウントが設定されていない（デフォルトの 0 に設定されている）場合は、グローバル カウントが使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー カウントをグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

次の例では、last-listener クエリー カウントを VLAN 10 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-interval	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN で IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピングの last-listener クエリー間隔を設定するには、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用します。この時間間隔は、Multicast Address Specific Query（MASQ）マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する最大時間です。クエリー時間をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval**

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー時間を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	MASQ を送信した後マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する時間（1000 秒単位）を設定します。指定できる範囲は 100 ～ 32,768 です。デフォルト値は 1000（1 秒）です。

コマンド デフォルト

デフォルトのグローバル クエリー間隔（最大応答時間）は 1000（1 秒）です。

デフォルトの VLAN クエリー間隔（最大応答時間）は 0 です（グローバル カウントが使用されます）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

MLD スヌーピングでは、IPv6 マルチキャスト ルータが MLD Leave メッセージを受信すると、マルチキャスト グループに所属するホストにクエリーを送信します。一定の時間、ポートから MASQ への応答がない場合、ルータはマルチキャスト アドレスのメンバシップ データベースからそのポートを削除します。last listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除する前にルータが待機する最大時間です。

VLAN クエリー間隔が設定されていると、グローバル クエリー間隔より優先されます。VLAN 間隔が 0 に設定されていると、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー間隔を 2 秒にグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

次の例では、VLAN 1 用の last-listener クエリー間隔を 5.5 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。

ipv6 mld snooping listener-message-suppression

IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング リスナー メッセージ抑制をイネーブルにするには、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。MLD スヌーピング リスナー メッセージ抑制をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

コマンド デフォルト

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

MLD スヌーピング リスナー メッセージ抑制は、IGMP レポート抑制に相当します。イネーブルの場合、グループに対する受信 MLDv1 レポートはレポート転送時間ごとに 1 回だけ IPv6 マルチキャスト ルータに転送されます。これにより、重複レポートの転送を避けられます。

例

次の例では、MLD スヌーピング リスナー メッセージ抑制をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

次の例では、MLD スヌーピング リスナー メッセージ抑制をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除するまでにスイッチが送信する IP version 6（IPv6）Multicast Listener Discovery（MLD）クエリーの数を設定するには、**ipv6 mld snooping robustness-variable** グローバル コンフィギュレーション コマンドを使用します。VLAN ごとに設定するには、VLAN ID を入力します。変数をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable**

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN にロバストネス変数を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 3 です。

コマンド デフォルト

デフォルトのグローバル ロバストネス変数（リスナーを削除する前のクエリー数）は、2 です。

デフォルトの VLAN ロバストネス変数（マルチキャスト アドレスが期限切れになる前のクエリー数）は 0 です。リスナーの期限の判断には、グローバル ロバストネス変数が使用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

ロバストネスは、ポートをマルチキャスト グループから削除する前に送信された応答がなかった MLDv1 クエリー数の点から測定されます。設定された回数送信された MLDv1 クエリーに対して受信した MLDv1 レポートがない場合、ポートが削除されます。グローバル値により、スイッチが応答しないリスナーを削除する前に待機するクエリー数が決定し、VLAN 値が設定されていない VLAN すべてに適用します。

VLAN に設定されたロバストネス値はグローバル値より優先されます。VLAN ロバストネス値が 0（デフォルト）の場合、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、スイッチが応答しないリスナー ポートを削除する前に 3 個のクエリーを送信するようグローバル ロバストネス変数を設定する方法を示します。

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

次の例では、VLAN 1 にロバストネス変数を設定する方法を示します。この値は VLAN のグローバル コンフィギュレーションより優先されます。

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping tcn

IP version 6（IPv6）Multicast Listener Discovery（MLD）Topology Change Notification（TCN; トポロジ変更通知）を設定するには、**ipv6 mld snooping tcn** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

flood query count *integer_value*	フラッディング クエリー カウントを設定します。これは、クエリーの受信を要求したポートだけにマルチキャスト データを転送する前に送信されるクエリー数です。指定できる範囲は 1 ～ 10 です。
query solicit	TCN クエリーの送信請求をイネーブルにします。

コマンド デフォルト

TCN クエリー送信請求はディセーブルです。

イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、TCN クエリー送信請求をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

次の例では、フラッディング クエリー カウントを 5 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping vlan

VLAN インターフェイスで IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング パラメータを設定するには、**ipv6 mld snooping vlan** グローバル コンフィギュレーション コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

（注） このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
immediate-leave	（任意）VLAN インターフェイス上で、MLD の即時脱退処理をイネーブルにします。この機能をインターフェイス上でディセーブルにするには、このコマンドの **no** 形式を使用します。
mrouter interface	（任意）マルチキャスト ルータ ポートを設定します。設定を削除するには、このコマンドの **no** 形式を使用します。
static *ipv6-multicast-address*	（任意）指定の IPv6 マルチキャスト アドレスでマルチキャスト グループを設定します。
interface *interface-id*	レイヤ 2 ポートをグループに追加します。マルチキャスト ルータまたはスタティック インターフェイスは、物理ポートまたはインターフェイス範囲 1 ～ 48 の**ポートチャネル** インターフェイスになることができます。

コマンド デフォルト

MLD スヌーピング即時脱退処理はディセーブルです。

デフォルトでは、スタティック IPv6 マルチキャスト グループは設定されていません。

デフォルトでは、マルチキャスト ルータ ポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

VLAN の各ポート上に 1 つのレシーバだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM に保存されます。

static キーワードは MLD メンバ ポートを静的に設定するために使用されます。

設定およびスタティック ポートとグループは、NVRAM に保存されます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

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

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

設定を確認するには、**show ipv6 mld snooping vlan** *vlan-id* ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	IPv6 MLD スヌーピング設定を表示します。

ipv6 traffic-filter

インターフェイス上で IPv6 トラフィックをフィルタリングするには、**ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスでの IPv6 トラフィックのフィルタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

no ipv6 traffic-filter {**in** | **out**}

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

access-list-name	IPv6 アクセス名を指定します。
in	着信 IPv6 トラフィックを指定します。
out	発信 IPv6 トラフィックを指定します。 （注）　**out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。**out** キーワードは、スイッチでメトロ IP アクセス イメージが稼動している場合にだけ、レイヤ 3 インターフェイスでサポートされます。

デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

スイッチでメトロ IP アクセス イメージが稼動している場合、ACL をレイヤ 3 インターフェイスの発信または着信トラフィック（ルータ ACL）、あるいはレイヤ 2 インターフェイスの着信トラフィック（ポート ACL）に適用することができます。スイッチでメトロ アクセス イメージが稼動している場合、ACL をレイヤ 2 インターフェイスの着信管理トラフィックだけに適用することができます。これらのイメージは、ルータ ACL をサポートしません。

*いずれか*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た場合、そのポート ACL がパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

例

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

```
Switch (config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter cisco in
```

関連コマンド

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

l2protocol-tunnel

アクセス ポート、トランク ポート、IEEE 802.1Q トンネル ポート、またはポート チャネルでレイヤ 2 プロトコルのトンネリングをイネーブルにするには、**l2protocol-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。Cisco Discovery Protocol（CDP）、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、または VLAN Trunking Protocol（VTP; VLAN トランキング 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。また、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP）、または UniDirectional Link Detection（UDLD; 単方向リンク検出）パケットのポイントツーポイント トンネリングをイネーブルにできます。インターフェイスでトンネリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトでは、レイヤ 2 プロトコルのトンネリングは設定されていません。

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

デフォルトでは、レイヤ 2 プロトコル パケット数のドロップしきい値は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

（注） スイッチは VTP をサポートしません。CDP および STP は、ネットワーク ノード インターフェイス（NNI）上ではデフォルトでイネーブルになっています。拡張ネットワーク インターフェイス（ENI）上ではデフォルトでディセーブルになっていますが、イネーブルにできます。ユーザ ネットワーク インターフェイス（UNI）は、これらのプロトコルをサポートしません。

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

（注） NNI および ENI だけが PAgP および LACP をサポートします。

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

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

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

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

シャットダウンしきい値に到達すると、インターフェイスが errdisable になります。**errdisable recovery cause l2ptguard** グローバル コンフィギュレーション コマンドを入力し、エラー回復をイネーブルにした場合、インターフェイスは errdisable ステートから抜け出し、すべての原因がタイムアウトになったときに動作を再開します。**l2ptguard** でエラー回復メカニズムをイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで errdisable ステートのままになります。

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

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

設定は、NVRAM に保存されます。

（注）　レイヤ 2 プロトコル トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、CDP パケットのプロトコル トンネリングをイネーブルにし、シャットダウンしきい値を 50 pps に設定する方法を示します。

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

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

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

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

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

関連コマンド

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

l2protocol-tunnel cos

トンネリングされたレイヤ 2 プロトコル パケットすべてに、サービス クラス（CoS）値を設定するには、**l2protocol-tunnel cos** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

構文の説明

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

デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

NVRAM に値が保存されます。

例

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

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

関連コマンド

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

lacp port-priority

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

lacp port-priority *priority*

no lacp port-priority

（注）　LACP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

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

デフォルト

デフォルトは 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイ モードに置かれるポートを判別します。このコマンドは、LACP が設定済みの EtherChannel ポートにのみ有効です。インターフェイスがユーザ ネットワーク インターフェイス（UNI）の場合 **lacp port-priority** を設定する前に NNI または ENI にインターフェイスを変更する、**port-type nni** または **port-type eni** インターフェイス コンフィギュレーション コマンドを使用します。

プライオリティの比較においては、数値が*小さい*ほどプライオリティが*高く*なります。ハードウェアの制限により互換性のあるすべてのポートをアクティブにできない場合は、プライオリティを使用して、スタンバイ モードにする必要があるポートを決定します。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定します。

（注）　LACP リンクを制御するスイッチ上にポートがある場合に限り、LACP ポート プライオリティは有効です。リンクを制御するスイッチの判別については、**lacp system-priority** グローバル コンフィギュレーション コマンドを参照してください。

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

物理ポート上の LACP の設定に関する情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000
```

設定を確認するには、**show lacp** [*channel-group-number*] **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lacp system-priority	LACP システム プライオリティを設定します。
show lacp [*channel-group-number*] **internal**	すべてのチャネル グループまたは指定のチャネル グループの内部情報を表示します。

lacp system-priority

Link Aggregation Control Protocol（LACP）のシステム プライオリティを設定するには、**lacp system-priority** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp system-priority *priority*

no lacp system-priority

（注）　LACP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

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

デフォルト

デフォルトは 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

lacp system-priority コマンドでは、ポート プライオリティを制御する LACP リンクのスイッチが判別されます。これはグローバル コンフィギュレーション コマンドですが、プライオリティは LACP にすでに設定されている物理ポートがある EtherChannel でのみ有効です。

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

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システム プライオリティのシステム値の数値が小さいスイッチ（より高いプライオリティ値）が制御スイッチになります。いずれのスイッチも同じ LACP システム プライオリティである場合（たとえば、いずれもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（スイッチの MAC アドレス）により制御するスイッチが判別されます。

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

ホットスタンバイ モードのポート（ポートステート フラグが H になっています）を確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、LACP のシステム プライオリティを設定する方法を示します。

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

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

関連コマンド

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

link state group

リンクステート グループのメンバーとしてポートを設定するには、**link state group** インターフェイス コンフィギュレーション コマンドを使用します。リンクステート グループからポートを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 2 です。デフォルトは 1 です。
upstream	ポートを特定のリンクステート グループのアップストリーム ポートとして設定します。
downstream	ポートを特定のリンクステート グループのダウンストリーム ポートとして設定します。

デフォルト

デフォルトのグループは group 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

特定のリンク ステート グループのアップストリームまたはダウンストリーム ポートとしてポートを設定するには、**link state group** インターフェイス コンフィギュレーション コマンドを使用します。グループ番号が省略されている場合、デフォルトのグループ番号が使用されます。

ポートの集合（EtherChannel）、アクセス モードまたはトランク モードの単一のスイッチ ポート、またはルーテッド ポートをインターフェイスに指定できます。個々のダウンストリーム インターフェイスは、1 つ以上のアップストリーム インターフェイスに関連付けることができます。アップストリーム インターフェイス同士はバンドルでき、各ダウンストリーム インターフェイスは、複数のアップストリーム インターフェイスで構成されたリンクステート グループと呼ばれる単一グループに関連付けることができます。

ダウンストリーム インターフェイスのリンクステートは、関連付けられているリンクステート グループのアップストリーム インターフェイスのリンクステートに依存します。リンクステート グループ内のすべてのアップストリーム インターフェイスがリンクダウン ステートにある場合、関連付けられたダウンストリーム インターフェイスは強制的にリンクダウン ステートになります。リンクステート グループ内のアップストリーム インターフェイスのいずれか 1 つがリンクアップ ステートである場合、関連付けられたダウンストリーム インターフェイスは、リンクアップ ステートに移行するか、またはリンクアップ ステートを維持することができます。

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- スイッチ 1 つにつき、設定できるリンクステート グループは 2 つだけです。

例

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

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/11 - 14
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

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

関連コマンド

コマンド	説明
link state track	リンクステート グループをイネーブルにします。
show link state group	リンクステート グループ情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

link state track

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

link state track [*number*]

no link state track [*number*]

構文の説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 2 です。デフォルトは 1 です。

デフォルト

リンクステート トラッキングは、すべてのグループでディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループをイネーブルにするには、**link state track** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、リンクステート グループの group 2 をイネーブルにする方法を示します。

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

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

関連コマンド

コマンド	説明
link state group	リンクステート グループのメンバとしてインターフェイスを設定します。
show link state group	リンクステート グループ情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

location（グローバル コンフィギュレーション）

エンドポイントのロケーション情報を設定するには、**location** グローバル コンフィギュレーション コマンドを使用します。ロケーション情報を削除する場合は、このコマンドの **no** 形式を使用します。

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

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

構文の説明

admin-tag	管理タグまたはサイト情報を設定します。
civic-location	都市ロケーション情報を設定します。
elin-location	Emergency Location Information（ELIN; 緊急ロケーション情報）を設定します。
identifier id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 **（注）** LLDP-MED TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
string	サイト情報またはロケーション情報を英数字形式で指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

都市ロケーション ID は 250 バイトを超えてはなりません。

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

例

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

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

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

次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

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

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

関連コマンド

コマンド	説明
location（インターフェイス コンフィギュレーション）	インターフェイスにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

location（インターフェイス コンフィギュレーション）

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

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

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

構文の説明

additional-location-information	ロケーションまたは場所に関する追加情報を設定します。
word	追加のロケーション情報を指定する語またはフレーズを指定します。
civic-location-id	インターフェイスにグローバル都市ロケーション情報を設定します。
elin-location-id	インターフェイスに緊急ロケーション情報を設定します。
id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 **（注）** LLDP-MED TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

都市ロケーション ID は 250 バイトを超えてはなりません。

例

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

```
Switch(config-if)# int g1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

```
Switch(config-if)# int g2/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

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

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

```
Switch(config)# int g2/0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

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

関連コマンド

コマンド	説明
location（グローバル コンフィギュレーション）	エンドポイントにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

logging event

インターフェイス リンク ステータス変更の通知をイネーブルにするには、**logging event** インターフェイス コンフィギュレーション コマンドを使用します。通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

イベント ロギングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、スパニングツリー ロギングをイネーブルにする方法を示します。

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

logging event power-inline-status

Power over Ethernet（PoE）イベントのロギングをイネーブルにするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。PoE 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。ただし、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

構文の説明

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

関連コマンド

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

logging file

ロギング ファイルのパラメータを設定するには、**logging file** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

filesystem:*filename*	フラッシュ ファイル システムのエイリアスです。ログ メッセージを持つファイルのパスおよび名前を含みます。 ローカル フラッシュ ファイル システムの構文： **flash:**
max-file-size	（任意）ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。
min-file-size	（任意）ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。
severity-level-number	（任意）ログ ファイルの重大度のレベルを指定します。指定できる範囲は 0 ～ 7 です。各レベルの意味については *type* オプションを参照してください。
type	（任意）ログ タイプを指定します。次のキーワードが有効です。 • **emergencies**：システムは使用不可（重大度 0） • **alerts**：早急な対応が必要（重大度 1） • **critical**：危険な状態（重大度 2） • **errors**：エラーが発生している状態（重大度 3） • **warnings**：警告状態（重大度 4） • **notifications**：通常ではあるが、重要なメッセージ（重大度 5） • **information**：情報メッセージ（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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ログ ファイルはスイッチの内部バッファに ASCII テキスト形式で保存されます。ロギングされたシステム メッセージにアクセスするには、スイッチの Command-Line Interface（CLI; コマンドライン インターフェイス）を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチに障害が生じた場合は、それ以前に **logging file flash:***filename* グローバル コンフィギュレーション コマンドを使用してフラッシュ メモリにログを保存していない限り、ログは失われます。

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

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

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

例

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

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

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

関連コマンド

コマンド	説明
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

mac access-group

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

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

no mac access-group {*name*}

構文の説明

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

デフォルト

MAC ACL は、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション（レイヤ 2 インターフェイスだけ）

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

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

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

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

例

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

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

設定を確認するには、**show mac access-group** 特権 EXEC コマンドを入力します。スイッチに設定された ACL を表示するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show access-lists	スイッチで設定される ACL を表示します。
show mac access-group	スイッチで設定される MAC ACL を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

mac access-list extended

非 IP トラフィックの MAC アドレスに基づいたアクセス リストを作成するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。このコマンドを使用すると、拡張 MAC アクセス リスト コンフィギュレーション モードに入ります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

（注）　レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

mac access-list extended *name*

no mac access-list extended *name*

構文の説明

name	MAC 拡張アクセス リストに名前を割り当てます。

デフォルト

デフォルトでは、MAC アクセス リストは作成されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

VLAN マップまたはレイヤ 2 インターフェイスに、名前付き MAC 拡張 ACL を適用できます。

レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

mac access-list extended コマンドを入力すると、MAC アクセス リスト コンフィギュレーション モードがイネーブルになります。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **default**：コマンドをそのデフォルトに設定します。
- **deny**：パケットを拒否するように指定します。詳細については、deny（MAC アクセス リスト コンフィギュレーション）MAC アクセス リスト コンフィギュレーション コマンドを参照してください。
- **exit**：MAC アクセス リスト コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト値を設定します。
- **permit**：パケットを転送するように指定します。詳細については、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。

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

例

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

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

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

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

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

関連コマンド

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

mac address-table aging-time

ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に維持される時間を設定するには、**mac address-table aging-time** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。エージング タイムはすべての VLAN、または指定の VLAN に対して適用されます。

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

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

構文の説明

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

デフォルト

デフォルト値は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

例

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

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

show mac address-table aging-time 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

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

mac address-table learning vlan

VLAN で MAC アドレス ラーニングをイネーブルにするには、**mac address-table learning** グローバル コンフィギュレーション コマンドを使用します。これがデフォルトの状態になります。VLAN で MAC アドレス ラーニングをディセーブルにして、MAC アドレスを学習できる VLAN を制御するには、このコマンドの **no** 形式を使用します。

mac address-table learning vlan *vlan-id*

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

構文の説明

デフォルト

デフォルトでは、MAC アドレス ラーニングはすべての VLAN でイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

サービス プロバイダー ネットワーク内のカスタマーは、ネットワーク経由で多数の MAC アドレスをトンネリングし、使用可能な MAC アドレス テーブル スペースに入力できます。VLAN で MAC アドレス ラーニングを制御する場合、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。

MAC アドレス ラーニングは、1 つの VLAN（例：**no mac address-table learning vlan 223**）または一連の VLAN（例：**mac address-table learning vlan 1-10, 15**）でディセーブルにすることができます。

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

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

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

RSPAN VLAN で MAC アドレス ラーニングはディセーブルにできません。設定すること自体できません。

セキュア ポートを含む VLAN で MAC アドレス ラーニングをディセーブルにする場合、セキュア ポートで MAC アドレス ラーニングはディセーブルになりません。後でインターフェイスのポート セキュリティをディセーブルにすると、ディセーブルになった MAC アドレス ラーニングの状態がイネーブルになります。

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

例

次の例では、VLAN 2003 で MAC アドレス ラーニ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 learning vlan 2003
```

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

関連コマンド

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

mac address-table move update

MAC アドレス テーブル移行更新機能をイネーブルにするには、**mac address-table move update** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

コマンド モード

グローバル コンフィギュレーション

デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次の例では、アップリンク スイッチが MAC アドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear mac address-table move update	MAC アドレステーブル移行更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレステーブル移行更新メッセージ処理をデバッグします。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

mac address-table notification

スイッチで MAC アドレス通知機能をイネーブルにするには、**mac address-table notification** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

no mac address-table notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

構文の説明

change	スイッチ上で MAC 通知をイネーブルまたはディセーブルにします。
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 1 ～ 500 エントリです。デフォルトは 1 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。デフォルト値は 1 秒です。
mac-move	MAC 移動通知をイネーブルにします。
threshold	MAC しきい値通知をイネーブルにします。
limit *percentage*	（任意）MAC 利用率しきい値を入力します。指定できる範囲は 1 ～ 100% です。デフォルト値は 50% です。
interval *time*	（任意）MAC しきい値通知の間の時間を入力します。指定できる範囲は 120 ～ 1000000 秒です。デフォルト値は 120 秒です。

デフォルト

デフォルトでは、MAC アドレス通知、MAC 移動、および MAC しきい値モニタリングがディセーブルです。

デフォルトの MAC 変更トラップ間隔は 1 秒です。

履歴テーブルのデフォルトのエントリ数は 1 です。

デフォルトの MAC 利用率しきい値は 50% です。

MAC しきい値通知間のデフォルトの時間は 120 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

MAC アドレス通知変更機能は、新しい MAC アドレスが転送テーブルに追加されたり、古いアドレスがそこから削除されたりするたびに、Simple Network Management Protocol（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 変更通知はダイナミックおよびセキュア MAC アドレスだけに生成され、セルフ 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 アドレスには生成されません。

history-size オプションを設定している場合、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

mac address-table notification change コマンドを使用すれば、MAC アドレス通知変更機能がイネーブルになります。また、**snmp trap mac-notification change** 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 change** 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。

また、**mac address-table notification mac-move** コマンドおよび **snmp-server enable traps mac-notification move** 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り、MAC アドレスが 1 つのポートから同じ VLAN の別のポートに移動した場合、常にトラップをイネーブルにできます。

MAC アドレス テーブルのしきい値制限に達するかそれを超えた場合に常にトラップを生成するには、**mac address-table notification** *threshold* [**limit** *percentage*] | [**interval** *time*] コマンドおよび **snmp-server enable traps mac-notification threshold** グローバル コンフィギュレーション コマンドを入力します。

例

次の例では、MAC アドレス テーブル変更通知機能をイネーブルにし、通知トラップの間隔を 60 秒、履歴テーブルのサイズを 100 エントリに設定する方法を示します。

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

show mac address-table notification 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
show mac address-table notification	すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp-server enable traps	**mac-notification** キーワードが追加された場合に SNMP MAC 通知トラップを送信します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC 通知トラップをイネーブルにします。

mac address-table static

MAC アドレス テーブルにスタティック アドレスを追加するには、**mac address-table static** グローバル コンフィギュレーション コマンドを使用します。スタティック エントリをテーブルから削除するには、このコマンドの **no** 形式を使用します。

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

構文の説明

mac-addr	アドレス テーブルに追加する宛先 MAC アドレス（ユニキャストまたはマルチキャスト）。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
interface *interface-id*	受信されたパケットを転送するインターフェイス。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。

デフォルト

スタティック アドレスは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先としてパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

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

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

mac address-table static drop

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、特定の送信元または宛先 MAC アドレスのトラフィックをドロップするようにスイッチを設定するには **mac address-table static drop** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id*

構文の説明

mac-addr	ユニキャスト送信元または宛先 MAC アドレス。この MAC アドレスを持つパケットはドロップされます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。

デフォルト

ユニキャスト MAC アドレス フィルタリングはディセーブルです。スイッチは、特定の送信元または宛先 MAC アドレスのトラフィックをドロップしません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能を使用する場合は、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、最初のコマンドを上書きします。

  たとえば、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* グローバル コンフィギュレーション コマンドの後に **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

  mac address-table static *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマンドの後に **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

例

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

次の例では、ユニキャスト MAC アドレス フィルタリングをディセーブルにする方法を示します。

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

show mac address-table static 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

macro apply

インターフェイスにマクロを適用するか、またはインターフェイスにマクロ設定を適用してこれを追跡するには、**macro apply** インターフェイス コンフィギュレーション コマンドを使用します。

macro {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

構文の説明

apply	指定したインターフェイスにマクロを適用します。
trace	インターフェイスにマクロを適用し、そのマクロをデバッグするには、**trace** キーワードを使用します。
macro-name	マクロ名を指定します。
parameter *value*	（任意）インターフェイスに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

macro trace *macro-name* インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをインターフェイスに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、そのインターフェイスに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

マクロをインターフェイスに適用する場合、マクロ名が自動的にインターフェイスに追加されます。**show running-configuration interface** *interface-id* ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

インターフェイスの範囲に適用されたマクロは、単一インターフェイスに適用されたマクロと同じ動作をします。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。

インターフェイスで適用されたマクロの設定は、次のいずれかの方法で削除できます。

- **default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを入力する（このコマンドによって、インターフェイス設定がデフォルト設定に戻ります）。
- マクロに含まれている各コマンドの **no** バージョンを入力する。
- マクロの **no** バージョンを適用する （**no** バージョンは一部のマクロには利用できません）。

例

macro name グローバル コンフィギュレーション コマンドを使用してマクロを作成したあとは、そのマクロをインターフェイスに適用できます。次の例では、**duplex** という名前のユーザ作成マクロをインターフェイスに適用する方法を示します。

```
Switch(config-if)# macro apply duplex
```

マクロをデバッグするには、**macro trace** インターフェイス コンフィギュレーション コマンドを使用して、マクロがインターフェイスに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、インターフェイス上の **duplex** という名前のユーザ作成マクロをトラブルシューティングする方法を示します。

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

関連コマンド

コマンド	説明
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro description

インターフェイスに適用されるマクロの説明を入力するには、**macro description** インターフェイス コンフィギュレーション コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

macro description *text*

no macro description

構文の説明

description *text*	指定したインターフェイスに適用されたマクロについての説明を入力します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスにコメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。単一インターフェイスに複数のマクロを適用する場合、説明テキストは最後に適用したマクロのものになります。

次の例では、インターフェイスに説明を追加する方法を示します。

```
Switch(config-if)# macro description duplex settings
```

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

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global

スイッチにマクロを適用するか、またはスイッチにマクロ設定を適用してこれを追跡するには、**macro global** グローバル コンフィギュレーション コマンドを使用します。

macro global {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

構文の説明

apply	スイッチにマクロを適用します。
trace	スイッチにマクロを適用してマクロをデバッグします。
macro-name	マクロ名を指定します。
parameter *value*	（任意）スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

macro trace *macro-name* グローバル コンフィギュレーション コマンドを使用して、スイッチ上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをスイッチに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter** *value* キーワードを使用して、そのスイッチに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

マクロをスイッチに適用する場合、マクロ名が自動的にスイッチに追加されます。**show running-configuration** ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

スイッチで適用されたグローバル マクロの設定を削除するには、マクロ内にある各コマンドの **no** バージョンを入力するか、またはマクロの **no** バージョンを適用します。（**no** バージョンは一部のマクロには利用できません）。

例

macro name グローバル コンフィギュレーション コマンドを使用してマクロを作成したあとは、そのマクロをスイッチに適用できます。次の例では、**snmp** マクロを表示する方法、およびそのマクロを適用してホスト名をテスト サーバに設定し、IP precedence 値を 7 に設定する方法を示します。

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

------------------------------------------------
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

マクロをデバッグするには、**macro global trace** グローバル コンフィギュレーション コマンドを使用して、マクロがスイッチに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、**ADDRESS** パラメータ値が入力されなかったために `snmp-server host` コマンドが失敗した一方で、残りのマクロがスイッチに適用されていることを示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global description

スイッチに適用されるマクロの説明を入力するには、**macro global description** グローバル コンフィギュレーション コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

macro global description *text*

no macro global description

構文の説明

description *text*	スイッチに適用されたマクロについての説明を入力します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチにコメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。複数のマクロがスイッチに適用されている場合、説明テキストは最後に適用されたマクロの説明になります。

次の例では、スイッチに説明を追加する方法を示します。

```
Switch(config)# macro global description udld aggressive mode enabled
```

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

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro name

設定マクロを作成するには、**macro name** グローバル コンフィギュレーション コマンドを使用します。マクロ定義を削除するには、このコマンドの **no** 形式を使用します。

macro name *macro-name*

no macro name *macro-name*

構文の説明

macro-name	マクロの名前

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

マクロには、最大 3000 文字を含めることができます。1 行に 1 つのマクロ コマンドを入力します。マクロを終了するには **@** 文字を使用します。マクロ内にコメント テキストを入力するには、行の先頭に # 文字を使用します。

ヘルプ文字列を使用してキーワードを指定し、マクロ内で必須キーワードを定義できます。**#macro keywords** *word* を入力してマクロで使用できるキーワードを定義します。スペースで分離することにより最大で 3 つのヘルプ ストリングを入力できます。4 つのキーワードを入力した場合、最初の 3 つ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** と **macro name sample-macro** は、2 つの別個のマクロとなります。

マクロを作成する際に、**exit** や **end** コマンド、または **interface** *interface-id* コマンドを使用してコマンド モードを変更しないでください。これらのコマンドを使用すると、**exit**、**end**、または **interface** *interface-id* に続くコマンドが異なるコマンド モードで実行されることがあります。

このコマンドの **no** 形式によって、マクロ定義のみが削除されます。マクロがすでに適用されているインターフェイスの設定には、影響はありません。**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスで適用されたマクロの設定を削除できます。また、元のマクロの対応するコマンドすべての **no** 形式を含む既存のマクロの *anti-macro* を作成できます。次に anti-macro をインターフェイスに適用します。

既存のマクロと同じ名前の新しいマクロを作成して、マクロを変更することができます。新規作成されたマクロは既存のマクロを上書きしますが、元のマクロが適用されたインターフェイスの設定には影響を与えません。

例

次の例では、デュプレックス モードおよび速度を定義するマクロを作成する方法を示します。

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

次の例では、**# macro keyword** でマクロを作成する方法を示します。

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

次の例では、インターフェイスにマクロを適用する前に、必須キーワード値を表示する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID ?
  WORD  Value of first keyword to replace

Switch(config-if)# macro apply test $VLANID 2
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID 2 $MAX ?
  WORD  Value of second keyword to replace
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

match（アクセス マップ コンフィギュレーション）

VLAN マップを設定して、パケットを 1 つまたは複数のアクセス リストと照合するには、**match** アクセスマップ コンフィギュレーション コマンドを使用します。一致パラメータを削除するには、このコマンドの **no** 形式を使用します。

match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

構文の説明

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

デフォルト

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

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

同じマップ エントリに、IP アドレスと MAC アドレスの両方を指定できます。

例

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

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

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

関連コマンド

コマンド	説明
access-list	番号付き標準 ACL を設定します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
action	パケットが Access Control List（ACL; アクセス コントロール リスト）のエントリに一致した場合に、実行されるアクションを指定します。
ip access-list	名前付きアクセス リストを作成します。構文情報については、『**Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2**』>「**IP Services Commands**」を選択してください。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
show vlan access-map	スイッチで作成された VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

match access-group

指定したアクセス コントロール リスト（ACL）に基づいて、クラス マップの一致基準を設定するには、**match access-group** 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。ACL 一致基準を削除するには、このコマンドの **no** 形式を使用します。

match access-group *acl-index-or-name*

no match access-group *acl-index-or-name*

構文の説明

acl-index-or-name	IP 標準または拡張 Access Control List（ACL）または MAC（メディア アクセス コントロール）ACL の番号または名前です。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match access-group コマンドは、パケットがクラス マップで指定されたクラスに属しているかどうかを確認するための一致基準として使用する番号付きまたは名前付き ACL を指定します。

match access-group コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

match access-group 分類は、入力ポリシー マップ上でのみ使用できます。

例

次に、一致基準としてアクセス コントロール リスト *acl1* を使用するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

match cos

レイヤ 2 サービス クラス（CoS）マーキングに基づいてパケットと一致するには、**match cos** 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。CoS 一致基準を削除するには、このコマンドの **no** 形式を使用します。

match cos *cos-list* |

no match cos *cos-list*

構文の説明

cos-list	着信パケットに対して一致する 4 つまでの CoS 値からなるリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match cos コマンドでは、一致基準として使用する CoS 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかが判別されます。

match cos コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

CoS 値との一致は、レイヤ 2 VLAN タグ付きトラフィックを伝送するポート上でだけサポートされます。つまり、**cos** 分類は、IEEE 802.1Q トランク ポート上でだけ使用できます。

match cos 分類は、入力および出力のポリシー マップ内で使用できます。

例

次に、CoS 値が 1 および 4 のすべての着信トラフィックに一致するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
Switch(config-cmap)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

match ip dscp

クラスの一致基準として特定の IPv4 DiffServ コード ポイント（DSCP）値を識別するには、**match ip dscp** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match ip dscp *dscp-list*

no match ip dscp *dscp-list*

構文の説明

ip-dscp-list	着信パケットに対して一致する 8 つまでの IPv4 DSCP 値からなるリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。また、よく使用される値にはニーモニック名を入力できます。 DSCP 値を指定するための他のオプションについては、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。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match ip dscp コマンドでは、一致基準として使用する DSCP 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかが判別されます。

このコマンドはクラス マップで使用され、パケット上の特定の DSCP 値マーキングを識別します。この場合、DSCP 値はマーキングとしてだけ使用され、数学的な意味はありません。たとえば、DSCP 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

match ip dscp コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

1 つの一致ステートメントで最大 8 つの DSCP 値を入力できます。たとえば、DSCP 値 0、1、2、3、4、5、6、または 7 が必要な場合は、**match ip dscp 0 1 2 3 4 5 6 7** コマンドを入力します。クラスに属するには、パケットは、指定されている IPv4 DSCP 値の 1 つだけ（すべてではなく）に一致している必要があります。

match ip dscp 分類は、入力および出力のポリシー マップ内で使用できます。

例

次に、DSCP 値が 10、11、および 12 のすべての着信トラフィックに一致するクラス マップ in*class* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

match ip precedence

クラスの一致基準として IPv4 precedence 値を識別するには、**match ip precedence** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match ip precedence *ip-precedence-list*

no match ip precedence *ip-precedence-list*

構文の説明

ip precedence *ip-precedence-list*	着信パケットに対して一致する 4 つまでの IPv4 precedence 値からなるリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match ip precedence コマンドでは、一致基準として使用する IPv4 precedence 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかが判別されます。

precedence 値はマーキングとしてだけ使用されます。この場合、IP precedence 値に数学的な意味はありません。たとえば、precedence 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

match ip precedence コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

1 つの一致ステートメントで最大 4 つの IPv4 precedence 値を入力できます。たとえば、IP precedence 値 0、1、2、または 7 が必要な場合は、**match ip precedence 0 1 2 7** コマンドを入力します。クラスに属するには、パケットは、指定されている IP precedence 値の 1 つだけ（すべてではなく）に一致している必要があります。

match ip precedence 分類は、入力および出力のポリシー マップ内で使用できます。

例

次に、IP-precedence 値が 5、6、および 7 のすべての着信トラフィックに一致するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

match qos-group

クラスの一致基準として特定の Quality Of Service（QoS）グループ値を識別するには、**match qos-group** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match qos-group *value*

no match qos-group *value*

構文の説明

qos-group *value*	Quality Of Service グループ値。指定できる範囲は 0 ～ 99 です。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match qos-group コマンドでは、一致基準として使用する QoS グループ値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかが判別されます。

QoS グループ値はマーキングとしてだけ使用され、数学的な意味はありません。たとえば、precedence 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

QoS グループ値はスイッチ内に限定されます。つまり、パケットがスイッチから送出されるとき、パケットでマーキングされた QoS グループ値はスイッチから送出されません。パケットとともに残るマーキングが必要な場合は、IP DiffServ コード ポイント（DSCP）値、IP precedence 値、またはパケット マーキングの別の方法を使用します。

match qos-group コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

match qos-group 分類は、出力ポリシー マップ上でのみ使用できます。

スイッチ（0 ～ 99）には、100 を超える QoS グループを指定することはできません。

例

次に、一致基準として QoS グループ 13 を使用してトラフィックを分類する例を示します。

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match qos-group 13
Switch(config-cmap)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	QoS クラス マップを表示します。

match vlan

所定のインターフェイスにユーザが指定した VLAN 上で伝送されるフレームに QoS ポリシーを適用するには、階層型ポリシー マップの親ポリシー内で **match vlan** 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。トランク ポートでの VLAN 単位の分類に階層型ポリシー マップを使用できます。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match vlan *vlan-list*

no match vlan *vlan-list*

構文の説明

vlan-list	着信パケットに対して一致する VLAN ID または VLAN 範囲を、トランク ポート上のポート単位、VLAN 単位 QoS 用の親ポリシー マップ内で指定します。VLAN ID は、30 個まで入力できます。VLAN の範囲を指定するには、ハイフンを使用します。1 つの VLAN 範囲は、2 つの VLAN ID として数えられます。個々の VLAN は、スペースを使用して区切ります。指定できる範囲は 1 ～ 4094 です。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能は、2 レベルの階層型入力ポリシー マップを使用する場合に限り、サポートされます。このポリシー マップは、親レベルで VLAN ベースの分類を定義し、子レベルで 1 つまたは複数の該当する VLAN に適用される QoS ポリシーを定義します。

親レベルで複数のサービス クラスを設定することにより、各種 VLAN の組み合わせを照合できます。また、子ポリシー マップを使用することにより、親サービス クラスごとに個別の QoS ポリシーを適用できます。

子ポリシー マップに関連付けられた 1 つまたは複数のクラスがあるポリシーは、親ポリシー マップと見なされます。親ポリシー マップ内の各クラスは、親クラスと呼ばれます。親クラスでは、**match vlan** コマンドだけを設定できます。子ポリシー マップ内のクラスでは、**match vlan** コマンドを設定できません。

ポート単位、VLAN 単位の親レベルのクラス マップでは、子ポリシー アソシエーションだけをサポートします。いずれのアクションも設定できません。さらに、親レベルのクラス マップでは、クラスの **class-default** のアクションまたは子ポリシー アソシエーションを設定できません。

子ポリシー マップ内では、レイヤ 2 とレイヤ 3 が混在するクラス マップを設定できません。このような子ポリシー マップを親ポリシーに関連付けようとすると、設定は拒否されます。ただし、レイヤ 2 とレイヤ 3 の子ポリシーを異なる親レベルのクラス マップに関連付けることはできます。

ポート単位、VLAN 単位 QoS は、IEEE 802.1Q トランク ポート上でだけサポートされます。

ポート単位、VLAN 単位の階層型ポリシーマップをインターフェイスに付加した後は、VLAN ベースの分類が含まれる親クラスを動的に追加または削除できません。そのような設定変更を行う前に、サービス ポリシーをインターフェイスから消去する必要があります。

VLAN または VLAN のセットに付加されている子ポリシー マップに、レイヤ 3 分類（**match ip dscp**、**match ip precedence**、**match IP ACL**）だけが含まれる場合、これらの VLAN は、必ずポート単位、VLAN 単位ポリシーが付加されているポート上でだけ実行されることに注意する必要があります。この制限事項に従わない場合は、これらの VLAN 上のスイッチに着信するトラフィックの QoS 動作が不適切になる場合があります。

また、ポート単位 VLAN 単位が適用されるトランク ポート上で、**switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用して、VLAN メンバーシップを制限することも推奨します。レイヤ 3 分類が設定されたポート単位、VLAN 単位のポリシーが含まれるトランク ポート間で VLAN メンバーシップが重複した場合も、予期せぬ QoS 動作が発生する可能性があります。

match vlan コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

例

次の例では、子レベルのポリシー マップのクラス マップが音声およびビデオ トラフィックの一致基準を指定して、子ポリシー マップが各トラフィック タイプの入力ポリシングに対するアクションを設定します。親レベルのポリシー マップは、指定されたポート上の子ポリシー マップが適用される VLAN を指定します。

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```

（注）　また、一致基準を **match vlan 100 200 300** と入力した場合でも、同じ結果になります。

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# exit
```

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

関連コマンド

コマンド	説明
class-map	指定したクラス名とパケットとの比較に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

mdix auto

インターフェイスで Automatic Medium-Dependent Interface crossover（Auto-MDIX）機能をイネーブルにするには、**mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。Auto MDIX をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdix auto

no mdix auto

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスで Auto-MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイスの速度とデュプレックスも **auto** に設定する必要があります。ポートがユーザ ネットワーク インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）の場合、**mdix auto** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス（NNI）はデフォルトでイネーブルです。

接続された一方または両方のインターフェイスで Auto-MDIX を（速度とデュプレックスの自動ネゴシエーションとともに）イネーブルにすると、必要なケーブル タイプ（ストレートまたはクロス）が間違っていてもリンクアップが発生します。

Auto-MDIX は、すべての 10/100-Mb/s インターフェイス上および 10/100/1000BASE-T/BASE-TX 小型フォーム ファクタ（SFP）モジュール インターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

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

インターフェイスの auto-MDIX の動作ステートを確認するには **show controllers ethernet-controller** *interface-id* **phy** 特権 EXEC コマンドを入力します。

関連コマンド

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

media-type

デュアルパーパス ポートのインターフェイスとタイプを手動で選択したり、最初にリンクが確立されたタイプをスイッチで動的に選択するように設定したりするには、**media-type** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no media-type

構文の説明

auto-select	最初に確立されたリンクに基づいてタイプをスイッチで動的に選択できるようにします。
rj45	RJ-45 インターフェイスを選択します。
sfp	小型フォーム ファクタ（SFP）モジュール インターフェイスを選択します。

デフォルト

デフォルトでは、スイッチは動的にリンクを選択します（**auto-select**）

コマンド モード

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

デュアルパーパス ポートの RJ-45 インターフェイスおよび SFP インターフェイスを同時に使用して、冗長リンクを提供することはできません。

auto-select を選択した場合、スイッチは最初にリンクが確立されたタイプを動的に選択します。これがデフォルトのモードです。スイッチはアクティブなリンクがダウンの状態になるまで、他のメディアタイプをディセーブルにします。アクティブなリンクがダウンの状態になると、いずれかのリンクがアップの状態になるまで、スイッチにより両方のタイプがイネーブル化されます。両方のメディアにアクティブ リンクがある場合、SFP リンクが優先されます。auto-select モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます（デフォルト）。

rj45 を選択した場合、スイッチは SFP モジュール インターフェイスをディセーブルにします。ケーブルを SFP ポートに接続した場合、RJ-45 がダウンしているか切断されている場合でも、リンクを確立できません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。

sfp を選択した場合、スイッチは RJ-45 インターフェイスをディセーブルにします。このポートにケーブルを接続した場合、SFP モジュール側がダウンしている場合または SFP モジュールが存在しない場合であっても、リンクを確立できません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。

デュアルパーパス ポートの速度またはデュプレックスを設定するには、まずメディア タイプを選択する必要があります。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドによる設定は行えません。インターフェイス タイプを変更すると、速度およびデュプレックス設定は削除されます。スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます（デフォルト）。

メディア タイプが **auto-select** の場合、スイッチは次の基準を使用してメディア タイプを選択します。

（注） SFP は、光ファイバ ケーブルまたは銅線ケーブルを SFP モジュールに差し込むまで*インストール*されません。

- インストールされているメディア タイプがただ 1 つの場合、このインターフェイスはアクティブとなり、メディアが削除されるかスイッチがリロードされるまではアクティブのままです。
- イネーブルなデュアルパーパス ポートに両方のメディア タイプをインストールしている場合、スイッチは最初にインストールされたタイプに基づいてアクティブ リンクを選択します。
- 接続されている両方のケーブルでスイッチの電源を投入した場合、または **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドでデュアルパーパス アップリンク ポートをイネーブル化した場合、SFP モジュール インターフェイスが選択されます。これ以外の場合、最初にアップの状態になったリンクのタイプに基づいて、アクティブなリンクが選択されます。

例

次の例では、SFP インターフェイスを選択するよう設定する方法を示します。

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

設定を確認するには、**show interfaces** *interface-id* **capabilities** または **show interfaces** *interface-id* **transceiver properties** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces capabilities	すべてのインターフェイスまたは特定のインターフェイスの機能を表示します。
show interfaces transceiver properties	すべてのインターフェイスまたは特定のインターフェイスの速度、デュプレックス、およびメディアタイプの設定を表示します。

monitor session

新規のスイッチド ポート アナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）送信元/宛先セッションを開始し、ネットワーク セキュリティ デバイス（Cisco IDS センサー アプライアンスなど）の宛先ポート上で着信トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスや VLAN を追加/削除し、SPAN 送信元トラフィックを特定の VLAN に制限（フィルタリング）するには、**monitor session** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元/宛先インターフェイスまたはフィルタを削除したりするには、このコマンドの **no** 形式を使用します。宛先インターフェイスの場合、**encapsulation dot1q** または **encapsulation replicate** キーワードは、このコマンドの **no** 形式では無視されます。

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

monitor session *session_number* **filter vlan** *vlan-id* [, | -]

monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

no monitor session {*session_number* | **all** | **local** | **remote**}

no monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate}**] [**ingress** {[**dot1q** | **untagged] vlan** *vlan-id*}] | {**remote vlan** *vlan-id*}

no monitor session *session_number* **filter vlan** *vlan-id* [, | -]

no monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は 1 ～ 66 です。
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（タイプおよびポート番号を含む）です。**送信元インターフェイス**の場合は、**ポート チャネル**も有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 48 です。
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。
encapsulation replicate	（任意）カプセル化方式を指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **dot1q**：IEEE 802.1Q カプセル化を指定します。 • **replicate**：宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 **（注）** 入力したこれらのキーワードは、ローカル SPAN にだけ有効です。RSPAN に対しては、RSPAN VLAN ID が元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。
ingress	（任意）入力トラフィック転送をイネーブルにします。

dot1q vlan *vlan-id*	入力トラフィックのデフォルト VLAN として指定されている VLAN で IEEE 802.1Q カプセル化を使用して入力トラフィックを転送するように指定します。
untagged vlan *vlan-id*	入力トラフィックのデフォルト VLAN として指定されている VLAN でタグなしカプセル化を使用して入力トラフィックを転送するように指定します
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。
remote vlan *vlan-id*	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 **（注）** RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
,	（任意）一連のインターフェイスまたは VLAN を指定します。または、以前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
filter vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
source	SPAN または RSPAN の送信元を指定します。物理ポート、ポート チャネル、VLAN が送信元になることができます。
both、**rx**、**tx**	（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
source vlan *vlan-id*	VLAN ID として SPAN の送信元インターフェイスを指定します。指定できる範囲は 1 ～ 4094 です。
all、**local**、**remote**	すべての SPAN および RSPAN、すべてのローカル SPAN、すべての RSPAN セッションをクリアするため、**no monitor session** コマンドに **all**、**local**、**remote** を指定します。

デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

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 がモニタリングされます。

ローカル SPAN の宛先ポートで **encapsulation dot1q** または **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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチ上で、合計 66 の SPAN および RSPAN セッションを保有できます。

スイッチ上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッション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、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,** | **-]** オプションを使用することにより、一連のインターフェイスまたはインターフェイス範囲、一連の VLAN または VLAN 範囲を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートで IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。（802.1x を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す。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元になることができません。

入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。
- その他のキーワードを指定せずに、**monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** を入力した場合は、出力カプセル化は送信元インターフェイス カプセル化を複製し、入力トラフィック転送はイネーブルにはなりません。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスのカプセル化を複製し、入力カプセル化はその後に続くキーワードが、**dot1q**、**untagged** のいずれであるかによって決まります （これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はその後に続くキーワードが **dot1q**、**untagged** のいずれであるかによって決まります。

例

次の例では、ローカル SPAN セッション 1 を作成し、送信元ポート 1 から宛先ポート 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 gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次の例では、複数の送信元インターフェイスをモニタリングする 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 gigabitethernet0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、モニタリング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 gigabitethernet0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ 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。出力トラフィックおよび入力トラフィックはタグなしです。

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

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN および RSPAN 設定を表示できます。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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

mvr（グローバル コンフィギュレーション）

スイッチ上のマルチキャスト VLAN レジストレーション（MVR）機能をイネーブルにするには、キーワードを指定せずに **mvr** グローバル コンフィギュレーション コマンドを使用します。このコマンドをキーワードとともに使用すると、スイッチの MVR モードの設定、MVR IP マルチキャスト アドレスの設定、またはグループ メンバーシップからのポートの削除を行う前に、クエリーの返答を待つ最大時間の設定、または MVR マルチキャスト VLAN の指定が行われます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **ringmode flood** | **vlan** *vlan-id*]

no mvr [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** | **ringmode flood** | **vlan** *vlan-id*]

構文の説明

group *ip-address*	スイッチの MVR グループ IP マルチキャスト アドレスを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 ～ 2000 です。ただし、モードが compatible の場合、512 より大きい値を入力しても、スイッチで許可されるグループは 512 だけです。ダイナミック モードでは、2000 のグループをサポートします。デフォルトは 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 メンバシップ加入は使用できません。
dynamic	MVR モードを設定して、送信元ポートでダイナミック MVR メンバシップを使用できるようにします。
querytime *value*	（任意）レシーバ ポートで IGMP レポート メンバシップを待機する最大時間を設定します。この時間は、レシーバ 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 ポートから送信された場合、スイッチは、デフォルトまたは設定された MVR クエリー時間が経過するまで IGMP グループ メンバシップ レポートを待ってから、ポートをマルチキャスト グループ メンバシップから削除します。 この値は 10 分の 1 秒単位の応答時間です。指定できる範囲は 1 ～ 100 です。デフォルトは 5/10 秒（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。

ringmode flood	（任意）アクセス リングの MVR リング モード フラッディングをイネーブルにします。このコマンドを入力して、リング環境で出力ポートのトラフィック フローを制御し、ユニキャスト トラフィックのドロップを防ぎます。
vlan *vlan-id*	（任意）MVR マルチキャスト データが受信される 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。デフォルトは VLAN 1 です。

デフォルト

MVR はデフォルトでディセーブルです。

デフォルトの MVR モードは、compatible モードです。

IP マルチキャスト アドレスは、デフォルトではスイッチで設定されます。

デフォルトのグループ IP アドレス カウントは 0 です。

デフォルトのクエリー応答時間は 5/10 秒（1/2 秒）です。

デフォルトの MVR 用マルチキャスト VLAN は VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

MVR に属するすべての IP マルチキャスト アドレスをスタティックに設定する場合は、**mvr group** コマンドを使用します。設定したマルチキャスト アドレスに送信されたマルチキャスト データは、スイッチのすべての送信元ポートおよびその IP マルチキャスト アドレスでデータを受信するよう登録されたすべてのレシーバ ポートに送信されます。

MVR モードが互換（デフォルト）の場合は、512 個のマルチキャスト エントリ（MVR グループ アドレス）を設定できます。コマンド ラインのヘルプに表示される範囲は 1 ～ 2000 ですが、スイッチで許可されるグループは 512 だけです。

MVR モードがダイナミックの場合は、スイッチで最大 2000 の MVR グループ アドレスを設定できます。同時にアクティブなマルチキャスト ストリームの最大数（受信できるテレビ チャネルの最大数）は 512 です。この上限に達すると、*グループの最大ハードウェアの上限に達しました*、というメッセージが生成されます。IGMP 加入がポートにある場合や、**mvr vlan** *vlan-id* **group** *ip-address* インターフェイス コンフィギュレーション コマンドを入力して、ポートをグループに加入するように設定する場合、ハードウェア エントリが発生することに注意してください。

MVR はスイッチのエイリアス IP マルチキャスト アドレスをサポートします。ただし、スイッチが Catalyst 3550 または 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。

mvr querytime コマンドはレシーバ ポートだけに適用されます。

スイッチ MVR が Catalyst 2900 XL または 3500 XL スイッチと相互動作している場合は、マルチキャスト モードを compatible に設定してください。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR はスイッチで IGMP スヌーピングと共存できます。

マルチキャスト ルーティングおよび MVR はスイッチ上で共存できません。MVR がイネーブルになっている状態で、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにした場合、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態で、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作はキャンセルされ、エラー メッセージが表示されます。

Cisco IOS Release 12.2(52)SE 以降、**mvr ringmode flood** 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、リング トポロジでのデータ転送がメンバとして検出されたポートに制限され、マルチキャスト ルータ ポートへの転送が除外されるようにすることができます。これにより、MVR マルチキャスト トラフィックが一方向に流れ、ユニキャスト トラフィックが逆方向に流れる場合に、ユニキャスト トラフィックがリング環境でドロップされません。

例

次の例では、MVR をイネーブルにする方法を示します。

```
Switch(config)# mvr
```

show mvr 特権 EXEC コマンドを使用すると、最大のマルチキャスト グループの現在の設定を表示できます。

次の例では、228.1.23.4 を IP マルチキャスト アドレスとして設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.4
```

次の例では、228.1.23.1 ～ 228.1.23.10 のマルチキャスト アドレスとともに 10 の連続 IP マルチキャスト グループを設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.1 10
```

設定済みの 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** 特権 EXEC コマンドを使用します。

次の例では、最大クエリー応答時間を 1 秒（10/10）に設定する方法を示します。

```
Switch(config)# mvr querytime 10
```

次の例では、VLAN 2 をマルチキャスト VLAN として設定する方法を示します。

```
Switch(config)# mvr vlan 2
```

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

関連コマンド

コマンド	説明
mvr（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	設定済み MVR インターフェイスのタイプ、モード、VLAN、ステータス、即時脱退設定を表示します。また、インターフェイスがメンバーであるすべての MVR グループを表示できます。
show mvr members	MVR マルチキャスト グループのメンバであるすべてのポートを表示します。グループにメンバがいない場合、そのステータスは Inactive として表示されます。

mvr（インターフェイス コンフィギュレーション）

レイヤ 2 のポートをマルチキャスト VLAN レジストレーション（MVR）のレシーバまたは送信元ポートとして設定することで、即時脱退機能を設定し、IP マルチキャスト VLAN と IP アドレスにポートをスタティックに割り当てるには、**mvr** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mvr {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}}

no mvr {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}}

構文の説明

immediate	（任意）ポートの MVR の即時脱退機能をイネーブルにします。この機能をディセーブルにするには、**no mvr immediate** コマンドを使用します。
type	（任意）ポートを MVR レシーバ ポートまたは送信元ポートとして設定します。 デフォルト ポート タイプは、MVR 送信元ポートおよびレシーバ ポートのどちらでもありません。**no mvr type** コマンドは、送信元ポートおよびレシーバ ポートのどちらでもないポートとしてポートをリセットします。
receiver	ポートを、マルチキャスト データの受信だけが可能な加入者ポートとして設定します。レシーバ ポートはマルチキャスト VLAN に属することはできません。
source	ポートを、設定済みのマルチキャスト グループとのマルチキャスト データの送受信が可能なアップリンク ポートとして設定します。スイッチの送信元ポートはすべて単一のマルチキャスト VLAN に属します。 **（注）** トランク ポートを MVR レシーバ ポートとして設定する場合は、送信元ポートをネットワーク ノード インターフェイス（NNI）として、MVR トランク レシーバ ポートをユーザ ノード インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）として設定することを推奨します。
vlan *vlan-id*	システムの mvr vlan を指定します。
group *ip-address*	（任意）指定されたマルチキャスト VLAN ID の指定された MVR IP マルチキャスト グループ アドレスをスタティックに設定します。これは、ポートまたは VLAN 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。
receiver vlan vlan-id	（任意）レシーバ VLAN を指定します。

デフォルト

ポートはレシーバとしても送信元としても設定されません。

即時脱退機能はすべてのポートでディセーブルです。

レシーバ ポートはどの設定済みマルチキャスト グループにも属していません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートが設定されたマルチキャスト グループ向けマルチキャスト データを送受信できるようにする場合は、ポートを送信元ポートとして設定します。マルチキャスト データは送信元ポートとして設定されているすべてのポートで受信されます。

スイッチのレシーバ ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。

MVR に参加していないポートは、MVR レシーバ ポートまたは送信元ポートとして設定しないでください。非 MVR ポートは通常のスイッチ ポートであり、通常のスイッチ動作でマルチキャスト データを送受信することができます。

即時脱退機能がイネーブルの場合、レシーバ ポートはより短時間でマルチキャスト グループから脱退します。即時脱退機能がなく、スイッチがレシーバ ポートのグループから IGMP Leave メッセージを受信した場合、スイッチは、そのポートに IGMP MAC 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 ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能では、IGMP Leave を受信したレシーバ ポートから IGMP MAC ベースのクエリーは送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバ 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、レシーバ装置が 1 つだけ接続されているレシーバ ポートに限定してください。

mvr vlan group コマンドは、IP マルチキャスト アドレスへ送信されたマルチキャスト トラフィックを受信するようにポートをスタティックに設定します。グループのメンバとしてスタティックに設定されたポートは、スタティックに削除されるまではそのグループのメンバのままです。compatible モードでは、このコマンドはレシーバ ポートだけに適用されます。dynamic モードでは送信元ポートにも適用されます。レシーバ ポートは、IGMP Join メッセージを使用してダイナミックにマルチキャスト グループに加入することもできます。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR ポートはプライベート VLAN ポートにはなれません。

例

次の例では、MVR レシーバ ポートとしてポートを設定する方法を示します。

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

設定されたレシーバ ポートおよび送信元ポートを表示するには、**show mvr interface** 特権 EXEC コマンドを使用します。

次の例では、ポートの即時脱退機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 のポートを IP マルチキャスト グループ 228.1.23.4 のスタティック メンバとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 228.1.23.4
```

次の例では、VLAN 100 のポート 2 を IP マルチキャスト グループ 228.1.23.4 のスタティック メンバとして追加する方法を示します。この例では、受信ポートがアクセス ポートです。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 100 group 228.1.23.4
```

次の例では、ポート 5 上で、レシーバ VLAN 201 を MVR VLAN 100 に追加する方法を示します。

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

次に、100 の MVR VLAN の IP マルチキャスト グループ 239.1.1.1 のスタティック メンバとしてポート 5 でレシーバ VLAN 201 を追加する例を示します。

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

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

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上でマルチキャスト VLAN レジストレーションをイネーブルにして、設定します。
show mvr	MVR グローバル パラメータまたはポート パラメータを表示します。
show mvr interface	設定済みの MVR インターフェイスを表示するか、またはレシーバ ポートが所属するマルチキャスト グループを表示します。インターフェイスがメンバであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャスト グループのメンバであるすべてのレシーバ ポートを表示します。

oam protocol cfm svlan

イーサネット仮想接続（EVC）運用管理および保守（OAM）プロトコルを IEEE 801.2ag 接続障害管理（CFM）として設定し、CFM ドメイン レベルのサービス プロバイダー VLAN-ID を識別するには、**oam protocol cfm svlan** EVC コンフィギュレーション コマンドを使用します。EVC の OAM プロトコル設定を削除するには、このコマンドの **no** 形式を使用します。

oam protocol cfm svlan *vlan-id* **domain** *domain-name*

no oam protocol

構文の説明

vlan-id	CFM のサービス プロバイダー VLAN ID。指定できる範囲は 1 ～ 4094 です。
domain *domain-name*	サービス プロバイダー VLAN ID の CFM ドメインを識別します。CFM ドメインが存在しない場合は、コマンドが拒否され、エラー メッセージが表示されます。

デフォルト

EVC に識別されるサービス プロバイダー VLAN はありません。

コマンド モード

EVC コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

domain *domain-name* を入力する場合は、**ethernet cfm domain** *domain-name* **level** *level-id* グローバル コンフィギュレーション コマンドを入力して、CFM ドメインを事前に作成する必要があります。CFM ドメインが存在しない場合は、コマンドが拒否され、エラー メッセージが表示されます。

例

次の例では、EVC コンフィギュレーション モードを開始して、OAM プロトコルを CFM として設定する方法を示します。

```
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 22 domain Operator
```

関連コマンド

コマンド	説明
ethernet evc *evc-id*	EVC を定義し、EVC コンフィギュレーション モードを開始します。
ethernet cfm domain	CFM ドメインを定義し、ドメイン レベルを設定します。

pagp learn-method

EtherChannel ポートから受信する着信パケットの送信元アドレスを学習するには、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp learn-method {**aggregation-port** | **physical-port**}

no pagp learn-method

（注） PAgP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

aggregation-port	論理ポート チャネルで学習するアドレスを指定します。スイッチは、EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートで学習するアドレスを指定します。スイッチは、送信元アドレスを学習したものと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャネルの一方の終端は、特定の宛先 MAC 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスがユーザ ネットワーク インターフェイス（UNI）の場合、**pagp learn-method** を設定する前に、**port-type nni** または **port-type eni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。学習は、リンクの両端で同じ方式に設定する必要があります。

（注） コマンドライン インターフェイス（CLI）で **physical-port** キーワードを指定しても、Cisco CGS 2520 スイッチがサポートするのは、集約ポートでのアドレス ラーニングのみです。**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及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

（注）　Cisco CGS 2520 スイッチへのリンク パートナーが物理ラーナーの場合、物理ポート ラーナーとしてスイッチを設定することを推奨します。**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、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して送信元 MAC アドレスに基づく負荷分散方式を設定します。この状況でだけ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

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

次の例では、学習方式を設定し、EtherChannel 内のポート チャネル上のアドレスを学習する方法を示します。

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

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp port-priority	EtherChannel を経由するすべてのトラフィックが送信されるポートを選択します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

pagp port-priority

EtherChannel を経由するすべての Port Aggregation Protocol（PAgP; ポート集約プロトコル）トラフィックが送信されるポートを選択するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼動状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*

no pagp port-priority

（注） PAgP を使用できるのは、ネットワーク ノード インターフェイス（NNI）および拡張ネットワーク インターフェイス（ENI）上だけです。

構文の説明

priority	プライオリティ番号は 0 ～ 255 です。

デフォルト

デフォルトは 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスがユーザ ネットワーク インターフェイス（UNI）の場合、**pagp port-priority** を設定する前に、**port-type nni** または **port-type eni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

同じ EtherChannel 内で動作可能な最も高いプライオリティを持ち、メンバーシップを持つ物理ポートが、PAgP 送信用として選択されます。

（注） コマンドライン インターフェイス（CLI）で **physical-port** キーワードを指定しても、Cisco CGS 2520 スイッチがサポートするのは、集約ポートでのアドレス ラーニングのみです。**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及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

Cisco CGS 2520 スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの送信元アドレスを学習する機能を提供します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

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て 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。アクセス コントロール リストから指定された Access Control Entry（ACE; アクセス コントロール エントリ）を削除するには、このコマンドの **no** 形式を使用します。

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**]

構文の説明

request	（任意）ARP 要求の照合を要求します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信側 IP アドレスを指定します。
any	すべての IP アドレスまたは MAC アドレスを許可します。
host *sender-ip*	指定された送信側 IP アドレスを許可します。
sender-ip sender-ip-mask	指定された範囲の送信側 IP アドレスを許可します。
mac	送信側 MAC アドレスを指定します。
host *sender-mac*	指定された送信側 MAC アドレスを許可します。
sender-mac sender-mac-mask	指定された範囲の送信側 MAC アドレスを許可します。
response ip	ARP 応答の IP アドレス値を定義します。
host *target-ip*	（任意）指定されたターゲット IP アドレスを許可します。
target-ip target-ip-mask	（任意）指定された範囲のターゲット IP アドレスを許可します。
mac	ARP 応答の MAC アドレス値を指定します。
host *target-mac*	（任意）指定されたターゲット MAC アドレスを許可します。
target-mac target-mac-mask	（任意）指定された範囲のターゲット MAC アドレスを許可します。
log	（任意）ACE と一致するパケットを記録します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードも設定している場合は、一致するパケットはロギングされます。

デフォルト

デフォルト設定はありません。

コマンド モード

ARP アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

permit 句を追加すると、一部の一致条件に基づいて ARP パケットを転送できます。

例

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

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

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

関連コマンド

コマンド	説明
arp access-list	ARP Access Control List（ACL; アクセス コントロール リスト）を定義します。
deny（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

permit（IPv6 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、**permit** IPv6 アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を削除するには、このコマンドの **no** 形式を使用します。

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

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

インターネット制御メッセージ プロトコル

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**] [**routing**] [**sequence** *value*] [**time-range** *name*]

伝送制御プロトコル

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

ユーザ データグラム プロトコル

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*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

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

このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/*prefix-length*	許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	許可条件の設定先である送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	許可条件を設定する宛先 IPv6 ネットワーク、またはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
host *destination-ipv6-address*	許可条件の設定先である宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、初期状態でないフラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

permit（IPv6 アクセス リスト コンフィギュレーション モード）コマンドは、**permit**（IPv4 アクセス リスト コンフィギュレーション モード）コマンドと類似していますが、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、パケットがアクセス リストを通過する条件を定義するには、**ipv6 access-list** コマンドの後ろに **permit**（IPv6）コマンドを使用します。

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

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

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

IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 ネイバー探索を許可します。ICMPv6 ネイバー探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な**拒否**エントリが ACL 内にある必要があります。3 つの暗黙的なステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

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

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

このスイッチは、すべての範囲のプレフィクス長で IPv6 アドレス マッチングをサポートしています。

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

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option

parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

例

次の例では、OUTBOUND および INBOUND という名の IPv6 アクセス リスト 2 つを設定し、そのアクセス リストをレイヤ 3 インターフェイス上の発信および着信トラフィックに適用する方法を示します。OUTBOUND リストの最初と 2 番めの許可エントリは、ネットワーク 2001:ODB8:0300:0201::/64 からの TCP および UDP パケットすべてがインターフェイスで送信されるのを許可します。OUTBOUND リストの拒否エントリは、ネットワーク FE80:0:0:0201::/64 でのすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとして、リンクローカル プレフィクス FE80:0:0:0201 のあるパケット）がインターフェイスで送信されるのを防ぎます。OUTBOUND リストの 3 番めの許可エントリは、すべての ICMP パケットがインターフェイスで送信されるのを許可します。

INBOUND リストの許可エントリは、すべての ICMP パケットをインターフェイスで受信するのを許可します。

```
Switch(config)#ipv6 access-list OUTBOUND
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# permit udp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# deny FE80:0:0:0201::/64 any
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)#ipv6 access-list INBOUND
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter OUTBOUND out
Switch(config-if)# ipv6 traffic-filter INBOUND in
```

（注） **permit any any** ステートメントが OUTBOUND または INBOUND アクセス リストの最後のエントリとして含まれていない場合、TCP、UDP、および ICMP パケットだけがインターフェイスの双方向（受信および送信）で許可されます（アクセス リストの末尾にある、暗黙の条件によりインターフェイス上のその他のパケット タイプはすべて拒否されます）。

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
deny（IPv6 アクセス リスト コンフィギュレーション）	IPv6 アクセス リストに拒否条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

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、**permit** MAC アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を拡張 MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

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

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

（注）　**appletalk** は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

構文の説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または SNAP カプセル化を使用して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、照合を行う前に Ethertype に適用される *don't care* ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を選択します。
amber	（任意）EtherType DEC-Amber を選択します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までの任意の Class of Service（CoS）値を選択します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニング ツリーを選択します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	（任意）EtherType DEC-Diagnostic を選択します。
dsm	（任意）EtherType DEC-DSM を選択します。

etype-6000	（任意）EtherType 0x6000 を選択します。
etype-8042	（任意）EtherType 0x8042 を選択します。
lat	（任意）EtherType DEC-LAT を選択します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を選択します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *mask* は、照合を行う前に LSAP 番号に適用される *don't care* ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を選択します。
mop-dump	（任意）EtherType DEC-MOP Dump を選択します。
msdos	（任意）EtherType DEC-MSDOS を選択します。
mumps	（任意）EtherType DEC-MUMPS を選択します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を選択します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを選択します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。表 2-4 に、Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を一覧表示します。

表 2-4　IPX フィルタ基準

IPX カプセル化タイプ		
Cisco IOS 名	**フレーム タイプ**	**フィルタ基準**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

mac access-list extended グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレス マスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

Access Control Entry（ACE; アクセス コントロール 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。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

（注） 名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、Ethertype 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny（MAC アクセス リスト コンフィギュレーション）	条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定された ACL を表示します。

police

分類したトラフィックにそれぞれポリサーを定義し、ポリシーマップ クラス ポリシング コンフィギュレーション モードを開始するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、超過バースト伝送サイズ、および最大値を超過した場合の対処法を定義します。ポリシーマップ クラス ポリシング コンフィギュレーション モードでは、パケットに複数のアクションを指定できます。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。

（注）　**police rate** キーワードおよび **percent** キーワードはコマンドラインのヘルプに表示されますが、サポートされていません。

police {**cir** *cir-bps* | *rate-bps*} [***burst-bytes***] | **bc** [***burst-value***] | **pir** *pir-bps* **[be** *burst-bytes*] [**conform-action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**violate-action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

no police {**cir** *cir-bps* | *rate-bps*} [***burst-bytes***] | **bc** [***burst-value***] | **pir** *pir-bps* [**be** *burst-bytes*] [**conform-action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**violate-action** [**drop | set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**] [**table** ***table-map name***]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**] [**table** ***table-map name***]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

（注）　**priority** ポリシーマップ クラス コマンドで **police** を使用してプライオリティ キューを無条件にレート制限すると、バースト サイズの値はサポートされず、*rate-bps* 範囲がより小さくなります。デフォルトの適合アクション **transmit** とデフォルトの超過アクション **drop** だけがサポートされます。

構文の説明

cir	トラフィック ポリシングに使用される認定情報レート（CIR）。
cir-bps	bps 単位の CIR レート。指定できる範囲は 8000 ～ 1000000000 bps です。 **（注）** 出力サービス ポリシーの **priority** コマンドで **police** に指定できる範囲は 64000 ～ 1000000000 です。
rate-bps	平均トラフィック伝送速度を b/s で指定します。指定できる範囲は 8000 ～ 1000000000 です。 **（注）** 出力サービス ポリシーの priority コマンドで police に指定できる範囲は 64000 ～ 1000000000 です。
burst-bytes	（任意）通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
bc [*burst- value*]	（任意）適合バースト。許容バースト バイト数。指定できる範囲は 8000 ～ 1000000 バイトです。 バースト値を入力しない場合は、CIR レートで 250 ミリ秒（ms）で送信できるバイト数と等しいバースト値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。
pir *pir-bps*	（任意）トラフィック ポリシングに使用する最大情報レート（PIR）です。指定できる範囲は 8000 ～ 1000000000 b/s です。
be *burst-bytes*	（任意）拡張バースト。許容拡張バースト バイト数。 指定できる範囲は 8000 ～ 1000000 バイトです。
conform-action	（任意）CIR に適合する（CIR 以下の）パケットに実行するアクション。
drop	（任意）パケットをドロップします。 **（注）** 適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。
set-cos-transmit *new-cos-value*	パケットの新しいサービス クラス（CoS）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit *new-dscp-value*	パケットの新しい DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit *new-precedence-value*	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit *qos-group-value*	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	（任意）着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
dscp	（任意）着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
precedence	（任意）着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。

table *table-map name*	（任意）上記の *from-type* キーワードとともに使用します。拡張パケット マーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの *from-type* パラメータに基づき、アクションの *to-type* がマーキングされます。
transmit	（任意）パケットを変更せずに送信します。
exceed-action	（任意）CIR を超過し、PIR 以下のパケットに実行するアクションです。
violate-action	（任意）PIR を超過するパケットに対して実行するアクション。

デフォルト

ポリサーは定義されません。適合バースト（**bc**）は、設定されている CIR で自動的に 250 ミリ秒に設定されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

適合アクション マーキングを設定するには、拡張パケット マーキングを使用し、変更されていないパケットを送信する超過アクションを設定し、明示的な値を使用してマーキングして、拡張パケット マーキングのすべての組み合わせを使用します。拡張パケット マーキングによって、あらゆる着信 QoS マーキングおよびテーブル マップに基づく QoS マーキングが変更されます。また、スイッチは、同じクラスの複数の QoS パラメータのマーキングと適合アクション、超過アクション、および違反アクション マーキングの同時設定をサポートします。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

スイッチは、最大 254 のポリサー プロファイルをサポートします。サポートされているポリサー インスタンスの数は 1024 - 1 で、スイッチ上の合計インターフェイス数より多い数です。複数インスタンスで同じプロファイルを適用できます。

- スイッチのすべてのポートに、256 のポート単位、VLAN 単位ポリシーマップ内の*固有の* VLAN 分類基準を指定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*VLAN label resources exceeded* というエラー メッセージが返されます。
- QoS ACE 分類リソース制限に達するまで、ポート単位およびポート単位、VLAN 単位のポリシーマップをスイッチのすべてのポートに付加できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*TCAM resources exceeded* というエラー メッセージが返されます。
- CPU 保護がイネーブルになっている場合、ポートごとに設定できるポリサーは 45 だけです。**no policer cpu uni all** 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 CPU 保護をディセーブルにし、スイッチをリロードすると、ポート当たり最大 64 のポリサーを設定できます。**show policer cpu uni-eni** {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。詳細については、**policer cpu uni** コマンドを参照してください。
- CPU 保護をディセーブルにする際はこれらの制限事項について注意してください。

- CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上で 62）を、すべてのスイッチの class-default に対して 1 つのポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*policer resources exceeded* というエラー メッセージが返されます。
- CPU 保護をディセーブルにすると、プラットフォームについてスイッチに最大 255 のポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*policer resources exceeded* というエラー メッセージが返されます。
- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

ポリシングは、**priority** ポリシーマップ クラス コンフィギュレーション コマンドでプライオリティ キューの帯域幅を削減するように設定された入力ポリシーまたは出力ポリシーだけでサポートされます。

（注） 出力ポリシーの **priority** コマンドで使用する場合、ポリシング レートの範囲は 64000 ～ 1000000000 bps です。ただし、コマンドライン インターフェイスのヘルプに表示される範囲は 8000 ～ 1000000000 です。範囲外のレートでは、出力サービス ポリシーを付加できません。

出力ポリシー マップは、元の値ではなく、アウトオブプロファイル トラフィックの変更された値にのみ一致する必要があります。

複数の適合アクションまたは超過アクションを設定するには、ポリシーマップ クラス ポリシング コンフィギュレーション モードを開始し、**conform-action**、**exceed-action**、および **violate-action** ポリシーマップ クラス ポリシング コンフィギュレーション コマンドを使用します。

violate-action を設定しない場合、デフォルトで違反クラスが超過アクションと同じアクションに割り当てられます。

ポリサーを定義し、Enter キーを押すと、複数のポリシング アクションを設定できるポリシーマップ クラス ポリシング コンフィギュレーション モードが開始されます。

- **conform-action**：CIR に適合する（CIR 以下の）パケットで実行するアクション。デフォルトのアクションは、パケットの**送信**です。詳細については、**conform-action** ポリシーマップ クラス police コマンドを参照してください。
- **exceed-action**：CIR を超過し、PIR 以下のパケットに実行するアクション。デフォルトのアクションは、パケットの**ドロップ**です。 詳細については、**exceed-action** ポリシーマップ クラス police コマンドを参照してください。
- **violate-action**：PIR を超過するパケットで実行するアクション。デフォルトのアクションは、**パケットのドロップ**です。 詳細については、**violate-action** ポリシーマップ クラス police コマンドを参照してください。
- **exit**：QoS ポリシーマップ クラス ポリシング コンフィギュレーション モードを終了します。複数のアクションを設定しない場合、他のポリシーマップ クラス police コマンドを入力しないで **exit** を入力できます。
- **no**：コマンドを無効にするか、デフォルトに設定します。

例

次に、バースト サイズが 20 KB の 1-Mb/s 平均レートでポリサーを設定する例を示します。ポリサーは、パケットがレートに準拠している場合は新しい DSCP precedence 値を設定し、トラフィックがレートを超過した場合はパケットをドロップします。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class inclass1
Switch(config-pmap-c)# police cir 1000000 20000 conform-action set-dscp-transmit 46
exceed-action drop
Switch(config-pmap-c)# exit
```

次に、ポリシーマップ コンフィギュレーション モードを使用して 2-rate、3-color ポリシングを設定する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit
exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードで同じ設定を作成する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
conform-action	CIR または PIR を満たし、レートが適合バーストよりも低いパケットのポリシーマップ クラスに対して複数のアクションを定義します。
exceed-action	CIR または PIR を超過し、適合値と超過バーストの間のレートを持つパケットのポリシーマップ クラスに対して複数のアクションを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
violate-action	CIR および PIR を超過し、適合レート + 超過バーストを超過するレートを持つパケットのポリシーマップ クラスに対して複数のアクションを定義します。
show policy-map	QoS ポリシー マップを表示します。

policer aggregate（グローバル コンフィギュレーション）

集約ポリサーを作成して、入力ポリシー マップ内の複数のクラスにおけるすべてのトラフィックのポリシングを行うには、**policer aggregate** グローバル コンフィギュレーション コマンドを使用します。集約ポリサーは、同一ポリシー マップ内の複数のクラスで共有できます。ポリサーは、最大許容伝送速度または認定情報レート、最大バースト伝送サイズ、および最大値に達するか超過した場合の対処法を定義します。指定されたポリサーを削除するには、このコマンドの **no** 形式を使用します。

policer aggregate *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [**bc** *burst- value*]| [**pir** *pir-bps* **[be** *burst-bytes*]] [**conform-action** [**drop** |**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos | dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed-action** [**drop | set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos | dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] **[violate-action** [**drop |** **set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

no policer aggregate *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [**bc** *burst- value*] | [**pir** *pir-bps* **[be** *burst-bytes*]] [**conform-action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos | dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos | dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**violate-action** [**drop |** **set-cos-transmit** {***new-cos-value*** | [**cos** | **dscp** | **precedence**]} | **set-dscp-transmit** {***new-dscp-value*** | [**cos | dscp** | **precedence**]} | **set-prec-transmit** {***new-precedence-value*** | [**cos** | **dscp** | **precedence**]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

構文の説明

aggregate-policer-name	集約ポリサーの名前です。
rate-bps	平均トラフィック伝送速度をビット / 秒（b/s）で指定します。指定できる範囲は 8000 ～ 1000000000 です。
cir *cir-bps*	認定情報レート（CIR）（b/ s）。指定できる範囲は、8000 ～ 1000000000 b/s です。

bc *burst- value*	（任意）適合バースト。許容バースト バイト数。指定できる範囲は 8000 ～ 1000000 バイトです。 バースト値を入力しない場合は、CIR レートで 250 ミリ秒（ms）で送信できるバイト数と等しいバースト値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。
pir *pir-bps*	（任意）トラフィック ポリシングに使用する最大情報レート（PIR）です。指定できる範囲は 8000 ～ 1000000000 b/s です。
be *burst-bytes*	（任意）拡張バースト。許容拡張バースト バイト数。指定できる範囲は 8000 ～ 1000000 バイトです。
conform-action	（任意）CIR に適合する（CIR 以下の）パケットに実行するアクション。
drop	（任意）パケットをドロップします。 **（注）**　適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。
set-cos-transmit *cos-value*	パケットの新しいサービス クラス（CoS）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit *dscp-value*	パケットの新しい DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit *precedence-value*	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit *qos-group-value*	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキング アクションの *to-type* が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	（任意）着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
dscp	（任意）着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
precedence	（任意）着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキング アクションの *from-type* が指定されます。
table *table-map name*	（任意）上記の *from-type* キーワードとともに使用します。拡張パケット マーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの *from-type* パラメータに基づき、アクションの *to-type* がマーキングされます。 **（注）**　テーブル マップは、違反アクションでサポートされません。
transmit	（任意）パケットを変更せずに送信します。

exceed-action	（任意）CIR を超過し、PIR 以下のパケットに実行するアクションです。
violate-action	（任意）PIR を超過するパケットに対して実行するアクション。

デフォルト

集約ポリサーは定義されません。

集約ポリサーを設定すると、適合バースト（**bc**）は、設定されている CIR で自動的に 250 ミリ秒に設定されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

適合アクション マーキングを設定するには、拡張パケット マーキングを使用し、変更されていないパケットを送信する超過アクションと違反アクションを設定し、明示的な値を使用してマーキングして、拡張パケット マーキングのすべての組み合わせを使用します。拡張パケット マーキングによって、あらゆる着信 QoS マーキングおよびテーブル マップに基づく QoS マーキングが変更されます。また、スイッチは、同じクラスの複数の QoS パラメータのマーキングと適合アクション、超過アクション、および違反アクション マーキングの同時設定をサポートします。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

violate-action を設定しない場合、デフォルトで違反クラスが**超過アクション**と同じアクションに割り当てられます。

スイッチでは、最大 254 の一意の集約ポリサーをサポートしています。

集約ポリシングは、入力ポリシー マップでだけサポートされます。

exceed-action のテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。

複数の適合、超過、違反アクションを集約ポリサーに **policer aggregate** グローバル コンフィギュレーション コマンドのパラメータとして同時に設定できますが、次の順序でアクションを入力する必要があります。

- **drop**、または **transmit** あるいは **set** アクションは、**conform-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

  set-dscp-transmit または **set-prec-transmit**

  set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**exceed-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

  set-dscp-transmit または **set-prec-transmit**

set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**violate-action** のあとに次の順序で入力する必要があります。

  set-qos-transmit

  set-dscp-transmit または **set-prec-transmit**

  set-cos-transmit

出力ポリシー マップは、元の値ではなく、アウトオブプロファイル トラフィックの変更された値にのみ一致する必要があります。

集約ポリサーを設定すると、特定のバースト サイズおよび適合アクションと超過アクションを設定できます。バースト サイズ（**bc**）を指定しない場合は、CIR レートで 250 ミリ秒で送信できるバイト数と等しい適切なバースト サイズ値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。

例

次に、*agg-pol-1* という名前の集約ポリサーを設定し、ポリシー マップ内の複数のクラスに付加する例を示します。

```
Switch(config)# policer aggregate agg-pol-1 10900000 80000 exceed-action drop
Switch(config)# class-map test1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map test2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy map testexample
Switch(config-pmap)# class test1
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-cmap-c)# exit
Switch(config-pmap)# class test2
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-9map)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

次に、2-rate、3-color 集約ポリサーを作成し、ポリシー マップ内の複数のクラスに付加する例を示します。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# policer aggregate example cir 10900000 pir 80000000 conform-action
transmit exceed-action drop violate-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
```

```
Switch(config-if)# exit
```

設定を確認するには、**show aggregate-policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policer aggregate	集約ポリサーの設定を表示します。

police aggregate（ポリシーマップ クラス コンフィギュレーション）

同一のポリシー マップにある複数のクラスに集約ポリサーを適用するには、**police aggregate** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。指定されたポリサーを削除するには、このコマンドの **no** 形式を使用します。

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

構文の説明

aggregate-policer-name	集約ポリサーの名前です。

デフォルト

集約ポリサーは定義されません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチ上では、ポートに関連付けられた最大 229 のポリサー インスタンスがサポートされます（228 のユーザ設定可能なポリサーと、1 つの内部使用に予約されたポリサー）。CPU 保護がイネーブルになっている場合（デフォルト）、ポート当たり 45 の入力ポリサーを設定できます。**no policer cpu uni all** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードして CPU 保護をディセーブルにすると、ユーザ定義クラスにはポート当たり最大 64 の入力ポリサー（すべての 4 番目のポート上で 63 ポリサー）を設定できます。詳細については、**policer cpu uni** コマンドを参照してください。

集約ポリシングは、入力ポリシー マップにだけ適用されます。

集約ポリサーは、個別のポリサーとは異なり、ポリシー マップ内の複数のトラフィック クラスで共有されます。インターフェイスに適用されたポリシー マップ内の複数のクラスにおけるトラフィック ストリームをポリシングするには、集約ポリサーを使用します。集約ポリシングは、複数のインターフェイス上のトラフィック ストリームの集約には使用できません。

1 つのポリシー マップだけが、任意の特定の集約ポリサーを使用できます。

例

次に、集約ポリシングをデフォルトのアクションを使用して設定し、同じポートのすべてのクラスに適用する例を示します。

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class in-class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class in-class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

設定を確認するには、**show aggregate policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policer aggregate	集約ポリサーの設定を表示します。

policer cpu uni

CPU 保護をイネーブルまたはディセーブルにし、スイッチのすべてのユーザ ネットワーク インターフェイス（UNI）および拡張ネットワーク インターフェイス（ENI）の CPU ポリシングしきい値を設定するには、**policer cpu uni** グローバル コンフィギュレーション コマンドを使用します。デフォルトレートに戻す場合、または CPU 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。

policer cpu uni {all | *rate-bps*}

no policer cpu uni {all | *rate-bps*}

構文の説明

all	CPU 保護をイネーブルまたはディセーブルにするには、このキーワードを入力します。CPU 保護をディセーブルにすると、ポートごとに 45 ではなく 64 のポリサーを設定できます。
rate-bps	CPU ポリシングしきい値をビット/秒（b/s）で指定します。指定できる範囲は 8000 ～ 409500 です。

デフォルト

CPU 保護がイネーブルになります。デフォルトのポリシングしきい値は 160000 b/s 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

偶発的または意図的な CPU 過負荷から保護するために、スイッチでは UNI および ENI の事前定義された 1 組のレイヤ 2 制御パケットおよび一部のレイヤ 3 制御パケットをドロップまたはレート制限することにより、自動的に CPU 保護またはコントロール プレーン セキュリティを実現します。スイッチは、CPU 保護のため、0 ～ 26 の番号が指定された 27 のコントロール プレーンのセキュリティ ポリサーを事前に割り当てます。ポリサー 26 は、廃棄ポリサーを意味します。ポリサー 0 ～ 25 は、ポートが制御プロトコルのレート制限ポリサーを使用することを意味します。

CPU ポリサーは事前に割り当てられています。**policer cpu uni** *rate-bps* コマンドを使用してレート制限しきい値だけを設定できます。設定されたしきい値は、すべての制御プロトコルおよびすべての UNI と ENI 適用されます。

CPU 保護ポリシングは、ポートごとに 19 のポリサーを使用します。これにより、ポートに最大 45 の入力ポリサーを付加することができます。ポートで 45 を超えるポリサーが必要な場合、45 を超えるポリサーを持つポリシー マップを付加する前に、**no cpu policer uni all** 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、CPU 保護をディセーブルにできます。CPU 保護をディセーブルにすると、ポートに最大 64 の入力ポリサーを付加できます。

- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

（注）　スイッチの各 4 ポート（ポート 1 ～ 4、5 ～ 8 など）では、最初の 3 ポートは、64 のポリサーをサポートしますが、4 番目のポートは、63 のポリサーだけをサポートできます。

CPU 保護機能をディセーブルまたはイネーブルにする場合、設定が反映される前に **reload** 特権 EXEC コマンドを入力することによって、スイッチをリロードする必要があります。

（注）　CPU 保護をオフにするとプロトコル パケットが CPU に到達可能となり、これが、CPU 処理の過負荷や、ソフトウェアによるストーム制御の原因となる可能性があります。

show policer cpu uni-eni {**drop** | **rate**} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。

コントロールプレーン セキュリティの詳細については、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

次に、CPU 保護しきい値を 10000 b/s に設定し、その設定を確認する例を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
```

設定を確認するには、**show policer cpu uni-eni rate** 特権 EXEC コマンドを入力します。

次に、CPU 保護をディセーブルにしてスイッチをリロードする例を示します。

```
Switch(config)# no policer cpu uni all
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

次に、CPU 保護がディセーブルの場合の **show policer cpu uni-eni rate** 特権 EXEC コマンドの出力例を示します。

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

関連コマンド

コマンド	説明
show policer cpu uni-eni rate	コントロールプレーン セキュリティ用に設定されたポリサーしきい値を表示します。

policy-map

複数の物理ポートに適用できるポリシーマップを作成または変更し、ポリシーマップ コンフィギュレーション モードを開始するには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。既存のポリシー マップを削除する場合は、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*

no policy-map *policy-map-name*

構文の説明

policy-map-name	ポリシー マップ名です。

デフォルト

ポリシー マップは定義されません。デフォルトでは、パケットは変更せずに送信されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチでは、最大 256 の一意のポリシー マップをサポートしています。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して、作成または変更するポリシー マップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシーマップのクラス ポリシーを設定または変更することができます。

policy-map コマンドを入力すると、ポリシーマップ コンフィギュレーション モードになり、次のコンフィギュレーション コマンドが使用可能になります。

- **class** : ポリシーのアクションが適用される指定トラフィック分類。分類は、**class-map** 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ます。詳細については、**class-map** コマンドを参照してください。
- **description** : ポリシー マップを説明します（最大 200 文字）。
- **exit** : ポリシーマップ 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。

（注） **no** policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。次に例を示します。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラス マップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

入力ポリシー マップおよび出力ポリシー マップを作成し、ポートに、入力ポリシー マップおよび出力ポリシー マップを 1 つずつ割り当てることができます。入力ポリシー マップは、ポート上の着信トラフィックに作用します。出力ポリシー マップは、発信トラフィックに作用します。

複数の物理ポートに対して、同一のポリシーマップを適用することができます。

入力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- スイッチのインターフェイスに付加できる入力ポリシー マップの合計数は、ハードウェア リソースのアベイラビリティにより制限されます。いずれかのハードウェア リソースの制限を超過する入力ポリシー マップを付加しようとすると、設定エラーになります。
- 入力ポリシー マップの最大クラス マップ数は 64 + **class-default** です。
- 1 つのポリシー マップ内の IP（IP 標準および拡張 ACL、DSCP または IP precedence）と非 IP（MAC ACL または CoS）分類を 1 つのクラス マップ内、またはポリシー マップ内のクラス マップにわたって設定することはできません。
- **service-policy input** ポリシーマップ コンフィギュレーション コマンドを使用してインターフェイスに入力ポリシー マップを付加した後に、入力ポリシー マップをインターフェイスから取り外さないでポリシーを変更できます。分類基準、クラス、またはアクションの追加または削除、もしくは設定されたアクション（ポリサー、レート、マッピング、マーキングなど）のパラメータの変更を行うことができます。
- **match qos-group** コマンド、クラスベース均等化キューイング（CBWFQ）の **bandwidth** コマンド、クラスベース プライオリティ キューイングの **priority** コマンド、重み付きテール ドロップ（WTD）の **queue-limit** コマンド、ポート シェーピングの **shape average** コマンド、クラスベース トラフィック シェーピングは、入力ポリシー マップでサポートされていません。

出力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- 出力ポリシー マップには、最大 4 つのクラス（1 つは **class-default**）を含めることができます。
- スイッチは、スイッチ上の各ポートに固有の出力ポリシー マップの設定および付加をサポートしています。ただし、これらの出力ポリシー マップには、それぞれキュー制限を 3 つしか設定できません。これら 3 つの固有のキュー制限設定は、スイッチ ポート数に応じた数の出力ポリシー マップに含めることができます。4 つ目のキュー制限設定を含む出力ポリシー マップを付加しようとすると、エラー メッセージが表示され、付加は許可されません。帯域幅、プライオリティ、またはシェーピングの設定には制限はありません。
- すべての出力ポリシー マップには、同じ数のクラス マップ（1 ～ 3）と同じ分類（つまり、同じクラス マップ）を含める必要があります。
- **service-policy output** インターフェイス 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に出力ポリシー マップを付加した後は、設定済みアクションのパラメータ（レート、パーセンテージなど）を変更すること、または、インターフェイスにポリシー マップが付加されている場合にクラス マップの分類基準を追加または削除することのみができます。クラスまたはアクションを追加、削除するには、すべてのインターフェイスからポリシー マップを消去して、変更し、再度インターフェイスに付加する必要があります。
- **match access-group** コマンド、マーキングの **set** コマンド、および **priority** コマンドを含まないポリシングの **police** コマンドは、出力ポリシー マップでサポートされていません。

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 ガイドを参照してください。

例

次に、3 つのクラスの入力ポリシー マップを作成する例を示します。

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

次に、レート制限が gold クラスのプライオリティを指定し、残りの帯域幅の少なくとも 20% を silver クラスに、10% を bronze クラスに保証する出力ポリシー マップを設定する示します。

```
Switch(config)# policy-map output-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

次の例では、ポリシー マップ *output-2* を削除する方法を示します。

```
Switch(config)# no policy-map output-2
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
service-policy（インターフェイス コンフィギュレーション）	ポートにポリシー マップを適用します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。

port-channel load-balance

EtherChannel のポート間で負荷分散方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

no port-channel load-balance

構文の説明

dst-ip	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 アドレスに基づいた負荷分散。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいた負荷分散。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散。
src-mac	送信元 MAC アドレスに基づいた負荷分散。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。

デフォルト

デフォルトは、**src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

これらの転送方式をどのような場合に使用するかについての詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、負荷分散方式を **dst-mac** に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show running-config	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「**Cisco IOS Commands Master List, Release 12.2**」を選択して、コマンドの項目へ移動します。

port-type

既存のポートタイプからネットワーク ノード インターフェイス（NNI）、ユーザ ネットワーク インターフェイス（UNI）、または拡張ネットワーク インターフェイス（ENI）にポート タイプを変更するには、**port-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。ポートをデフォルト値設定に戻すには、このコマンドの **no** 形式を使用します。

port-type {**eni** | **nni** | **uni**}

no port-type

構文の説明

eni	拡張ネットワーク インターフェイス。ENI は、デフォルト設定が UNI と同じですが、設定により Cisco Discovery Protocol（CDP）、スパニング ツリー プロトコル（STP）、リンク層検出プロトコル（LLDP）、および EtherChannel のリンク集約制御プロトコル（LACP）またはポート集約プロトコル（PAgP）用のプロトコル制御パケットをサポートできます。
nni	ネットワーク ノード インターフェイス。
uni	ユーザ ネットワーク インターフェイス。

デフォルト

コンフィギュレーション ファイルが存在しない場合は、すべての 10/100 ポートは、UNI で、小型フォーム ファクタ（SFP）モジュール スロットは NNI です。ポートは、ENI ポートとなるように設定します。

ENI として設定されたポートに UNI ポートと同じデフォルトがあっても、ENI の制御プロトコル（CDP、STP、LLDP、LACP と PAgP）を設定できます。これらのプロトコルは、UNI ではサポートされていません。

UNI または ENI のデフォルト ステータスは、スイッチを設定する場合に無許可のユーザが他のポートにアクセスするのを防止するため、管理上のダウンとなっています。これを設定する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して、UNI または ENI をイネーブルする必要があります。

NNI のデフォルト ステータスは管理上アップであり、サービス プロバイダーは初期設定時にリモート スイッチへのアクセスを許可されます。

ポートを ENI として設定すると、ポートの管理ステートは変わりません。ポートタイプの変更前にポート ステートが**シャットダウン**の場合は、**シャットダウン** ステートのままとなります。ステートが**シャットダウン以外**の場合は **シャットダウン以外の**ステートのままとなります。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートが別のポート タイプに再設定できます。別のインターフェイス タイプとして再設定されるポートは、現在のインターフェイス タイプの特性をすべて継承します。デフォルトでは、スイッチのすべてのポートは、UNI または NNI です。すべてのポートは常に、UNI、NNI、または ENI です。

一部の機能は、すべてのポート タイプでだけサポートされされていません。制御プロトコル（CDP、STP、LLDP、EtherChannel LACP および PAgP）のサポートは、ポート タイプによって異なります。

- NNI では、これらの機能はデフォルトでイネーブルになっています。
- ENI 上では、これらの機能はデフォルトでディセーブルになっていますが、コマンドライン インターフェイスを使用して、イネーブルにできます。
- これらの機能は、UNI ではサポートされていません。

特定の機能のサポートについては、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。1 つのタイプから別のタイプにポートを変更する場合、特定のインターフェイスの設定オプションの矛盾を防ぐために、ポート タイプに特化した機能が設定から削除されます。

スイッチのすべてのポートは UNI または ENI にすることができますが、スイッチでメトロ アクセス イメージが稼動している場合、4 つのポートを同時に NNI にすることができます。スイッチでメトロ IP アクセス イメージが稼動している場合、すべてのポートを NNI として設定できます。

no port-type インターフェイス コンフィギュレーション コマンドまたは **default port-type** インターフェイス コンフィギュレーション コマンドを入力すると、ポートがデフォルト ステート（ファスト イーサネット ポートの場合は UNI、ギガビット イーサネット ポートの場合は NNI）に戻ります。

トラフィックは UNI または ENI の間ではスイッチングされません。また、UNI または ENI に着信するすべてのトラフィックは、ユーザが別のユーザのプライベート ネットワークにアクセスするのを防止するため、NNI から発信される必要があります。スイッチ内でトラフィックを 2 つ以上の UNI または ENI により交換するのが適切であれば、インターフェイスをコミュニティ VLAN に割り当てることができます。コミュニティ VLAN には、最大 8 つの UNI または ENI を含めることができます。同じコミュニティ VLAN に UNI および ENI を混在させることは推奨しません。

VLAN の設定の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、ポートを NNI に変更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 fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

次の例では、ポート タイプを ENI に変更する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# end
```

関連コマンド

コマンド	説明
no shutdown	インターフェイスをイネーブルにします。
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。
show port-type	インターフェイスのポート タイプを表示します。

power inline

Power over Ethernet（PoE）ポート上で電力管理モードを設定にするには、スイッチで **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** | **police [action log]** | **port** ***maximum*** | **static** [**max** *max-wattage*]}

no power inline {**auto** | **never** | **police** | **port** | **static**}

構文の説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。
max *max-wattage*	（任意）ポートに供給される電力を制限します。指定できる範囲は 4000 ～ 15400 mW です。値を指定しない場合は、最大電力が供給されます。
never	装置の検出とポートへの電力供給をディセーブルにします。
police [**action log**]	リアルタイムの消費電力のポリシングをイネーブルにします。これらのキーワードの詳細については、**power inline police** コマンドを参照してください。
static	受電装置の検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます（確保します）。
port *maximum*	ポートの最大電力レベル値（20 W まで）を設定します。

デフォルト

デフォルトの設定は **auto**（イネーブル）です。

最大ワット数は、15400 mW です。

コマンド デフォルト

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline auto
                   ^
% Invalid input detected at '^' marker.
```

max *max-wattage* オプションを使用して、受電装置の電力が制限を超えないようにします。この設定によって、受電装置が最大ワット数より多い電力を要求する Cisco Discovery Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル パワー バジェットに送られます。

（注）　**power inline max** *max-wattage* コマンドが 15.4 W 未満に設定されている場合、スイッチはクラス 0 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供給を拒否する場合（受電装置が CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは power-deny ステートになります。スイッチはシステム メッセージを生成し、**show power inline** 特権 EXEC コマンド出力の Oper カラムに *power-deny* が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max** *max-wattage* コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。電力が事前割り当てされているので、最大ワット数以下の電力を使用する受電装置は、スタティック ポートに接続されていれば電力が保証されます。ただし、受電装置の IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電装置が最大ワット数を超えた量を要求していることをスイッチが認識すると、受電装置がシャットダウンします。

（注）　Cisco IOS Release 12.2(53)EX 以降のリリースでは、拡張 PoE がサポートされます。**power inline port *maximum*** インターフェイス コンフィギュレーション コマンドを使用して、最大電力レベルが 20 ワットのデバイスをサポートできます。

ポートが static モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、パワー バジェット全体がすでに別の自動ポートまたはスタティック ポートに割り当てられているなど）、次のメッセージが表示されます。`Command rejected: power inline static: pwr not available`。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電装置であるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定する場合、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコの受電装置が接続されている場合は、**power inline never** コマンドでポートを設定しないでください。不正なリンクアップが生じ、ポートが errdisable ステートになる可能性があります。

power inline never コマンドで設定したポートにシスコの受電装置を接続しないでください。

例

次の例では、スイッチ上で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 gigabitethernet1/0/2
Switch(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電装置を受け入れるように、スイッチ上で PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、スイッチ上で PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline never
```

次の例では、接続されたデバイスに 20 W を提供するようにポートを設定する方法を示します。

```
Switch(config-if)# power inline port maximum 20000
```

設定を確認するには、**show power inline** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
show controllers power inline	指定した PoE コントローラのレジスタ値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline consumption

各受電デバイスが使用するワット数を指定することにより、デバイスの IEEE 分類によって指定された電力量を無効にするには、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

（注）　**default** キーワードは、グローバル コンフィギュレーション コマンドでだけ表示されます。

構文の説明

wattage	スイッチがポート用に確保する電力を指定します。指定できる範囲は 4000 ～ 15400 mW です。

デフォルト

Power over Ethernet（PoE）ポートのデフォルトの電力は 15400 mW 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol（CDP）を使用して装置が消費する *CDP 独自の*電力量を決定し、CDP メッセージに基づいて電力バジェットを調整します。これに従って、スイッチは電力バジェットを調整します。この機能は、IEEE サードパーティの受電装置には適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じてパワー バジェットを調整します。受電装置が Class 0（クラス ステータスは不明）または Class 3 である場合、CDP 独自で必要な電力量に関係なく、スイッチはポート用に 15400 mW の電力を確保します。受電装置が CDP 固有の消費よりも高いクラスを報告してきたり、または電力分類（デフォルトはクラス 0）をサポートしていない場合、スイッチは IEEE クラス情報を使用してグローバル電力バジェットを追跡するため、電力供給できるデバイスが少なくなります。

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で、IEEE 分類のデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル パワー バジェットに入れられます。したがって、スイッチのパワー バジェットを拡張してもっと効率的に使用できます。

power inline consumption *wattage* コンフィギュレーション コマンドを入力する前に、**power inline police** [**action log**] インターフェイス コンフィギュレーション コマンドを使用してリアルタイムの電力消費のポリシングをイネーブルにすることを推奨します。

注意　慎重にスイッチのパワー バジェットを計画し、電源装置がオーバーサブスクライブ状態にならないようにしてください。

power inline consumption default *wattage* または **no power inline consumption default** グローバル コンフィギュレーション コマンドを入力するか、**power inline consumption** *wattage* または **no power inline consumption** インターフェイス コンフィギュレーション コマンドを入力すると、次の注意メッセージが表示されます。

```
%CAUTION: Interface 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.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```

（注）　手動でパワー バジェットを設定する場合、スイッチと受電装置の間のケーブルでの電力消失を考慮する必要があります。

IEEE 分類に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

このコマンドは、PoE 対応ポートだけでサポートされています。PoE をサポートしていないスイッチまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

例

次の例では、グローバル コンフィギュレーション コマンドを使用して、各 PoE ポートに 5000 mW の電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline  consumption/allocation'
command may cause damage to the switch and void  your warranty.Take precaution not to
oversubscribe the power supply.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```

次の例では、インターフェイス コンフィギュレーション コマンドを使用して、特定の PoE ポートに接続された受電装置に 12000 mW の電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline consumption 12000
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline  consumption/allocation'
command may cause damage to the switch and void  your warranty.Take precaution not to
oversubscribe the power supply.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```

設定を確認するには、**show power inline consumption** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
power inline	PoE ポート上で電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline police

リアルタイム電力消費のポリシングをイネーブルにするには、スイッチで **power inline police** インターフェイス コンフィギュレーション コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

power inline police [action log]

no power inline police

構文の説明

action log	（任意）リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、スイッチは接続された装置に電力を供給しながら Syslog メッセージを生成します。 **action log** キーワードを入力しない場合に、リアルタイムの電力消費がポートの最大電力割り当てを超過すると、スイッチはポートへの電力供給をオフにします（デフォルトのアクション）。

デフォルト

受電装置のリアルタイムの電力消費のポリシングは、ディセーブルです。スイッチは、リアル タイムの電力消費をポリシングしません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Power of Ethernet（PoE）対応ポートのみでサポートされています。PoE をサポートしていないスイッチまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

power inline police [**action log**] コマンドは、PoE ポートを備えたスイッチのみでサポートされています。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電装置が割り当てられた最大電力より多くの量を消費すると、スイッチが対処します。

PoE がイネーブルである場合、スイッチは受電装置のリアルタイムの電力消費を検知します。この機能は、*パワー モニタリング*または*パワー センシング*といわれます。また、スイッチは*パワー ポリシング*機能を使用して消費電力をポリシングします。

電力ポリシングがイネーブルの場合、スイッチは次の順序でいずれかの値を PoE ポートでのカットオフ電力の値とします。

1. スイッチがポートに対して予定しているユーザ定義電力レベルを設定している場合は、**power inline consumption default** *wattage* グローバル コンフィギュレーション コマンドまたは **power inline consumption** *wattage* インターフェイス コンフィギュレーション コマンドを使用して手動で行う。

2. ポートで許可されている電力を制限するユーザ定義電力レベルを設定している場合は、**power inline auto max** *max-wattage* または **power inline static max** *max-wattage* インターフェイス コンフィギュレーション コマンドを使用して手動で行う。
3. スイッチにおいてデバイスの電力消費が設定されている場合は、CDP 電力ネゴシエーションまたは IEEE 分類を使用して自動的に行われる。
4. スイッチにおいて電力消費がデフォルト値の 15.4 W に設定されている場合は自動的に行われる。

   power inline consumption default *wattage* グローバル コンフィギュレーション コマンド、**power inline consumption** *wattage* インターフェイス コンフィギュレーション コマンド、または **power inline** [**auto** | **static max**] *max-wattage* コマンドを入力して、カットオフ電力値を手動で設定するには、上記リストの 1 番めおよび 2 番めの方式を使用します。カットオフ電力値を手動で設定しない場合、スイッチは CDP 電力ネゴシエーションまたは受電装置の IEEE 分類を使用して、自動的に値を求めます。これは前述のリストの 3 番めの方法です。スイッチがこれらのいずれかの方法によっても値を求めることができない場合、スイッチはデフォルト値の 15.4 W（前述のリストの 4 番めの方法）を使用します。

（注） カットオフ電力値、スイッチが使用する電力消費値、および接続装置の実際の電力消費値については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章の「Power Monitoring and Power Policing」の項を参照してください。

パワー ポリシングがイネーブルである場合、スイッチはリアルタイムの電力消費を PoE ポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（または*カットオフ電力*）を超える電力をポートで使用している場合、スイッチでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながら Syslog メッセージが生成されて LED（ポート LED はオレンジ色に点滅）が更新されます。

- ポートへの電力供給をオフにして、ポートを errdisable ステートとするようスイッチを設定するには、**power inline police** インターフェイス コンフィギュレーション コマンドを使用します。
- 装置に電力を供給しながら、Syslog メッセージを生成するようスイッチを設定するには、**power inline police action log** コマンドを使用します。

  action log キーワードを入力しない場合のデフォルトのアクションは、ポートのシャット ダウン、ポートへの電力供給のオフ、およびポートを PoE errdisable ステートに移行、になります。PoE ポートを errdisable ステートから自動的に回復するよう設定するには、**errdisable detect cause inline-power** 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、PoE 原因に対する errdisable 検出をイネーブルにして、**errdisable recovery cause inline-power interval** *interval* グローバル コンフィギュレーション コマンドを使用して、PoE errdisable 原因の回復タイマーをイネーブルにします。

注意 ポリシングがディセーブルである場合、受電装置がポートに割り当てられた最大電力より多くの量を消費しても対処されないため、スイッチに悪影響を与える場合があります。

例

次の例では、電力消費のポリシングをイネーブルにして、スイッチの PoE ポートで Syslog メッセージを生成するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline police action log
```

設定を確認するには、**show power inline police** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause inline-power	PoE 原因に対する errdisable 検出をイネーブルにします。
errdisable recovery cause inline-power	PoE 回復メカニズム変数を設定します。
power inline	PoE ポート上で電力管理モードを設定します。
power inline consumption	IEEE 分類によって受電装置に指定された電力量を上書きします。
show power inline police	リアルタイムの電力消費に関するパワー ポリシング情報を表示します。

priority

出力ポリシー マップに属するトラフィックのクラスに対してクラスベース プライオリティ キューイングを設定するには、**priority** 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。スイッチでは、完全プライオリティ キューイングまたは **police** ポリシーマップ コマンドと併用されるプライオリティをサポートしています。クラスに指定されているプライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority

no priority

（注） **priority** ポリシーマップ クラス コマンドで **police** コマンドを使用してプライオリティ キューを無条件にレート制限すると、**police** コマンドでバースト サイズの値はサポートされません。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

単独で使用されている場合（**police** ポリシーマップ コマンドの前ではなく）、**priority** コマンドは低遅延パスにトラフィックを割り当て、クラスに属するパケットの遅延が設定可能な最小遅延になるようにします。完全プライオリティ キューイングを使用すると、プライオリティ キューのパケットはキューが空になるまでスケジューリングされ、送信されます。

（注） **policy** コマンドなしで **priority** コマンドを使用する際は注意してください。完全プライオリティ キューイングを過剰に使用すると、他のキューで輻輳が発生する場合があります。

プライオリティ キューで使用される帯域幅を削減するには、**priority** を **police** {*rate-bps* | **cir** *cir-bps*} ポリシーマップ コマンドと併用します。これは、出力ポリシー マップでサポートされる唯一のポリシング形式です。このようにコマンドを組み合わせて、プライオリティ キューの最大レートを設定します。また、他のクラスに **bandwidth** および **shape average** の各ポリシーマップ コマンドを使用すると、他のキューのトラフィック レートを割り当てることができます。

（注） 出力ポリシーで **police** コマンドと **priority** コマンドを併用する場合に、コマンドライン ヘルプで表示される範囲が 8000 ～ 1000000000 bps であっても、ポリシング レートの範囲は 64000 ～ 1000000000 bps です。出力サービス ポリシーを付加しようとすると、設定済みのバースト サイズは無視されます。

出力ポリシー マップに **police** コマンドを使用せずにプライオリティを設定する場合に他のキューを設定するには、**bandwidth remaining percent** ポリシーマップ コマンドを使用して、共有するしかありません。このコマンドは、割り当てられた帯域幅を保証しませんが、分散レートは保証されます。

出力ポリシー マップに **police** コマンドを使用してプライオリティを設定する場合に他のキューを設定するには、**bandwidth** ポリシーマップ コマンドを使用して共有し、**shape average** ポリシーマップ クラス コマンドを使用してシェーピングするしかありません。

priority コマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスにのみ関連付けられます。

priority コマンドは、出力ポリシー マップの **class-default** に関連付けられません。

同一クラスでは、プライオリティとその他のスケジューリング アクション（**shape average** または **bandwidth**）を設定できません。

priority コマンドは、クラスのデフォルト キュー制限を使用します。キュー制限を変更するには、**queue-limit** ポリシーマップ クラス コマンドを使用し、**priority** コマンドによって設定されたデフォルト設定を上書きします。

例

次に、クラス *out-class1* を完全プライオリティ キューとして設定し、このクラスのすべてのパケットが他のトラフィック クラスより先に送信される例を示します。他のトラフィック キューでは、*out-class2* は残りの帯域幅の 50%、*out-class3* は残りの帯域幅の 20% を取得するように設定されます。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

次に、**priority** コマンドと **police** コマンドを併用して、*out-class1* をプライオリティ キューとして設定し、キューに着信するトラフィックを 20000000 ビット/秒（bps）に制限して、プライオリティ キューがそれを超えるレートを使用しないようにする例を示します。このレートを超えるトラフィックは、廃棄されます。その他のトラフィック キューは、前述の例のとおり設定されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。

private-vlan

プライベート VLAN を設定して、プライベート VLAN のプライマリおよびセカンダリ VLAN 間のアソシエーションを設定するには、**private-vlan** VLAN コンフィギュレーション コマンドを使用します。通常の VLAN 設定に VLAN を戻すには、このコマンドの **no** 形式を使用します。

private-vlan {**association** [**add** | **remove**] *secondary-vlan-list* | **community** | **isolated** | **primary**}

no private-vlan {**association** | **community** | **isolated** | **primary**}

構文の説明

association	プライマリ VLAN とセカンダリ VLAN とのアソシエーションを作成します。
secondary-vlan-list	プライベート VLAN 内のプライマリ VLAN に関連付ける 1 つまたは複数のセカンダリ VLAN を指定します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアします。
community	VLAN をコミュニティ VLAN として指定します。
isolated	VLAN をコミュニティ VLAN として指定します。
primary	VLAN をコミュニティ VLAN として指定します。

デフォルト

デフォルトでは、プライベート VLAN が設定されていません。

コマンド モード

VLAN コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定して、レイヤ 2 データベースを結合し、プライベート VLAN トラフィックのフラッディングを防ぐ必要があります。

プライベート VLAN には、VLAN 1 または VLAN 1002 ～ 1005 を設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN として設定できます。

セカンダリ（隔離またはコミュニティ）VLAN を 1 つのプライマリ VLAN だけに**関連付ける**ことができます。プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。

- セカンダリ VLAN をプライマリ VLAN として設定できません。
- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。

- プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN に関連付けられたポートが非アクティブになります。

コミュニティ VLAN は、コミュニティ ポート間、およびコミュニティ ポートから対応するプライマリ VLAN の混合ポートにトラフィックを伝送します。コミュニティ VLAN には、最大 8 つのユーザ ネットワーク インターフェイス（UNI）を含めることができます。

隔離 VLAN は、混合ポートと通信を行うために隔離ポートによって使用されます。同一のプライマリ VLAN ドメインで他のコミュニティ ポートまたは隔離ポートにトラフィックを伝送しません。

プライマリ VLAN は、ゲートウェイからプライベート ポートのカスタマー エンド ステーションにトラフィックを伝送する VLAN です。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

VLAN コンフィギュレーション モードを終了するまで、**private-vlan** コマンドは作用しません。

プライベート VLAN ポートを EtherChannel として設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。

プライベート VLAN は、リモート スイッチド ポート アナライザ（RSPAN）VLAN にすることはできません。

プライベート VLAN は、User Network Interface-Enhanced Network Interface（UNI-ENI）にすることはできません。VLAN が UNI-ENI 隔離 VLAN（デフォルト）の場合、**private-vlan VLAN** コンフィギュレーション コマンドを入力して、プライベート VLAN に変更できます。VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、最初に **no uni-vlan** VLAN コンフィギュレーション コマンドを入力してから、プライベート VLAN として設定する必要があります。

プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは 1 つの STP インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

ホスト ポートおよび混合ポートの設定の詳細については、**switchport private-vlan** コマンドを参照してください。

（注） プライベート VLAN の他の機能との相互作用に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、VLAN 20 をプライマリ VLAN に、VLAN 501 を隔離 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、プライベート VLAN に関連付ける方法を示します。この例では、VLAN 502 および VLAN 503 は、事前に UNI-ENI コミュニティ VLAN として設定されていると想定します。

```
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)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
```

```
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

設定を確認するには、**show vlan private-vlan** または **show interfaces status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces status	所属する VLAN を含むインターフェイスのステータスを表示します。
show vlan private-vlan	スイッチ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 private-vlan	ホスト ポートまたは混合ポートとしてプライベート VLAN ポートを設定します。

private-vlan mapping

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 間でマッピングを作成して、両方の VLAN で同じプライマリ VLAN インターフェイスを共有できるようにするには、**private-vlan mapping** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスからプライベート VLAN のマッピングを削除するには、このコマンドの **no** 形式を使用します。

private-vlan mapping {[**add** | **remove**] *secondary-vlan-list*}

no private-vlan mapping

構文の説明

secondary-vlan-list	プライマリ VLAN インターフェイス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 インターフェイス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 インターフェイス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 のマッピングが設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

プライマリ VLAN の SVI は、レイヤ 3 で作成されます。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。

セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN のインターフェイスによってルーティングされます。

セカンダリ VLAN は、1 つのプライマリ VLAN だけにマッピングできます。プライマリ VLAN がセカンダリ VLAN として設定されると、このコマンドで指定されたすべての SVI はダウンします。

有効なレイヤ 2 プライベート VLAN のアソシエーションがない 2 つの VLAN 間のマッピングを設定する場合、マッピングの設定は作用しません。

例

次の例では、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする方法を示します。

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

次の例では、セカンダリ VLAN 303 ～ 305、および 307 からのセカンダリ VLAN トラフィックのルーティングを VLAN 20 SVI を介して許可する方法を示します。

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

設定を確認するには、**show interfaces private-vlan mapping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	インターフェイスまたは VLAN SVI に対するプライベート VLAN のマッピング情報を表示します。

queue-limit

出力ポリシー マップの重み付きテール ドロップ（WTD）のキューの最大しきい値を設定するには、**queue-limit** 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。このコマンドをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

queue-limit [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]

no queue-limit [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]

構文の説明

cos *value*	（任意）各サービス コスト（CoS）値のパラメータを設定します。指定できる範囲は 0 ～ 7 です。
dscp *value*	（任意）各 DiffServ コード ポイント（DSCP）値のパラメータを設定します。指定できる範囲は 0 ～ 63 です。
precedence *value*	（任意）各 IP precedence 値のパラメータを設定します。指定できる範囲は 0 ～ 7 です。
qos-group *value*	（任意）各 Quality Of Service（QoS）グループ値のパラメータを設定します。指定できる範囲は 0 ～ 99 です。
number-of-packets [**packets**]	キューのパケット数として WTD の最大しきい値を設定します。指定できる範囲は 16 ～ 544 で、256 バイトのパケットを表します。デフォルトは 160 パケットです。**packets** キーワードは任意です。 **（注）** 最適なネットワーク パフォーマンスを得るには、最大キュー制限を 272 以下に設定することを強く推奨します。

デフォルト

デフォルトのキュー制限は 160（256 バイト）パケットです。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

出力トラフィックを制御するには、**queue-limit** ポリシーマップ クラス コマンドを使用します。キュー制限設定は、入力ポリシー マップでサポートされません。

Cisco IOS Release 12.2(35)SE 以降では、インターフェイスごとに 1 つの出力ポリシー マップがサポートされます。ただし、すべての出力ポリシー マップにおいて 3 つの固有のキュー制限設定は有効なままとなります。複数のポリシー マップで同じキュー制限設定を使用できます。

出力ポリシー マップ内で許容されるキュー（クラス）は 4 つだけです（クラス デフォルトを含む）。各キューには 3 つのしきい値が定義されています（キュー制限）。スイッチに許可されるのは 3 つのキュー制限設定のみですが、複数のポリシー マップで同じキュー制限を共有できます。2 つのポリシー マップがキュー制限の設定を共有する場合、両方のポリシー マップのすべてのクラスで、すべてのしきい値が同じでなければなりません。

4 つ目のキュー制限設定を含む出力ポリシー マップをインターフェイスに付加しようとすると、エラー メッセージが表示され、付加は許可されません。

queue-limit コマンドは、出力ポリシー マップの **class-default** で **queue-limit** を設定している場合を除き、**bandwidth**、**shape-average**、または **priority** などのスケジューリング アクションを最初に設定した後にのみサポートされます。

queue-limit コマンドで、WTD 修飾子（**cos**、**dscp**、**precedence**、**qos-group**）に 3 つ以上の一意のしきい値を設定できません。ただし、これらのしきい値には、任意の数の修飾子をマッピングできます。修飾子なしの **queue-limit** コマンドを使用することにより、3 番目の一意のしきい値を設定して、最大キューを設定できます。

queue-limit コマンドを使用して、クラス マップ内のしきい値を設定する場合、WTD しきい値は、キューの最大しきい値以下にする必要があります。これは、修飾子なしで設定されたキュー サイズが修飾子で設定されているキュー サイズ大きい修飾子に設定されているいずれのキュー サイズよりも大きい必要があることを意味します。

例

次に、*out-class1*、*out-class2*、*out-class3*、および **class-default** がそれぞれ最低 40、20、10、および 10% のトラフィック帯域幅を取得するように、WTD を設定する例を示します。対応するキューサイズは、48、32、16、および 272（256 バイト）パケットに設定されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、*outclass1*、*outclass2*、および *outclass3* がそれぞれ最低 50、20、および 10% のトラフィック帯域幅を取得するようにファスト イーサネット ポートの WTD を設定する例を示します。**class-default** は、残りの 20% を得します。対応する各キュー サイズは、64、32、および 16（256 バイト）パケットに設定されます。また、この例では、*outclass1* が dscp 46、56、57、58、60、63 に一致する場合、DSCP 値 46 が 32（256 バイト）パケットのキュー サイズ、DSCP 値 56、57、および 58 が 48（256 バイト）パケット、残りの DSCP 値 60 および 63 はデフォルト キュー サイズの 64（256 バイト）パケットを取得することを示します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 64
Switch(config-pmap-c)# queue-limit dscp 46 32
Switch(config-pmap-c)# queue-limit dscp 56 48
Switch(config-pmap-c)# queue-limit dscp 57 48
Switch(config-pmap-c)# queue-limit dscp 58 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

スイッチ上の複数の出力ポリシー マップで同じキュー制限値を使用できます。ただし、クラスのキュー制限値の 1 つを変更すると、新たな固有のキュー制限設定が作成されます。インターフェイスに付加できる出力ポリシー マップの固有のキュー制限設定は、どの時点でも 3 つだけです。4 つ目のキュー制限が設定された出力ポリシー マップを付加しようとすると、次のエラー メッセージが表示されます。

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	QoS ポリシー マップを表示します。

radius-server dead-criteria

RADIUS サーバが使用不可または *デッド*状態であると考えられる場合に決定する条件を設定するには、**radius-server dead-criteria** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

no radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

構文の説明

time *seconds*	（任意）RADIUS サーバからの有効な応答をスイッチが取得するのに必要としない時間（秒）を設定します。指定できる範囲は 1 ～ 120 秒です。
tries *number*	（任意）サーバが使用不可と見なされる前に RADIUS サーバから有効な応答をスイッチが取得するのに必要としない回数を指定します。指定できる範囲は 1 ～ 100 です。

デフォルト

スイッチは、10 ～ 60 秒の *seconds* 値を動的に決定します。

スイッチは、10 ～ 100 の *tries* 値を動的に決定します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

次の *seconds* および *number* パラメータを設定することを推奨します。

- IEEE 802.1x 認証が期限切れになる前に RADIUS サーバへの応答を待機する時間（秒）を指定するには、**radius-server timeout** *seconds* グローバル コンフィギュレーション コマンドを使用します。スイッチは、10 ～ 60 秒のデフォルトの *seconds* 値を動的に決定します。
- RADIUS サーバが使用不能と見なされる前に RADIUS サーバへの送信を試行する時間（秒）を指定するには、**radius-server retransmit** *retries* グローバル コンフィギュレーション コマンドを使用します。スイッチは、10 ～ 100 のデフォルトの *tries* 値を動的に決定します。
- *seconds* パラメータは、IEEE 802.1x 認証が期限切れになる前に再送信を試行する秒数以下か、または同じです。
- *tries* パラメータは、再送信試行回数と同じである必要があります。

例

次の例では、RADIUS サーバが使用不可と見なされた場合に決定する条件として、**時間**に 60 を設定し、**試行**回数に 10 を設定する方法を示します。

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication event	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
radius-server retransmit *retries*	RADIUS サーバが使用不可と見なされる前にスイッチが RADIUS サーバに送信を試行する回数を指定します。構文情報については、『**Cisco IOS Security Command Reference, Release 12.2**』>「**Server Security Protocols**」>「**RADIUS Commands**」を選択してください。
radius-server timeout *seconds*	IEEE 802.1x 認証が期限切れになる前にスイッチが RADIUS サーバへの応答を待機する時間（秒）を指定します。構文情報については、『**Cisco IOS Security Command Reference, Release 12.2**』>「**Server Security Protocols**」>「**RADIUS Commands**」を選択してください。
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、『**Cisco IOS Configuration Fundamentals Command Reference, Release 12.2**』>「**File Management Commands**」>「**Configuration File Management Commands**」を選択してください。

radius-server host

RADIUS アカウンティングおよび RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host *ip-address* **[acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]

no radius-server host *ip-address*

構文の説明

ip-address	RADIUS サーバの IP アドレスを指定します。
acct-port *udp-port*	（任意）RADIUS アカウンティング サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
auth-port *udp-port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
test *username* *name*	（任意）RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
idle-time *time*	（任意）スイッチがテスト パケットをサーバに送信した後の間隔（分）を設定します。指定できる範囲は 1 ～ 35791 分です。
ignore-acct-port	（任意）RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。
ignore-auth-port	（任意）RADIUS サーバ認証ポートのテストをディセーブルにします。
key *string*	（任意）スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。

デフォルト

RADIUS アカウンティング サーバの UDP ポートは 1646 です。

RADIUS 認証サーバの UDP ポートは 1645 です。

自動サーバ テストはディセーブルです。

アイドル時間は 60 分（1 時間）です。

自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。

認証キーおよび暗号キー（*string*）は設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。

RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定するには、**test username** *name* キーワードを使用します。

radius-server host *ip-address* **key** *string* または **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用して認証キーおよび暗号キーを設定できます。必ずこのコマンドの最終項目として key を設定してください。

例

次の例では、アカウンティング サーバの UDP ポートを 1500、認証サーバの UDP ポートを 1510 に設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

次の例では、アカウンティング サーバおよび認証サーバの UDP ポートを設定し、RADIUS サーバ ステータスの自動テストをイネーブルにし、使用されるユーザ名を指定し、キー ストリングを設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication event	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
radius-server key {**0** ***string*** | **7** ***string*** | ***string***}	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。構文情報については、『**Cisco IOS Security Command Reference, Release 12.2**』> 「**Server Security Protocols**」> 「**RADIUS Commands**」を選択してください。
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、『**Cisco IOS Configuration Fundamentals Command Reference, Release 12.2**』> 「**File Management Commands**」> 「**Configuration File Management Commands**」を選択してください。

reload

オペレーティング システムをリロードするには、**reload** 特権 EXEC コマンドを使用します。

reload [**warm**] [**in** [*hh*:]*mm* | **at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [*text*]

構文の説明

warm	（任意）ストレージからイメージを読み取らずにスイッチをリロードします。スイッチのリブート時間が大幅に短縮され、システム全体の可用性が高まります。
in [*hh*:]*mm*	（任意）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、約 24 日以内に実行する必要があります。
at *hh*:*mm*	（任意）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、約 24 日以内に実行する必要があります。
month	（任意）月の名前。任意の文字数からなる一意のストリングです。
day	（任意）1 ～ 31 の範囲で日付を指定します。
cancel	（任意）スケジューリングされているリロードをキャンセルします。
text	（任意）リロードの理由（1 ～ 255 文字）。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

reload コマンドはシステムを停止させます。エラー発生時に再起動するようにシステムが設定されている場合は、自動的に再起動します。**reload** コマンドは、コンフィギュレーション情報がファイルに入力され、スタートアップ コンフィギュレーションに保存された後で使用します。

システムが自動ブートに設定されていない仮想端末からはリロードできません。これは、システムが ROM モニタにドロップし、リモート ユーザの制御からシステムを削除することを防止するためです。

コンフィギュレーション ファイルを変更すると、コンフィギュレーションを保存するように指示するプロンプトが表示されます。存在しないスタートアップ コンフィギュレーション ファイルを変数 CONFIG_FILE が示している場合は、保存動作中に、保存を進めるかどうかの確認が要求されます。この状況で [Yes] と応答すると、リロード時にセットアップ モードが開始されます。

後でリロードを実行するようにスケジュールする場合は、約 24 日以内にリロードを実行するようにする必要があります。

at キーワードを使用できるのは、ルータでシステム クロックが（NTP、ハードウェア カレンダー、または手動で）設定されている場合だけです。この時間は、ルータの設定された時間帯と相対的です。複数のルータで同時にリロードが行われるように設定する場合は、各ルータの時刻を NTP によって同期させる必要があります。

ストレージからイメージを読み取らずにスイッチをリロードするには、**warm** キーワードを使用します。Cisco IOS イメージは、ROM モニタ モード（ROMMON）の介入なしでリブートします。これにより、以前 RAM に保存されたコピーから読み取り / 書き込みデータが復元され、イメージのフラッシュ メモリから RAM へのコピーやイメージの自己解凍なしで実行が開始されます。したがって、スイッチはより高速でリブートします。

warm キーワードを使用すると、手動で起動するように設定しても、スイッチは自動的に起動します。

スケジューリングされたリロードの情報を表示するには、**show reload** EXEC コマンドを使用します。

例

次に、ただちにスイッチのソフトウェアをリロードする例を示します。

```
Switch# reload
```

次の例では、スイッチのソフトウェアは 10 分以内にリロードされます。

```
Switch# reload in 10

Switch# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload?[confirm]
Switch#
```

次の例では、スイッチのソフトウェアは本日 13:00 にリロードされます。

```
Switch# reload at 13:00

Switch# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload?[confirm]
Switch#
```

次の例では、スイッチのソフトウェアは 4 月 20 日の 2:00 にリロードされます。

```
Switch# reload at 02:00 apr 20

Switch# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload?[confirm]
Switch#
```

次に、保留中のリロードを取り消す例を示します。

```
Switch# reload cancel

%Reload cancelled.
```

次の例では、本日 4:00 にウォーム リブートを実行します。

```
Switch# reload warm at 4:00
```

関連コマンド

コマンド	説明
copy system:running-config nvram:startup-config	コピー元からコピー先に任意のファイルをコピーします。
show reload	ルータのリロード ステータスを表示します。

remote-span

VLAN を Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）VLAN として設定するには、**remote-span** VLAN コンフィギュレーション コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span

no remote-span

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション（config-VLAN）

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

有効な RSPAN VLAN ID は 2 ～ 1001 および 1006 ～ 4094 です。RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。

RSPAN **remote-span** コマンドを設定する前に、**vlan** グローバル コンフィギュレーション コマンドで VLAN を作成してください。

- VLAN を User Network Interface-Enhanced Network Interface（UNI-ENI）隔離 VLAN（デフォルト）から RSPAN VLAN に変更するには、**rspan-vlan** VLAN コンフィギュレーション コマンドを入力します。
- UNI-ENI コミュニティ VLAN を RSPAN VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN を削除する必要があります。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックだけが流れます。
- Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）は RSPAN VLAN 内では稼動できますが、RSPAN 宛先ポートでは稼動しません。Cisco CGS 2520 スイッチでは、STP がイネーブルにされているネットワーク ノード インターフェイス（NNI）と拡張ネットワーク インターフェイス（ENI）だけが STP に参加します。

また、RSPAN VLAN ID を使用して、手動で送信元スイッチ、宛先スイッチ、および中間スイッチを設定する必要があります（送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定）。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

例

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

show vlan remote-span ユーザ EXEC コマンドを入力すると、設定を確認することができます。

関連コマンド

コマンド	説明
monitor session	ポートで Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。
vlan	VLAN 1 ～ 4094 を設定できる config-vlan モードに変更します。

renew ip dhcp snooping database

DHCP スヌーピング バインディング データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

renew ip dhcp snooping database [**validation none**] [{**flash:**/*filename* | **ftp:**//*user:password@host/filename* | **nvram:**/*filename* | **rcp:**//*user@host/filename* | **tftp:**//*host/filename*}] [**validation none**]

構文の説明

validation none	（任意）URL によって指定されたバインディング ファイルのエントリに対して、Cyclic Redundancy Check（CRC; 巡回冗長検査）を検証しないようにスイッチに指定します。
flash:/*filename*	（任意）データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。
ftp://*user*:*password*@*host*/*filename*	（任意）データベース エージェントまたはバインディング ファイルが FTP サーバ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 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 Copy Protocol（RCP; リモート コピー プロトコル）サーバにあることを指定します。
tftp://*host/filename*	（任意）データベース エージェントまたはバインディング ファイルが TFTP サーバにあることを指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

URL を指定しない場合は、スイッチは設定された URL からファイルを読み込もうとします。

例

次の例では、CRC 値のチェックを省略して、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

設定を確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

rep admin vlan

Resilient Ethernet Protocol（REP; レジリエント イーサネット プロトコル）が Hardware Flood Layer（HFL; ハードウェア フラッド レイヤ）メッセージを送信するように REP 管理 VLAN を設定するには、**rep admin 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（VLAN 1 が管理 VLAN）に戻す場合は、このコマンドの **no** 形式を使用します。

rep admin vlan *vlan-id*

no rep admin vlan

構文の説明

vlan-id	VLAN ID の範囲は 1 ～ 4094 です。デフォルトは VLAN 1 のため、設定する範囲は 2 ～ 4094 です。

デフォルト

管理 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

VLAN がまだ存在していない場合、このコマンドにより VLAN が作成されることはありません。

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体の管理 VLAN を設定することにより、これらのメッセージのフラッディングを管理できます。

REP 管理 VLAN が設定されていない場合、デフォルトは VLAN 1 になります。

スイッチとセグメントで 1 つの管理 VLAN だけが可能です。

管理 VLAN は RSPAN VLAN になりません。

例

次の例では、VLAN 100 を REP 管理 VLAN として設定する方法を示します。

```
Switch (config)# rep admin vlan 100
```

設定を確認するには、**show interface rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep block port

Resilient Ethernet Protocol（REP）VLAN ロード バランシングを設定するには、REP プライマリ エッジ ポートで**rep block 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

rep block port {id *port-id* | *neighbor_offset* | **preferred} vlan {*vlan-list* | all}**

no rep block port {**id** *port-id* | *neighbor_offset* | **preferred**}

構文の説明

id *port-id*	REP イネーブル時に自動的に生成される一意のポート ID を入力することで、VLAN ブロック代替ポートを識別します。REP ポート ID は、16 文字の 16 進数値です。インターフェイスのポート ID を表示するには、**show interface** *interface-id* **rep detail** コマンドを入力します。
neighbor_offset	ネイバーのオフセット番号を入力することで、VLAN ブロック代替ポートを識別します。指定できる範囲は –256 ～ +256 で、値 0 は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジ ポート（オフセット番号 –1）とダウンストリーム ネイバーを識別します。
preferred	VLAN ブロック代替ポートを、**rep segment** *segment-id* **preferred** 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セグメント ポートとして識別します。 **（注）** **preferred** キーワードを入力しても確実に代替ポートは指定されませんが、他の類似のポートより優先されます。
vlan	ブロックする VLAN を識別します。
vlan-list	ブロックする VLAN について、1 ～ 4094 の範囲の VLAN ID を入力するか、VLAN ID の範囲または連続番号（1-3、22、41-44 など）を入力します。
all	すべての VLAN をブロックするように入力します。

デフォルト

rep preempt segment 特権 EXEC コマンド（手動プリエンプション）を入力した場合のデフォルトのアクションは、プライマリ エッジ ポートで VLAN すべてがブロックされます。この動作は **rep block port** コマンドを設定するまで継続されます。

プライマリ エッジ ポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンプションなし、および VLAN ロード バランシングなしです。

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

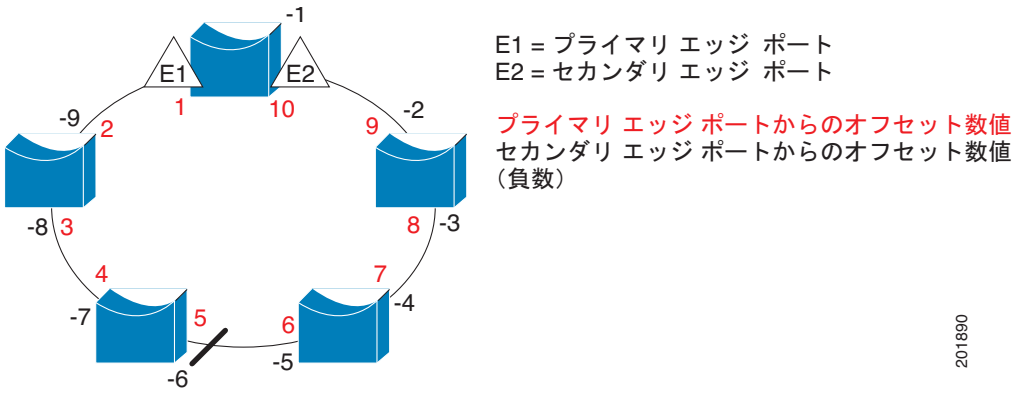
リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジ ポート（オフセット番号 –1）とダウンストリーム ネイバーを識別します。「REP セグメントのネイバー オフセット番号」図 2-1 を参照してください。

図 2-1　REP セグメントのネイバー オフセット番号



（注） 番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

rep preempt delay *seconds* 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でプリエンプション遅延時間を設定していて、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロード バランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメント ポートのブロックを解除します。プライマリ エッジ ポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID の形式は、スパニング ツリー アルゴリズムで使用されるものと同様で、MAC アドレス（ネットワーク内で一意）に関連付けられるポート番号（ブリッジ上で一意）となります。ポートのポート ID を判別するには、**show interface** *interface-id* **rep detail** 特権 EXEC コマンドを入力します。

例

次の例では、スイッチ B プライマリ エッジ ポート（ギガビット イーサネット ポート 0/1）の REP VLAN ロード バランシングを設定して、スイッチ A のギガビット イーサネット ポート 0/2 を代替ポートとして設定して VLAN 1 ～ 100 をブロックする方法を示します。代替ポートは、スイッチ A ポートの **show interface rep detail** コマンドの出力に太字で表示されるポート ID により識別されます。

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
```

```
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

Switch B# config t
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

次の例では、ネイバー オフセット番号を使用して VLAN ロード バランシングを設定する方法と、**show interfaces rep detail** 特権 EXEC コマンドを入力して設定を確認する方法について示します。

```
Switch# config t
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

関連コマンド

コマンド	説明
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロード バランシングがトリガーされるまでの待機期間を設定します。
rep preempt segment	手動でセグメント上の REP VLAN ロード バランシングを開始します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 詳細設定およびステータスを表示します。

rep lsl-age-timer

REP インターフェイスが REP ネイバーから hello を受信せずに起動し続ける時間の Link Status Layer（LSL）エージング タイマーを設定するには、Resilient Ethernet Protocol（REP）ポートで **rep lsl-age-timer** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age timer *value*

no rep lsl-age timer

構文の説明

value	エージアウト時間（ミリ秒）。指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。

デフォルト

REP リンクは、5000 ミリ秒間ネイバーから hello メッセージを受信しなければ、シャットダウンされます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

LSL エージング タイマーの間に少なくとも 2 つの LSL hello が送信されるように、LSL Hello タイマーはエージング タイマーの値を 3 で割った値に設定されます。この期間に hello が受信されない場合、REP リンクはシャットダウンします。

Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）から 120 ～ 10000 ミリ秒（40 ミリ秒単位）に変更されています。REP ネイバー デバイスで Cisco IOS Release 12.2(52)SE 以降が稼動していない場合、デバイスは以前の範囲を逸脱する値を受け付けないため、時間の範囲を短くする必要があります。

EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。

例

次の例では、REP リンクの REP LSL エージイング タイマーを 7000 ms に設定する方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep lsl-age-timer 7000
Switch (config-if)# exit
```

設定されたエージアウト時間を確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	設定済みの LSL エージアウト タイマー値を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep preempt delay

セグメント ポートの障害および回復の発生後 Resilient Ethernet Protocol（REP）VLAN ロード バランシングがトリガーされるまでの待機時間を設定するには、REP プライマリ エッジ ポートで **rep preempt delay** インターフェイス コンフィギュレーション コマンドを使用します。設定された遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay *seconds*

no rep preempt delay

構文の説明

seconds	REP プリエンプションを遅延させる秒数を設定します。指定できる範囲は 15 ～ 300 です。

デフォルト

プリエンプション遅延は設定されていません。**rep preempt delay** コマンドを入力しない場合、デフォルトは遅延のない手動プリエンプションとなります。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

リンク障害とリカバリ後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力してプリエンプション時間遅延を設定する必要があります。

VLAN ロード バランシングが設定されている場合、セグメント ポート障害とリカバリの後、VLAN ロード バランシングが発生する前に REP プライマリ エッジ ポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、（**rep block port** インターフェイス コンフィギュレーション コマンドを使用して設定された）VLAN ロード バランシングを実行するように REP プライマリ エッジが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジ ポートでブロックされます。

例

次の例では、プライマリ エッジ ポートで REP プリエンプション時間遅延を 100 秒に設定する方法を示します。

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep preempt delay 100
Switch (config-if)# exit
```

設定を確認するには、**show interfaces rep** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep	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 REP 設定およびステータスを表示します。

rep preempt segment

セグメントで Resilient Ethernet Protocol（REP）VLAN ロード バランシングを手動で開始するには、**rep preempt segment** 特権 EXEC コマンドを使用します。

rep preempt segment *segment_id*

構文の説明

segment-id	REP セグメントの ID。指定できる範囲は 1 ～ 1024 です。

デフォルト

デフォルト動作は手動プリエンプションです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

rep preempt segment *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

プライマリ エッジ ポートのあるセグメントのスイッチにこのコマンドを入力します。

VLAN ロード バランシングを設定しない場合、このコマンドを入力するとデフォルトの動作になります（プライマリ エッジ ポートですべての VLAN がブロックされます）。

手動でプリエンプションを開始する前に、REP プライマリ エッジ ポートで **rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**} 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、VLAN ロード バランシングを設定します。

このコマンドには、**no** バージョンはありません。

例

次の例では、確認メッセージ付きで、セグメント 100 で REP プリエンプションを手動でトリガーする方法を示します。

```
Switch)# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep segment

インターフェイスで Resilient Ethernet Protocol（REP）をイネーブルにして、セグメント ID を割り当てるには、**rep segment** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで REP 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。

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

構文の説明

segment-id	セグメント ID をインターフェイスに割り当てます。指定できる範囲は 1 ～ 1024 です。
edge	（任意）2 つの REP エッジ ポートの 1 つとしてインターフェイスを識別します。**primary** キーワードなしで **edge** キーワードを入力すると、ポートがセカンダリ エッジ ポートとして設定されます。
primary	（任意）エッジ ポートで、ポートがプライマリ エッジ ポートであると指定します。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。
preferred	（任意）ポートを優先代替ポートまたは VLAN ロード バランシングの優先ポートに指定します。 **（注）** ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

デフォルト

REP はインターフェイスでディセーブルです。

REP がインターフェイスでイネーブルの場合、デフォルトでは通常のセグメント ポートであるポートに対して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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

REP ポートは、レイヤ 2 トランク ポートである必要があります。

非 ES REP ポートは、IEEE 802.1Q トランク ポートまたは ISL トランク ポートのいずれかになります。

REP ポートは次のいずれかのポート タイプとして設定してはいけません。

- SPAN 宛先ポート
- プライベート VLAN ポート
- トンネル ポート

- アクセス ポート
- REP ポートは、ネットワーク ノード インターフェイス（NNI）である必要があります。ユーザ ネットワーク インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）を REP ポートにはできません。

各 REP セグメント上には、プライマリ エッジ ポートと、セカンダリ エッジ ポートとして機能するポートの、2 種類のエッジ ポートを設定しなければいけません。たとえば別のスイッチにあるポートなどの、セグメント内の 2 つのポートをプライマリ エッジ ポートとして指定すると（設定は可能です）、REP によりその内の 1 つがセグメントのプライマリ エッジ ポートとして機能するように選択されます。

- REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。

別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。いずれのポートがプライマリ エッジ ポートかを確認するには、**show rep topology** 特権 EXEC コマンドをセグメント内のポートに入力します。

REP インターフェイスはブロック ステートで起動し、安全にブロック解除可能と通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

ネイバー スイッチ上のポートで REP がサポートされていないネットワークでは、非 REP 側ポートを非ネイバー エッジ ポートとして設定できます。非ネイバー エッジ ポートはエッジ ポートのすべてのプロパティを継承するため、非ネイバー エッジ ポートをその他のいずれのエッジ ポートとしても設定できます。これには、STP または REP トポロジ変更通知をアグリゲーション スイッチに送信することも含まれます。この場合、送信される STP Topology Change Notification（TCN; トポロジ変更通知）は、Multiple Spanning-Tree（MST）STP メッセージです。

例

次の例では、通常の（非エッジ）セグメント ポートで REP をイネーブルにする方法を示します。

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep segment 100
```

次の例では、ポートの REP をイネーブルし、REP プライマリ エッジ ポートとして指定にする方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge primary
```

次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 100 edge no-neighbor primary
```

次の例では、ポートの REP をイネーブルし、REP セカンダリ エッジ ポートとして指定にする方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge
```

設定を確認するには、**show interfaces rep** 特権 EXEC コマンドを入力します。セグメントのいずれのポートがプライマリ エッジ ポートであるか確認するには、**show rep topology** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。
show rep topology [**detail**]	プライマリ エッジ ポートとして設定および選択されたポートを含む、セグメント内のすべてのポートに関する情報を表示します。

rep stcn

REP Segment Topology Change Notification（STCN; セグメント トポロジ変更通知）を他のインターフェイス、他のセグメントまたは Spanning Tree Protocol（STP）ネットワークに送信する設定を行うには、Resilient Ethernet Protocol（REP）エッジ ポートで **rep stcn** インターフェイス コンフィギュレーション コマンドを使用します。STCN をインターフェイス、セグメント、または STP ネットワークに送信すること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。

rep stcn {**interface** *interface-id* | **segment** *id-list* | **stp**}

no rep stcn {**interface** | **segment** | **stp**}

構文の説明

interface *interface-id*	STCN を受信するように物理インターフェイスまたはポート チャネルを識別します。
segment *id-list*	STCN を受信する 1 REP セグメントまたはセグメントのリストを識別します。有効範囲は 1 ～ 1024 です。一連のセグメント（たとえば 3-5、77、100 など）を設定することもできます。
stp	STCN を STP ネットワークに送信します。

デフォルト

他のインターフェイス、セグメント、または STP ネットワークへの STCN の送信がディセーブルです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドをセグメント エッジ ポートに入力します。

このコマンドを使用して、ローカル REP セグメントで発生しているトポロジ変更をレイヤ 2 ネットワークの他の部分に通知します。これにより、ネットワークの他部分にあるレイヤ 2 転送テーブル内の廃止エントリが削除され、より高速なネットワーク コンバージェンスが可能になります。

例

次の例では、REP プライマリ エッジ ポートでセグメント 25 ～ 50 に STCN を送信する設定方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

設定を確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

reserved-only

Dynamic Host Configuration Protocol（DHCP）アドレス プールに予約済みのアドレスだけ割り当てるには、**reserved-only** DHCP プール コンフィギュレーション モード コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

reserved-only

no reserved-only

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、プール アドレスは制限されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

reserved-only コマンドを入力すると、DHCP プールから事前設定された予約への割り当てが制限されます。ネットワークまたはプール上の範囲の一部である予約されていないアドレスがクライアントには提供されず、他のクライアントはプールによるサービスを受けられません。

このコマンドの入力により、ユーザは、共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視する DHCP プールを持つスイッチのグループを設定できます。

DHCP プール コンフィギュレーション モードにアクセスするには、**ip dhcp pool** *name* グローバル コンフィギュレーション コマンドを入力します。

例

次の例では、予約済みのアドレスだけを割り当てるように DHCP プールを設定する方法を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

設定を確認するには、**show ip dhcp pool** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp pool	DHCP アドレス プールを表示します。

reserved-only